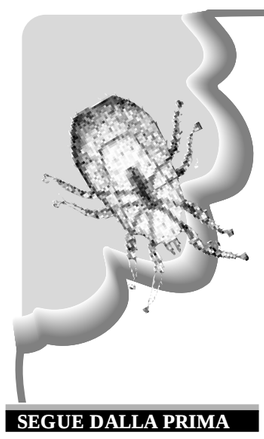
10INT01A1002 ZALLCALL 11 00:56:15 02/10/99



◆ *Colpite ieri Amazon.com, E-Bay Cnn.com, Buy.com, E-Trade Datek Online e Ziff-Davis*

◆ *Come per Yahoo! i server sono stati sommersi da milioni di richieste fittizie di lettura*

◆ *La nuova offensiva sferrata non è stata per adesso rivendicata da alcun gruppo o sigla*

Gli hackers bombardano la Rete

Grande attacco a compagnie commerciali e di comunicazione

SEGUE DALLA PRIMA

Che si tratti di una offensiva pianificata con una certa cura, e soprattutto con obiettivi attentamente studiati, lo dimostra anche la scelta degli «obiettivi». Ad esempio Buy.com, che proprio ieri debuttava a Wall Street con la prima quotazione delle sue azioni. Solo una delle moltissime «IPO's» (offerte di azioni al pubblico di società più o meno legate a Internet) che negli ultimi mesi hanno letteralmente dilagato sul mercato finanziario.

Per adesso, le prime indagini della Fbi non hanno prodotto risultati. Non è impossibile, affermano gli esperti, riuscire a rintracciare gli sconosciuti hackers protagonisti dell'attacco. Ma se l'azione è stata condotta da gente in grado di muoversi con competenza nel mondo dell'informatica e della telematica, è possibile che le ricerche per via elettronica siano destinate a dare risultati modesti. Molto più probabile, invece, che le indagini di tipo convenzionale - ovvero con la classica attività investigativa «non virtuale» - si rivelino più efficaci. Qualcuno, nel mondo ampio ma non infinito della galassia hacker, si vanterà, o farà un passo falso in grado di allertare la Fbi. Non è da escludere, comunque, che ulteriori attacchi distruttivi, anche se dannosi soltanto temporaneamente, si verifichino nei prossimi giorni.

Non c'è dubbio, qualunque sia l'identità e lo scopo dell'azione, che la campagna contro la «Rete dei soldi» rappresenta un punto di svolta di grande rilievo per tutti. Da qualche anno a questa parte Internet aveva perduto il primitivo carattere di faccenda per pochi addetti ai lavori, esperti, o semplici privati. Molti avevano visto con orrore la crescente commercializzazione della Rete, che la vera e propria Internet-mania dei mercati di Borsa (a volte, senza alcun reale fondamento finanziario e produttivo, come forse un giorno, con dolore, gli investitori poco avveduti scopriranno) aveva moltiplicato in modo esponenziale.

Nel giro di poche settimane sono state realizzate vere e proprie fortune, persino con la vendita online di cibo per cani. Passando a un terreno più solido, l'intreccio tra la Rete e il complesso mondo delle telecomunicazioni (telefonia fissa e cellulare, informatica diffusa, «personal digital assistants») da un lato, e le opportunità di adoperare il Web come «sportello» per la commercializzazione di ogni tipo di prodotto dall'altro, stanno letteralmente trasformando il modo di comunicare, produrre e vendere. E, a quanto pare, a qualcuno questo cambiamento forse inevitabile non piace.

Il «punto di svolta», la scoperta per molti del tutto inattesa, è che l'errore, il difetto, il buco nella sicurezza è inerente e implicito in tutti i sistemi informatici. A volte è un buco molto piccolo, e serve grandissima competenza per trovarlo e sfruttarlo; a volte, è evidente e clamoroso. Da sempre si confrontano, in campo informatico, mezzi offensivi e mezzi difensivi. Il perfezionamento delle capacità di offesa mette in moto un processo di adeguamento delle misure di protezione. In linea teorica, arrivare a una sicurezza «totale» è praticamente impossibile; sicuramente, è possibile migliorare e rendere più efficienti le garanzie.

