Tutti diversi... e pericolosi!

Non basta avere il software di protezione più potente e aggiornato per difendersi dalle insidie della Rete. Come in tutte le battaglie, la miglior arma è conoscere bene il proprio nemico.

di Elena Avesani

Due mesi fa il primo virus per personal computer ha compiuto 20 anni: si chiamava Brain, e si diffondeva da un computer all'altro tramite i piccoli floppy disk, i dischetti che ormai quasi nessuno usa più. Agli inizi di febbraio, quest'anno, la minaccia all'ordine del giorno si chiamava Kama Sutra, un worm diffuso via posta elettronica, in grado di disattivare l'antivirus, cancellare i file di Microsoft Office presenti nel disco fisso, nonché di autoinviarsi a tutti i contatti presenti in rubrica. Nei vent'anni trascorsi tra Brain e Kama Sutra, ne abbiamo viste un po' di tutti i colori: Sasser, Anna Kournikova, Nimda, Melissa, Sobig, Mydoom, Blaster, Bugbear, I love you, Back Orifice, Michelangelo, Sober sono solo alcuni dei nomi più celebri da cui abbiamo dovuto imparare a difenderci.
Ma il mondo del malware è complicato: esistono i virus, i worm, i trojan, i dialer, gli spyware, le backdoor, gli hijacker... sono tutti software dannosi che differiscono l'uno dall'altro per metodo di contagio, sistema di propagazione, tipologia di infezione e danno causato.
La panoramica che segue mira a essere una guida per capire meglio il mondo del "**malware**": conoscere il proprio nemico è il modo migliore per difendersi, e purtroppo avere installato un antivirus e un firewall è una condizione necessaria, ma non più sufficiente, per considerarsi protetti al 100%. La barriera tecnologica è solo uno degli ostacoli che dovete frapporre tra voi e il malware. Un comportamento attento e una maggiore consapevolezza di come si propagano le infezioni digitali vi permetterà di non cadere in trappole costruite apposta per cogliervi in fallo di sorpresa.

È un'infezione contagiosa?

Il malware viene comunemente suddiviso in due categorie in base alla propagazione dell'infezione: virale e non virale. È virale quando è in grado di replicarsi e diffondersi in autonomia contaminando altri PC: fanno parte di questa categoria i virus e i worm. Il malware è considerato non virale quando non ha la capacità di contagiare autonomamente altre macchine, limitandosi a danneggiare solo il PC in cui è installato. Facciamo un esempio, il più semplice possibile: un worm come Kama Sutra è classificato come malware virale perché è programmato per replicarsi e diffondersi da solo. Invece una finta e-mail della vostra banca che mira a rubare i dati di accesso al conto corrente (tipico esempio di phishing, ne parliamo a pagina 58) è un malware non virale tanto quanto Back Orifice, una backdoor (letteralmente una "porta posteriore") che, una volta installata sul PC, è in grado di "aprire" le porte del computer a qualsiasi **hacker**, garantendogli un accesso pressoché totale ai dati e alle funzionalità del PC.

