Cyberwar

Attacco a

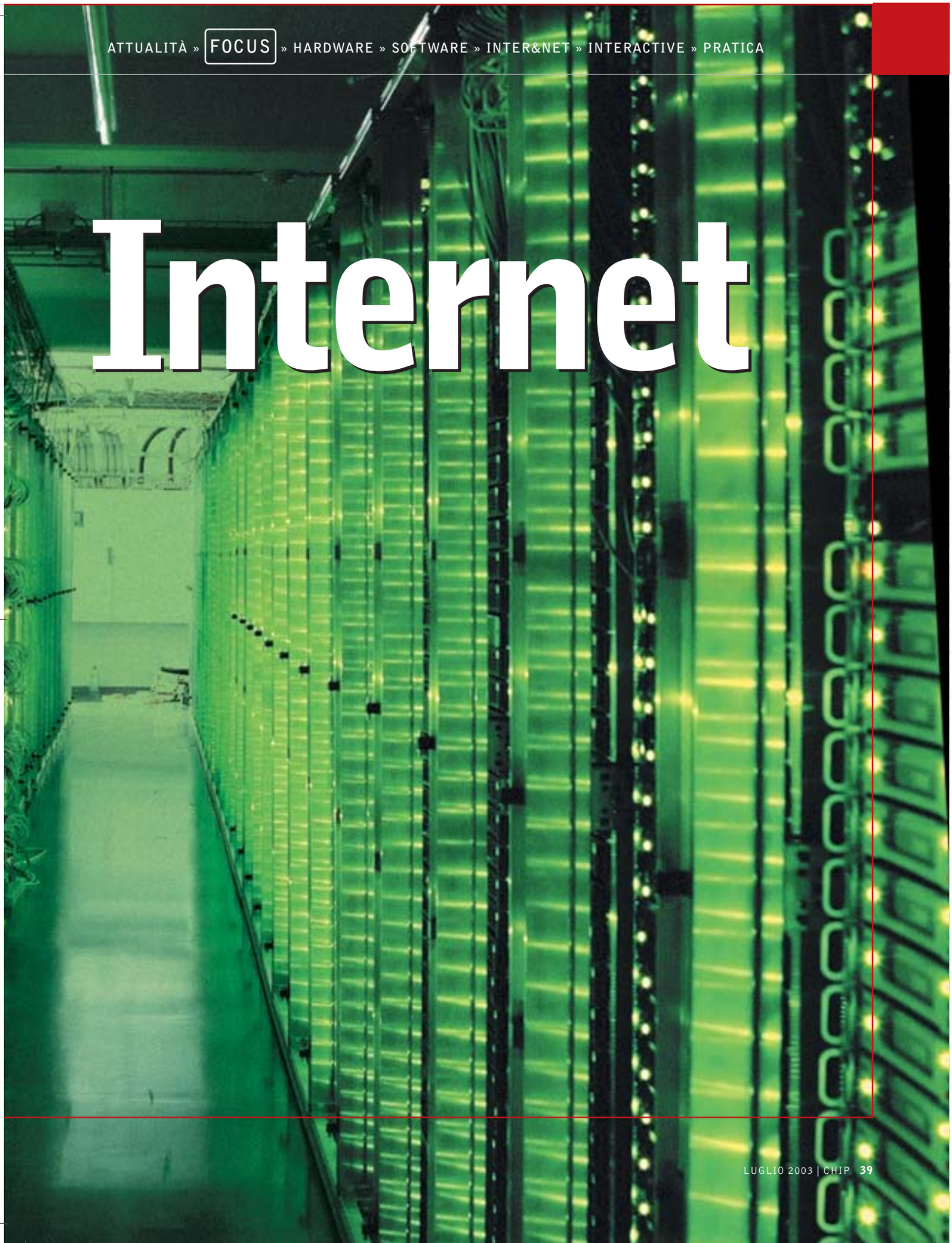
Un mondo che fa sempre maggior affidamento sull'infrastruttura digitale per condurre i suoi affari si interroga sui possibili effetti della cosiddetta cyberwar. Minaccia reale o nuovo flop in stile Millennium Bug? *Di Andrea Lawendel*

