I VIRUS INFORMATICI

Cosa sono, come possono essere classificati, come funzionano, come difendersi

Introduzione

Il termine *virus*, da anni a questa parte, è entrato tristemente a far parte del vocabolario di chi utilizza un computer: difficile è infatti dimenticare quel "qualcosa" che arriva nel nostro pc a distruggere o rovinare i nostri dati e ad impedirci di lavorare. Ma cos'è esattamente un *virus informatico*?

Un virus informatico non è nient'altro che un semplice piccolo programma, un frammento di codice progettato e scritto per riprodursi e diffondersi da un sistema informatico ad un altro all'insaputa dell'utente, quindi senza la sua autorizzazione.

Il termine *virus* dato a questi programmi è particolarmente indovinato. Il loro comportamento, infatti, può essere paragonato in tutto e per tutto a quello dei *virus biologici*: mentre un virus informatico sfrutta le risorse del computer per riprodursi, quello biologico utilizza il sistema di riproduzione delle cellule del corpo umano, non possedendone uno proprio. Ma niente paura! A differenza di quello che qualcuno potrebbe pensare, i virus informatici non possono contagiare le persone!

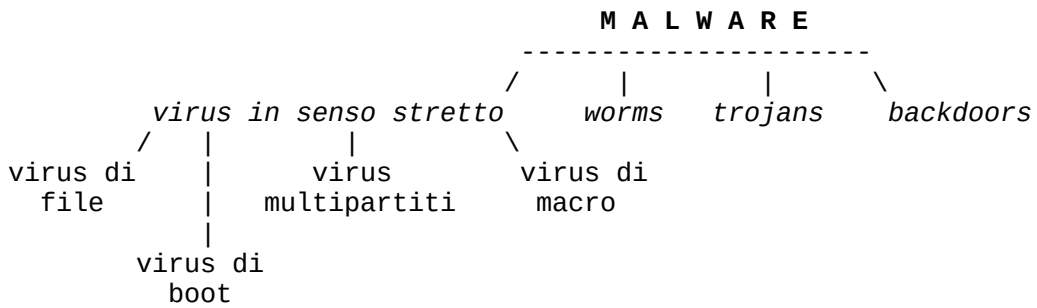
Molti virus, purtroppo, non si limitano solamente a riprodursi. Essi portano anche un "carico", il cosiddetto **payload** (per analogia con quello dei missili). Si tratta di una parte del programma che compie qualche altra operazione, solitamente eseguita al verificarsi di certe particolari condizioni, come ad una data o ad un'ora precise (*time bomb*), o dopo una particolare sequenza di eventi (*logic bomb*). Tale operazione può avere effetti più o meno pesanti: da un semplice messaggio mostrato a video, all'emissione di suoni da parte del pc, fino alla cancellazione o al danneggiamento dei dati contenuti nell'hard disk. E' questo il caso del virus *November17th* (conosciuto anche come il famigerato *855*), molto diffuso in Italia negli anni '90: scatenava il suo payload in una data compresa tra il 17 ed il 30 Novembre dopo 500 pressioni di tasti mediante tastiera, cancellando irrecuperabilmente i dati contenuti nel disco fisso (formattazione), oppure cancellando il contenuto della memoria CMOS.

Per quanti danni possano provocare ai nostri dati, è bene ricordare che i virus informatici **non possono danneggiare l'hardware**. Immagini a video distorte o disturbate, caratteri premuti sulla tastiera che non compaiono a video, mouse impazzito, stampe con simboli senza senso possono essere le conseguenze di un virus che sta interferendo solamente **sul software** che regola e fa funzionare tali periferiche.

Classificazione

Dopo aver visto in generale cosa sono i virus, passiamo alla loro *classificazione*. Classificare i virus è tutt'altro che semplice (almeno al giorno d'oggi): molteplici sono infatti le modalità di diffusione, i metodi di infezione e le capacità di questi programmi maligni. Tutto ciò rende difficile la suddivisione in gruppi aventi caratteristiche simili.

