Virus

Non solo virus

Nel numero scorso abbiamo fatto un riassunto di dieci anni di virus del computer. Ne risulta un quadro piuttosto sconfortante: ci sono al mondo centinaia di milioni di persone che affidano quotidianamente il proprio lavoro a un PC senza curarsi dei rischi che corrono: vuoi per fatalismo ("tanto con queste macchine c'è poco da fare..."), vuoi per spavalderia ("tanto a me non succederà mai"), vuoi per incoscienza o ignoranza del problema.
Il mercato degli antivirus gode di ottima salute. Infatti l'approccio seguito dalla maggior parte degli utenti è di correre a comprare l'antivirus non appena si ritrovano infettati, con il risultato di sprecare il doppio o il triplo del tempo che sarebbe stato necessario a installare l'antivirus prima, e talvolta succede che una parte del lavoro archiviato nel PC vada perduto.

di Stefano Toria

Si potrebbe pensare che, nonostante tutto, gli utenti abbiano imparato la lezione e si siano resi conto che i PC sono sistemi intrinsecamente insicuri ma che è possibile fare qualcosa per garantirsi una maggiore sicurezza nel proprio lavoro, e che non serve spendere grosse cifre perché le soluzioni sono tutte più o meno di basso costo.

Invece non è così. Infatti sono ben pochi gli utenti che fanno regolarmente i backup, e inoltre sta apparendo una nuova minaccia all'orizzonte, un problema di sicurezza che promette di diventare per il nuovo decennio quello che sono stati i virus negli anni '90. Vediamo se stavolta si riesce ad affrontare la situazione nel modo corretto.

"... Alle tre e mezzo del mattino, tremando di freddo davanti al Macintosh che uso a casa, mi collego con il computer del mio osservatorio. E' una workstation Sun, con la versione Berkeley di Unix. Ci sono ancora quelle centinaia di job in esecuzione... accidenti, il mio sistema è saturo. Ma non c'è nessun hacker collegato; ci sono solo io.

Chiamo Darren Griffiths all'LBL. "E' un virus" mi dice. "Lo vedo che si replica... prova a sopprimere i job: li vedrai ricomparire".

Il "Back Orifice" in azione: da questa interfaccia si può prendere il controllo di un PC remoto su cui sia installato l'apposito server

"Da dove?".

"Le connessioni mi arrivano da cinque posti: Stanford, l'università di Rochester, Aerospace Company, il campus di Berkeley e un posto che si chiama BRL".

"E' il laboratorio di ricerca balistica dell'Esercito" rispondo, ricordando una conversazione di qualche tempo prima. "Ma come fa il virus a entrare nel sistema?".

"Non te lo so dire, Cliff. Le connessioni arrivano tutte dall'Arpanet, ma non nel solito modo. Sembra che il virus stia sfruttando un buco nel sistema di posta elettronica".

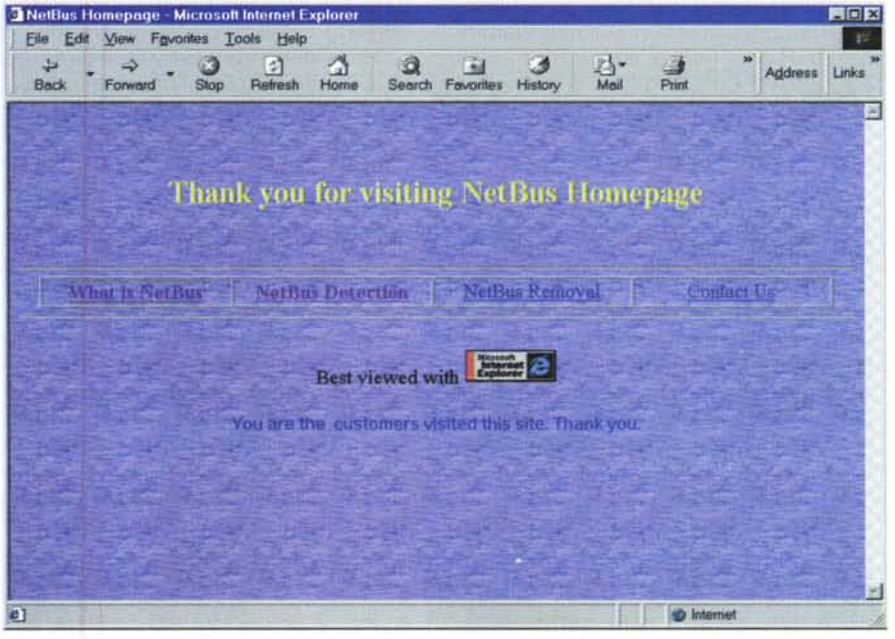
Qualcuno ha costruito un virus che sfrutta una falla nella sicurezza dei sistemi Unix. La falla è nel sistema che gestisce la posta elettronica, e il virus si sta diffondendo sulla rete. Ma cosa sta facendo esattamente? Si limita a riprodursi oppure c'è dentro una bomba a tempo?

