Autore: Raoul Chiesa - *Febbraio 2000*

La bolla di sapone che ha sconvolto il mondo: …e cosa succede se gli hackers arrivano davvero?

- Lunedì 7 febbraio 2000, ore 13.30 NYC Time: Yahoo! viene "attaccato" e paralizzato per alcune ore

- Martedì 8 febbraio 2000: ha inizio un'interminabile serie di comunicati stampa che fanno il giro del mondo: dagli USA all'Europa passando per l'Asia, la notizia della violazione scatena paure ed angosce.

- La seconda settimana di febbraio prosegue con i blocchi di E-Bay, CNN, ZdNet, Amazon, E-Trade...

- L'ultimo aggiornamento, del 17 febbraio, narra di improbabili hacker italiani e di un Federal Bureau of Investigation che indaga addirittura in Italia.

Il concetto stesso di ***"P&P"*** (***Panico e Paura,*** come dice spesso un mio caro amico) cresce a dismisura: interviene la Casa Bianca, l'FBI si scatena (pare senza enormi successi), il palleggio delle colpe varia, in una ***bailamme*** di teorie strane.

I fatti

Una serie di sistemi informatici connessi alla rete Internet ed eroganti servizi web sono stati attaccati. Una prima precisazione: non c'è stato alcun tipo di intrusione, intesa nel senso puro del termine: vi sono state operazioni di DoS, Denial of Service. Ciò avviene quando un sistema - in più modi e con differenti mezzi e logiche - viene reso non operativo, vale a dire quando il sistema stesso non è più in grado di erogare una serie di servizi.

Questi servizi possono essere le pagine web (quindi informazioni utili alle persone, sia a titolo gratuito che a pagamento), i servizi di posta elettronica o di scambio file, etc...

Un attacco di questo tipo, in genere, non necessita di grandi capacità e conoscenze tecniche, richiede il semplice utilizzo di uno o più software (reperibili in Rete) e - per "lavorare" al meglio - un sistema informatico di "partenza", connesso alla rete Internet ad alta velocità.

I mass-media hanno ampiamente spiegato - dopo aver parlato per una decina di giorni di "sofisticate tecniche di attacco" - le modalità di un attacco di questo tipo, le simpatiche analogie per spiegare all'utenza comune cos'è un DoS, paragonando la Rete ad un'autostrada, ed i pacchetti inviati volutamente in grandi quantità come le automobili che intasano quest'autostrada.

Un'intrusione si ha quando, mediante un insieme di tecniche, conoscenze e programmi, si diventa utenti - non autorizzati - di un sistema informatico. Esistono più tipologie di reti dati (Internet è la più conosciuta, rivolta ad un pubblico di massa a livello mondiale) e, spesso, i sistemi informatici governativi, bancari e di multinazionali - intesi come le macchine che hanno il compito vero e proprio di scambiare dati ed aggiornare informazioni essenziali e/o vitali - si trovano su altre reti.

Evito quindi volutamente, per quanto sopra esposto, ogni tipo di spiegazione, preferendo illustrare ed evidenziare alcune riflessioni.

Le teorie

Io, da hacker e primo tra i professionisti nel campo dell'I.T. Security in Italia, penso che non siano stati "hacker" ad effettuare queste manomissioni ed interruzioni di servizio: perché ?

1. La tipologia di attacco

Si è trattato di un attacco "stupido", vale a dire senza l'utilizzo di tecnologia o tecniche particolari. Sono stati presi di mira i siti Internet delle società più conosciute a livello mondiale, ma non necessariamente le più critiche. La chiara intenzione è stata quella - peraltro ben riuscita - di scatenare i mass-media, generare panico (causato a propria volta dall'ignoranza in materia di sicurezza e dall'enorme amplificazione prodotta dagli organi di informazione).

