Virus e antivirus
Introduzione

Il termine **virus** in informatica indica una porzione di codice che ha la caratteristica di autoreplicarsi e inserire se stesso in *file* eseguibili preesistenti sul sistema.

Virus è in realtà una parola latina che significa veleno e che viene utilizzata comunemente in medicina per indicare microrganismi patogeni dell'uomo, degli animali, delle piante e dei batteri. Il virus biologico è un organismo parassita, privo di meccanismi enzimatici propri, che si sviluppa nelle cellule di altri organismi, utilizzando i meccanismi enzimatici di queste ultime. Una volta sviluppatosi nella cellula ospite, il virus si diffonde contagiando altri organismi.

Per analogia il nome virus è stato utilizzato per indicare un tipo di attacco alla sicurezza dei sistemi informatici, basato su un *software* che ha le seguenti caratteristiche:

- non esegue autonomamente ma necessita di un programma eseguibile ospite, che viene infettato, la cui esecuzione attiva il virus;
- si riproduce e si propaga infettando altri sistemi;
- si attiva ed esegue le attività per cui è stato implementato; raramente è innocuo, più spesso produce danni alla **sicurezza** ed in particolare all'integrità dei dati e alla disponibilità dei sistemi;
- è di piccole dimensioni rispetto al sistema che aggredisce.

Ciclo di vita

Il ciclo di vita di un **virus** è caratterizzato da tre attività fondamentali:

- **creazione** del virus: è il momento in cui il virus viene creato dal programmatore e immesso nei primi sistemi;
- **epidemia**: è il momento in cui il virus passa da un *computer* all'altro allargando il suo raggio d'azione;
- **disattivazione**: è il momento in cui il virus viene eliminato, ovvero viene rimosso da tutti i *computer*.

La fase in cui il virus si propaga è a sua volta scandita da diversi momenti:

- **infezione**: quando il virus individua un potenziale sistema ospite, verifica che questo non sia già infettato da una copia di sé e, nel caso sia libero, lo infetta. Il virus resta poi latente per un certo periodo in cui l'unica attività che effettua è tentare di replicare l'infezione, passando da un ospite all'altro;
- **attivazione**: al verificarsi di un certo evento, detto ***trigger***, il virus scatena l'azione vera e propria per la quale è stato progettato, che viene chiamata ***payload*** e in genere è distruttiva e mira alla cancellazione dei dati e all'indisponibilità del sistema in generale.

Anche la fase di disattivazione è articolata:

- **riconoscimento**: il virus viene identificato e viene riconosciuta la stringa identificativa che lo contraddistingue;
- **estirpazione**: utilizzando un antivirus, il virus viene rimosso completamente dal sistema.

Tipologie

I virus fanno parte di una famiglia di attacchi alla sicurezza nota come **malicious software** (*malware*) che comprende altri tipi di programmi caratterizzati dal fatto che si diffondono da un

computer all'altro con lo scopo di produrre danni ai sistemi.

In realtà i virus più recenti mescolano le caratteristiche di diversi tipi di *malware* con lo scopo di diventare più difficili da individuare e più efficaci nel diffondere l'infezione e in particolare spesso sono **virus** e **worm** ovvero *software* che hanno i medesimi meccanismi riproduttivi dei virus ma che utilizzano (come i *worm*) la rete per propagarsi. Questa caratteristica accomuna la maggior parte dei virus recenti poiché lo scambio di *file* (che è il meccanismo base per il propagarsi dell'infezione) avviene ormai prevalentemente attraverso la rete.

I virus possono essere classificati in base a diverse caratteristiche, tra cui la più significativa è l'ambiente attraverso cui si propaga l'infezione e si sviluppa il virus. Sono distinguibili in questa ottica diverse tipologie di virus:

- i **boot virus**, che infettano il *Boot Sector* o il *Master Boot Record* dei dischi in modo da essere caricati all'avvio del sistema;
- i **file virus**, che infettano, con modalità molto varie, i *file* eseguibili e utilizzano lo scambio di questi ultimi per propagare l'infezione;
- i **macrovirus**, che sono scritti in VBA (*Visual Basic for Application*) un linguaggio per la scrittura di macro negli ambienti applicativi *Office*;
- i ***network* virus**, che si diffondono sfruttando le **vulnerabilità** dei protocolli di Internet.

