CACCIA AL VIRUS!

SAPER RICONOSCERE ED ELIMINARE VIRUS
CARATTERISTICHE - TIPI – PROTEZIONE

Microsoft
GIUNTI labs
the X learning Company

Di cosa parleremo

- Definizioni di virus e malware.
- Danni che i virus possono provocare.
- Rimedi che possiamo applicare.
- Cenni di storia e documentazione.

Cosa sono virus e malware

- Un **virus** è una parte di codice del computer che può essere contenuto in un programma oppure in un file. Può danneggiare l'hardware, il software e le informazioni presenti sul computer. Lo **scopo** di un virus è quello di **riprodursi** e **diffondersi** attraverso la **condivisione** di file o l'invio di messaggi di posta elettronica.

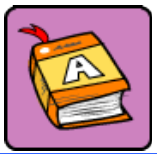
- **Malware** è un termine che deriva dalle parole *malicious* e *software* (letteralmente "software malizioso") e identifica **software** creati da malintenzionati che vogliono impadronirsi dei nostri dati personali: dal semplice indirizzo e-mail, alle password di accesso ai servizi on line della nostra banca. Di solito il malware non blocca il PC, ma ne ruba – appunto - dati preziosi.

Altri oggetti dannosi
Cos'è il worm

- Il **worm** è simile a un virus, ma a differenza di questo non necessita di legarsi ad altri eseguibili per diffondersi. Tipico di Internet, il **worm** usa la rete per diffondersi da un computer all'altro, di solito "rubando" gli indirizzi nella rubrica delle e-mail.

Altri oggetti dannosi
Cosa sono i trojan

- I **trojan** (o **trojan horse**) devono il nome al fatto che le loro funzionalità sono nascoste all'interno di un programma apparentemente innocuo. L'utente, installando ed eseguendo certi programmi (per lo più videogiochi), installa ed esegue senza rendersene conto anche il codice trojan nascosto.



Altri oggetti dannosi
Cosa sono spyware e dialer

Spyware e **dialer** sono software "camuffati" da programmi utili e installati dallo stesso utente.

- Lo **spyware** raccoglie informazioni sull'attività on line di un utente (siti visitati, acquisti effettuati ecc.) e può trasmetterle a organizzazioni che le utilizzeranno per trarne profitto, ad esempio tramite l'invio di pubblicità mirata.
- Il **dialer** è il software che si occupa di gestire la connessione a Internet tramite la normale linea telefonica. Utilizzato in modo truffaldino sostituisce il numero telefonico chiamato dalla connessione predefinita con uno a tariffazione speciale.

Altri oggetti dannosi
Cos'è il mail bombing

- Il **mail-bombing** (" bombardamento di posta") è fatto da appositi programmi, detti *Mail-Bomber*, che mandano ripetitivamente allo stesso destinatario centinaia o migliaia di e-mail tutte uguali, intasando la casella di posta elettronica e rendendola inutilizzabile.
- Il **Google-bombing** ("bombardamento di Google") è l'indirizzamento artificioso di link in modo da collegare parole chiave a determinati siti, "confondendo" il motore di ricerca. Esso sfrutta una caratteristica di Google che attribuisce importanza a una pagina in rapporto a quanti link verso di essa si trovano all'interno di altri siti web.

Perché vengono creati

I motivi per cui vengono creati virus e malware possono essere diversi. Ne citiamo alcuni:

- **danneggiare** gli utenti di computer;
- **deteriorare** il funzionamento di un programma;
- **bloccare** l'attività di una banca o di un'impresa;
- **gettare discredito** su un'attività informatica;
- **intasare caselle di posta elettronica** con una mole enorme di messaggi per impedire il regolare funzionamento del server.

