Comune di Gesico

NOZIONI DI SICUREZZA INFORMATICA PER L'UTENTE

Che cosa sono i virus?

Per virus si intende un programma che ha la capacità di autoriprodursi, cioè di creare copie di se stesso, e andarsi a infiltrare in altri programmi che a loro volta vengono utilizzati come mezzo trasmissivo per infettare altri Pc attraverso lo scambio di floppy disk, la comunicazione in Rete le altre forme interazione tra computer.
Il virus informatico è del tutto simile al virus biologico, in quanto si diffonde silenziosamente, in maniera del tutto anonima e colpisce soprattutto chi non ha provveduto alla necessaria prevenzione.
I virus possono essere trasportati da un "PC portatore" ad un altro tramite i supporti utilizzati per il trasferimento di dati (floppy, cartucce, CD, …) ma anche e in maniera più aggressiva, tramite posta elettronica.
I virus sono software (file con estensione exe o zip) e con tutta probabilità restano innocui fino al momento in cui qualcuno li lancia (con un semplice doppio click).

Ma chi è che fa girare i virus? E perchè?

I virus sono software scritti e progettati da programmatori più o meno esperti in grado di sviluppare file eseguibili intrusivi. Questi programmatori sono a volte ragazzini che vanno ancora a scuola o tecnici che già lavorano o hanno lavorato in società informatiche. Non sono necessariamente altamente preparati sulle tecnologie moderne, ma conoscono alcuni trucchi per attaccare i file di un PC, si muovono sfruttando il crescente utilizzo di posta elettronica tra gli utenti di internet, creano un software più o meno dannoso per chi lo riceve e lo mandano in rete.
Da non confondersi con i pirati informatici, propriamente detti hacker, coloro che si introducono nei sistemi informatici di grandi aziende superando ogni barriera di sicurezza. Gli hacker possono appartenere a diverse tipologie: per gli hacker "più giovani" o solo "più clementi" il successo dell'intrusione da loro creato è spesso motivo d'orgoglio personale, una dimostrazione di bravura, e questo gli basta. Gli hacker "professionisti", forse i più pericolosi, tentano invece di forzare i sistemi di difesa aziendali per un ritorno economico attaccando i computer per ottenere informazioni segrete da rivendere al proprio committente.

Come è fatto un virus? Possiamo riconoscerlo?

I virus sono veri e propri programmi in grado, a seconda dei casi, di distruggere, confondere, nascondere dati. Possono entrare nel vostro PC con floppy, CD, ecc. ma solitamente arrivano direttamente nella vostra posta elettronica. Solitamente sono messaggi senza mittente e senza oggetto, con allegato un file dal nome variabile e con estensione .exe .
Ma il testo di un messaggio di posta elettronica è assolutamente privo di rischi. Questo significa che aprire un messaggio di posta elettronica non può in alcun modo danneggiare il vostro Pc.
Bisogna invece stare attenti agli allegati. Un file allegato a una mail, come qualsiasi altro file, può effettivamente contenere un virus. Anche in questo caso però il semplice fatto di ricevere un file infetto non vuol dire che il computer sia ormai contagiato. Un virus, perché si attivi, deve essere "eseguito". Questo significa che finché non si apre il file in questione il vostro computer non può subire dei danni.
Alcuni virus possono rilevare nella rete un invio di email (per esempio da voi ai vostri clienti), e prelevarne il contenuto compresi tutti gli indirizzi ai quali il messaggio è stato inviato. Questo non significa che se avete ricevuto un messaggio con virus siete ormai nella loro lista, perchè i virus non mantengono archivi, ma potrebbe anche capitare che riceviate un messaggio da un contatto della vostra rubrica, con mittente e oggetto di vostra conoscenza, con un allegato di dubbia provenienza.
E' buona regola non aprire mai file allegati con programmi .exe, .zip, e con nomi o formati strani, dei quali non conoscete il contenuto. Piuttosto ricontattate il mittente del messaggio accertandovi che il contenuto allegato sia sicuro. Resta chiaro che il mittente non ha alcuna responsabilità sul contenuto dell'allegato e spetta solamente a voi gestire il problema. Il motivo per cui non si dovrebbero accettare file di dubbia provenienza è dovuto al fatto che potrebbero rivelarsi dei programmi in grado di aprire una back door (ingresso segreto) nel vostro computer.
Per evitare inutili allarmismi, chiariamo che i file di normale spedizione con estensione doc, jpg, gif, xls, … non possono contenere alcun virus mentre necessitano di una certa attenzione i file di tipo exe, zip, avi, …e altri formati sconosciuti. Ma attenzione anche ai Macro Virus.
Questa tipologia di virus viene realizzata tramite il linguaggio Macro di Microsoft Word (WordBasic). Questo linguaggio permette di creare dei piccoli codici (macro) per eseguire una serie di comandi. Se per esempio si intende inserire un'immagine con la vostra foto in tutte le pagine di un documento si può fare una macro che faccia quest'operazione in modo automatico. Sfortunatamente questo linguaggio può anche essere utilizzato per creare dei virus.
Generalmente una macro è parte di un documento di Word o di Excel quindi anche un Macro Virus è parte integrante di un documento di questo tipo. Ogni volta che si apre una file di Word o Excel vi viene segnalata la presenza di una macro. Se si può riporre piena fiducia in chi vi ha inviato il documento si può aprirlo senza preoccupazione. Altrimenti occorre sempre fare una certa attenzione.

