

Comunque chi usa un sistema operativo Microsoft è obbligato a dotarsi di un antivirus, perché la possibilità di avere il PC infettato, navigando in rete, *chattando* usando programmi IM, scaricando file da 2p2 o la posta elettronica è elevatissima. Inoltre alcuni programmi Microsoft, per lo più Word ed Excel, aprono, in *default* senza chiedere permesso, documenti contenenti macro, che a loro volta possono celare “malware”. Più sicuri invece altri sistemi operativi, in particolare Mac OSX e GNU/Linux, in quanto meno diffusi e per questo obiettivi minori dei cybercriminali.

Da quando la sicurezza informatica è diventata una priorità, sono disponibili numerosi software antivirus. Funzionano tutti bene poiché dalla massima efficienza registrata (McAfee con il 99,8%) alla più bassa (Symantec al 98,2%) la differenza percentuale non è vistosa, anche se rapportata ai grandi numeri di “malware” attivi ha un suo peso. Di alcuni antivirus vi sono anche rilasci gratuiti; la differenza consiste nel fatto che la versione a pagamento protegge da tutte le categorie di “malware”, mentre quella gratuita solo dalle principali (es. Avira a pagamento ha un rendimento del 99,2%, mentre lo stesso antivirus in versione gratuita si riduce al 95,2%). [Dati aprile 2009].

Caratteristica comune di tutti gli antivirus è quella di impegnare moltissima memoria RAM, rallentando di conseguenza la velocità del PC; dunque anche per permettere a questi software di funzionare i PC diventano sempre più potenti, più costosi e maggiormente bisognosi di energia. Inoltre alcuni sostengono, ma non vi è nessuna prova a tal proposito, che siano le stesse case produttrici di antivirus ad alimentare la continua nascita di nuovi “malware”. Ma ormai i guadagni illeciti derivano soprattutto dal furto di dati personali, password e informazioni finanziarie (il 76% degli attacchi rilevati è stato verso servizi finanziari e ormai in rete esiste un mercato nero dove si possono trovare migliaia di dati sensibili; qui i dati più richiesti sono per clonare le carte di credito).

I consigli possono essere molti, anche se non tutti risolutivi. Per limitarsi ai principali:

1. diffidare sempre degli allegati, anche se inviati da persone conosciute, a meno che non siano attesi e/o di questi si parli espressamente nella e-mail;
2. evitare almeno di usare i programmi più diffusi, e dunque più conosciuti e attaccabili, in particolare INTERNET EXPLORER e OUTLOOK EXPRESS; esistono alternative buone e gratuite (per es. il browser FIREFOX e il email client THUNDERBIRD) che migliorano, almeno un po', la sicurezza;
3. meglio ancora aprire la posta elettronica su browser, senza usare il client;
4. navigando su internet evitate siti che offrono gratis prodotti che sono in realtà a pagamento;
5. abilitare, in Microsoft-Office, la richiesta per l'esecuzione delle macro;
6. non spedire allegati in formato Microsoft-Office ma in formato testo, e chiedere lo stesso ai vostri corrispondenti, così da evitare la trasmissione di macro;
7. mantenere sempre aggiornati antivirus e firewall;
8. non memorizzare le proprie password in un file del computer, e tanto meno nominare questo file «password»;
9. scansionare il proprio disco rigido avviando il PC da un altro sistema operativo (come spiegato nelle guide n° 2 e 3);
10. immunizzare la pendrive, o altre memorie di massa USB, utilizzate per il trasporto di software e documenti (come spiegato nella guida n° 4).

**I.T.I.S. «Carlo Zuccante»
CORSO SERALE PER ADULTI
corsi di Informatica e di Elettronica**

LE PICCOLE GUIDE PRATICHE

INFORMATICA

5

**VIRUS
E
ANTIVIRUS**

sede del corso serale:

Via Astorre Baglioni 22 – 30173 Mestre-Venezia

<http://serale.zuccante.it>

serale@zuccante.it

VIRUS

Innanzitutto una precisazione sui termini: nel linguaggio informatico di uso comune vengono chiamati “virus” i software creati per compiere delle azioni dannose nel personal computer (PC). In realtà il termine corretto è “malware”, di cui “virus” sono una categoria. Malware è un biscarto di due parole inglesi *malicious* e *software*, tradotto in italiano con “codice maligno”.

Non sempre queste categorie di software sono maligne. Talvolta sono nati con una funzione utile (come i “backdoor” che permettono di recuperare le password dimenticate), ma utilizzabili con intenti dolosi (carpire le password e accedere al PC).

In questo campo nessun elenco può essere esaustivo, sia per il grande numero di classi di “malware”, sia per la rapida evoluzione di questi software. Basti pensare che nel solo 2008 sono stati rintracciati nel web circa 15 milioni di “malware”, il 265% in più rispetto al 2007, ed è probabile che questi numeri possano aumentare.

Ormai la creazione di “malware” (soprattutto “virus”) fatta quasi per gioco è terminata, in quanto oggi lo scopo dei cybercriminali quello di controllare il maggior numero di computer. Nel mirino ci sono tutti: imprese, enti pubblici e semplici utenti del web: ovunque ci sia la possibilità di profitto c’è il rischio che qualcuno cerchi di approfittare delle falle e delle vulnerabilità dei sistemi informatici, soprattutto di Windows che, essendo il sistema operativo più diffuso (lo usano circa il 91% dei computer del mondo) è quello per cui sono costruiti la quasi totalità dei “malware”.