2. L'etica hacker

Ho esordito, ed è tuttora la mia convinzione, dicendo che non si è trattato di un attacco lanciato da hacker nel senso puro della parola. Questo in quanto l'hacker, per definizione stessa del termine, non apporta mai danni ad un sistema informatico. Come scrisse Steven Levy, ***"l'hacker pratica l'esplorazione intellettuale a ruota libera delle più alte e profonde potenzialità dei sistemi di computer, o la decisione di rendere l'accesso alle informazioni quanto più libera e aperta possibile. Ciò implica la sentita convinzione che nei computer si possa ritrovare la bellezza, che la forma estetica di un programma perfetto possa liberare mente e spirito"***

Possiamo dunque capire da questa frase quanto un hacker (il quale poi ha differenti provenienze e background conoscitivi, dalla programmazione hardware a quella software, dalla specializzazione nelle reti dati alla cifratura dei dati....) ami l'informatica. A questo si aggiunge, forse con un'importanza primaria, la volontà di libertà

dell'informazione, il libero diffondersi ed uso delle risorse informatiche e della basi di dati. Tutto questo si traduce, infine, nella libertà di utilizzo e consultazione della Rete (Access for All, http://www.xs4all.nl/, in Olanda, rimane un esempio europeo da seguire..).

La cosiddetta ***filosofia hacker,*** sebbene vi siano hacker in ogni parte del mondo, ognuno con propri differenti credi politici e religiosi, è ben chiara, definita e comune a tutti: rispetta le risorse altrui, non fare mai danni al sistema informatico che violi, non arrecare danni all'utenza finale (privata).

Tempo fa stilai una classificazione degli hacker sotto il profilo psicologico e le relative modalità di azione (http://www.apogeonline.com/informaz/art_173.html): chi desiderasse approfondire l'argomento può reperire all'indirizzo http://www.internos.it/archivio/rc3.pdf) "le dieci regole dell'hacking", pubblicato sul quotidiano La Stampa da Salvatore Romagnolo.

Abbiamo dunque i fattori per distinguere l'hacker etico dall'adolescente con alcune capacità, tanta voglia di fare danni e suscitare clamore: se poi il clamore è a livello mondiale, possiamo ben comprendere quanto gli organi di informazione abbiano - probabilmente - fatto il gioco dei responsabili.

Fatti analoghi: nessun clamore, nessuno panico

Il 18 gennaio di quest'anno **Radio 10**5 subisce un DoS al proprio sito web: un breve e soffocato comunicato stampa, un flash dell'Adn Kronos (il cui sistema informatico interno - e non semplice sito web - fu violato diversi anni fa, primo tra le agenzie d'informazione italiane) di seguito riportato:

Milano, 18 gen.(Adnkronos) -Il sito internet di Radio 105 è vittima degli hackers, i pirati informatici, che hanno giá creato danni quantificati in circa 100 mln. "Da quattro giorni - denuncia l'emittente radiofonica - siamo vittime dei pirati della rete con azioni di disturbo, giá denunciate alla polizia informatica. Tramite l'invio di pacchetti dati gli hackers hanno reso praticamente impossibile l'accesso al sito, che registra quotidianamente oltre 30 mila contatti, e soprattutto bloccato gli inserzionisti pronti ad investire in pubblicitá". (Red/Bdp-Pe/Adnkronos)

Il 3 febbraio **Fineco On-line SIM**, società del gruppo Bipop-Carire che raggruppa le attività di trading on-line, ha "inavvertitamente inviato in un mailing list dati riservati di clienti" del loro servizio di transazioni borsistiche on-line: su un mailing list del servizio di trading online, dunque, sono circolati messaggi contenenti dati personali, comprensivi di riferimenti bancari, di molti clienti abbonati al servizio.

Prima si è parlato di possibile sequestro del server (a che scopo poi ? In questi anni nulla è stato imparato? Esistono i backup, e sono la soluzione migliore..), per passare direttamente a sdrammatizzare l'accaduto, spiegando che "i dati inviati XXXXXXX solo dati generici XXXXXX". Sarà anche vero, ma se per caso quel modulo dati fosse stato di un altro tipo, i dati sensibili sarebbero usciti fuori: magari bastava il mouse un pochino più in su per selezionare un altro file...