Come si propagano

- La diffusione dei virus e dei malware oggi avviene soprattutto tramite Internet, attraverso programmi infetti o allegati di e-mail.
- L'esecuzione può provocare l'attivarsi di processi di distruzione di file, con blocco di programmi e arresto del sistema operativo.
- Un virus può presentarsi anche senza l'estensione ".exe", attualmente la più comune.
- I virus possono annidarsi in file HTML (ActiveX), in macro, in javascript, in file .dll (librerie dinamiche) e addirittura in immagini.

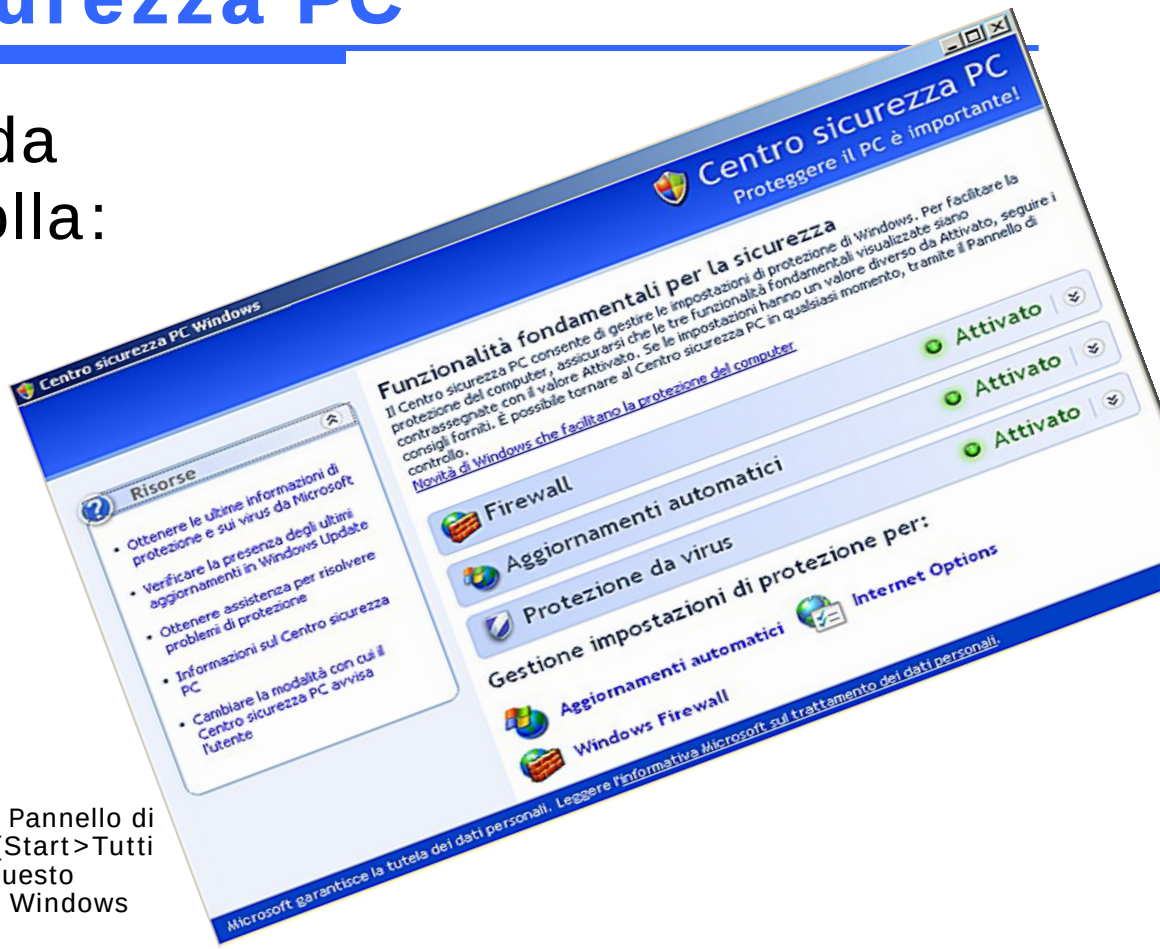
Quali i sintomi

- Il PC rallenta?
- Alcuni programmi cessano di funzionare?
- Si moltiplicano messaggi d'errore?
- Si aprono automaticamente siti non richiesti?
- Riceviamo posta indesiderata, o qualcuno ci avverte di aver ricevuto e-mail da noi, ma noi non le abbiamo inviate?
- Si creano flussi di dati in uscita dal computer, anche riservati?