Boot virus

I **boot virus** si propagano inserendo una copia di se stessi nel **Boot Sector** dei dischetti o nel **Master Boot Record** del disco fisso. Una volta riavviato il *computer*, la componente del sistema operativo che si occupa del caricamento, il *bootstrap loader*, porta in memoria il *boot* virus e lo mette in esecuzione.

I *boot* virus sono tipicamente più complessi da realizzare dei *file* virus, perché devono entrare in azione prima che sia caricato il sistema operativo. Devono essere anche implementati utilizzando pochissima memoria in modo da consentire loro di salvarsi nel *Boot Sector* di un dischetto, che è di soli 512 *byte*. *Boot* virus più lunghi si spezzano in una prima parte che invade il *Boot Sector* (o il *Master Boot Record*) e che carica la seconda parte, e in una seconda parte che viene memorizzata in aree poco utilizzate del supporto di memoria di massa (per esempio l'ultima traccia del dischetto). Una volta in memoria, per replicarsi su altri dischetti, il *boot* virus deve intercettare le attività di lettura e scrittura del sistema operativo, facendo attenzione a non insospettire l'utente rallentando troppo le attività di accesso ai *floppy*.

Esempi noti di *boot* virus sono Brain, Ping Pong e Michelangelo [**The Probert E-Text Encyclopaedia**].

File virus

Sono ***file* virus** quei **virus** che utilizzano i *file* come mezzo di diffusione e le proprietà del *file system* per propagarsi. Dovendo entrare in esecuzione, scelgono come ospite un *file* eseguibile (di qualunque tipo, dai .COM alle DLL) che rimane apparentemente inalterato, ma che in realtà diviene pericoloso.

Quando l'utente o il sistema avviano il *file* eseguibile ospite, avviano anche il virus che viene caricato in memoria e inizia l'attività di propagazione. Per non farsi individuare immediatamente il virus lascia eseguire anche il *file* ospite in modo che l'utente non percepisca l'inizio dell'infezione. I meccanismi con cui i *file* virus si agganciano al programma ospite sono innumerevoli e vanno dalla sovrascrittura del codice dell'ospite alla creazione di eseguibili ombra che mascherano l'esecuzione del virus. Un semplice metodo di contraffazione usato da alcuni *file* virus per DOS consisteva nel

scegliere un *file* .EXE e creare un *file* .COM con lo stesso nome. Il nuovo *file* conteneva le istruzioni per il caricamento del virus in memoria e, di seguito, l'esecuzione del *file* .EXE. Il sistema operativo, rispondeva ai comandi digitati dall'utente eseguendo il *file* con estensione .COM (primo tipo di *file* nella sequenza di esecuzione).

Macrovirus

I **macrovirus** sono i virus più diffusi attualmente e sono scritti per eseguire all'interno di applicazioni molto diffuse (tipicamente applicazioni di *office automation* o *client* Internet per la posta e per il *Web*). Sono dunque incorporati in *file* apparentemente innocui, come i *file* .DOC, come se fossero *routine* interne utilizzate dall'autore per calcoli specifici. Il linguaggio utilizzato per le macro viene usato per scrivere il virus.

Poiché gli stessi applicativi sono basati sull'esecuzione di macro predefinite, è relativamente facile scrivere un virus che ha alte probabilità di entrare in esecuzione e dunque di divenire attivo. Per esempio il virus può attivarsi in corrispondenza della macro che viene lanciata all'apertura di un *file*. Questo tipo di virus ha avuto recentemente ampissima diffusione ed esistono numerosi macrovirus che hanno provocato danni su larga scala.

Il problema dei macrovirus è stato in passato sottovalutato e solo dopo diverse epidemie devastanti sono state attivate alcune forme di prevenzione minime, quale la scansione dei *file* documento da parte degli antivirus e la possibilità di impedire l'esecuzione delle macro all'interno delle applicazioni.