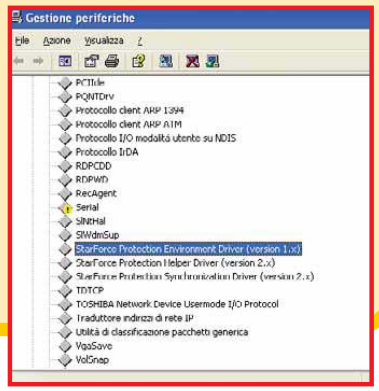
I virus

Anche se nel linguaggio comune è consueto utilizzare la parola "virus" per indicare qualsiasi malware, in realtà il virus è solo uno dei tanti tipi di codice dannosi. Si tratta di un programma che si inserisce all'interno del codice di un altro programma o di un documento. Quando l'utente avvia il file infetto, il virus entra in azione contaminando altri file e provocando i danni per i quali è stato programmato. Per esempio il celebre Michelangelo, virus in grado di infettare i **settori di avvio** di dischetti e dischi fissi, aveva come fastidioso effetto collaterale di restare silente fino alla data di "innesco": il 6 marzo 1992. In quella data formattò molti dischi fissi, sovrascrivendo i dati con sequenze numeriche casuali (rendendo così più difficoltoso il recupero dei dati cancellati).
Nel tempo i virus si sono evoluti fino alla forma di **macro** virus, quelli in grado di infettare soprattutto i documenti di Office, inserendo al loro interno dei comandi di macro in grado di compromettere seriamente il computer: tra questi ricordiamo Melissa che, infettava il file **normal.dot** di Word e inoltrava a destinatari raccolti dalla Rubrica un documento Word infetto tra quelli aperti dopo il contagio.

E il rootkit?

In una panoramica dedicata al **malware** non ci si può scordare di nominare il rootkit, software salito agli onori della cronaca nell'autunno dell'anno scorso, quando Mark Russinovich, esperto programmatore, lanciò una bomba destinata a scuotere il mondo dell'informatica e della musica: i CD musicali di Sony BMG Music Entertainment incorporavano un software nascosto e sospetto, in grado di trasferire informazioni dal computer che riproduceva il CD ai server Sony. Per questa via il rootkit era in grado di impedire attivamente la copia del CD e inviava a Sony BMG informazioni sull'utente. Dopo questo fatto clamoroso, si intendono come "rootkit" tutti quei programmi installati sul PC all'insaputa dell'utente e che impediscono attivamente la copia di file musicali.

È stata diffusa da poco la notizia di un rootkit incorporato in una serie di videogiochi per PC, tra cui Still Life, gioco che abbiamo recensito su Computer Idea. Dopo una veloce verifica abbiamo rilevato la presenza di StarForce Protection nel nostro computer, un software installato a nostra insaputa e capace di limitare le capacità di masterizzazione nei sistemi operativi Windows 2000 e Xp



Glossario

Banner Finestra pubblicitaria che appare durante la navigazione nei siti Web.

Connessione dial-up È chiamata così la connessione via modem 56 Kbps.

Cookie tracciante Poezione di codice con le istruzioni necessarie per inviare informazioni sulle abitudini dell'utente, a più siti Web.

Hacker Persona che per hobby e divertimento entra nei computer altrui. Diverso dai "cracker" che entrano nei computer per fare dei danni gravi. A volte le due diciture sono confuse, anche perché la parola hacker è più diffusa e conosciuta.

Macro Serie di comandi per automatizzare l'esecuzione di operazioni nei programmi di Office.

Malware Contrazione di "malicious software" ossia "programma maligno". Il termine indica la vasta categoria dei software dannosi, e in senso lato i "pericoli" della Rete.

Normal.dot File di Word contenente le impostazioni principali del foglio. Quando apriamo un nuovo documento, apriamo il file Normal.dot

Patch Integrazione di un software o del sistema operativo per migliorarne le funzionalità.

Registro di sistema File di Windows contenente tutte le informazioni relative alle impostazioni dei programmi.

Server remoto Computer in grado di comunicare, inviare comandi e ricevere risposte da un altro computer.

Settori di avvio Settori di un disco che contengono le informazioni per l'esecuzione dei programmi necessari all'avvio del PC.