È probabile che questi eventi scatenino una irrazionale ondata di «terrore», di insicurezza e di diffidenza verso uno strumento come la Rete. Uno strumento ancora poco «compreso», e spesso trattato dai mezzi di informazione con sensazionalismo e superficialità. Ma forse, se si potrà ricavarne una lezione, sarà una lezione semplice e di buon senso: la sicurezza globale non esiste. I sistemi informatici «crollano», ma la Rete continua a essere un mezzo eccezionale che aumenta le potenzialità degli uomini e delle donne. Anche le automobili, i treni e gli aerei non sono totalmente sicuri. Ma continuiamo ad adoperarli ogni giorno.

ROBERTO GIOVANNINI

MENTALITÀ

Un'etica c'è: scoprire tutto e «saltare» oltre gli ostacoli

ROMA Per riassumere la mentalità e la filosofia dei veri hackers, basta leggere il motto che troneggia in testa al sito del gruppo «L0pht Heavy Industries» (www.l0pht.com). «"Questa presunta vulnerabilità dei sistemi è del tutto teorica" disse la Microsoft. L0pht dal 1992 trasforma in fatti quanto sarebbe solo teoria». Insomma, quello che anima i veri gruppi di hackers, quelli seri e organizzati, non è affatto una volontà criminale e perversa di seminare paura e terrore. La «sfida» - sfida di conoscenza e saperi, sfida tra intelligenze - è quella di verificare il funzionamento dei sistemi informatici, hardware e software. Provarne la solidità, individuarne i limiti, mostrarne le insufficienze. Alcune sono evidenti e facili da dimostrare, come le notorie «bombe» che rendono Windows, in tutte le sue versioni, un sistema pesante, macchinoso e facilissimo a «impallarsi». Altre, invece, richiedono un lavoro notevolissimo, sapienza vera e propria, organizzazione, sforzi concertati.

L0pht, così come molti altri gruppi «storici» di hackers, non ha nulla a che vedere con la campagna condotta in queste ore contro i principali portali commerciali su Internet. Gli informatici di questo gruppo preferiscono cancellare dalla Rete i siti pornografici di pedofilia; e recentemente, a sorpresa, la decisione di annunciare la nascita di una nuova società che venderà servizi di sicurezza informatica, la @Stake. Da una parte, i «misteriosi» ex-pirati; dall'altra serissimi e ufficialissimi informatici, provenienti dalla Compaq e dalla Forrester Research. E nell'impresa ci sono anche 10 milioni di dollari investiti come «venture capital». Il patto è che la nuova azienda non venderà specifici prodotti di sicurezza (ma consulenza), che non prenderà soldi dalle aziende di software, e che non interferirà con la «normale» attività di L0pht, cioè la diffusione di «buchi» e inadeguatezze nei sistemi informatici.

Lo scenario dell'hacking, comunque, è molto variegato. Ci sono questi hackers in «camice bianco», ma anche gruppi più o meno politicamente targati: in genere, il «messaggio» è contro la commercializzazione della Rete e contro il dominio di danarosi portali e della pubblicità. E ci sono anche, gruppetti di ragazzi brillanti e più o meno brufolosi, che impiegano il loro tempo e la loro bravura in incursioni in giro per Internet. Quasi sempre, tutti gli hackers sono uniti da una certa «etica», che è l'etica della curiosità, del divertimento nel far saltare le cose che funzionano, nel superare un ostacolo frapposto da altri alla loro volontà di «scoprire».

Questa era la «filosofia» di Kevin Mitnick, per molti un eroe, per molti un criminale. Mitnick, il primo famoso «pirata», a lungo si divertì a penetrare nei sistemi della banche, di aziende come Nokia, Motorola e Sun), persino della Difesa Usa. Poi venne rintracciato, arrestato e condannato. Proprio in questi giorni, dopo aver scontato cinque anni di prigione, è stato scarcerato. È più «pirata» Mitnick, o la catena televisiva Cbs, che ha a lungo sovrapposto digitalmente alle sue riprese tv immagini pubblicitarie inesistenti e solo «virtuali», ma ben visibili dai telespettatori, e lautamente pagate dagli sponsor?

