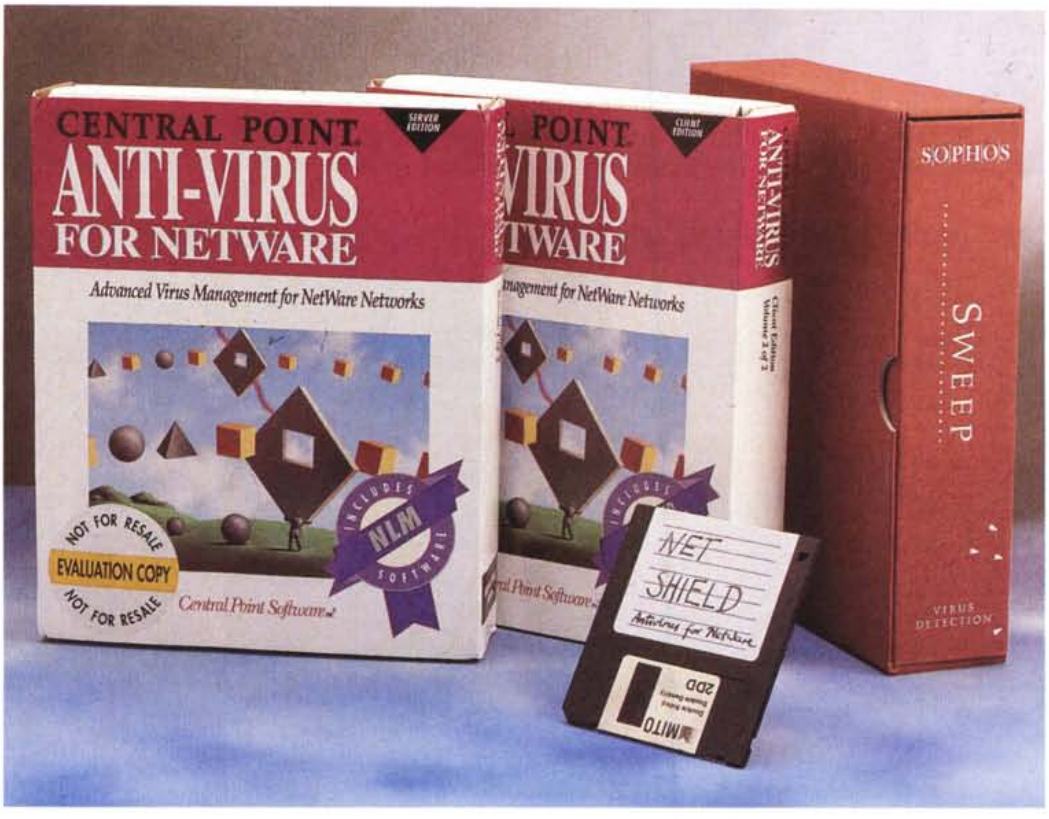
Come funzionano gli antivirus

Per difendersi dai virus sono sufficienti gli strumenti che mette a disposizione il sistema operativo. In pratica però è sempre meglio servirsi di uno o più programmi costruiti appositamente. Vediamo come districarsi nel labirinto e quali criteri consentono di scegliere i migliori programmi

di Stefano Toria



A caccia di virus

Un virus è un pezzo di software come qualsiasi altro. Pertanto dovrà consistere in una sequenza di istruzioni codificate nel linguaggio binario del microprocessore, registrate su un supporto in modo da essere pronte per il trasferimento in memoria e l'esecuzione.

Così come le istruzioni che compongono il virus possono essere lette per l'esecuzione, possono essere lette anche per analizzarle. In particolare è possibile stabilire, in base a una serie di criteri che tra poco esamineremo, se sia probabile che un determinato programma contenga o costituisca un virus.

La foto segnaletica

Il metodo più semplice per trovare un virus consiste nel cercarne l'esatta immagine, ovvero una parte sufficientemente rappresentativa. Equivale a possedere la foto segnaletica di un criminale: è sufficiente distribuirla a tutte le questure, tutti gli uffici di polizia e le caserme dei carabinieri e il primo che lo vede lo arresta.