I worm arrivano via posta... ma non solo

Il worm, a differenza del virus, è un programma che non necessita di essere ospitato da nessun altro software o documento: vive da solo ed è in grado di replicarsi e quindi di diffondersi in totale autonomia soprattutto tramite le reti di computer. Ovviamente Internet è l'ambiente elettivo per i worm, e la posta elettronica è il veicolo in grado di recapitare in poche ore a milioni di utenti "infezioni" come NetSky, capace di moltiplicarsi e inoltrarsi a uno svariato numero di utenti camuffando il nome del mittente.
Ma i worm non arrivano solo per posta: per essere infettati da Sasser, per esempio, bastava essere collegati a Internet, in quanto il worm, per entrare nel computer, sfruttava una vulnerabilità di Windows, un suo punto debole.
Lo ricordate lo spiacevole "effetto collaterale" di Sasser? Il PC si riavviava di punto in bianco! La soluzione, una **patch** sviluppata in tutta fretta da Microsoft, ha risolto la vulnerabilità, ma ormai milioni di PC erano già infetti.
MyDoom, invece, arrivava per posta e, una volta attivo, si posizionava nella cartella dei file condivisi di Kazaa (un software di peer to peer molto diffuso), contaminando documenti destinati allo scambio.
I danni provocati dai worm possono essere dei più svariati: cancellazione di file, danni al sistema operativo o invio di documenti via posta elettronica; tuttavia le ripercussioni più gravi si hanno sulla connessione. Badate bene, non ci riferiamo alla connessione casalinga, ma all'intera Rete mondiale: milioni di e-mail contenenti allegati che vengono inoltrate contemporaneamente dalle caselle di tutto il mondo, generano un traffico di dati non indifferente che causa rallentamenti a qualsiasi servizio. Inoltre i worm possono essere veicolo di altre tipologie di attacchi: il già citato MyDoom, in alcune delle sue numerose emanazioni, installava una backdoor nel PC e lanciava un attacco contro alcuni siti Web, cercando di bloccarne il funzionamento (il cosiddetto "Denial of Service").

▲ *I keylogger possono essere anche impiegati come programmi di controllo parentale, per controllare le abitudini di navigazione di un figlio minorenne. In questo caso però, le trascrizioni vengono mantenute all'interno del computer e vengono utilizzate dai genitori. I keylogger catalogati come malware sono installati all'insaputa dell'utente e vengono inviati a chissà quale server remoto nel mondo*

Il cavallo di Troia

Ricordate il mito del cavallo di Troia narrato nell'Odissea? Per riuscire a penetrare nella città di Troia i greci costruirono un immenso cavallo di legno cavo, vi si nascosero

Tipo di malware	Cosa fa	Come ci si infetta?	I più celebri
Adware	Invia informazioni commerciali a terze parti	Installando software che incorpora moduli adware	Cool Web Search
Backdoor	Permette l'accesso al PC agli hacker	Installando programmi non sicuri	Back Orifice
Cookie traccianti	Traccia le abitudini di navigazione dell'utente	Navigando in Rete	Cookie Web-stat
Dialer	Riprogramma la connessione a Internet indirizzandola verso un numero telefonico a pagamento	Navigando su siti pornografici e poco affidabili con suonerie, file MP3 e software gratuiti	PornDial-101
Hijacker	Cambia la pagina principale di Internet Explorer	Navigando su siti pornografici e poco affidabili con suonerie, file MP3 e software gratuiti	Cool Web Search
Keylogger	Registra tutto quello che viene digitato sulla tastiera e lo invia a terze parti	Installando software che incorpora moduli spyware	KeyLogger.c.cfg
Trojan	Installa nel computer un programma dannoso	Installando programmi non sicuri	Spymaster.A
Virus	Contamina un file e una volta attivato, ne danneggia altri	Eseguendo file infetti	Michelangelo, Melissa
Worm	Contamina i file nel computer, si auto-invia per posta elettronica, può aprire backdoor	Aprendo allegati della posta elettronica, non aggiornando il sistema operativo e l'antivirus	Sasser, MyDoom, Kama Sutra
Malware di "ingegneria sociale"			
Hoax	Attraverso il racconto di eventi di pura fantasia vengono ingannate e truffate le persone	Dando credito a e-mail fasulle	Truffa nigeriana
Phishing	Attraverso e-mail o pagine Web fasulle studiate ad arte vengono carpiti i dati personali ai malcapitati	Dando credito a e-mail fasulle	E-mail Banca Sella, Unicredit, eBay