R. Gi.

L'INTERVISTA

Nuti, MC-link: «Ce l'aspettavamo Non vogliono il mercato on line»

GIAMPIERO ROSSI

MILANO E dopo le tante interviste agli esperti per cercare idee utili a fermare il fenomeno della criminalità diffusa, ecco le nuove allarmate domande: chi sono questi famigerati pirati informatici? Come fanno a combinare guai così grossi? Perché lo fanno? Come si possono fermare? E, attenzione, perché la prima e più convinta risposta offerta da Paolo Nuti (amministratore delegato di Mc Link e quindi Internet provider di professione) sembra ricalcare quelle già sentite a proposito della lotta al crimine non-virtuale: «La prima cosa da fare, il terreno principale su cui avviare la lotta alla pirateria informatica - spiega infatti Nuti - è quella dell'educazione al senso di responsabilità nei confronti di tutti gli utilizzatori di Internet, è quella che potremmo chiamare l'educazione alla legalità. Inutile illudersi con altri rimedi...».

Ingegner Nuti, davvero siamo di fronte alla necessità di educare gli utenti più ancora di quella di combattere il fenomeno degli hacker, i pirati informatici?

«Sicuramente c'è l'esigenza di correre ai ripari. Circa il come, penso sinceramente che il primo rimedio debba essere individuato nell'educazione del pubblico rispetto al proprio senso di responsabilità, come avviene per qualsiasi comunità. Solo che per la rete questo aspetto suona un po' strano perché in molte situazioni viene vissuto come il luogo dell'assenza di responsabilità dei singoli».

Ma un conto è il singolo che fa dispetti coperto dall'anonimato, un altro è l'attacco in massa per mettere fuori uso un colosso come Yahoo: si direbbe proprio che c'è qualcosa di organizzato...

«Certo, e in questi casi spesso non c'è difesa che tenga. L'episodio che ha colpito Yahoo viene definito un atto di "bombing", cioè di bombardamento, il cui scopo è quello di tappare la bocca a qualcuno. Per farlo possono bastare poche centinaia di computer».

E chi può averne interesse?

«Sicuramente chi vuole fare dell'aggiotaggio nei confronti di un concorrente quotato in borsa, per esempio, ma anche l'ex dipendente che è stato licenziato, per fare un dispetto; ma soprattutto, e credo anche in questo caso, si tratta di un'azione di anarchia informatica, perché la rete viene considerata uno spazio per la comunicazione e quindi l'attuale crescita delle forme di sfruttamento commerciale vengono osteggiate. Ce lo aspettavamo, del resto...»

Come ve lo aspettavate? Circolavano voci di "attacchi" degli hacker?

«No, però sono almeno sei mesi che a ogni convegno dei provider ci diciamo che c'è nell'aria qualcosa, e il segnale di ciò è stato il proliferare dei virus pensati proprio per colpire l'e-commerce. Ce ne sono di intelligentissimi: per esempio uno che si installa in un computer senza fare danni ma si mette subito in contatto con il suo "padrone" e gli comunica tutto dal computer in cui si trova. Così succede che l'hacker che lo ha messo in circolazione può controllare diverse funzioni di quel computer e anche fare danni con la posta elettronica, facendola circolare a proprio piacimento».

E tutto questo perché?

«Per qualcuno perché dà soddisfazione riuscire a realizzare una cosa del genere, per altri per danneggiare dolosamente qualcuno, per esempio un concorrente, nella maggioranza dei casi per sancire che la rete è uno spazio di libertà, riservato solo alla comunicazione e non al commercio. Per tutti, comunque, va usata l'arma dell'educazione alla legalità».

GLOSSARIO MINIMO

Le parole dei pirati

Back door. È una «porta di sicurezza» nascosta in un programma. Può essere usata, se individuata, per superare le difese.