Prevenire
Centro sicurezza PC

Dispone di una guida aggiornata e controlla:

- Firewall
- Aggiornamenti
- Antivirus



Si accede al Centro Sicurezza PC attraverso il Pannello di Controllo oppure attraverso il menu di avvio (Start>Tutti i Programmi>Accessori>Utilità di Sistema). Questo strumento è disponibile sul sistema operativo Windows XP dall'introduzione del Service Pack 2.

Cos'è il Firewall

- Letteralmente "muro di fuoco", è una difesa costruita intorno al PC e alla connessione: l'utente - tramite le *eccezioni* - consente solo ai programmi legittimi di accedere al Web e di lavorare sul PC.

A cosa serve l'aggiornamento del sistema operativo

- Un sistema operativo aggiornato è più protetto in quanto, con l'uso, ne vengono individuate ed eliminate eventuali falle (*bugs*).
- Il Service Pack 2 di Windows XP è un esempio di aggiornamento periodico automatico del sistema operativo.

Gli antivirus

Gli antivirus oggi, sono generalmente installati da quasi tutti gli utenti, ma occorre tenerli **aggiornati** e seguire alcune regole fondamentali:

- Aggiornare con regolarità l'antivirus scelto attraverso Internet o apposito CD-rom.
- Fare una scansione periodica di tutto il disco rigido.
- Far partire l'antivirus **all'accensione** del sistema operativo.
- Impostare il controllo delle **e-mail**.

Come rimanere protetti

- Fare regolarmente una copia dei file importanti e metterla al sicuro.
- Non aprire gli allegati delle e-mail provenienti da mittenti sconosciuti.
- Non comunicare mai dati personali di accesso a siti web o alla posta elettronica.
- Scaricare file solo da siti sicuri e affidabili.
- Stare alla larga da siti che trattano di pirateria informatica e pornografia.
- Rispettare gli altri per guadagnare rispetto.

C'era un volta il dischetto infetto

- Nella storia dei virus per computer, il dischetto (floppy disk) è stato il principale strumento di trasmissione.
- I virus infettavano i file di avvio della macchina.
- I virus depositavano una traccia nelle memorie di massa (la "firma") che rendeva superflua una replica da parte dell'infestatore ma faceva riconoscere la sua presenza ai programmi di rimozione.

Hit parade dei virus

per novità e obiettivi

- 1986 – *Brain*, su floppy: danneggiava il file di avvio dei programmi.
- 1988 – *Morris Worm,* su internet, capace di forzare le password nei sistemi Unix.
- 1991 – *Michelangelo, s*ovrascriveva i file d'avvio dei dischi; virus ad orologeria, doveva colpire il 6 marzo.
- 1999 – *Melissa*, il primo virus importante con obiettivo Outlook e la posta elettronica.
- 2000 – *I Love You*, in 10 minuti metteva a tappeto 350 mila pc in tutto il mondo.
- 2004 – *Cabir*, il primo virus all'attacco dei telefonini.

Link utili

Per approfondire questi temi in Rete:

- http://www.microsoft.com/italy/security/default.mspx
- http://www.microsoft.com/italy/mscorp/twc/security/default.mspx
- http://www.microsoft.com/italy/mscorp/twc/privacy/default.mspx
- http://www.sicuramenteweb.it/
- http://www.ilwebperamico.it/
- http://www.commissariatodips.it/stanze.php?strparent=10