Macrovirus, la nuova generazione

...attenzione anche ai Macro Virus. Questa tipologia di virus viene realizzata tramite un linguaggio che permette di creare dei piccoli codici (macro) per eseguire una serie di comandi. Se per esempio intendi inserire un'immagine con la tua foto in tutte le pagine di un documento puoi fare una macro che faccia quest'operazione in modo automatico. Sfortunatamente questo linguaggio può anche essere utilizzato per creare dei virus.
Generalmente una macro è parte di un documento di Word o di Excel quindi anche un Macro Virus è parte integrante di un documento di questo tipo. Ogni volta che apri una file di Word o Excel ti viene segnalata la presenza di una macro. Se puoi riporre piena fiducia in chi ti ha inviato il documento puoi aprirlo senza preoccupazione. Altrimenti occorre sempre fare una certa attenzione.
La nuova generazione dei virus è formata da virus che non attaccano programmi eseguibili ma i documenti di Word, Access, PowerPoint e Excel sottoforma di Macro, piccoli programmi creati con il linguaggio di programmazione Visual Basic for Application (VBA) utilizzato normalmente per aggiungere potenzialità ai fogli di calcolo, a lettere e relazioni.
I MacroVirus sono in rapida crescita.
Un MacroVirus si nasconde in un documento Office infetto. Una volta portato su un Pc sano e aperto il documento che lo contiene, il MacroVirus si diffonde infettando il Normal.dot, il modello di foglio bianco sul quale sono basati tutti i documenti vuoti creati con Word o i fogli di calcolo di Excel.

Tipologie dei virus

Si stimano più di 1000 famiglie virali in circolazione. Se però si considerano le varianti ai virus base, il numero sale paurosamente intorno ai 20.000. Le varianti possono essere anche minime, con risultati finali leggermente diversi, ma questo basta a moltiplicare il numero di virus conosciuti e le procedure antivirus che dovranno contrastarli.
Virus innocui
Vengono chiamati virus in quanto penetrano nei PC altrui senza che i proprietari ne siano al corrente, e lanciano programmini che disturbano le normali procedure. Possono essere testi che appaiono sullo schermo, o immagini, o icone che cadono dal desktop. Sono innocui, ma spesso fastidiosi.
Uno degli esempi più comuni è il virus Marijuana, completamente innocuo, che fa apparire sullo schermo del computer la parola Legalise. Successivamente qualcuno ha modificato il codice originale in modo che il virus scriva la parola Legalize. Ecco che, ritornando al conto precedente, i virus sono già diventati due.
Virus Trojan Horse (Cavallo di Troia)
Questo tipo di virus deve il proprio nome alla tradizione omerica: il virus si nasconde all'interno di file eseguibili, non eseguibili e anche compressi, in modo da evitare il rilevamento. Una volta entrati in un Pc assumono la forma di utility o librerie di sistema, ma il loro reale contenuto non è altro che un codice virale.
I Cavalli di Troia sono virus di vecchio tipo: ormai tutti i software antivirus riescono a rilevarne la presenza.
Virus Polimorfici
I virus polimorfici nascondono se stessi auto-codificandosi, si trasformano in qualcos'altro, in modo da evitare l'intercettazione da parte dell'antivirus. Il virus è composto da una procedura di attacco, e una di codifica-decodifica. Il virus entra in un Pc con la propria porzione di attacco codificata in modo da sfuggire ai controlli. Una volta che la procedura di decodifica è attiva nel Pc, questa richiama la procedura di attacco. A questo punto l'attacco virale può avere luogo.
L'evoluzione dei virus polimorfici ha fatto in modo che essi riescano a cambiare la codifica da un'infezione a un'altra, come se il programma modificasse se stesso dopo ogni attacco.
In questo modo in un Pc possono diffondersi decine di virus formalmente diversi che in realtà sono lo stesso virus polimorfico mutato.
Per intercettare un virus polimorfico il vostro antivirus deve possedere una funzione detta scansione crittografica che riesce a intercettare il corpo criptato del virus. Gli ultimi software antivirus sono in grado di farlo.
I **Virus Stealth** (invisibili)
Un virus Stealth può essere o non essere di tipo parassitario: attacca sia i file che i settori di boot dei dischi e per rendersi invisibile manipola le funzioni di sistema o i risultati delle interrogazioni del sistema operativo.
Un virus Stealth riesce così a sfuggire facilmente ai controlli degli antivirus.
Quando però il virus è attivo e si trova nella memoria RAM, diventa visibile. Gli antivirus di ultima generazione non solo cercano di cogliere in fallo il virus Stealth quando questo è in memoria, ma riescono a rilevarlo anche in fase di latenza, quando è addormentato, con sofisticati strumenti di interrogazione.
I **Virus Slow** (lenti)