Sono le quattro del mattino. E ora che si fa? Forse dovrei chiamare il controllo dell'Arpanet e avvisarli. So che nel Network Operations Centre c'è un tecnico in servizio ventiquattr'ore al giorno, per tenere sotto controllo la rete. Chiamo, ma nessuno sa ancora nulla. "Meglio spargere la voce, perché prima delle nove sarà arrivato dappertutto".

Il NOS non ne sa nulla, il virus è in giro soltanto da poche ore, e intanto mi arrivano replicazioni del virus da dozzine di altri siti. E' estremamente virulento: entro la mattinata potrebbe aver raggiunto centinaia di altri sistemi. Abbiamo un problema, un problema enorme.

Un'epidemia...".

Così raccontava brevemente nel 1990 Clifford Stoll, nel suo libro "L'uovo del cuculo" (ed. in Italia da Sperling-Kupfer), lo scatenarsi del problema che resterà poi noto come "il verme di Internet". I fatti sono noti: uno studente universitario, Robert T. Morris Jr., scrive un programma che sfrutta alcune falle delle versioni più diffuse di Unix per trasferirsi da un sistema all'altro. Il programma sfugge al controllo dell'autore, che ha largamente sottostimato la possibilità di circolazione rapida di un oggetto simile su quella che allora si chiamava ancora "Arpanet", cioè l'odierna Internet. Il risultato è che si infettano migliaia di sistemi, vanno perdute milioni di ore-uomo, Morris viene identificato, incriminato e condannato.



Netbus è un altro sistema client-server per attacchi e azioni di disturbo: questo è il sito del produttore

Reti informatiche, condivisione e sicurezza

L'ironia della sorte vuole che Robert Morris Sr., padre dello studente autore del virus (ma sarebbe più corretto definire "verme" un programma del genere), sia tuttora riconosciuto come uno dei massimi esperti di sicurezza informatica; tra l'altro, fece parte del gruppo di persone che svilupparono l'algoritmo che rende sicure le password del sistema operativo Unix.

Il fatto che una rete informatica potesse costituire un ambiente insicuro iniziò a diventare rilevante solo dopo un certo tempo. I primi esperimenti di collegamenti tra computer risalgono agli anni '50, l'interfaccia RS-232 è dei primi anni '60, e per assistere alla nascita del nucleo di quella che diventerà Internet bisogna aspettare la fine degli anni '60. In questo periodo le reti erano qualcosa di sperimentale, che si studiava negli istituti di ricerca chiedendosi se mai avrebbero potuto trovare applicazioni pratiche.

Dieci anni dopo le principali università americane, poi europee e poi mondiali, erano collegate tra di loro, e scambiavano quotidianamente migliaia di messaggi, file e connessioni. La parola d'ordine era "sharing", "condivisione". Forse erano pochi a rendersene conto, ma alla base di tutto c'era anche un'altra parola d'ordine, importante quanto la prima e forse di più: "trust", "fiducia". Migliaia di amministratori di sistema dormivano sonni relativamente tranquilli pur sapendo che i propri computer tramite un cavo potevano essere raggiunti da milioni di persone. Ritenevano di potersi fidare.