Secondo le cifre pubblicate ufficialmente dal ministero degli Interni britannico in seguito a un'interrogazione parlamentare, e riportate da molti notiziari Web, i siti Internet riferibili alle autorità governative che fanno capo a Downing Street avrebbero subito, verso la fine dell'anno 2002, non meno di 6.500 attacchi di natura digitale. L'ufficio di Gabinetto è uno dei bersagli principali, con oltre 1.100 attacchi, che secondo il ministro Douglas Alexander non avrebbero tuttavia causato danni, compromissioni o perdite di alcun tipo. Perfino il ministero della Difesa ha ammesso di essere soggetto a "frequenti tentativi" di indebito sondaggio rilevato a quelli che vengono definiti i "confini elettronici" di una geografia che contrariamente alle normali entità geopolitiche, non risiede, almeno in principio, da nessuna parte. La Difesa britannica non ha fornito cifre precise, limitandosi a parlare di una decina di attacchi subiti da imprecisati hacker.

Ma oltre alla sicurezza logica di un sistema, c'è anche l'aspetto della sicurezza fisica. E dopo l'11 settembre del 2001, quel tipo di sicurezza desta ancora più preoccupazione. Negli uffici e nei sotterranei del World Trade Center, erano installati router e apparecchiature di molti data carrier, i gestori pubblici e privati che hanno contribuito a realizzare l'infrastruttura commerciale di Internet (si suppone che quelle militari, finanziate dall'ormai mitica Advanceded Research Projects Agency della Difesa Usa siano protette anche contro attacchi di natura fisica).

Per molto tempo il traffico telefonico e digitale aveva smesso di transitare da quel nodo importante. Tanto che nel giro di pochi mesi, l'amministrazione Bush faceva passare il Cyber Security Research and Development Act, una legge di febbraio 2002 che stanziava un totale di 900 milioni di dollari per le ricerche coordinate in materia di sicurezza digitale dalla National Science Foundation e dal National Institute for Standards. Nell'introduzione al documento ufficiale si legge che "tra le vulnerabilità della Nazione sono le nostre reti informatiche e di telecomunicazione, da cui dipendono i sistemi finanziario, dei trasporti, dell'energia e della distribuzione idrica. →

Internet



Queste vulnerabilità mettono in questione la capacità dei programmi di ricerca tecnologica, formazione e gestione delle interconnessioni di affrontare le sfide poste dalla cyber warfare (guerra informatica) nel XXI secolo."

Quali sono i possibili scenari di un attacco combinato alla sicurezza delle infrastrutture? Tenendo conto anche della possibilità di compromettere le reti e le centrali telefoniche e i punti per la distribuzione dell'energia elettrica le conseguenze, nei casi peggiori, potrebbero davvero essere spaventose.

- I numeri dei vari servizi di pronto intervento smettono di funzionare (questo è un rischio che anche il carico eccessivo di chiamate dovuto a un'improvvisa ondata di panico può provocare).
- Le strumentazioni e i sistemi informativi degli ospedali smettono di funzionare in toto o in parte, alimentati soltanto dai generatori di emergenza.

A destare preoccupazione sono i probabili attacchi infrastrutturali ai centri nevralgici di Internet

- I sistemi di controllo del traffico sulle strade, a incominciare dai semplici semafori, vanno in tilt, scatenando il caos nelle aree metropolitane. Il traffico aereo strettamente legato alle comunicazioni aerei-torri di controllo, si paralizza.
- La produzione industriale, che dipende a ogni livello dalla disponibilità di corrente elettrica, subisce un pesante arresto.
- I media di informazione subiscono anch'essi un blocco significativo, rendendo ancora più estremo il panico nei cittadini che restano, in tutti i sensi, all'oscuro.
- Le conseguenze più imprevedibili sul lungo termine riguardano un sistema di transazioni finanziarie che ha già reso elettronica gran parte del nostro denaro.