dentro, e lo portarono in dono ai troiani. Una volta introdotto il cavallo nelle mura, i greci attesero la notte per uscire dal nascondiglio, aprire le porte della città, far entrare l'esercito e attaccare di sorpresa gli ignari troiani. I trojan funzionano alla stessa maniera: sono programmi che a prima vista possono sembrare totalmente innocui ma, sotto sotto, nascondono del codice dannoso sconosciuto all'utente. Possono essere incorporati in normali file di programma (per esempio un videogioco pirata) oppure essere "travestiti" da software di una qualche utilità, magari gratuito. Classificati come malware non virale, i trojan non sono in grado moltiplicarsi e propagarsi da soli: questo significa che, una volta entrati nel computer ospite, si limitano a svolgere il lavoro per cui sono programmati. Qui iniziano i veri problemi, perché spesso sono veicoli di altro malware. I trojan più famosi sono i RAT (Remote Access Tool, strumento per l'accesso remoto), conosciuti anche con il nome di backdoor, programmi capaci di aggirare le protezioni di un computer (o di una rete informatica) e di aprire delle porte attraverso le quali un hacker potrà entrare nel sistema. Tuttavia un trojan può contenere anche worm, virus, spyware... il che complica un po' le cose: in realtà basta solo avere chiaro il concetto che il trojan è un programma veicolo di altre infezioni dopo essere penetrato nel PC. Il modo migliore per trovare un trojan nel proprio computer è scaricare software pirata.

Il fastidioso hijacker

Hijacker significa "dirottatore". Nel mondo informatico gli hijacker sono quei programmi in grado di sfruttare una vulnerabilità di Internet Explorer per modificare la pagina principale del browser, inserire nuovi collegamenti sul desktop e cambiare la lista dei Preferiti... insomma, cercano di dirottare i nostri interessi verso altri lidi, probabilmente a pagamento. Per esempio l'hijacker più famoso, e pernicioso (CoolWebSearch, noto anche come CWS) è in grado di filtrare qualsiasi ricerca effettuata in Internet, proponendo i risultati a esso più congeniali, inserendo link a siti erotici, di giochi d'azzardo o altre simili amenità. Sbarazzarsi di un hijacker non è semplice e non basta cambiare le impostazioni del browser, né cancellare i nuovi collegamenti. Questo tipo di programmi, infatti, interviene in modo profondo nel **Registro di sistema**, rigenerando le modifiche a ogni riavvio nonostante la cancellazione. Gli hijacker, tanto quanto lo spam, possono essere utilizzati in modo scorretto come strumento di marketing per veicolare attività a volte al limite del lecito: la loro classificazione come malware non è però così scontata come potrebbe sembrare a prima vista. Il fatto è che molti software vengono distribuiti in versione gratuita a patto che l'utente installi una "barra di navigazione" che, a tutti gli effetti, dirotta la navigazione verso siti che pagano per avere una particolare visibilità. Per questo motivo la maggior parte dei software che provvedono a scovare trojan, spyware, adware e hijacker non disabilitano automaticamente qualsiasi presunta minaccia, ma si limitano a segnalare all'utente la sua presenza.
A noi personalmente non è mai capitato di installare volontariamente un hijacker, quindi questa precisazione presente un po' in tutte le "enciclopedie del malware" disponibili in Rete, sa più di puntualizzazione per evitare le possibili cause legali intentate da parte di aziende di marketing che preferiscono non vedere classificati i loro prodotti commerciali alla stregua dei virus.

Le regole per tenere il malware alla larga

- Installate un antivirus e mantenetelo sempre aggiornato (quotidianamente, se possibile)
- Installate un firewall e fate verifiche approfondite per qualsiasi scambio di dati che non sia ricollegabile a un'applicazione conosciuta
- Evitate siti con materiale pornografico, contenuti pirata, suonerie o MP3 gratuiti
- Non aprite MAI gli allegati delle catene di Sant'Antonio, né quelli provenienti da mittenti che non conoscete
- Se un amico vi invia un allegato, ma il testo del messaggio è inconsueto, diverso da quello che vi aspettereste, non aprite l'allegato
- Anche se rallenta il download della posta, mantenete attivo lo scudo antivirus anche per la posta elettronica: è il modo migliore per non cadere farvi infettare da un worm
- Non utilizzate mai i link contenuti all'interno dei messaggi di posta elettronica prima di verificare l'autenticità del mittente
- Installate tutti gli aggiornamenti critici proposti dal sistema di aggiornamento automatico del vostro sistema operativo
- Imparate a conoscere il vostro computer: se di punto in bianco notate qualche malfunzionamento, cercate di ricordare se avete tenuto un comportamento a rischio nei giorni precedenti e fate una scansione con l'antivirus aggiornato
- Non fate mai clic all'interno dei banner pubblicitari, soprattutto quando ne appaiono più di due contemporaneamente. Per chiuderli non servitevi del mouse, ma a tastiera premete contemporaneamente i tasti ALT e F4
- Per evitare gli hijacker vi consigliamo di utilizzare un browser che non sia Internet Explorer: Opera e Firefox sono immuni da questi pericoli