Cracker. È chi, solo per gusto vandalistico o a finalità di furto, si diverte a superare i sistemi di sicurezza. È un software cracker chi «spezza» le protezioni dei programmi commerciali.

Denial of service attacks. Sono gli attacchi che stanno mettendo in ginocchio i principali portali: i server vengono inondati («flooded») di false richieste di collegamento a pagine Web, molte milioni di richieste. Il server cerca prima di rispondere, e poi crolla.

Mailbombing. Bombardamento di posta. Una casella di posta Internet viene «bombardata» con appositi programmi da centinaia di messaggi, che contengono allegati con manuali o filmati da decine di MB. Sempre che non crolli prima il server di posta del provider, la casella di posta della vittima diventa inutilizzabile.

Hacker. Una persona che si diverte a esplorare le possibilità e i limiti di un sistema informatico, dotato di notevoli capacità tecniche. Il vero hacker lo fa solo per divertimento, per dimostrare che lui è capace a farlo, che la vittima non investe in sicurezza. Talvolta, l'hackeraggio può avere scopi di più ampio respiro.

Phreaking. L'utile arte di «crackare» le reti telefoniche per chiamare gratis o a spese di altri utenti ignari.

Sneaker. È chi «entra di nascosto» dentro un sistema, quasi sempre un pirata «affittato» da un'azienda per verificare la sicurezza del sistema.

Time bomb. Bomba a orologeria. È una sottospecie di «bomba logica», ovvero un programma «dormiente» che si attiva solo se a determinate condizioni. Una «time bomb» esplode in un momento prestabilito: talvolta, è un regalino dei programmatori licenziati ai loro ex-padroni.

Virus. Virus, «vermi», cavalli di Troia, «bombe logiche» sono programmi invasivi, in alcuni casi molto pericolosi. I virus possono «copiarsi» all'interno del computer, e attivarsi all'improvviso per compiere diverse funzioni: da scritte più o meno spiritose alla formattazione totale del disco fisso. Alcuni attivano il modem del Pc, e gli fanno chiamare chat line erotiche in Moldavia. Lo si scopre con la prima bolletta.

R. Gi.

LA STORIA

Informatico preso di mira si ribella Gli rovinano matrimonio e lavoro

ROMA Dove si vede che gli hacker «cattivi» possono provocare anche problemi seri. La versione digitale del settimanale Usa «Forbes» racconta la storia di Jay Dyson, un informatico della Nasa, che ha scatenato con due hackers una vera e propria guerra privata che gli è costata (nell'ordine) il divorzio dalla moglie, la perdita della sua aziendina privata, e un pauroso aumento di peso. E per giunta, ha ricominciato a fumare.

I fatti. Alle 10 di mattina del 5 marzo 1997, il nostro (37 anni, dipendente dell'agenzia spaziale Usa, per la quale gestisce la sicurezza del sito), si accorge che la pagina Web della Nasa era stata hackerata. Un gruppo autodefinito Hagis (ovvero «Hackers Contro gli Informatici Scemi in Giacconi da neve») aveva istoriato la homepage Nasa con un altisonante messaggio: «tutti coloro che fanno i soldi abusando di Internet saranno vittime del nostro futuro regno di terrorismo digitale».

Dyson prende la faccenda sul personale, e sul proprio sito se la prende con i pirati, accusandoli di essere solo «un gruppo di bambini deficienti». Mal gliene incoglie. Due membri dell'Hagis, «u4ea» e «tr0ut» (sta per «Euphoria» e «Trout«, trota) si arrabbiano di brutto, e decidono di fargliela pagare. Ecco come. Prima entrano nella pagina Web di Dyson, e gliela «riscrivono». Lui la rimette a posto, e loro la ricambiano: «pagherai per la tua stupidità». Lui replica: «non volete la libertà di parola?». Loro, per tutta risposta, stroncano per due settimane l'Internet provider che dava accesso alla Rete al «nemico». Dyson si mette ossessivamente a inseguire le tracce dei suoi avversari, e (già in piena paranoia) decide di comprarsi una pistola. Nel dicembre del '97, il nostro scopre che i suoi telefoni, a casa e sul lavoro, sono stati staccati: «qualcuno» lo aveva ordinato alla compagnia telefonica. Una settimana dopo, i cattivissimi pirati scrivono una minacciosissima mail alla moglie di Dyson; la poveretta si impaurisce, si dispera, e comincia a litigare col marito, ormai completamente perso nella sua guerra personale. A fine gennaio '98, «tr0ut» e «u4ea» sabotano il secondo provider di Dyson, quello della sua impresa privata (costruzione di siti Web). Lui cerca di rimettere a posto le cose, ma improvvisamente mentre lavora appare in diretta un messaggio degli hackers. Dyson chiede: «che volete?». E loro: «Mettiti su una gamba sola, salta tre volte, e grida "gli Hagis sono i più forti!"».