Il presupposto è di avere avuto per le mani, almeno per un attimo, il criminale in questione. Se lo si è potuto bloccare davanti a una macchina fotografica, per il tempo sufficiente a uno scatto, si potrà utilizzare la foto come il migliore mezzo identificativo. Lo stesso criterio vale per un virus: se se ne possiede un campione si può guardare a come è fatto e estrarne una sorta di foto segnaletica, una «firma». Si potrà affermare quindi che tutti i programmi che contengono la stessa firma contengono quel particolare virus. Se il lavoro di identificazione della firma è svolto bene la probabilità di errore è prossima allo zero. È sempre possibile che in luogo di un ricercato finisca in manette un suo sosia, ma non è molto probabile.

Quando i virus si contavano a decine il sistema della ricerca di firme funzionava perfettamente, gli antivirus

erano velocissimi e non commettevano mai errori.

Con oltre tremila virus in circolazione il sistema delle firme è divenuto troppo pesante. Se si pensa che mediamente una firma affidabile è lunga 16 byte, un programma che contenga le firme di tremila virus avrebbe quasi 50K di dimensione occupati dalle sole impronte; inoltre si dovrebbe cercare ciascuna firma in ciascuno dei programmi candidati all'infezione, e ne risulterebbe un lavoro dal peso insopportabile. Peraltro i ragionamenti che abbiamo appena fatto sono teorici, in quanto esistono diversi virus che non possono essere identificati con il sistema delle firme, inoltre la stessa firma talvolta è in grado di riconoscere più varianti etc. Non era nostra intenzione essere rigorosi ma semplicemente illustrare i limiti della scansione di firme.

L'impronta digitale

Un metodo alternativo alla firma consiste in un algoritmo caratteristico di ciascun virus, che consente di rilevarne la presenza in modo altrettanto affidabile. Per mantenere il parallelo «poliziesco», equivale all'impronta digitale: se si possiede l'impronta di un ricercato, teoricamente confrontandola con le impronte di tutti coloro che vengono controllati prima o poi si trova la persona che si sta cercando.

Nel caso di un virus l'algoritmo può consistere in un calcolo preciso da effettuare su byte in posizioni prestabilite (somme di controllo, CRC e simili). Se il risultato ottenuto da un particolare file eseguibile è uguale a quello impostato nel programma antivirus, allora il programma contiene il virus.

Ottenere un buon algoritmo non è molto più facile che ottenere una buona firma. In entrambi i casi occorre molta competenza, per cui vale la regola secondo la quale più un produttore spende in ricerca, migliore sarà il suo prodotto antivirus.

Firme e impronte digitali condividono più o meno gli stessi pregi e difetti; in realtà non esistono quasi più programmi di ricerca di firme, in quanto la maggior parte dei produttori si è adeguata alla nuova tecnologia della ricerca algoritmica, che consente di scrivere software più compatto e rapido.

Il pregio principale di questi programmi è nella loro diffusione. Su oltre cento milioni di personal computer installati nel mondo si stima che il 50-70% montino un antivirus, di qualsiasi genere o marca esso sia. Molti usano versioni vecchie, altri versioni modificate o adattate; si tratta comunque di programmi molto comuni, di cui è facile venire in possesso.

Altro pregio dei programmi di scansione consiste nella possibilità di utilizzarli in un sistema infetto. Una volta che l'incidente si è verificato, o che se ne ha il sentore, è sufficiente spegnere il computer, farlo ripartire da un dischetto di sistema pulito e protetto e quindi eseguire l'antivirus. Se il virus responsabile dell'infezione è noto all'antivirus, ossia se il laboratorio del produttore dell'antivirus ha ricevuto una copia di un campione di questo virus in tempo utile per includerlo nel proprio sistema, allora verrà identificato e l'utente avrà a disposizione uno o più strumenti per rimuoverlo.

Il difetto principale dei programmi di scansione consiste nella necessità di mantenerli aggiornati. Un antivirus scaduto, vecchio di sei mesi, è quasi peggio che nessun antivirus. Darà all'utente un falso senso di sicurezza, fino a quando non si verificherà un incidente malgrado l'antivirus (scaduto) e l'utente dovrà rivedere le proprie strategie di sicurezza.

Dimmi con chi vai...

... e ti dirò chi sei, la regola vale anche per il software. Vi sono due categorie di programmi antivirus assai simili come concezione, sebbene totalmente diversi nel funzionamento.