Spyware: keylogger e adware

Gli spyware sono programmi che, senza il consenso dell'utente, inviano a un **server remoto** informazioni di vario tipo su ciò che accade durante l'utilizzo del computer. Possono essere programmi adware capaci di spiare e riferire abitudini commerciali, facilitando la visualizzazione di **banner** pubblicitari mirati.
Esistono però degli spyware più malefici, i keylogger, che registrano i comandi premuti a tastiera dall'utente e li inviano a qualcuno che, prima o poi, ne farà uso.
Anche in questo caso, come per gli hijacker, la consapevolezza dell'utente di aver installato sul PC un software spia svolge un ruolo importante nell'identificazione di un programma come spyware: solo l'assenza del consenso dell'utente delinea un abuso, un reato. Il modo migliore per stare ben alla larga dai software spia, quindi, è fare attenzione quando si installano nuovi programmi nel computer, perché può capitare che incorporino spyware. Installare un buon software antispyware è la soluzione per cancellare applicazioni indesiderate e **cookie traccianti**.

La chiamano "ingegneria sociale"...

Ora che tutti gli utenti di PC sono allertati riguardoi pericoli della Rete e sono protetti da sofisticati software antivirus, il fronte del malware (costituito da hacker o organizzazioni criminali) ha deciso di puntare su un altro punto debole, ben più delicato delle vulnerabilità di Windows: l'ingenuità della gente. Le bufale e il phishing (letteralmente "prendere all'amo") fanno parte di quella categoria di malware non virale che mira soprattutto a suggestionare l'utente, ingannandolo con messaggi falsi, ma sufficientemente verosimili da indurre in errore una minima percentuale dei destinatari di queste e-mail. Vi sembra poco? Non lo è, tenuto conto che hoax (letteralmente "truffa, inganno") e phishing sono diffusi via posta elettronica con la stessa tecnica dello spam: pensate che da ottobre 2004 a ottobre 2005 sono circolati 165.698 messaggi di phishing (Fonte: Elaborazione Eurispes su dati APWG).

Le bufale perniciose

"Attenzione: se trovate nel vostro computer il file Jdbgmgr.exe con l'icona di un tenero orsacchiotto... cancellatelo, perché è un virus pericolosissimo!" Così recita uno dei più famosi hoax del mondo informatico, diffusosi circa nel 2002, ma sempre agli onori della cronaca quanto le migliori leggende metropolitane. Il messaggio, se non lo sapete ancora, è falso, è un falso allarme. Il file in questione è un'applicazione di debug di Microsoft: cancellarlo non provoca nulla di grave, ma non va bene cadere in questi sciocchi tranelli. Per fortuna la gran parte degli antivirus è in grado di individuare gli hoax e cancellarli per evitare che l'utente, preso dal panico, comprometta le funzionalità del proprio computer oppure venga coinvolto in celebri truffe. Come quella secondo cui Bill Gates sarebbe disposto a dare 5 dollari a chiunque inoltri il messaggio a un'altra persona. Da non crederci!