Si può utilizzare allora una classe generale, chiamata **MALWARE** (derivante da **MAL**icious soft**WARE**, = software dannoso) che racchiude tutti i tipi di virus: i *virus in senso stretto* (suddivisi a loro volta in 4 gruppi), i *worms*, i *trojans* e le *backdoors*. Possiamo riassumere la classificazione in questo modo:



Come si evince dallo schema, i worms, i trojans e le backdoors non sono considerati dei veri e propri virus, in quanto agiscono in maniera diversa da essi; inoltre, ai trojans e alle backdoors manca un requisito fondamentale per rientrare in questa categoria: la **capacità di riprodursi**.

Vediamo ora di analizzare le singole tipologie di virus.

Virus in senso stretto

I virus in senso stretto sono quelli che erano maggiormente in circolazione prima che Internet divenisse un fenomeno di massa, spianando la strada alla diffusione delle altre tipologie di malware (worm, trojans e backdoors).

I virus in senso stretto non possono entrare in un pc da soli (a differenza di come potrebbero fare i worm, come vedremo successivamente). Per contagiare il computer è necessario che l'utente svolga una tra le seguenti azioni:

- **eseguire un'applicazione infetta**;
- **avviare da un dischetto infetto**;
- **avviare delle macro infette**.

Ogni volta che un oggetto infetto viene eseguito, all'insaputa dell'utente viene eseguito anche il virus: esso si attiva e può così riprodursi infettando altri oggetti, installarsi residente in memoria o attivare il *payload* (di cui abbiamo già parlato in precedenza), scatenando così la sua azione più o meno devastante.

Come qualsiasi altro programma, anche i virus sono solitamente registrati su un floppy o sull'hard disk, ma ovviamente non si tratta di file a sé stanti, altrimenti verrebbero subito scoperti. Vediamo come si comportano le diverse tipologie di virus in senso stretto.

Virus di file

I virus di file sono quei programmi maligni che, per nascondersi o per far in modo di essere eseguiti più facilmente, utilizzano una di queste tecniche:

- **si sostituiscono completamente ad un programma** (file aventi estensione .EXE, .COM, .SCR, .BAT, ecc.). Nel momento in cui il sistema operativo o l'utente andrà ad eseguire quel programma, in realtà sarà eseguito il virus;
- **si copiano all'interno di un altro programma** (file con estensione .EXE, .COM, .SCR, .BAT, ecc.), solitamente alla sua fine, senza sostituirlo completamente, ma "infettandolo". Quindi, nello stesso programma, saranno presenti sia il codice originale sia il codice virale. Al momento dell'esecuzione dell'applicazione infetta verrà eseguito il virus che, a sua volta, provvederà a mandare in esecuzione anche il programma legittimo, simulando così un corretto funzionamento. In conseguenza all'infezione, il programma originale solitamente *aumenta di dimensione*;
- **sfruttano delle priorità del filesystem nell'eseguire i programmi**. Un primo metodo consiste nella localizzazione di una cartella contenente un eseguibile con estensione *.exe* da parte del virus, che quindi si copia nella medesima cartella con estensione *.com*. I file di quest'ultimo tipo hanno la priorità di esecuzione rispetto agli *.exe*: se viene invocato il nome del programma senza che ne venga specificata l'estensione, verrà eseguito prima il file *.com* e quindi il virus, che può decidere o meno di mandare in esecuzione anche il programma originale. Il secondo metodo invece consiste nello sfruttare i percorsi preferenziali memorizzati nella variabile di ambiente *PATH* per la ricerca di eseguibili sprovvisti di percorso assoluto. Se la variabile PATH, ad esempio, contiene nell'ordine i percorsi *c:*\ e *c:**windows*, un programma generico al momento della sua invocazione verrà ricercato prima in c:\ e quindi in c:\windows. Se il virus si copia nella cartella c:\ utilizzando il nome di un *file di sistema* contenuto nella cartella c:\windows, la richiesta di esecuzione del file legittimo porterà invece all'attivazione del virus, in quanto si trova in una cartella a più alta priorità di ricerca.

Virus di boot

I virus di boot, a differenza di quelli di file, sfruttano per diffondersi il **settore di boot** e il **master boot record (MBR)**, due zone speciali dei dischi che contengono le informazioni necessarie al caricamento e all'avvio del sistema operativo. I due tipi di infezione sono analoghi: esiste solo una sottile differenza.

I virus che si inseriscono nel *settore di boot* vengono eseguiti ad ogni avvio del computer prima del caricamento del sistema operativo: essi rimangono in memoria quindi fino allo spegnimento del pc, svolgendo le proprie azioni dannose, consistenti solitamente nel copiarsi in tutti i floppy inseriti nel lettore (che diventano un veicolo di diffusione, se usati per avviare altri sistemi) e nel danneggiamento dei dati.