Un vero incubo. Nei mesi successivi, il divorzio, problemi con l'Fbi, insospettita per le attività di Dyson, il crollo fisico e psicologico. Infine, nell'aprile del '98, in Canada viene arrestato il 22enne Jason Mewhiney, alias «tr0ut». Un ragazzetto definito «molto timido», poi condannato a sei mesi di prigione. Invece, «u4ea» è ancora libero: Dyson pensa di sapere chi sia, ma a «Forbes» dichiara di non aver nessuna intenzione di denunciarlo alla Fbi. Accarezzando la sua pistola, spiega che «è un affare privato, tra me e lui».

R. Gi.

LETTERATURA

Gli eroi amari e romantici della fantascienza cyberpunk

ROMA «Il cielo sopra l'astroporto aveva il colore di una tv sintonizzata su un canale morto». Tutto cominciò con questa frase. Tutto ovvero il *cyber-punk*, l'ultimo capitolo della letteratura di fantascienza. Inventore del genere Williams Gibson, americano di nascita e canadese di adozione, padre putativo di tutti gli hackers del mondo. I suoi racconti (talvolta firmati con l'amico Bruce Sterling) e soprattutto i suoi romanzi cominciando da «Neuromante» (1984) fondano una mitologia che finirà per rivelarsi molto meno fantastica di quanto si poteva supporre. Certo nel nostro presente non ci sono astroporti, non ci sono «agglomerati» (così sono ribattezzate le megacittà), non ci sono pianeti artificiali e l'uomo non ha colonizzato Marte.

C'è invece la rete che all'epoca muoveva i suoi primi passi e non sembrava affatto destinata a diventare un media invasivo e di massa, ci sono le grandi compagnie che controllano questa industria immateriale e che Gibson aveva ribattezzato alla giapponese «zaibastu». E ci sono gli hackers, ovvero dei ragazzi capaci di navigare nella rete e di rompere le difese dei diversi siti. Per lo scrittore sono loro gli eroi (dei veri cavalieri solitari punk) di questo futuro non proprio invidiabile. La serie di romanzi di William Gibson, pubblicati in Italia da Mondadori, prosegue con «Giù nel cyberspazio» (1986), con «Mona Lisa Cyber-punk» (1988), per arrivare ai più recenti - e forse un po' più stanchi - «Luce virtuale» e «Aidoru» scritti negli anni novanta, quando ormai la rivoluzione informatica cominciava a mostrare le sue caratteristiche e le sue dimensioni.

Perché tanta passione per gli hackers? Perché Gibson non si fida della rete, o meglio ne coglie da una parte l'elemento di unificazione e di controllo, di vero e proprio dominio commerciale (nei suoi libri la politica e gli Stati sono stati «azzerati») e dall'altra ne individua la debolezza, rappresentata proprio dalle crepe che vi possono essere aperte da una incursione «anarchica».

Per Gibson - e questo è l'elemento più lontano dalla realtà ma forse più affascinante - esiste un rapporto corporeo, anche se di una fisicità tutta astratta, tra gli oggetti visibili e immateriali che si trovano nella rete e chi vi entra per «farla saltare». Qualcosa di molto più amaro e romantico di quella serie infinita di clik che ha mandato a gambe all'aria Yahoo.