Il concetto funzionale di questi sistemi è che per comprendere se un programma contiene o meno un virus è sufficiente mettersi a guardarlo, studiarne il comportamento e determinare se è in grado di riprodursi autonomamente, di danneggiare i dati o altro.

Questo modo di agire è simile a quello della mente umana. La nostra mente è in grado di effettuare un grande numero di associazioni simultanee su quanto proviene dai sensi: per rimanere nell'informatica, una persona che conosca più interfacce grafiche differenti è in grado di affermare a colpo d'occhio, vedendo uno schermo video acceso, «è un Macintosh» oppure «è un terminale X-Windows» o «è OS/2». Per spiegare a un'altra persona i criteri di riconoscimento del tipo di interfaccia grafica ci vorrebbe un po' di tempo; per riconoscere l'interfaccia è sufficiente guardarla.

In modo simile, seppure con i limiti del sistema, operano due tipi di programmi antivirus: gli euristici e i monitor.

I monitor

Iniziamo da questi ultimi. Concettualmente sono piuttosto datati: fu un monitor il primo programma antivirus in assoluto, l'ormai quasi dimenticato FLU-SHOT+ che Ross Greenberg, un ricercatore della prim'ora, distribuiva gratuitamente. Si tratta di un TSR che si installa in memoria, intercetta le chiamate al DOS e prima di passarle al sistema le controlla, per verificare se si tratta di chiamate legittime o meno. Ad esempio la richiesta di formattare un dischetto è del tutto legittima se il comando dell'utente, che il sistema sta eseguendo, è «FORMAT A:»; non è legittima la formattazione della traccia 0 del disco fisso se il comando che l'utente ha dato per ultimo è stato «DIR B:*.PAS».

Un monitor, se è ben scritto, è in grado di riconoscere queste situazioni e di dare l'allarme all'utente il quale, se ritiene che l'operazione che il monitor ha intercettato sia invece ciò che egli desiderava fare, può dare disposizione al monitor di lasciar comunque soddisfare la richiesta.

Tre sono i pregi principali dei monitor: il primo sta nella sua azione preventiva, che consente di impedire le infezioni e quindi risparmia del tutto il lavoro di disinfezione che è comunque necessario anche qualora il rilevamento del virus avvenga in fase precoce. Il secondo consiste nella quasi totale indipendenza dall'azione consapevole

All'assalto dell'antivirus

Abbiamo accennato alla nuova, preoccupante tendenza riscontrata negli autori di virus: non più in cerca del camuffaggio più efficace ma della più efficiente tecnica di attacco agli antivirus. Virus che disattivano i monitor residenti, virus che evitano di infettare gli antivirus più noti per ritardare ulteriormente il proprio riconoscimento.

Recentemente è iniziata la corsa all'euristico.

Sono stati riscontrati alcuni virus scritti in modo da non essere riconosciuti da F-PROT o da TBAV, i due principali antivirus dotati di capacità euristiche.

Il problema di per sé è relativamente grave da un punto di vista tecnico perché i produttori degli antivirus non impiegheranno molto a correggere i propri programmi in modo da controbattere all'attacco; ma dimostra, se ce ne fosse stato bisogno, che il passaggio degli autori di virus dalla difesa all'attacco è ben reale.

Esiste un altro tipo di monitor, che effettua una scansione di firme senza il controllo diretto dell'utente. Nell'immagine TBAV ha identificato il virus 'Cascade' durante una copia.

dell'utente, il quale deve limitarsi a installare il monitor e poi può dimenticarsene.

Il terzo pregio consiste nel fatto che un monitor è svincolato dalla conoscenza di ciascun virus; poiché riconosce i comportamenti e non le immagini, non è necessario che un virus sia stato studiato dal laboratorio che produce il monitor perché questi sia in grado di riconoscerlo.

In realtà quest'ultima circostanza è alla base dei difetti dei monitor: l'indipendenza è più teorica che reale, in quanto spesso si verificano falsi allarmi che portano l'utente, dopo un certo tempo, a ignorare la presenza del virus. Inoltre un monitor residente in memoria è facile da disattivare, e molti virus sanno bene come fare.

Questi difetti hanno portato al declino del favore dei monitor tra gli esperti, sebbene nel grande pubblico essi continuino a riscontrare un certo gradimento, legato essenzialmente a campagne di marketing che allettano gli utenti con l'argomento dell'«installa e dimentica».