I virus che si inseriscono nel *master boot record*, come già detto, si comportano in modo analogo ai primi, tranne che per un particolare: al momento dell'infezione, il virus provvede a spostare in un'altra parte del disco le informazioni essenziali per il caricamento del sistema operativo, sostituendovi il proprio codice. La conseguenza è che in computer dotati di Windows NT o 2000 che usano partizioni NTFS il sistema non riesce ad avviarsi, mentre i sistemi Windows95, 98 e ME si avviano ugualmente (poiché il virus riesce a comunicare loro la nuova posizione delle informazioni precedentemente spostate), eseguendo anche il codice virale.

I virus di boot erano molto diffusi in passato. Oggi, grazie ad una maggior attenzione e ad un maggior controllo dedicati a queste zone del disco, i programmatori di virus stanno tralasciando questa tecnica, considerata ormai inefficace.

Virus multipartiti

Questi tipi di virus sono indubbiamente i più complessi dal punto di vista della realizzazione e sono tra i più pericolosi. Come si può intuire dal loro nome, essi possono infettare sia i settori di boot dei dischi (come i virus di boot), sia i programmi (come i virus di file).

Facilmente intuibile è quindi come questi virus siano abbastanza complicati da rimuovere: anche se si elimina il virus dal settore di boot, non appena verrà eseguito un programma infetto il virus provvederà a ricopiarvisi immediatamente. Analogamente, se i programmi infetti vengono ripuliti, al successivo riavvio del sistema il virus sarà attivato e reinfetterà nuovi programmi.

Virus di macro

Questi tipi di virus infettano solamente i **file di dati** (e non i programmi) e precisamente quei file di documenti al cui interno possono essere contenute le *macro definizioni*.

Le *macro* sono delle sequenze di istruzioni (i famosi *script*) scritti in linguaggio **VBA** (**V**isual **B**asic for **A***pplication*) utilizzate nei programmi della suite Office, come Word ed Excel, allo scopo di automatizzare certe operazioni sui documenti ed aumentarne quindi la flessibilità e le potenzialità. Questi processi di automazione, però, possono venire sfruttati dai virus di macro. Generalmente, per assicurarsi di venire eseguiti il più spesso possibile, essi vanno ad infettare i modelli standard (nel caso di Word il file *Normal.dot*), cioè quei documenti nuovi e vuoti che ci vengono presentati all'apertura di un programma di Office. In questo caso ogni nuovo documento creato sarà automaticamente infetto. Altra tecnica usata da questi virus è quella di andare a modificare le macro associate alle voci di menù (ad esempio Apri, Salva, Salva con nome, ecc.); quando si andrà a scegliere una di queste voci sarà eseguito anche il codice virale e potranno così essere infettati nuovi documenti.

Esistono moltissimi virus di macro poiché sono solitamente più semplici da realizzare rispetto ai virus delle tipologie precedenti; se creati adeguatamente, inoltre, possono colpire anche sistemi operativi completamente diversi tra di loro (considerato che esiste Office per Macintosh...).

Dopo aver visto in dettaglio il funzionamento dei diversi tipi di virus in senso stretto, passiamo a delle considerazioni di carattere generale.

Considerato che lo scopo di un virus è quello di infettare più programmi e più sistemi possibili, esso deve necessariamente prolungare il più possibile la sua esistenza, nascondendo la sua presenza. Tanto più piccolo è un oggetto, tanto più grandi sono le possibilità che esso passi inosservato: la dimensione di tali programmi maligni infatti generalmente non supera le poche decine di KB, grazie anche alla codificazione di molti di loro in linguaggio *Assembly*.

Ma non è tutto: alcuni virus "intelligenti" utilizzano altre tecniche per cercare di rendersi invisibili e di passare inosservati ai software antivirus: la tecnica **stealth** e la tecnica del **polimorfismo**.