Quello che segue è il comunicato apparso su deandreis.it (http://www.deandreis.it/p.asp?i=30562):

03/02/00 - News - Roma - Definire imbarazzante quanto accaduto nelle scorse ore a FINECO è quantomeno riduttivo. Uno dei principali servizi di trading online italiani si trova infatti nell'occhio del ciclone perché dati personali e riferimenti bancari di numerosi utenti sono girati pubblicamente su una mailing list dedicata.

Va detto che la mailing list è aperta ai numerosi utenti del servizio e lo scambio di molte email "compromettenti" è stato originato da un primo messaggio di un cliente, messaggio indirizzato alla mailing list ("per errore", secondo FINECO). Nella pioggia di email generate dal buco nella sicurezza gli utenti, tra l'altro, hanno denunciato con forza l'inefficienza complessiva del servizio.

Di fronte a questi eventi il Centro Servizi Legali, come richiesto da uno degli utenti FINECO, ha immediatamente presentato alla magistratura competente denuncia civile e penale, con richiesta conseguente di danni e di sequestro del server dell'azienda.

Alle proteste dell'utente, che ha poi deciso di intraprendere l'azione giudiziaria, finora da FINECO è pervenuta soltanto una mail firmata dal direttore generale della società. Un messaggio nel quale si sostiene che l'azienda "NON ha direttamente distribuito dati personali, ma, attraverso la propria lista di distribuzione, ha INVOLONTARIAMENTE e PER POCHI MINUTI diffuso messaggi tra gli utenti". Una lettera nella quale si afferma tra l'altro che "l'episodio (...) può essere ricondotto ad una situazione particolare e non invece ad una leggerezza". Una risposta stigmatizzata dai legali secondo cui "si ammette il grave errore commesso tentando una puerile giustificazione tecnicamente non accettabile".

Dinanzi ad una palese violazione della riservatezza dei dati finanziari, della privacy dei dati personali, dinanzi alla divulgazione di numeri di conto corrente e loro ubicazione, la risposta della FINECO ha indubbiamente caratteristiche di inaspettata superficialità.

In un momento nel quale con l'hacking ai server Visa, ammessi dalla stessa azienda, con gli scandali delle transazioni online denunciati ripetutamente da MSNBC, l'e-commerce e il business online sono "sfidati" come mai prima, la reazione della FINECO appare ancora più "disastrosa" perché non sembra prendere in serissima considerazione l'intera problematica della sicurezza che appare, al contrario, ampiamente sottovalutata.

Ben tre mesi prima il sistema del **Nasdaq** fu violato, rendendo possibile agli intrusi variare in tempo reale il valore delle azioni, oggetto delle transazioni borsistiche. Tutto quello che rimane di questo attacco è una frase che recita più o meno: "potremmo cambiare i valori azionari di alcuni titoli e fare speculazione: invece vi lasciamo questo messaggio e torniamo ad impacchettare hambuger al Mac Donald's..."

Constatazioni

L'ondata di panico che è scaturita da questi avvenimenti ha dell'incredibile: tra disinformazione ed amplificazione a livello mondiale del caso, prime pagine dei giornali e speciali Tv, il mondo ha scoperto la parola hacker, nel senso più spregiativo, sporco e corrotto del termine.

Iniziano le ipotesi, dove si immagina che il tutto è una montatura di Bill Gates in vista del lancio ufficiale di Windows 2000, “sistema sicuro” della Microsoft; si ipotizzano potenze straniere, ex paesi del blocco dell’Europa orientale, che attaccano sistemi informatici statunitensi per “rappresaglia politica”.

Intanto il governo USA stanzia 2 miliardi di dollari per la sicurezza informatica nazionale, The Mudge dei L0pht (il più famoso gruppo hacker americano) fa da consigliere a Bill Clinton e fonda la @Stake Inc. (http://www.atstake.com): persone provenienti da realtà e background totalmente differenti l’uno dall’altro (Digital, Compaq, At&t, le migliori università americane, l’underground hacker statunitense....).
Tutte queste persone, probabilmente, supereranno insieme i risultati raggiunti da Chris Darby, attuale C.E.O. (Chief Executive Officer and President) di @Stake: in soli due anni quest’uomo ha portato la Interpath - suo precedente impiego - da 3 a 78 milioni di dollari di fatturato, passando da 4 a 650 dipendenti.