Virus polimorfi

Gli **antivirus** basano il riconoscimento dei **virus**, necessario alla loro rimozione, su un codice identificativo univoco che è contenuto nel virus e che è detto **impronta virale**. Un virus diventa quindi particolarmente difficile da individuare se riesce a mascherare la propria impronta ovvero a renderla diversa ogni volta che si replica su un nuovo ospite.

L'impronta virale è costituita da codice eseguibile del virus per cui non può essere tutta alterata per mimetizzare il *software* nocivo. Per nasconderla si può invece **crittografarla** con una funzione che ha alcune caratteristiche casuali e poi replicare il codice del virus criptato e la funzione per decriptarlo.

Questo tipo di virus è detto **virus polimorfo**, poiché contiene un sistema (il *polymorphic engine*) che gestisce le chiavi e le funzioni di cifratura e decifratura. Un virus polimorfo è quindi costituito dal codice del virus, dal *polymorphic engine* (entrambi cifrati) e dalla funzione per decifrarli. Quando il virus polimorfo viene caricato, la funzione di decifratura decripta il virus e il *polymorphic engine*. Il virus lancia poi il *polymorphic engine* ogni volta che vuole ottenere la coppia di funzioni (cifratura, decifratura) che serve a generare una nuova copia mutata di se stesso.

Epidemie

I **virus** maggiormente invasivi e dannosi sono in realtà combinazioni di molte delle tecniche fin qui esposte, di altre tecniche che non sono state trattate per brevità e a queste si aggiungono anche metodologie proprie di altri tipi di **malicious software**, come i **worm** e i **cavalli di Troia**.

Mescolare le diverse tecniche consente al virus:

- di diffondersi meglio, utilizzando più modalità di trasmissione ovvero di trovare un numero maggiore di potenziali ospiti. In questo caso il virus aumenta la velocità di diffusione e di conseguenza la dimensione. Questo tipo di virus è indicato come **virus multipartito**.

- Di nascondersi meglio, utilizzando più tecniche di mascheramento e meccanismi innovativi. In questo caso il virus aumenta la dimensione dell'epidemia garantendosi un tempo più lungo per essere scoperto e quindi per essere rimosso.

Entrambi questi due fattori determinano quanto vasta sarà l'epidemia del virus. Per contro, per contrastare le epidemie, è cruciale il tempo che occorre alla comunità per individuare il virus e comprendere quali sono i meccanismi di rimozione. A questo scopo vengono mantenuti elenchi aggiornati dei virus e delle loro impronte. Alcuni di questi elenchi costituiscono, di fatto, un osservatorio sull'evolversi delle epidemie [**Wild List**].

La diffusione dei macrovirus

In tempi recenti le epidemie più vaste e dannose sono state prodotte da **macrovirus**, che attualmente sono i virus più diffusi e hanno surclassato le altre tipologie di **virus**.

Diversi sono i motivi che hanno reso superati i *boot* virus e i *file* virus rispetto ai macrovirus. In primo luogo va citato il fatto che i macrovirus hanno un maggior numero di potenziali vittime, poiché sfruttano applicativi diffusissimi e disponibili anche su più piattaforme. A questo fattore va aggiunto il fatto che la maggior parte dei macrovirus sfruttano i servizi Internet (la posta o il *Web*) per infettare nuovi ospiti. La combinazione di questi due fattori rende le epidemie fulminee e devastanti poiché ogni ospite infettato ha il mezzo (la rete) per contagiare moltissimi altri *computer* (tutti in grado di far funzionare la macro che ospita il virus).

Infine va ricordato che un macrovirus viene scritto con un linguaggio di alto livello come *Visual Basic for Application*, che è alla portata di moltissimi programmatori, mentre l'*assembler* che veniva usato per le altre tipologie di virus richiedeva programmatori più esperti. Vediamo nel seguito due macrovirus (**Melissa** e **Iloveyou**) che hanno segnato la storia recente dei virus.

Melissa

Un virus innovativo dal punto di vista dei meccanismi di diffusione è stato **Melissa** (1999) un **macrovirus** che sfruttava diverse vulnerabilità delle applicazioni di produttività personale della *Microsoft*, per diffondersi attraverso la rete. Si tratta di un **worm** scritto in VBA (*Visual Basic for Application*) incorporato in una macro contenuta a sua volta in *file* .DOC.