La tecnica *stealth* (propria dei *virus stealth*) consente al virus di monitorare, grazie ad una parte di esso che rimane costantemente in memoria, le chiamate dei programmi ad alcune funzioni del sistema operativo. In questo modo, ad esempio, un virus di boot può "accorgersi" del tentativo di un'applicazione di leggere dal settore di boot o dall'MBR, ripulendo preventivamente quel settore dal suo codice, per poi reinfettarlo nuovamente a lettura conclusa. In maniera del tutto analoga i virus di file possono ripulire temporaneamente i programmi infetti. Il rovescio della medaglia è che i software antivirus possono facilmente rilevare la parte di codice virale costantemente presente in memoria.

Una delle prime operazioni che un virus effettua prima di infettare un oggetto è quello di controllare che in quell'oggetto non sia già presente una copia di se stesso: una duplice infezione, infatti, potrebbe compromettere la sua funzionalità e quindi la sua esistenza. Per svolgere questa azione, il virus cerca nell'oggetto in questione la presenza o meno di una **stringa** che lo caratterizza. Se la stringa viene trovata, significa che l'oggetto è già infetto; nel caso opposto, viene effettuata l'infezione. Se da una parte questa tecnica assicura la sopravvivenza al virus, dall'altra lo rende vulnerabile: la stringa rappresenta infatti la sua *firma*, che sta alla base delle definizioni utilizzate dai software antivirus per il riconoscimento dei codici virali. La tecnica del *polimorfismo*, propria dei virus detti *polimorfici* (nonché anche più evoluti), permette loro di superare questa vulnerabilità utilizzando la *crittografia*: un codice criptato è infatti difficilmente analizzabile se non se ne conoscono l'*algoritmo* tramite il quale è stato criptato e la relativa *chiave*. I virus polimorfici hanno al loro interno diverse funzioni di cifratura, o addirittura un generatore di cifratura casuale, usati per criptare ogni loro copia attraverso algoritmi sempre differenti. Solo la conoscenza di tutte queste funzioni di cifratura può per-

mettere ad un antivirus di riconoscere il codice virale.

Worms

I *worms* (*verme* in inglese) sono quella tipologia di malware che è apparsa sulla scena mondiale con l'avvento di Internet, facendo sembrare quasi "scomparsi" i virus in senso stretto.

I concetti di virus e worm sono simili, ma si differenziano per una aspetto: a differenza dei virus, i worm sono **frammenti di codice indipendenti ed autonomi** che agiscono principalmente in memoria, consumando risorse del sistema e propagandosi velocemente tra sistemi differenti. I worm infatti non sono dei "parassiti" e non hanno bisogno di un programma ospite per replicarsi; il loro fine resta comunque quello di infettare il maggior numero di sistemi possibile propagandosi velocemente. Il loro payload (sempre che ne contengano uno) generalmente non mira a danneggiare i dati, ma si limita a creare malfunzionamenti al sistema operativo o, peggio, a carpire dati ed informazioni personali della vittima.

Per essere eseguiti, spesso i worm **non necessitano di azioni particolari da parte dell'utente**, come vedremo tra poco.

Mentre per i virus in senso stretto il veicolo di diffusione è rappresentato da dischetti e programmi, i worm sfruttano per propagarsi la **rete**, sia **locale** (LAN aziendali o domestiche) che **Internet**: vediamo da dove possono provenire le minacce.