La borsa americana impazzisce, e le ripercussioni si fanno sentire anche in Europa: se il Nasdaq o il New York Stock Exchange fanno le bizze, i “piccoli cugini” europei seguono ad occhi chiusi il trend...

Abbiamo poi l’ondata di ripercussioni mondiali, e leggo sulle news specializzate dei primi hacking “ufficiali” in Cina, leggo di un paese come il Giappone - altamente tecnologico ma con precisi principi di comportamento - dove i ragazzini hanno abbandonato le Playstation e hanno scoperto che “hacking è bello”: prima non vi erano mai stati episodi di intrusioni in questi paesi, anche perché il solo ad averne subite (la Cina nella fattispecie) condannò a morte lo scorso anno, a dicembre, due hacker cinesi colpevoli di avere sottratto 2.000 $ da una banca, violandola via computer. 2.000 dollari valgono ***la vita*** di due persone.... Dovremmo riflettere anche su questo.

Proseguiamo con la Commissione Europea, la quale dichiara “guerra agli hacker”, e vedremo allora la politica e la logica ben nota delle mega-aziende, fornitrici ""ufficiali” dei governi, aumentare il fatturato con prodotti non adatti, insicuri, non pensati da ***chi sa*** come si viola un sistema.

Conclusioni

Si parla tanto di globalizzazione, ma forse gli episodi delle ultime settimane, le ripercussioni economiche e politiche, i “down” delle borse mondiali non sono altro che i primi avvertimenti: sono questi i primi punti deboli identificati di un mercato ***globale e virtuale?***

La situazione mondiale della I.T. Security sta attraversando - per diversi motivi oltre che per l’ovvia esplosione della diffusione di sistemi informatici connessi alla rete Internet - un brutto periodo: in Italia rasenta la nullità. Non esistono, nella maggior parte delle aziende, un budget per la sicurezza informatica, la figura di un Security Manager specifico e competente, contratti con aziende specializzate per l’aggiornamento e la verifica periodica della propria vulnerabilità.

La mia ultima riflessione è forse la più pessimista: e cosa succede se gli hackers, ma quelli veri, si arrabbiano ? Su 2600.com (http://www.2600.com), magazine underground hacker, una specie di “organo ufficiale di stampa” della comunità hacker mondiale, è apparso un messaggio di dissociamento e condanna verso le interruzioni di servizio provocate. La comunità hacker non condivide queste operazioni, ma nel contempo vede associare dai mass-media il termine “hacker” a gruppi di imbecillotti che rovinano sistemi informatici e siti web.
L’hacking non è cambiare una pagina web: hacking è abbattere ogni barriera, cercare la perfezione, riuscire a “guardare oltre” e cercare, ove possibile, di mettere le proprie capacità al servizio della comunità. Internet, Linux, il progetto Open Source, le licenze GNU....tutto è stato ideato, concepito e sviluppato da una serie di persone, accomunate dall’ideologia del Freedom of Information, la libertà dell’informazione: gli hackers.

Cosa succederà allora, se i veri hacker si arrabbieranno ? Ai posteri l’ardua sentenza, ma non credo che dovremo attendere a lungo per vedere cos’è il ***vero hacking ad alto livello***.....

Ringraziamenti

Manù, per il suo sopportarmi così amabilmente nei periodi di “isolamento” che spesso mi caratterizzano;
i miei due editori, per lo spazio sempre più ampio che mi concedono;
Daniele Poma, responsabile commerciale di Mediaservice.net, per il lavoro di cui si prende carico in mia vece, quando io sono in fase di “scrittura avanzata”;
Luca M. De Grazia, per il costante supporto informativo e legale;
l’evoluzione tecnologica che stiamo vivendo la quale, con i suoi pro e contro, ci permette ancora di fare qualche riflessione e di immaginarci il futuro....

Raoul Chiesa