Melissa opera nel modo seguente:

- arriva un messaggio contenente l'allegato (LIST.DOC) e l'utente lo apre, mandando in esecuzione Melissa;
- il virus si propaga spedendo automaticamente via *email* una copia del *file* .DOC a 50 indirizzi scelti tra quelli contenuti nella rubrica dell'utente colpito;
- una volta propagatosi, il virus diventa nocivo modificando i documenti dell'utente o spedendo sue informazioni personali.

La tecnica di propagazione usata è tale da ingannare l'utente che vede arrivare il messaggio da un suo conoscente e quindi non utilizza particolare prudenza e lo apre.

Nella prima versione la *email* riferiva all'*attach* spiegando che conteneva una lista di *password* per accedere a siti pornografici e, per assicurarsi un efficace inizio dell'infezione, l'autore del virus lo inserì in un *newsgroup* su tematiche sessuali.

Il virus è multipiattaforma, cioé è in grado di infettare utenti che utilizzano sistemi operativi diversi purché siano presenti *Word*, *Outlook* e una connessione a Internet.

Iloveyou

Iloveyou (2000) è un macrovirus *worm* molto famoso che è stato citato dai telegiornali di tutto il mondo che è riuscito a propagare la sua infezione anche in contesti importanti. Le vittime illustri di *Iloveyou* vanno dagli uffici governativi di diverse nazioni (come il parlamento inglese e gli uffici del Pentagono, della Cia e della *Federal Reserve* americana) ad aziende di rilevanza mondiale (come Vodafone o *Time Warner*).

Per diffondersi *Iloveyou* utilizza lo stesso metodo di **Melissa**, riproduce un *attach* e lo invia ai conoscenti. A differenza di Melissa, che sceglie 50 indirizzi, *Iloveyou* spedisce se stesso a tutti gli indirizzi della rubrica e in questo modo la sua propagazione risulta molto più veloce e capillare. Un'altra differenza da Melissa è nell'azione di *Iloveyou* che è molto più distruttivo: è riuscito a produrre danni per diversi miliardi di dollari.

Iloveyou è scritto in *VBScript* (*Visual Basic Script*) per *Windows Scripting Host* (WSH) e dunque riesce a infettare solo *computer* che hanno installato WSH. Ma WSH viene installato automaticamente in *Windows* 98 e *Windows* 2000 ed è presente in tutte le piattaforme con installato *Internet Explorer* 5.

La diffusione e i danni derivanti da *Iloveyou* hanno spinto *Microsoft* a produrre apposite patch per *Outlook* in modo da limitarne la vulnerabilità.

Nimda

Nimda è un **virus worm multipartito**, scritto in Visual C++, che ha provocato una delle infezioni più diffuse del 2001. Sfrutta diverse vulnerabilità dei sistemi *Microsoft*, infettando molte piattaforme, da *Windows* 95 e *Windows* ME a *Windows* 2000.

Durante l'infezione Nimda effettua numerosi interventi sui *file* del sistema vittima con l'obiettivo di saturare lo spazio fisico dei dischi e di rendere indisponibili le risorse (**denial of service**). Ma la caratteristica più significativa di Nimda è che il virus utilizza contemporaneamente numerosi canali di diffusione per assicurare la propagazione dell'infezione. In particolare i meccanismi di propagazione di Nimda sono:

- ***email***: l'invio di *email* contenenti il virus; gli indirizzi di posta elettronica a cui spedire Nimda sono ottenuti dai *file* .HTM e .HTML memorizzati sul *computer* ospite. Al messaggio, in formato HTML, è allegato un *file* README.EXE, che attiva il virus;
- ***Web***: attacco ai *server* HTTP *Internet Information Server* (IIS): sfruttando le **vulnerabilità** del *software* o possibili *backdoor* lasciate da infezioni virali precedenti, Nimda attacca le macchine su cui sono installati servizi *Web* basati su IIS;
- **LAN**: la propagazione attraverso le risorse condivise della LAN. La diffusione del virus attraverso la LAN avviene con diversi meccanismi, tra i quali la scansione della rete sulla porta HTTP/80 e la creazione di condivisioni dei *drive* locali.