- **Posta elettronica**. Essendo il principale mezzo per la trasmissione di informazioni, è anche il più utilizzato dai worm per propagarsi, generalmente in due modi: attraverso gli *allegati* o sfruttando *vulnerabilità insite in alcuni client di posta elettronica*.
  Gli allegati sono il metodo di propagazione più usato dai worm, anche se presenta un significativo punto debole: *l'utente deve aprire l'allegato per infettare il proprio computer*. A tale scopo il worm inserisce come oggetto del messaggio frasi "invitanti": ricordate ad esempio *I Love You*, alias *Loveletter*? Il messaggio di posta infetto portava l'oggetto *ILOVEYOU* e come allegato il file *LOVE-LETTER-FOR-YOU.TXT.vbs*. Poiché solitamente l'estensione dei file non viene visualizzata da parte del sistema operativo, molti utenti, credendo di avere a che fare con un file di testo, spinti dalla curiosità lo aprivano senza preoccupazioni: in realtà l'allegato era uno *script* (*.vbs*) che conteneva il codice dannoso.
  Non tutti i worm però necessitano di una "mano" per essere eseguiti: sfruttando le vulnerabilità (se non corrette tramite le opportune patch) di alcuni client di posta elettronica (due su tutti *Outlook* ed *Outlook Express*) che interpretano non correttamente alcuni tipi di comandi a cui vengono sottoposti, alcuni worm riescono ad autoeseguirsi anche nel momento in cui viene visualizzata solamente *l'anteprima* del messaggio, senza che ne venga effettuata l'apertura (come *BugBear*, *Wallon* e molti altri).
  Cosa succede quando viene eseguito il codice maligno? Dopo aver eseguito l'eventuale payload, il worm si attiva subito per replicarsi: cerca tutti gli indirizzi di posta elettronica memorizzati nel sistema (verificando i file che li potrebbero contenere al loro interno, come *.wab*, *.msg*, *.eml*, *.doc*, *.txt*, *.html*, ecc.), quindi si autospedisce loro tramite allegato di posta elettronica (nella speranza che la vittima lo apra): il messaggio infetto di solito ha l'indirizzo del mittente falsificato (preso anche a caso tra quelli della vittima precedente) o nascosto.
- **Web**. I pericoli di contrarre un worm in questo caso possono provenire dai *download incontrollati* e dalle *vulnerabilità insite nel sistema operativo* (generalmente quelli Microsoft, da Windows 2000 in poi).
  E' risaputo ormai che aprire programmi e/o archivi scaricati dalla rete (specialmente se da siti poco raccomandabili) senza averli sottoposti preventivamente ad un adeguato controllo antivirus è un'operazione estremamente rischiosa e in alcuni casi fatale al proprio pc.
  Meno risaputa, a giudicare dall'incredibile numero di computer colpiti in tutto il mondo, sembra essere invece la gravità di due falle (se non adeguatamente corrette) scoperte nei sistemi operativi Microsoft, a partire da Windows 2000. Chi non ha mai sentito parlare di *Blaster* o del recentissimo *Sasser*? Ebbene, questi due worms, per insediarsi in un computer, sfruttano due altrettante vulnerabilità del sistema operativo: il primo un bug nell'**RPC** (**R**emote **P**rocedure **C**all, un protocollo usato da Windows), mentre il secondo una falla dell'**Lsass** (**L**ocal **S**ecurity **A**utorithy **S**ubsystem **S**ervice, un servizio che si occupa della gestione delle password al login di un utente), tra l'altro documentata già da tempo. Il payload ed il modo in cui si propagano i due worms sono simili: entrambi provvedono a mandare in crash ripetutamente ed a distanza di pochi minuti i relativi servizi vulnerabili (RPC e Lsass) causando l'arresto ed il riavvio forzato del sistema operativo; Blaster inoltre tenta di rendere inaccessibile il sito *windowsupdate.com* da dove è possibile scaricare la patch risolutiva della vulnerabilità RPC, mentre Sasser è addirittura in grado di fungere da backdoor. Se è attiva una connessione ad Internet, per propagarsi i due worms generano degli **indirizzi IP** casuali (un indirizzo IP è una stringa numerica che identifica un computer connesso alla rete), tentando quindi di sferrare l'attacco verso quegli IP: se a rispondere è una macchina vulnerabile, essa viene immediatamente infettata.

Trojans

I *trojans* (detti anche *cavalli di Troia*) sono un altro tipo di malware che svolge delle funzioni diverse rispetto ai tipi descritti precedentemente. Sono subdoli e molto insidiosi: il loro nome deriva infatti dal trucco usato dagli Achei per conquistare la città di Troia (il famoso cavallo di legno).

Un trojan è solitamente un normalissimo programma, che fa credere all'utente di compiere funzioni utili. Una volta lanciato, il programma può effettivamente svolgere quelle funzioni oppure no; il punto centrale però è che esso svolge un'azione secondaria, che l'utente sicuramente non approverebbe: questa azione spesso consiste nell'installazione nel computer vittima di una *backdoor*, oppure nel reperire, manomettere o modificare i dati o le informazioni contenuti nell'hard disk, nonché di danneggiarli.

A causa della diffusione dei programmi peer-to-peer (tipo WinMX, Kazaa, ecc.), il pericolo di venire infettati da un trojan è notevolmente aumentato, in quanto il download di file eseguibili da queste fonti spesso non sicure è un'operazione molto a rischio.