Questi "worst case scenarios" sono probabilmente lontani dal potersi concretizzare fuori dagli schermi di un film di avventure. Ma bisogna pur ammettere che le scene apocalittiche viste l'11 settembre sarebbero state giudicate nello stesso modo fino a pochi secondi prima del primo impatto sulla torre Sud dell'edificio più alto di Manhattan. E se al di là del pesantissimo tributo di vittime umane il tragico attentato di New York ha avuto conseguenze tutto sommato circoscritte nel tempo, nessuno di chi ha avuto esperienza diretta dell'episodio potrà mai scordare le lunghe ore di assoluta inaccessibilità di tante migliaia di parenti, amici e conoscenti, sopravvissuti ma del tutto irrintracciabili attraverso il telefono, il cellulare e la posta elettronica.

Un attacco coordinato e mirato

Un attacco forse meno spettacolare ma ancora più coordinato e mirato, potrebbe in linea teorica portare a risultati vicini a quelli appena descritti. Per non parlare dell'ondata di emotività e di improvviso rafforzamento dei sistemi di sicurezza, che hanno sicuramente influito su un aspetto importante della nostra economia come il trasporto aereo e continuano ancora oggi a pesare sul clima che si respira sulle maggiori piazze finanziarie.

Anche limitandosi agli aspetti della vulnerabilità del "sistema" Internet, i motivi di allarme non mancano e vanno ben oltre il già fastidioso fenomeno - sentito come non mai - dei virus della posta elettronica e dello spamming. Con l'aiuto della ricca documentazione fornita dal famoso Cert Coordination Center, un trademark della Carnegie Mellon Universities, che non corrisponde a un vero e proprio acronimo ma che può essere ricondotto al termine "computer emergency response team", proviamo a capire come viene definito e affrontato il problema della sicurezza nella Rete delle reti.

Il ruolo di questo centro, in funzione presso il Software Engineering Institute della stessa Università e finanziato con fondi federali Usa, è diventato istituzionale dal 1988. In quell'anno, il primo vero "incidente" di natura maligna aveva portato al sostanziale blocco di almeno il 10% dell'infrastruttura di Internet, che alla fine del 1989 contava circa 700.000 host collegati. Fu infatti nel novembre del 1988 che uno studente della Cornell University, Robert Morris, scrisse in via del tutto sperimentale un programma capace di autoreplicarsi e di propagarsi in Rete sfruttando una vulnerabilità del comando Unix sendmail. Il Morris' Worm, il primo "verme" dell'era di Internet, infettò nel giro di poco tempo un'enorme quantità di sistemi, accademici, scientifici, civili e militari. Secondo le stime di chi ha successivamente ricostruito l'incidente, i costi per il ripristino della normalità costarono da 200 a 53.000 dollari per sistema. Morris fu uno dei primi hacker – anche se probabilmente

mosso da una curiosità scientifica – a essere condannato in tribunale, in base alla normativa allora vigente in materia di frodi e abusi: dovette scontare tre anni di arresti domiciliari, 400 ore di servizio comunitario e una multa di 10.000 dollari. Prima di questo incidente, il primo a provocare un sostanziale blocco di parte dell'infrastruttura, c'era stato l'attacco descritto nel celebre libro di Clifford Stoll, *L'uovo del cuculo*. Stoll, giovane astronomo di Berkeley, nel 1986 aveva smascherato il primo complotto internazionale ufficialmente segnalato nella storia, già quasi ventennale, di Internet. Allora si era trattato di un gruppo di hacker tedeschi che facendo leva sulle vulnerabilità di un computer avevano compromesso la sicurezza di diversi sistemi militari, trafugando copie di documenti classificati.

Sette modi per attaccare Internet

Secondo il Cert gli incidenti di natura soprattutto logica che riguardano la sicurezza su Internet ricadono in sette categorie principali: probe (sonde), scan, compromissione di un account, compromissione del root, packet sniffing, Denial of Service, abuso della fiducia, codici maligni e attacchi diretti alla infrastruttura della Rete. Vediamo brevemente il significato di ciascuno.

▶ Le "sonde" sono caratterizzate dal tentativo non espressamente autorizzato di ottenere l'accessibilità o le informazioni relative a un sistema informatico. Di solito si effettua cercando di inserire il nome e la password di un account. Si tratta in altre parole dell'equivalente elettronico di un topo di appartamenti che gira la maniglia di una porta alla ricerca di un facile passaggio.