Nel frattempo anche le banche e altre aziende commerciali si erano interessate alle tecnologie di interconnessione tra computer; tuttavia, rese enormemente più sospettose dal banale fatto che anziché maneggiare dati scientifici maneggiavano denaro, avevano adottato un approccio assai più pragmatico, e già dai primi anni '70 si videro comparire le prime applicazioni di crittografia nella trasmissione dei dati. Il dibattito sulla crittografia va avanti tuttora, e non se ne vede la fine; è interessante notare come sin dall'inizio dello sviluppo delle reti informatiche convivessero due atteggiamenti completamente opposti: la fiduciosa condivisione degli accademici, e la gelosa riservatezza delle applicazioni commerciali, entrambe dettate da ragioni ben precise.

Non è necessario ripercorrere la storia della crescita galoppante di Internet perché l'abbiamo vissuta tutti, si può dire quasi l'altroieri. Gli anni '90 hanno assistito a una serie di innovazioni che hanno portato il PC nelle case e sulle scrivanie di tutti, e molti di questi PC sono collegati a un modem che apre ai loro utenti la scena mondiale di Internet.

Il nostro PC quindi entra a far parte di una rete che avvolge tutto il mondo, ma una rete speciale: infatti la struttura di questa rete risente fortemente del fatto di essere nata per lavorare in condizioni di "sharing" e "trust", di "condivisione" e "fiducia". E questo può creare molti problemi, che affronteremo e vedremo come possono essere risolti.

Il TCP/IP in due parole

Il TCP/IP, il protocollo di rete su cui Internet è fondata, nasce per collegare tra di loro sistemi paritetici. Non importa se un sistema è un megacomputer con decine di processori paralleli, centinaia di milioni di gigabyte in linea e velocità astronomiche, e un altro è un 486/33 con Windows 3.11 e una vecchia versione di Eudora Light: dal punto di vista del TCP/IP sono identici, si tratta di due "nodi" che hanno ciascuno un identificativo IP, costituito da una quartina di numeri

separati da punti.

Ciascun nodo della rete è in grado di comunicare con qualsiasi altro nodo, purché conosca il suo numero identificativo IP e un paio di altre informazioni aggiuntive (protocollo e porta). Per comodità poi gli indirizzi IP sono stati sostituiti dai nomi simbolici estesi del Domain Name System, il DNS.

Qualsiasi sistema collegato a Internet è in grado di eseguire dei software che possono sostanzialmente svolgere due funzioni: richiedere servizi offerti da altri sistemi, oppure offrire servizi in proprio. I "servizi" sono quelli che abbiamo da tempo imparato a conoscere: posta elettronica, prelievo e deposito di file, lettura di pagine Web, conversazioni in diretta, etc., nonché alcuni un po' più complessi, destinati alla gestione delle funzioni interne della rete.

Questa struttura (il termine esatto è "*client/server*") è molto efficiente, perché con poca spesa e poco sforzo si può mettere qualsiasi sistema in condizione di lavorare in rete con qualsiasi altro, ovunque si trovi.

Da quando Internet è diventata un fenomeno di massa i produttori di informatica hanno incluso nei propri prodotti le funzioni essenziali per comunicare con la rete. PC, stazioni grafiche, e altri dispositivi sono quindi tutti equipaggiati con tutta una serie di *client* (e in alcuni casi anche qualche *server*), per agevolare il collegamento con Internet. E l'aggiunta di altre funzioni è rapida e semplice: basta acquistare, o prelevare dalla stessa Internet, il *client* o il *server* opportuno, installarlo in pochi minuti, e le funzioni del PC in rete si estendono.