Come i worms, inoltre, anche i trojans usano come altro veicolo di diffusione gli allegati di posta elettronica, usando lo stesso loro metodo. Non sempre però il messaggio e-mail può provenire da un mittente sconosciuto: qualche persona che ha il vostro indirizzo e-mail, interessata a "mettere in naso" o a compiere altre operazioni dannose ed a vostra insaputa nel vostro computer, potrebbe infatti spedirvi un trojan, magari specificando che il programma in allegato è un'utilità di sistema o comunque un programma benigno, invitandovi a provarlo.

Backdoors

Spesso si tende ad associare i trojans alle *backdoors*: in realtà questa associazione è **errata**. Il trojan compie delle azioni all'insaputa dell'utente, ed è concepito per creare danni o per attivare a sua volta altre applicazioni; la backdoor (alla lettera in inglese *porta sul retro*) è un programma dannoso insediato nel computer vittima e spesso nascosto o camuffato, il cui scopo è quello di aprire un "corridoio" con l'esterno sfruttabile da chi sa che su quella macchina è installata la backdoor.

Ma come funziona e cosa può fare in genere una backdoor? Vediamo di descriverlo di seguito.

Una backdoor è generalmente composta da tre parti: il **server**, il **client** e lo **scanner** (che può anche essere integrato nel client). Il modulo server è quello che deve essere eseguito e quindi installato nel computer vittima, per aprire una determinata porta e renderlo quindi vulnerabile ad attacchi dall'esterno. Colui il quale ha intenzione di portare l'attacco usa in primo luogo lo scanner per effettuare un controllo su un determinato *range* (gruppo) di indirizzi IP, per ognuno dei quali viene effettuata una richiesta di accesso basata sulla porta in cui è in "ascolto" il server. Nel momento in cui un IP "risponde", significa che nella macchina associata a quell'indirizzo è in esecuzione il server. A questo punto, basta inserire nel client l'IP che ha risposto per accedere senza alcuna autorizzazione al computer vittima.

Abbiamo dunque visto che per penetrare in un sistema tramite backdoor è necessario un indirizzo IP. Come molti di voi ben sanno, gli indirizzi IP nella stragrande maggioranza dei casi sono *dinamici*: essi variano cioè ad ogni nuova connessione alla rete. Una volta perso il collegamento client/server a causa della disconnessione da Internet della vittima sarebbe quindi necessario ricontrollare il range di IP per ritrovarla in un secondo momento. Molte tra le backdoor superano questo problema: possono essere infatti settate per *notificare*, ad ogni nuova connessione, il relativo indirizzo IP. La notifica può avvenire tramite e-mail, IRC o ICQ.

Una volta stabilito il collegamento client/server, le backdoor consentono di **prendere il totale controllo della macchina**. Esistono infatti delle opzioni che permettono di svolgere azioni di disturbo che mandano nel panico la vittima (apertura e chiusura cassetto CD-ROM, blocco del mouse o della tastiera, spegnimento dello schermo o rovesciamento delle immagini e molto altro), ma anche altre che consentono di recuperare *informazioni personali*, quali le password memorizzate (casella e-mail, chat, ecc.) nonché di esplorare il contenuto dell'hard disk, scaricare i file in esso contenuti o offendo anche la possibilità di formattarlo!

Molte backdoor consentono inoltre di installare un ulteriore strumento maligno: un **keylogger**. Si tratta di una parte del server preposta a monitorare i tasti premuti tramite tastiera e di salvarli in un apposito file sul disco fisso. Questo file è consultabile attraverso il client o il suo contenuto può venire inviato dal server mediante posta elettronica nel momento in cui viene stabilita una connessione ad Internet. E' facile intuire quindi come sia semplice scovare anche in questo modo password, numeri di carte di credito, nonché altre informazioni strettamente personali della vittima.

Per poter svolgere il suo compito, il server della backdoor viene generalmente eseguito ad ogni avvio del sistema operativo (usando diverse modalità che verranno descritte in seguito). A differenza delle altre applicazioni, spesso fa in modo di non comparire nella lista dei *processi attivi* (*task*) per non destare sospetti.

Per concludere, *Back Orifice*, *NetBus* e *SubSeven* sono tra le backdoors più diffuse e conosciute.