I 13 ROOT NAMESERVER

L'infrastruttura Dns poggia su 13 root nameserver la maggior parte dei quali è concentrata negli Stati Uniti

▶ Lo "scan" definisce una serie più o meno nutrita di sonde, spesso gestite in automatico con l'aiuto di speciali software. A volte sono solo il preludio di un attacco successivo rivolto a un sistema già identificato come vulnerabile.

▶ Un account compromesso è molto semplicemente una "userid" rubata o in qualche modo individuata da una persona non autorizzata. A seconda dei privilegi assegnati a quel determinato account si possono prevedere danni di natura varia, ma limitata. Di solito tuttavia, gli hacker compromettono un account generico proprio per cercare di colpire punti ancora più delicati.

▶ Un root compromesso, nell'ambiente operativo Unix, è il rischio peggiore perché a esso fanno capo i privilegi del cosiddetto "superuser", un utente capace di fare il bello e il cattivo tempo sul computer. Paradossalmente, sottolinea

I PILASTRI DI INTERNET

Root nameserver	Operatore	Dislocato a	Indirizzo Ip
A	VeriSign Global Registry Services	Dulles (Virginia, Usa)	198.41.0.4
B	Information Sciences Institute	Marina Del Rey (California, Usa)	128.9.0.107
C	Cogent Communications	Herndon (Virginia, Usa); Los Angeles (California, Usa)	192.33.4.12
D	University of Maryland	College Park (Maryland, Usa)	128.8.10.90
E	NASA Ames Research Center	Mountain View (California, Usa)	192.203.230.10
F	Internet Software Consortium	Palo Alto, San Jose, San Francisco, Los Angeles (California, Usa); New York City (New York, Usa); Madrid (Spagna); Hong Kong (Cina)	IPv4: 192.5.5.241 IPv6: 2001:500::1035
G	U.S. DOD Network Information Center	Vienna (Virginia, Usa)	192.112.36.4
H	U.S. Army Research Lab	Aberdeen (Maryland, Usa)	IPv4: 128.63.2.53 IPv6: 2001:500:1::803f:235
I	Autonomica	Stockholm (Svezia)	192.36.148.17
J	VeriSign Global Registry Services	Dulles, Sterling (2 postazioni) (Virginia, Usa); Mountain View (California, Usa); Seattle (Washington, Usa); Atlanta (Georgia, Usa); Amsterdam (Olanda)	192.58.128.30
K	Reseaux IP Europeens - Network Coordination Centre	London (Gran Bretagna)	193.0.14.129
L	Internet Corporation for Assigned Names and Numbers	Los Angeles (California, Usa)	198.32.64.12
M	WIDE Project	Tokyo (Giappone)	202.12.27.33

→

Yann Bongiovanni, l'esperto in sicurezza che *CHIP* ha consultato in questa occasione, un sistema operativo come Microsoft Windows, considerato da molti poco sicuro per le vulnerabilità proprie e dei suoi applicativi, in alcuni casi può essere considerato meno rischioso. Windows 2000, per esempio, prevede una tipologia di utenti di default privi del carattere di superuser. Sotto Unix, la compromissione del root serve all'hacker non solo per fare ogni sorta di danni, ma per cancellare le tracce del proprio passaggio.

▶ La tecnica del packet sniffing si basa su programmi nascosti capaci di catturare le informazioni trasportate dalla Rete. Ovviamente i dati possono contenere password, userid e altre informazioni che consentono di raggiungere l'ambito risultato della compromissione di un account. A questa categoria di attacchi corrispondono a grandi linee anche i cosiddetti spyware.

▶ Denial of Service o Dos. Una forma indiretta di attacco che non consiste nel tentativo di penetrazione non autorizzata di un sistema, ma nell'impedire totalmente l'accesso da parte degli utenti legittimi. Un attacco Dos comporta per esempio una raffica di richieste che mandano rapidamente in tilt le limitate risorse di un Web server, ma può anche riguardare bersagli di carattere più infrastrutturale, come gli stessi router.

▶ Un hacker che abusa la fiducia di un sistema sfrutta le relazioni che spesso sussistono tra un sistema informatico e un altro. A volte per esempio un computer non esegue un determinato comando se prima non ha verificato che la richiesta proviene effettivamente da una identità (un utente, una seconda macchina) considerata sicura.