I Virus Slow sono virus parassitari che infettano solo i file, e non i programmi eseguibili, e per questo risultano particolarmente difficili da intercettare. In particolare entrano in funzione solo quando è l'utente ad effettuare operazioni sui file (solitamente i file di sistema), diffondendosi principalmente per via parassitaria attraverso copie ripetute.
Quando si modificano file di sistema e si salvano, il virus intercetta l'operazione e si infila nella copia. L'antivirus rileverà la modifica e vi avvertirà del fatto che è in atto un'infezione. Il virus slow si propaga perchè spesso l'utente non dà troppa importanza all'avvertimento dell'antivirus.
Per intercettare un virus Slow il vostro antivirus deve essere dotato di uno scudo di integrità (Integrity Shell) in grado di monitorare costantemente la creazione di ogni file. L'antivirus tenta di modificare file di sistema COM e file EXE traendo in inganno il virus slow che esce allo scoperto per replicarsi. A questo punto scatta la trappola e il virus è debellato.

Virus Retro

Il virus Retro è un virus che tenta di sfuggire all'antivirus attaccandolo direttamente. Questo tipo di virus è anche chiamato virus-anti-virus proprio per il suo funzionamento.
Il virus Retro funziona in maniera perfetta se entra in un Pc prima dell'antivirus. A questo punto, quando l'antivirus viene installato, il Retro vi si copia dentro e lo blocca disattivandolo.

Virus Multiparte (o ad attacco multiplo)

Questi virus infettano il Pc in modi differenti comportandosi come virus di altre razze. Un multiparte solitamente prima infetta il settore di boot del disco. Al riavvio del Pc vengono infettati tutti i file eseguibili che poi vengono ricopiati su disco. Gli antivirus sul mercato bloccano i virus multiparte basandosi sul fatto che essi sono solitamente più grandi dei virus normali. E' però più probabile prevenire un'infezione e non debellarla.

Virus Armored (Corazzati)

I Virus Armored possono essere sia virus di boot che virus parassitari, il termine corazzati identifica più la loro protezione che il loro funzionamento.
Questo tipo di virus infatti cerca di sfuggire all'antivirus facendogli credere di essere da un'altra parte.

Virus Phage

I Virus Phage modificano i file originari invece di nidificarvisi. Sono chiamati così perché esiste un virus biologico che opera allo stesso modo chiamato Phage. I Virus Phage sostituiscono il codice dell'eseguibile originario con un virus. Nel momento in cui richiamate il file eseguibile entra in funzione il virus invece del software lanciato.

Virus Companion (di Accompagnamento)

Questi virus sono programmi virali che modificano i file eseguibili originali (*.exe) creando un file com (*.com) che viene eseguito prima che venga aperto un programma. A questo punto il Virus si diffonde infettando il sistema. Si trovano spesso abbinati ai Virus Phage.

Virus Worm (verme)

Questo programma colpisce solo i computer con sistema operativo Windows installando una copia di se stesso nella cartella System e modificando la libreria di sistema WSOCK3.DLL, che gestisce le connessioni a Internet in Windows 95 e 98. Il più noto virus worm si chiama Happy99, forse ne avrete già sentito parlare o lo avete ricevuto direttamente in posta.
Uno degli effetti di Happy99 è che ogni volta che spedite un messaggio di posta elettronica, lui ne cancella il testo e allega una copia di se stesso al messaggio: il tutto senza che voi possiate accorgervene (in compenso se ne accorge chi riceve il vostro messaggio con annesso il regalo).
Naturalmente il virus infetta il vostro computer solo se eseguite l'allegato: quindi se non avete mai aperto un file chiamato Happy99.exe arrivato via email, che una volta aperto mostra una bella finestra con dei fuochi di artificio e gli auguri per il nuovo anno, non dovete preoccuparvi.
Se invece avete commesso l'imprudenza di aprirlo senza prima esaminarlo con un software antivirus aggiornato, niente panico: esiste una procedura molto semplice per liberarsene.
Uscite da Windows ed entrate in Ms-Dos (o aprite una sessione Dos)
Andate nella directory System di Windows
Eliminate i file: ska.exe - ska.dll - wsock32.dll
Rinominate il file wsock32.ska in wsock32.dll
Inoltre, ricordatevi di avvertire tutte le persone cui avete mandato messaggi recentemente. Ulteriori notizie le potete trovare sul sito Symantec.

Come ci proteggiamo?

Il modo migliore per difendersi da tali inconvenienti è quello dotarsi dell'ultima versione del proprio antivirus e di provvedere ad aggiornare costantemente la libreria dei virus che quest'ultimo è in grado di riconoscere.
In rete esistono software gratuiti adatti all'uso ma soprattutto per chi non è molto pratico di internet e di inglese.