Come difendersi

Il miglior strumento di difesa contro virus e malware in generale è ovviamente un buon software **antivirus** che deve essere costantemente **aggiornato** (almeno un paio di volte al mese). Ogni giorno infatti "nascono" decine e decine di nuovi virus. Essenziale è la sua presenza nel caso dei virus in senso stretto, poiché esso è in grado di ripulire i files infetti (anche se è sempre preferibile reinstallare gli originali). Non meno fondamentale è la sua funzione (quasi sempre presente) di scansione delle e-mail in arrivo.

Unitamente all'antivirus è di estrema importanza dotarsi anche di un software **firewall**, preposto al controllo del traffico Internet in entrata ed in uscita dal proprio pc, nonché alla respinta di eventuali attacchi provenienti dall'esterno. Il firewall infatti avvisa immediatamente l'utente circa le applicazioni che tentano di accedere alla rete, offrendo la possibilità di permettere o bloccare il tentativo (si pensi all'utilità nel caso di una backdoor presente nel proprio sistema...); inoltre rende *invisibili* (*stealth*) le porte aperte dal proprio sistema durante la connessione, rendendo così invisibile anche il computer sulla rete. L'esempio più pratico è dato proprio dal worm Blaster, di cui abbiamo parlato in precedenza. Per infettare un computer esso infatti effettua l'attacco sulla porta 135, quella utilizzata dal protocollo RPC: se nel sistema è presente un firewall, anche se si è sprovvisti della relativa patch il worm non riuscirà a penetrare nel computer in quanto non riceverà alcuna risposta dalla porta (resa *stealth* dal firewall).
Ad ogni modo, l'installazione di un firewall **non deve sostituire** la presenza delle patch risolutive delle vulnerabilità del sistema operativo.

Oltre ad antivirus e firewall, ci sono altri modi per difendersi dalle minacce provenienti dalla rete. Quando si riceve un messaggio e-mail "strano" (con ad esempio l'oggetto in inglese ed allegati) proveniente da un mittente sconosciuto, è bene cancellarlo, poiché nella stragrande maggioranza dei casi si tratta di un worm. Va comunque prestata la massima attenzione al mittente del messaggio poiché i worms più recenti inseriscono come oggetto anche parole in italiano. In generale comunque è bene diffidare dalle e-mail che **invitano espressamente ad aprire gli allegati**.
Nel caso si riceva un'e-mail da un mittente conosciuto, è buona norma accertarsi che questa persona l'abbia effettivamente spedita; inoltre è sempre bene controllare che nel testo del messaggio si parli espressamente di eventuali allegati e che ne venga fornita una sommaria descrizione.

Per evitare di venire in qualche modo imbrogliati dalle doppie estensioni dei files (vedi *Loveletter*), il consiglio è quello di settare il sistema operativo in modo che visualizzi le *estensioni per i tipi di file conosciuti*. Ciò in genere si effettua aprendo una qualsiasi cartella, cliccando su *Strumenti*, *Opzioni* e disabilitando l'opzione che nasconde le estensioni.

Ultima, ma non meno importante, è la raccomandazione di effettuare periodicamente il **WindowsUpdate** per mantenere sempre aggiornato il proprio sistema con le relative patch di sicurezza.

Cosa fare invece quando si sospetta che nel proprio sistema si sia annidato un virus?
Per quanto riguarda i virus in senso stretto, è bene affidarsi all'antivirus oppure sostituire i files infetti con una copia degli originali.
Nel caso di altri malware, spesso, è possibile intervenire anche manualmente. Worms, trojans e backdoors come abbiamo visto non hanno bisogno di un "ospite" ma sono files a sé stanti. Per essere sempre attivi essi devono necessariamente eseguirsi ogni volta che il sistema operativo viene avviato.
L'*autostart* (*autocaricamento*) in Windows avviene generalmente attraverso specifiche *chiavi* del registro di sistema, mediante la cartella *Esecuzione automatica* oppure, per le vecchie versioni, anche tramite i files di sistema *system.ini* e *win.ini*.

- **Chiavi del registro di sistema**. Una volta aperto il registro di sistema (c:\windows*regedit.exe*), le principali chiavi da monitorare per la presenza di qualcosa di strano sono le seguenti:
  `[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]`
  `[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]`
  `[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]`
  `[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]`
  `[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]`
  `[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]`
  `[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices]`
  sul pannello di destra verranno visualizzate le applicazioni che vengono eseguite all'avvio del sistema operativo.
- **Cartella Esecuzione automatica**. I *link* (*collegamenti*) presenti all'interno della cartella `Avvio/Start`, `Programmi`, `Esecuzione automatica` (e quindi i programmi ad essi associati) vengono eseguiti ad ogni avvio del sistema operativo.