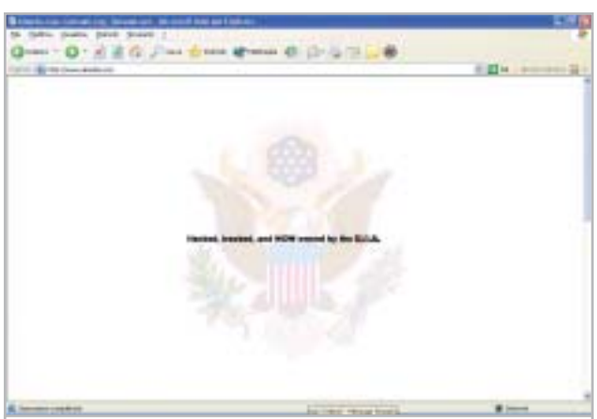
▶ Sui codici maligni esiste purtroppo una vasta letteratura e soprattutto un'estesa consapevolezza, anche da parte degli utenti meno esperti di Internet. Nella categoria ricadono i programmi software che una volta eseguiti provocano una serie di risultati più o meno imprevedibili e devastanti. Il vero inconveniente è che sui sistemi non protetti ed esposti agli attacchi, la presenza di un virus o di un altro codice maligno viene individuata solo a frittata già fatta. A sua volta, il codice maligno può essere solo una tappa di un incidente più articolato.

▶ Infine, gli attacchi di natura infrastrutturale sono i più rari, ma anche i più temibili. Si riferiscono a tecniche

SCENARI ALTERNATIVI

» Info-guerriglia via Internet

Dorothy Denning, autrice di un fondamentale libro di testo in materia di sicurezza e lotta contro la cosiddetta information war o "infowar", nel corso di un'udienza parlamentare sul cyberterrorismo (Parlamento Usa, maggio 2000) ha spiegato che Internet può facilmente diventare un'arma per diffondere o impedire la diffusione di informazioni. Siano esse veritiere, propagandistiche o destabilizzanti. I casi allora citati dalla Denning, partivano da un episodio del 1996, quando un militante del gruppo razzista Supremazia Bianca aveva attaccato i server del provider che aveva censurato le pagine curate dalla "associazione", fino alla guerra nel Kossovo, quando i computer della Nato furono bombardati da spamming e tentativi di Denial of Service. L'uso degli strumenti telematici - a colpi di infuocati siti Web incitanti all'odio, o di attacchi che mirano a distruggere questi siti - è diventato di routine in molti teatri di scontro, a incominciare da quello medio-orientale. E molti si chiedono se oggi il rischio è quello di vedere attaccati i siti che gestiscono i servizi telematici al cittadino, il cosiddetto e-go-



Il sito *www.alneda.com* direttamente collegato al partito di Osama Bin-Laden è stato totalmente oscurato

Sul Web continuano a diffondersi rapidamente siti che inneggiano a presunti gruppi fondamentalisti islamici

aggressive simili a quelle appena descritte, ma rivolte ai centri nevralgici di Internet, come i sistemi dei principali provider o addirittura le macchine "root", principali, del Domain Name Server.

La sicurezza di questi ultimi sistemi merita un particolare approfondimento perché il cuore della struttura ad albero che contiene la lista degli alias alfanumerici assegnato agli indirizzi numerici (Ip) di Internet è molto delicato. Il sistema Dns si basa su una struttura ad albero che parte dai cosiddetti "root nameserver", transita per i server primari e arriva ai Dns locali. Un danno esteso subito dai root, il punto di partenza di una ricerca che non vada immediatamente a buon porto su scala locale, renderebbe praticamente non navigabile l'intera Internet. Nessuno saprebbe più letteralmente come trovare tanti milioni di server identificati dalla tipica espressione *www.nomedelsito.com*.

L'attuale infrastruttura Dns poggia su 13 root nameserver dislocati in tutto il mondo presso i maggiori registri dei nomi di dominio (si veda la tabella a pag. 41). Nell'ottobre del 2002, per la precisione il giorno 21, questo sistema ha subito un attacco Dos coordinato che ha suscitato un certo scalpore, evidenziando anche agli occhi del grande pubblico alcuni punti di vulnerabilità che sono intrinseci in determinati protocolli di Internet. In realtà il problema non aveva avuto esiti particolarmente negativi ed è stato misurato solo in virtù della costante azione di monitoraggio che l'organismo Iana ha imposto nel "dopo 11 settembre", proprio per generare maggior tranquillità nei confronti di Internet, visto come possibile bersaglio di cyberguerriglia.