Condivisione e fattori di rischio

Lo scenario così raffigurato è tutt'altro che privo di problemi. Se si tiene in mente quello che accadde nel 1988 con il "verme di Internet", non occorre un ragionamento particolarmente brillante o ardito per rendersi conto che la stessa cosa potrebbe succedere di nuovo, anzi in realtà succede continuamente. Solo che adesso non fa più notizia, le intrusioni via Internet da un computer all'altro sono cosa di tutti i giorni ma nessuno ne parla.Però nel frattempo qualcuno si muove, quanto meno per scuotere la consapevolezza di chi dovrebbe occuparsi di prevenire i rischi. Un paio di anni fa venne sviluppato un programma a cui fu dato il nome grottesco di "Back Orifice", il ..."buco di dietro". Serviva a dimostrare la possibilità, anzi l'assoluta attualità di un rischio che fino ad allora era stato considerato teorico.Sostanzialmente il Back Orifice (che d'ora innanzi chiameremo per comodità "BO") è un banale server, portato in giro da un tipo di programma che gli esperti di virus conoscono da tempo: un "dropper", un cavallo di Troia che installa nel sistema una funzione, di nascosto, per fini particolari. In questo caso il fine è di ottenere che dopo l'esecuzione del dropper il PC vittima si ritrovi a essere server, sostanzialmente per delle funzioni di controllo remoto. Utilizzando un apposito client chiunque è in grado, una volta che il PC vittima si colleghi a Internet, di svolgere le operazioni per cui il server è sviluppato.

E queste operazioni, nel caso del BO, sono piuttosto preoccupanti, in quanto il server del BO fornisce all'ignoto utente del client tutta una serie di informazioni e di possibilità di manovra sul PC vittima. Il proprietario del PC vittima si ritrova governato, maneggiato e controllato da un terzo, perfettamente estraneo, che potrebbe trovarsi in qualsiasi punto del mondo dove sia disponibile una connessione Internet; fintanto che il PC è collegato alla rete, il "burattinaio invisibile" può farne ciò che vuole.

Questo scenario, all'apparenza pauroso, è in realtà meno preoccupante di quanto si potrebbe pensare. Il BO esiste, e come lui esistono molte altre tecnologie di intrusione e attacco su Internet. Ma esistono anche una serie di strumenti di difesa, molto efficaci e di basso costo, di cui l'utente medio può servirsi senza dover essere uno specialista, proprio come nel caso dei virus. Però è importante che l'utente medio acquisisca quanto meno la consapevolezza del problema, altrimenti nessuno strumento di difesa può avere effetto se non si ha la percezione di essere minacciati.

E' inutile nasconderlo: se opportunamente attrezzato, infatti, un intruso potrebbe entrare in qualsiasi computer, e una volta entrato potrebbe fare ciò che vuole: leggere, cercare, modificare o distruggere le informazioni archiviate nel PC vittima dell'attacco. E nessun PC, collegato a Internet, è immune dal rischio.

Una prima linea di difesa è costituita, guarda caso, proprio dai buoni vecchi programmi antivirus. Se è vero che un "server-fantasma" come il BO ha bisogno di un dropper per essere installato, allora qualsiasi antivirus può essere istruito a riconoscere il dropper come oggetto minaccioso, allo stesso modo in cui è istruito a riconoscere gli altri cavalli di Troia.

E infatti così accade: se si utilizza un antivirus in grado di elencare i nomi dei virus che riconosce, utilizzando questa funzione si ottiene un lunghissima lista (siamo ormai vicini ai ventottomila virus) che tra l'altro contiene anche nomi quali Back Orifice, NetBus e altri: si tratta di programmi di installazione di server occulti. L'antivirus identifica il cavallo di Troia, non lo disinfetta (ovviamente, perché non è un programma infetto) ma attira l'attenzione dell'utente sul fatto che il programma non va utilizzato. E così, se l'antivirus viene usato nel modo corretto, una prima linea di difesa è in grado di schermare la maggior parte degli attacchi; ad esempio, l'utente riceve un programma in allegato a un messaggio di posta elettronica, prima di eseguirlo lo passa al controllo dell'antivirus, quest'ultimo segnala la presenza ad es. di BO, e l'utente getta via il programma eseguibile e si salva.