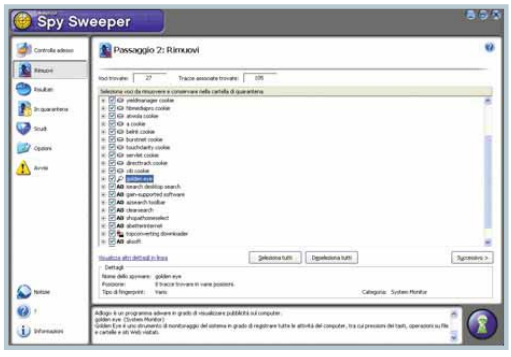
Non abboccate all'amo

Il phishing è un sistema di truffa che deve la sua fortuna all'ingenuità della gente. Vere e proprie organizzazioni criminali costruiscono delle e-mail finte, a volte allarmistiche che, all'apparenza, sembrano inviate da banche on-line. Nel testo del messaggio inseriscono un modulo per l'accesso al conto corrente on-line: e si dovrà inserire nome utente e password. Su milioni e milioni di e-mail inviate, qualche ignaro utente cadrà nel tranello, affidando i propri dati di accesso a dei perfetti sconosciuti. Il pericolo del phishing è all'ordine del giorno: avrete sicuramente già letto false e-mail di Banco Posta, Fineco, Banca Intesa, Unicredit e di altri istituti. Sono inoltre molto frequenti anche le false e-mail provenienti da eBay, studiate ad arte allo scopo di estorcere i dati di accesso al sito. Il modo migliore per non cadere in queste truffe è sapere che mai nessun servizio on-line richiede tramite posta elettronica i dati di accesso di un cliente.

▲ *Quando ricevete un messaggio di posta elettronica dalla vostra banca o da qualsiasi servizio on-line, leggetelo con molta attenzione prima di fare quello che vi chiede. Se avete qualche dubbio, prima di inserire qualsiasi dato o utilizzare un link incorporato presente nel testo, contattate l'assistenza del servizio per chiedere delucidazioni*

Dialer

La tempesta dei dialer sembra ormai finita, tuttavia non è passato molto tempo da quando decine di migliaia di italiani si sono ritrovati bollette telefoniche astronomiche solo per aver cercato di scaricare un MP3, una ricetta di cucina, una suoneria polifonica o qualche fotografia erotica. I dialer sono piccoli programmi che si installano nel computer e modificano le impostazioni della connessione telefonica a Internet: colpiscono solo le **connessioni dial-up**, ossia quelle via modem, inoltrando la telefonata di connessione a un numero a pagamento. I dialer agiscono in modo simile agli hijacker: basta visitare il sito Web sbagliato e nel giro di pochi secondi lo schermo viene messo sottosopra da pop-up, banner, schermate interlocutorie e, mentre l'utente è distratto da tutti questi eventi, il dialer entra in azione e avvia una nuova connessione remota... e salata!



▶ *Il miglior modo per evitare di cadere nelle maglie degli spyware è installare un software antispyware da affiancare a firewall e antivirus e aggiornarlo con la dovuta frequenza. Potrebbero passare dei mesi prima di accorgersi di essere stati infettati da un programma spia. Il migliore software della categoria secondo noi è Webroot Spy Sweeper, che abbiamo provato nel N. 150 di Computer Idea*

Pasticcio misto

Non è facile uscire da questo "calderone" di malware con le idee chiare. Il fatto è che, come dice il vecchio adagio, le disgrazie non vengono mai sole. Il virus non bussa più alle porte del vostro computer nascosto in un dischetto: piuttosto sarà incorporato in un worm. Un dialer potrà anche includere un hijacker. Un worm ricevuto per posta potrà aprire una backdoor. Nel settore, queste, sono chiamate "minacce blended" (dall'inglese "to blend": mescolare). Le minacce saranno anche "mescolate", ma le soluzioni non sono da meno: avrete notato come, negli ultimi anni, i software antivirus e le suite di sicurezza per Internet siano diventati sempre più ricchi di funzionalità.
Oggi non si limitano solo ad analizzare i file alla caccia di codice maligno: includono moduli per bloccare modifiche indesiderate al Registro di sistema, notificano con puntualità qualsiasi scambio di dati con la Rete, cancellano messaggi di posta contenenti worm, hoax e phishing... a questi software manca solo una cosa: la furbizia. Potete mettercela voi, facendo un po' di attenzione e conoscendo i rischi che correte quando lasciate per tante ore il PC collegato alla Rete.