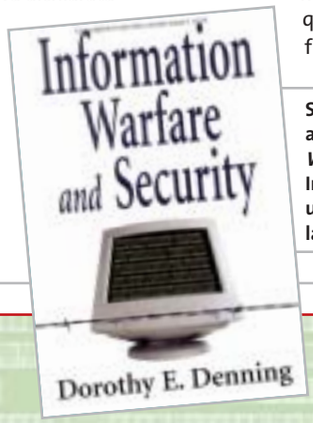
Le teste di ponte della cyberwar

A Yann Bongiovanni, di Live Network Security, *CHIP* ha chiesto un commento su questo episodio e sul possibile livello di rischio per la Rete come infrastruttura. "In alcuni protocolli su cui si fonda l'infrastruttura di Internet (in particolare Dns e Bgp) sono assenti misure di sicurezza importanti quali l'autenticazione", risponde Bongiovanni riferendosi alla mancanza di un'effettiva barriera di controllo degli accessi per un sistema come il Dns. "È possibile sfruttare queste debolezze per creare attacchi Dos

Haganah, un blog filo-israeliano, pubblica e aggiorna costantemente tutte le notizie relative al fronte della e-Jihad

vernment. Nel recentissimo conflitto in Iraq, ha destato molta sensazione un tentativo, riuscito, di hackeraggio nei confronti del sito Web ufficiale della televisione satellitare di Baghdad, trasformato in un volantino propagandistico per un gruppo religioso oltranzista cristiano.

Prima, c'erano state molte segnalazioni di analoghi tentativi, questa volta di parte avversa, inclusi quelli condotti dalla stessa Al Qaida. Cacciata dal consesso dei provider ufficiali di spazio Web, la cellula terroristica globale ricorrerebbe all'infowar per fare la sua propaganda attraverso il "sequestro" di altri siti Web. Mentre gruppi e individui di opposta fazione hanno usato le stesse armi per colpire un indirizzo come *www.alneda.com*. Fino all'anno scorso il sito, ospitato da un provider malese, faceva dichiaratamente capo al partito di Osama Bin-Laden. Quando il provider lo cancellò dai suoi registri su pressione americana, Jon Messner si impossessò del controllo di quello stesso dominio e per diversi giorni, nel luglio del 2002, giocò a fare della contropropaganda, utilizzando un software di traduzione automatica in arabo. Oggi, secondo il sito di Aaron Weisburd (*www.weisburd.net/jihadi/active.php*) Al Qaida continuerebbe a prendere possesso di piccoli, insospettabili siti Web, inserendo le sue pagine nelle sottodirectories più nascoste. Il problema della infoguerriglia è che spesso è quasi impossibile distinguere la reale matrice degli attacchi o della propaganda. Fa fede l'interessante blog di un gruppo pro-israeliano, *haganah.us/haganah/index.php*, che pubblica le ultime notizie sul fronte della e-Jihad, la guerra santa condotta sugli incerti territori del Web da presunti gruppi fondamentalisti islamici. Il confine tra verità e disinformazione è veramente labile quando si tratta di anonimi flussi di bit.



Secondo Dorothy Denning, autrice di *Information Warfare and Security*, Internet può diventare un'arma per impedire la diffusione delle notizie

→

su larga scala. A facilitare lo sfruttamento di vulnerabilità esistono milioni di server connessi a Internet senza adeguate protezioni. Questi server possono fare da testa di ponte, come avviene comunemente per i cossiddetti Ddos, dopo che sono stati manomessi con l'installazione di programmi dormienti (chiamati nel gergo "zombie"), attivati simultaneamente al momento dell'attacco". Bongiovanni in questo caso parla di attacchi Dos di tipo "distribuito", effettuati di solito prendendo possesso di un certo numero di macchine e facendo partire da queste una salva di attacchi concomitanti. "Credo comunque"

»Tutti i server attualmente collegati a Internet senza adeguate protezioni fungono da testa di ponte durante gli attacchi«

Yann Bongiovanni, fondatore di Live Network Security

conclude, "che un attacco all'infrastruttura debba avere come target più di un tipo di vulnerabilità per essere efficace. Le ripercussioni di un attacco Dos ai root nameserver danno per esempio luogo a un semplice disservizio, lasciando abbastanza tempo per la reazione. Sarebbe più distruttivo alimentare i Dns con dati falsati".