La combinazione dei sistemi di diffusione ha reso l'epidemia di Nimda molto rapida e capillare. Nimda si diffonde infatti molto rapidamente su Internet, attraverso un meccanismo di scelta degli indirizzi bersaglio che passa rapidamente da una comunità di utenti all'altra. Una volta penetrato su un sistema della LAN, Nimda tenta poi di diffondersi sulle stazioni vicine per cercare di compromettere l'intero sottosistema.

Difendersi

Secondo *Computer Economics* gli attacchi da **virus** hanno causato danni nel 2001 per 13,2 miliardi di dollari. La spesa è in forte riduzione rispetto al 2000, anno in cui si è diffuso il virus

complessivamente più dannoso a tutto il 2001, **Iloveyou** che ha prodotto da solo danni per 8.75 miliardi di dollari.

La migliore difesa contro i virus è ovviamente la **prevenzione** che va affrontata sia in termini tecnologici che comportamentali. In particolare per prevenire i virus occorre:

- evitare comportamenti rischiosi, quali scambio e *download* di *file* sospetti, installazione di pacchetti non licenziati, apertura degli *attach*. Quest'ultima precauzione è molto importante per difendersi dai **macrovirus** poiché se l'allegato non viene eseguito, il virus rimane latente. Aprire i messaggi di posta elettronica può diventare causa di infezione solo se il *client* di posta è impostato per eseguire gli allegati in automatico. Per questo motivo è opportuno disabilitare l'anteprima dei messaggi.
- Aggiornare il *software* in modo da ridurre le **vulnerabilità** al minimo. L'attacco dei virus viene infatti condotto sfruttando errori nel *software* o nei protocolli e tutte le azioni volte a ridurre il numero di errori presenti nei programmi (come per esempio l'installazione delle *patch*) sono forti forme di prevenzione dei virus.
- Utilizzare un *software* **antivirus** ovvero un *software* in grado di identificare i virus e rimuoverli prima che entrino in azione. Per rilevarli l'antivirus cerca all'interno della memoria (centrale e di massa) l'impronta identificativa del virus. Per questo motivo l'antivirus va tenuto costantemente aggiornato.
- Effettuare comunque un *backup* periodico dei dati in modo da poter ripristinare efficacemente il sistema anche in caso di danni.

Antivirus

Per difendersi dai virus occorre dotarsi di un *software* antivirus che si occupi di:

- prevenire l'infezione, ovvero rilevare il virus prima che abbia realmente infettato il sistema. L'antivirus può scandire a questo scopo i *file* scaricati da Internet, gli *attach* delle *email*, i supporti di memoria di massa removibili. Se l'antivirus entra in funzione in questa fase, il virus non ha ancora avuto modo di riprodursi e di agire per cui non è necessaria una fase di recupero ma è sufficiente la rimozione del codice virale.
- Recuperare dopo una infezione. Il virus ha già infettato l'ospite e in alcuni casi ha anche prodotto danni. L'antivirus non si può limitare a rilevarlo ma deve anche mettere in atto un insieme di meccaniche che consentano di estirparlo, ovvero rimuoverlo dal sistema ospite.

Le verifiche del *software* antivirus vengono tipicamente fatte in via automatica:

- all'avvio del sistema, verificando almeno il *Master Boot Record* e i *file* di sistema.
- Periodicamente, scandendo la memoria centrale.
- Ogniqualvolta si effettua una operazione rischiosa (come l'apertura di un **attach** di posta elettronica, l'inserimento di un dischetto nel *drive*, il *download* di un *file*), verificando i *file* potenzialmente pericolosi.

Le attività di recupero sono invece avviate automaticamente ogniqualvolta un virus attivo viene intercettato.

Rilevamento

Le attività di rilevamento effettuate dagli **antivirus** hanno lo scopo di verificare se il *computer* è o no affetto da un **virus** e, se sì, da quale.

L'antivirus cerca il virus, verificando la presenza sulla macchina dell'**impronta virale**, che identifica il virus univocamente e che consente dunque di decidere quali politiche di rimozione applicare.

L'antivirus deve essere aggiornato continuamente in modo da avere un insieme di impronte da ricercare il più completo possibile.