Il firewall: un nuovo strumento di difesa

Ma potrebbe accadere che l'utente non controlli tutto ciò che riceve; inoltre c'è sempre la possibilità che l'antivirus non riconosca un particolare programma, bisogna infatti rammentare che un antivirus può riconoscere soltanto ciò che conosce, e se incontra un nuovo dropper, non ancora analizzato dal laboratorio antivirus, potrebbe anche non rendersene conto.

Inoltre esiste sempre la possibilità che un ignoto aggressore sfrutti una debolezza, una falla del sistema operativo. I sistemi che utilizziamo sui nostri PC sono il frutto di centinaia di migliaia di ore di lavoro di squadre di esperti; ma sono tutt'altro che privi di errori, tant'è che gli stessi produttori lo dichiarano (andarsi a leggere ogni tanto le condizioni di uso dei programmi che si installano sul proprio PC non è affatto una cattiva idea). E così come fece Robert T. Morris Jr. nel 1988, qualcun

altro potrebbe fare oggi: approfittare cioè di una falla per guadagnarsi l'accesso al nostro PC mentre siamo collegati a Internet.

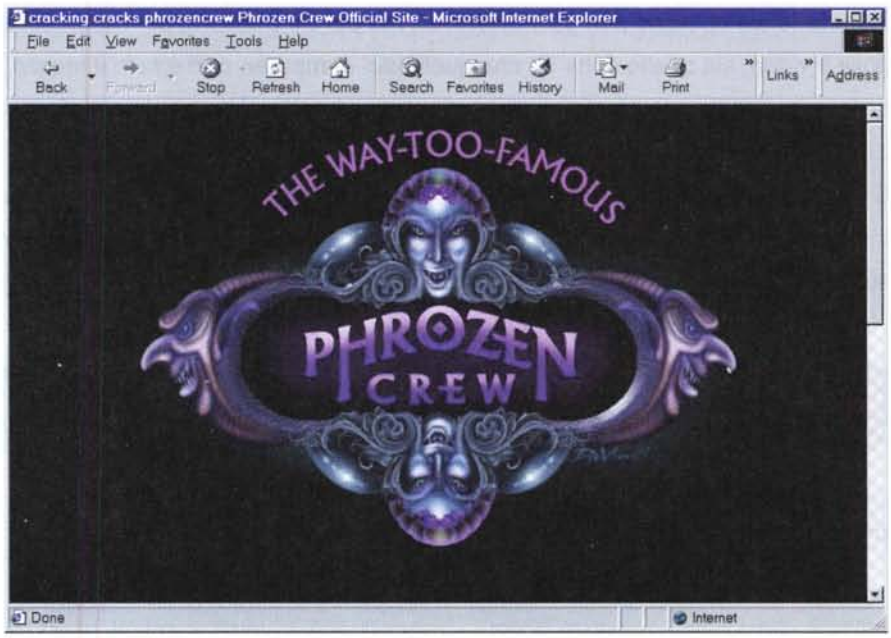
Nel 1994 William Cheswick e Steven Bellovin pubblicarono un libro che si intitolava "Firewalls and Internet Security". Al di là del contenuto del volume (un ottimo testo di riferimento, anche se leggermente datato rispetto ad alcuni aspetti tecnici), agli autori va riconosciuto il merito di aver coniato un termine che è diventato di uso comune tra chi si occupa di Internet. L'idea del "muro rompifiamma", che consente a chi sta dentro di dormire sonni tranquilli mentre fuori infuria la battaglia, è stata lanciata dagli autori di questo manuale, ma in realtà è frutto di un lavoro collettivo di sviluppo che da diversi anni proseguiva in tutto il mondo.