Una lunga lista

La lista di vulnerabilità di Internet, dei suoi protocolli e delle sue numerose istanze nel mondo fisico è lunga. Ma questo non basta a impedire che sulla problematica della cyberwar vengano espresse anche caute perplessità. La più ovvia si basa sull'esperienza recente. Fino a pochi minuti dalla mezzanotte del primo gennaio del 2000, erano in parecchi a pronosticare una sorta di fine del mondo informatica. I computer, in generale, non si sono affatto bloccati e nessun sistema davvero critico ha provocato danni di una certa entità per colpa del temutissimo baco. C'è chi ribatte che il paragone non è calzante: il Millennium Bug non ha provocato grossi problemi semplicemente perché i programmatori e consulenti di mezzo mondo hanno lavorato per evitarli. Contro la guerriglia informatica si possono invece prendere solo delle contromisure, nell'attesa di doverle verificare sul campo (mai, si spera). Probabilmente si deve anche distinguere tra attacchi di matrice militare o politica ma del tutto convenzionali e azioni di tipo terroristico, imprevedibili per loro natura. Chi esprime scetticismo sulla portata reale di certi rischi sottolinea per esempio che i guasti provocati da malfunzionamenti accidentali, errori di manovra e perfino quelli di origine maligna, hanno sempre provocato danni di portata limitata e agevole reversibilità, fin dai tempi del Morris' worm.

La questione è stata posta anche a Bruce Schneier, uno degli esperti più quotati al mondo in materia di sicurezza. In particolare, un giornale iraniano ha chiesto a Schneier se il Pentagono fosse in possesso di un'arma segreta che potesse rendere del tutto inutilizzabile Internet (la cyberwar, in effetti, potrebbe anche essere difensiva). Schneier ha provato a rispondere in un recente numero della sua newsletter, Cryptogram: "Non c'è dubbio che gli organismi militari meglio preparati e finanziati abbiano formulato piani relativi a una possibile cyberwar, in chiave di attacco e di difesa. I militari possono attaccare le infrastrutture di comunicazione del nemico in termini fisici - bombardando impianti e sistemi di cablaggio - o virtuali. Sarebbe stupido per un militare ignorare questa minaccia e non investire in capacità difensive, o trascurare la possibilità di lanciare un attacco informatico offensivo in periodo di guerra dichiarata. E se la storia ci ha insegnato che molti militari sono stupidi, altri non lo sono. Secondo me è quindi possibile che i militari Usa siano in grado di disattivare grosse porzioni di Internet, almeno per un po', se lo volessero. Ma dubito che vogliano davvero farlo; si tratta di un bene troppo importante, di una parte troppo consistente della nostra economia. È più interessante chiedersi se è possibile un tentativo di disattivazione parziale della Rete. Se fossimo in guerra contro la nazione X, cercheremmo o no di

»Gli organismi militari hanno sicuramente formulato piani relativi a una possibile cyberwar per l'attacco ma anche per la difesa«

Bruce Schneier, fondatore di Counterpane Internet Security

disabilitare le parti di Internet da loro controllate o di rimuovere le connessioni tra la nostra Internet e la loro? (…) Non dobbiamo dimenticare che è auspicabile disattivare la rete di comunicazione di un nemico solo nella misura in cui non si riesca a ricavarne delle informazioni".

Insomma, la cyberwar è possibile, ma non è detto che sia davvero intelligente. La cosa più probabile è che certe possibilità finiscano per essere accettate, in modo che possano fungere da deterrente. Come la bomba atomica dopo Hiroshima, anche l'arma non convenzionale della cyberwar non verrà mai utilizzata, almeno fuori dai tragici contesti del terrorismo. ■