L'attività di rilevamento viene fatta con diverse tecniche:

- ***scanning***, ovvero ricerca dell'impronta virale all'interno della memoria, centrale e di massa. Tipicamente l'antivirus verifica spesso la memoria centrale e solo su richiesta i dischi. Lo *scanning* può utilizzare anche tecniche euristiche per individuare virus la cui impronta non sia ancora censita nell'insieme delle sequenze da cercare;
- **monitoraggio** delle attività pericolose o sospette, come per esempio la scrittura in alcune *directory* o di alcuni tipi di *file*;
- ***detection***, ovvero meccanismi di verifica dell'integrità dei dati che calcolano periodicamente il *checksum* dei *file* critici e rilevano così eventuali modifiche indesiderate.

I meccanismi euristici inseriti nelle versioni più efficaci degli antivirus possono scambiare per impronte virali sequenze di *byte* del tutto innocue, evidenziando dunque un **falso positivo** ovvero un caso in cui una porzione di codice o di dati qualunque viene scambiata per virus. Tutte le rilevazioni di potenziali nuovi virus vengono solitamente comunicate dal *software* antivirus al suo produttore che risponde entro breve all'utente, sia in caso di falso positivo che in caso di nuovo virus appena identificato.

Ripristino

La fase successiva al rilevamento di un virus all'interno di un sistema è quella del ripristino, nella quale si cerca di riportare il sistema a uno stato antecedente l'infezione. In fase di ripristino il *software* antivirus deve:

- rimuovere il virus dalla memoria e disattivarlo. Questa operazione è particolarmente critica perché essendo il virus stesso in esecuzione è possibile che contrasti l'azione dell'antivirus. In particolare i virus spesso intercettano parte delle chiamate al sistema operativo.
- Rimuovere il virus dalla memoria di massa, ripristinando il contenuto del disco, sia dei *file* che del *Master Boot Record*, che delle FAT. In particolare il virus deve essere rimosso da tutti i *file* infetti cercando di invertire la procedura invasiva con cui si è replicato. Non sempre è possibile una rimozione indolore e in alcuni casi i *file* infetti hanno perso il loro contenuto originario che non è quindi più ripristinabile.
- Recuperare dai danni, ovvero ripristinare completamente lo stato del *computer* prima che avvenisse l'infezione.

Il recupero completo del sistema dipende dal tipo di aggressione effettuata dal virus e dal tempo che il virus ha avuto per danneggiare il sistema. Per garantirsi la possibilità di un completo ripristino non ci si può affidare esclusivamente allo *scanning* dell'antivirus ma occorre:

- creare i dischetti di emergenza da utilizzare in caso di ripristino del sistema;
- effettuare molto spesso un *backup* dei dati per avere a disposizione all'occorrenza una copia aggiornata degli stessi da utilizzare durante il ripristino.

Antivirus: licenze

Esistono numerosi *software* antivirus che offrono un insieme di funzionalità di base comuni.

Alcuni *software* sono *free*, ovvero completamente gratuiti, ma la maggioranza dei *software* antivirus prevede l'acquisto della **licenza d'uso**. La gran parte dei produttori concede in uso gratuito il *software* in prova per un breve periodo (*shareware* o *evaluation licence*).

Le politiche dei prezzi sono molto variabili, ma solitamente sono previste riduzioni per:

- licenze multiple.
- Licenze *educational*.
- Aggiornamenti di *software* già licenziati o allungamento della durata della licenza.
- Aumento del numero delle licenze in possesso.

Sono previste due tipologie di aggiornamento: l'aggiornamento delle impronte virali, che è gratuito per tutta la durata del contratto, e l'aggiornamento del *software* antivirus (che migliora periodicamente in termini di efficacia). Molti fornitori prevedono licenze con scadenza temporale per cui tutto il pacchetto, compresi gli aggiornamenti delle versioni dell'antivirus, risulta gratuito per il periodo di validità del contratto. In alcuni casi sono disponibili anche licenze perenni il cui contratto prevede un costo iniziale maggiore e un costo annuale minimo per il mantenimento della licenza.

Molti fornitori offrono anche un contratto di assistenza tecnica, attraverso il quale offrono supporto nel momento della rimozione dei virus. Forme di assistenza vengono date anche via *email* e via *Web*, offrendo informazioni sui nuovi virus, sulle modalità di rimozione e su altre problematiche correlate.