- **Files di sistema**. Entrambi reperibili nella cartella *c:\windows*, i files di sistema *system.ini* e *win.ini* possono contenere informazioni relative ai programmi lanciati all'avvio del sistema operativo.
  Nel caso del *system.ini* va controllata la riga `shell=` contenuta all'interno della sezione `[boot]`; nel caso del *win.ini* ,ad essere visionate devono essere le righe `load=` o `run=` eventualmente presenti nella sezione `[windows]`. In entrambi i casi i programmi specificati dopo le righe riportate vengono eseguiti ogni volta che si avvia il pc.

Da segnalare, per il controllo delle suddette voci di autostart, un programma totalmente freeware denominato *Autoruns* scaricabile da http://www.sysinternals.com/files/autoruns.zip

Meno conosciute, e per questo motivo utilizzate soprattutto da molte backdoor, sono invece le chiavi di registro che, se opportunamente modificate, consentono l'esecuzione di un programma nel momento in cui ne viene eseguito un altro. Queste chiavi sono:

```
[HKEY_CLASSES_ROOT\exefile\shell\open\command]
[HKEY_CLASSES_ROOT\comfile\shell\open\command]
[HKEY_CLASSES_ROOT\batfile\shell\open\command]
[HKEY_CLASSES_ROOT\htafile\Shell\Open\Command]
[HKEY_CLASSES_ROOT\piffile\shell\open\command]
[HKEY_LOCAL_MACHINE\Software\CLASSES\batfile\shell\open\command]
[HKEY_LOCAL_MACHINE\Software\CLASSES\comfile\shell\open\command]
[HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command]
[HKEY_LOCAL_MACHINE\Software\CLASSES\htafile\Shell\Open\Command]
[HKEY_LOCAL_MACHINE\Software\CLASSES\piffile\shell\open\command]
```

il valore della stringa predefinita di queste chiavi dovrebbe sempre essere `"%1" %*`. Se una o più tra queste stringhe dovesse risultare modificata in qualcosa come **`"programma.exe`** `%1" %*`, significa che quel *programma.exe* verrebbe lanciato ogniqualvolta verrebbe eseguito un file con l'estensione relativa alla chiave in cui la stringa è stata modificata (per esempio, se ad essere cambiata risulta la stringa contenuta nella chiave `[HKEY_CLASSES_ROOT\exefile\shell\open\command]`, l'avvio di un qualsiasi file con estensione *.exe* causerà anche l'esecuzione di *programma.exe*).
Considerando che all'avvio il sistema operativo deve avviare anche diversi programmi necessari al suo funzionamento, questo appena descritto è considerato come un metodo di *autostart*.

Link utili

Patch per la risoluzione della vulnerabilità sfruttata dal worm Blaster (KB828741)
http://www.microsoft.com/technet/security/bulletin/MS04-012.mspx

Patch per la risoluzione della vulnerabilità sfruttata dal worm Sasser (KB835732)
http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

Patch per la risoluzione delle vulnerabilità di Outlook Express
http://www.microsoft.com/technet/security/bulletin/MS03-014.mspx (Q330994)
http://www.microsoft.com/technet/security/bulletin/MS04-013.mspx (Q837009)

Osservatorio virus de IlSoftware.it
http://www.ilsoftware.it/av.asp

Tools di rimozione per i worm più diffusi
http://www.nod32.it
http://www.kaspersky.com/removaltools
http://securityresponse.symantec.com/avcenter/tools.list.html

Antivirus		**Firewall**	
NOD32	http://www.nod32.com	Outpost (v. 1.0 free)	http://www.agnitum.com
Kaspersky	http://www.kaspersky.com	Sygate	http://www.sygate.com
F-Secure	http://www.f-secure.com	ZoneAlarm	http://www.zonelabs.com
Norton Antivirus	http://www.symantec.com	Norton Personal Firewall	http://www.symantec.com
AVG (free)	http://www.grisoft.com	Tiny Firewall	http://www.tinysoftware.com
Avast! (free)	http://www.avast.com	Kerio	http://www.kerio.com