Il concetto del firewall è semplicissimo, e si può descrivere facendo il confronto con la sede di una grande azienda, al cui ingresso si trovi un sorvegliante. A costui, presumibilmente armato, spetta il compito di decidere chi può entrare e chi, invece, deve rimanere fuori.

Tradotto in termini tecnici, un firewall è un sistema (software, eventualmente installato su hardware dedicato) che protegge un determinato contesto da possibili tentativi di aggressione provenienti dal vasto e selvaggio mondo di Internet. Il contesto può essere costituito da un singolo PC o da una intera rete aziendale; il firewall osserva i pacchetti in transito (il "pacchetto" è l'unità minima di informazione che viaggia su una rete), ne studia brevemente alcune caratteristiche e decide se il pacchetto va lasciato passare oppure se va bloccato. In quest'ultimo caso è prevista la possibilità di alzare una serie di allarmi a seconda dei casi.

A poco tempo dall'uscita del libro, si cominciavano a trovare in commercio i primi firewall, segno del fatto che l'idea era già in circolazione da tempo. Oggi i firewall si trovano dappertutto, eppure nonostante ciò le aggressioni in rete si moltiplicano; "Teardrop", "Land", "Smurf" sono i nomi di alcune delle tecniche di attacco più diffuse su Internet, e l'aspetto preoccupante consiste nel fatto che non serve essere esperti di TCP/IP per lanciare un attacco: basta trovare un sito da cui prelevare l'apposito programma, il "kit del pirata informatico", e il gioco è fatto.

Quasi tutti i firewall poi svolgono egregiamente la propria funzione quando vengono installati all'ingresso di una rete; ma non possono fare nulla per evitare gli attacchi che si verificano all'interno della rete stessa, e comunque si tratta pur sempre di sistemi di un certo costo, abbordabile da molte aziende ma fuori della portata dell'utente individuale.



Di siti underground come questo ne esistono a centinaia. Contengono informazioni per l'uso illegittimo di programmi registrati, l'accesso a sistemi protetti, le azioni di disturbo su Internet e attività simili.

Prevenire è meglio...

Dieci anni fa qualcuno timidamente avanzò l'ipotesi che i virus sarebbero diventati un problema di grossa rilevanza. Nessuno vi fece caso, i previdenti furono considerati delle Cassandre, e il risultato è sotto gli occhi di tutti.

Oggi la nuova minaccia si chiama "intrusione via Internet". I virus non hanno segnato la "fine dell'era del computer", come qualche sciocco si affrettò ad annunciare. Nemmeno le intrusioni segneranno la "fine di Internet"; tuttavia è importante che ciascun rischio venga preso nella giusta considerazione man mano che si manifesta e si rende evidente.

Si può ipotizzare che gli hacker affineranno le loro armi, i produttori di strumenti di difesa perfezioneranno le difese, fino al punto in cui diventerà necessario installare un firewall su ciascun PC.

E in effetti già oggi potrebbe essere opportuno farlo. I firewall aziendali sono strumenti grossi e costosi, come abbiamo visto; sono flessibili, configurabili e potenti, ma hanno anche alcune limitazioni. Recentemente sono stati affiancati da sistemi più snelli e ridotti, dal costo accessibile anche all'utenza individuale.

E' per far fronte alle esigenze del singolo, infatti, che è nata una seconda generazione di sistemi firewall. Pur rimanendo basati sullo stesso concetto, cioè di definire un "interno" da mantenere protetto rispetto all'"esterno", si tratta di programmi assai più compatti e maneggevoli, facili da installare, configurare e utilizzare. Dal punto di vista della protezione non hanno nulla da invidiare ai programmi di maggiori dimensioni, e offrono all'utente la possibilità di scegliere la linea di difesa preferenziale, ovvero se filtrare i dati in transito oppure stabilire i diritti di accesso alle funzioni di rete a livello di singola applicazione (es. Internet Explorer sì, il server di Back Orifice no).

Nel prossimo articolo l'anatomia di un attacco in rete e il funzionamento degli strumenti di difesa.

MC