Antivirus: prodotti

Esistono numerosi *software* antivirus che offrono un insieme di funzionalità di base comuni.

Di seguito è riportato un elenco dei più diffusi *software* antivirus con i rispettivi siti:

- *Norton Antivirus* della *Symantec*, http://www.symantec.com/
- *McAfee Viruscan* della *Network Associates*, http://www.mcafee.com
- *Panda Antivirus* della *Panda software*, http://www.pandasoftware.com/
- *PC-Cilling* della *Trend Micro Inc.*, http://www.trendmicro.com
- *F-Prot* della *Frisk software International*, http://www.f-prot.com
- *F-Secure Anti-Virus* della *F-Secure*, http://www.f-secure.com
- *AVG Antivirus* distribuzione *free* della *Grisoft Inc.*, http://www.grisoft.com/
- *Inoculate* della *Computer Associate* http://www.cai.com
- *Esafe* della *Aladdin*, http://www.esafe.com

Funzionalità aggiuntive

I prodotti di **antivirus**, oltre a proteggere le macchine *client*, possono offrire diverse tipologie di funzionalità supplementari:

- possono assicurare la protezione dal lato ***server***, ovvero proteggere *file server* e *print server*. I *server* sono infatti maggiormente vulnerabili in quanto fornitori di servizi e i normali antivirus realizzati per stazioni *client* non riescono a proteggere questo tipo di piattaforme in modo adeguato.
- Possono assicurare, in modo **centralizzato** la protezione dei *client*, consentendo la gestione unificata delle *policy* antivirus e degli aggiornamenti. La protezione dei *client* può avvenire via *Web* e non ed essere completamente trasparente all'utente. Questa funzionalità consente all'amministratore di installare, aggiornare e gestire gli antivirus attraverso un unico sistema integrato senza dover effettuare queste attività da ciascuna postazione *client*. Questo tipo di antivirus offre tipicamente una interfaccia grafica per il controllo del sistema, che tra l'altro produce report sugli attacchi subiti.
- Possono proteggere la **posta** elettronica, agendo sui *server*. Questo tipo di *software* controlla la presenza di virus su tutti i messaggi in transito sul *server* di posta elettronica e in questo modo previene la diffusione dei virus spediti assieme alla *email*, rimuovendoli prima che l'utente

possa inavvertitamente attivarli.
- Possono agire direttamente sui protocolli (HTTP, FTP e SMTP) rimuovendo il virus mentre transita sulla rete. Anche in questo caso, il virus non raggiunge l'utente finale e quindi non si rischia un'attivazione involontaria.
- Possono integrare le funzionalità di un **firewall**, offrendosi come piattaforma per la gestione integrata della sicurezza del sistema.

Conclusioni

Scopo di questo approfondimento è stato quello di affrontare le tematiche essenziali relative ai *computer* virus, introducendo le principali tipologie di virus, con alcuni casi specifici, e di antivirus. L'argomento è di importanza cruciale sia per affrontare in modo proattivo le problematiche di sicurezza dei dati sia, in modo più generale, per cercare di prevenire i danni al sistema. La difesa dai virus deve essere affrontata sia attraverso la conoscenza del problema dal punto di vista tecnico, sia attraverso aspetti organizzativi e comportamenti prudenti. Nessuna delle due strategie, da sola, è completamente efficace.

La principale tecnologia di difesa dai virus, l'antivirus, è un supporto ormai indispensabile sia per la prevenzione dell'infezione, che per la sua rimozione e per il successivo ripristino dei sistemi. Esistono numerosi *software* che offrono la possibilità di proteggere le postazioni *client* in modo efficace. In sistemi di media complessità in cui sono presenti *server*, servizi di posta o anche solo un numero elevato di PC deve essere valutata l'opportunità di acquisto di *software* più evoluti che proteggano le piattaforme *server* e che offrano supporto alla gestione degli aggiornamenti.

I **riferimenti bibliografici** *on line* consentono di svolgere autonomamente ulteriori attività di approfondimento, sia su tematiche generali che su aspetti tecnici specifici.