Proponiamo qui di seguito un elenco delle principali classi di “malware”, anche se molto spesso questi software sono composti da più parti indipendenti; per es. gli “spyware” vengono mascherati da un “rootkit”.

Trojan	92.898
Virus	92.574
Worm	72.179
Backdoor	57.158
Bot	43.298
Spyware	33.095
Virus polimorfi	32.924
Keylogger	11.884
Macro virus	5.124
Script virus	2.831
Rootkit	290

*Le minacce rilevate e attive
(aprile 2009) sono 444.225*

Adware: si insediano nel sistema operativo ed eseguono ordini dati da un PC offuscato tramite dei rootkit driver. Rallentano il sistema e rubano i dati personali rilevando indirizzo IP password e scambio di file tramite p2p o file sharing.

Backdoor: letteralmente “porta sul retro”: consentono di accedere al sistema in cui sono in esecuzione; spesso si diffondono con un “trojan” o un “worm”.

Batch: non sono sempre pericolosi in quanto ne esistono anche di utili. Sono dei software semplici (detti anche “amatoriali” perché creati dai “cyberbulli”) ma che possono provocare gravi danni, per esempio dando l’ordine di formattare il PC perdendo tutti i dati. Sono file di comando che gli antivirus non rilevano come pericolosi (ce ne sono così tanti che il PC sarebbe inutilizzabile se si fermasse ogni volta); non si aprono da soli ma dev’essere l’utente a dare l’ordine di esecuzione. Chi sa leggere le linee di comando può aprirli con il “blocco note” per verificarne l’eventuale pericolosità. Bisogna però anche ricordare che esistono modi per camuffarli e farli sembrare dei file “.exe”, aumentandone fittiziamente il peso per non destare sospetti.

Dialer: questi programmi si occupano di gestire la connessione ad Internet tramite la

normale linea telefonica. Sono presenti in tutti i sistemi operativi; diventano “malware” quando vengono utilizzati per sostituire il numero chiamato con un altro a tariffazione speciale. La rete ADSL elimina il rischio poiché non si avvale di “dialer”.

Keylogger: possono registrare tutto ciò che un utente digita sulla tastiera, rendendo così possibile il furto di password o di dati sensibili. Sono particolarmente pericolosi per chi utilizza la *home banking*. Il PC non si accorge della loro presenza, ma sono invece individuabili i “trojan” o i “worm” con cui viaggiano sul web.

Rootkit: i rootkit solitamente sono composti da un driver e, a volte, da delle copie modificate di programmi normalmente presenti nel sistema. I rootkit non sono dannosi in sé ma hanno la funzione di nascondere, sia all’utente che a programmi tipo antivirus, la presenza di particolari file o impostazioni del sistema. Vengono quindi utilizzati per mascherare “spyware” e “trojan”.

Spyware: vengono usati per raccogliere informazioni dal sistema su cui sono installati; le informazioni carpite, una volta ritrasmesse al mandante, possono essere utilizzate per sostituirsi all’utente o inviargli pubblicità mirata.

Trojan: si rifanno nel nome al mitico cavallo di Troia, come archetipo di un ingresso truffaldino. Oltre ad avere delle funzionalità “lecite”, utili per indurre l’utente ad utilizzarli, spesso contengono istruzioni dannose che vengono eseguite all’insaputa dell’utilizzatore. Poiché non si possono auto replicare, devono essere consapevolmente inviati alla vittima.

Virus: Possono provocare qualsiasi tipo di danno (anche se per lo più rallentano il sistema con operazioni inutili o dannose), anche a livello hardware (es. surriscaldando la CPU mediante *overclocking*). Si trasmettono da un computer a un altro tramite lo spostamento di file infetti ad opera degli utenti.

Worm: letteralmente *verme*; simili ai “virus” sono però in grado di auto replicarsi. Per indurre gli utenti ad eseguirli utilizzano ammiccamenti di *ingegneria sociale*, oppure sfruttano dei difetti (“bug”) di alcuni programmi.

...E ANTIVIRUS

Come si può combattere un software maligno? Con un software benigno!

In effetti gli “antivirus” (che però spesso trovano e distruggono i “malware” in genere) sono dei software che analizzano le sequenze di byte di ogni programma o documento che viene aperto nella RAM: quando viene individuata una stringa conosciuta come sequenza di un “malware”, ne viene bloccata l’esecuzione. Altre volte invece gli antivirus utilizzano la tecnologia euristica, che cerca sequenze di byte simili a quelle già note e archiviate e, supponendo che sia un virus leggermente modificato, lo riconosce comunque per tale.

Entrambe le tecnologie hanno dei limiti: la prima perché un virus dev’essere già catalogato per essere riconosciuto, e perciò un “nuovo” virus può agire indisturbato; la seconda perché riconoscendo come virus delle sequenze simili a quelle conosciute l’incidenza dell’errore è molto elevata.

Un altro elemento utile per bloccare l’intrusione di un “malware” nel PC è senza dubbio l’utilizzo di un “firewall”, meglio se allocato nel modem/router ADSL.