La domanda che gli esperti si sentono fare più di frequente è se sia possibile una difesa costante e permanente contro i virus; se non si considerano i difetti, i monitor sembrano soddisfare questo desiderio degli utenti e pertanto è facile che un utente inesperto sia invogliato ad acquistare e installare un monitor, salvo poi ad accorgersi dei problemi in un secondo tempo.

Gli euristici

Si tratta di una categoria di programmi antivirus piuttosto nuova. Il concetto in questo caso è diverso: l'antivirus non si limita a attendere che il virus tenti di agire, ma cerca di identificarlo prima, effettuando una scansione del tutto analoga a quella che fanno i programmi di ricerca di firme o impronte (e infatti di solito l'euristica è una funzione che questi ultimi offrono in più) ma andando alla ricerca di cose completamente diverse.

Un antivirus euristico è in grado di leggere il codice binario del microprocessore, analizzare istruzione dopo istruzione, ponendole in relazione tra di loro per capire se una determinata sequenza di istruzioni sia male intenzionata. Generalmente il programma si servirà di una tabella di possibilità, ponderate secondo un peso attribuito dal produttore, e assegnerà un punteggio a ciascuna situazione di rischio eventualmente presente in un programma oggetto di analisi; quando il punteggio supera un determinato valore l'antivirus lo dichiara «probabilmente infetto» e lo segnala all'utente.

Gli euristici uniscono i pregi dei programmi di scansione a quelli dei monitor. Poiché non sono residenti non intercettano il comportamento dell'utente, il quale ne richiede esplicitamente l'esecuzione e pertanto sa cosa aspettarsi. Inoltre un antivirus euristico ben fatto sa riconoscere un virus anche se l'autore dell'antivirus non è in possesso di un campione del virus.

Il principale svantaggio degli euristici consiste nel fatto che allo stato attuale sono riservati agli esperti. La tecnologia del software antivirus euristico non è riuscita ancora a produrre un sistema sufficientemente preciso e al tempo stesso sufficientemente semplice da essere utilizzato anche dall'utenza meno esperta. Sono relativamente frequenti i falsi allarmi, e pertanto le segnalazioni fornite da un programma euristico vanno interpretate alla luce di una specifica competenza.

Puro siccome un angelo...

L'ultima classe di prodotti antivirus si compone dei programmi di controllo di integrità. Dal punto di vista del rilevamento di infezione, se vengono utilizzati correttamente hanno una percentuale di infallibilità pari al 100%. Infatti non è possibile, per definizione, un virus che infetti un personal computer senza apportare qualche modifica a qualche oggetto eseguibile (file o settore di avvio). Poiché le ROM sono, anch'esse per definizione, immutabili, è evidente che un programma che tenga d'occhio le variazioni degli eseguibili rileverà senza possibilità di errore una modifica apportata da un virus.

Generalmente un programma di controllo di integrità consiste in un algoritmo di CRC o simili, che applicato su un file ne estrae un dato fortemente dipendente dal contenuto del file, tale per cui anche una minima variazione nel contenuto determina una variazione enorme nel risultato. I valori risultanti, generalmente brevi (pochi byte per ciascun file) vengono archiviati in modo sicuro; periodicamente vengono ricalcolati tutti i valori per essere confrontati con quelli conservati in archivio: se qualcuno di essi differisce occorrerà indagare sulla causa della differenza.

Il pregio dei sistemi di controllo di integrità consiste nella loro infallibilità. Come si è detto, se correttamente utilizzati rileveranno con certezza tutte le variazioni apportate ai file eseguibili.

Tuttavia questi programmi hanno anche una serie di difetti. Innanzitutto la procedura di controllo di integrità richiede necessariamente l'avvio da un dischetto di sistema pulito e protetto. Normalmente si consiglia questa procedura anche prima di effettuare un controllo con un programma di scansione, ma mentre per questi ultimi l'avvio da dischetto pulito è una precauzione, nel caso del controllo di integrità è una sine qua non.

Un programma di scansione sarà quasi sempre in grado di riconoscere la presenza in memoria di un virus insidioso e segnalarla, suggerendo all'utente di interrompere la ricerca e avviare da un dischetto pulito; un programma di controllo di integrità non è in grado di farlo, e se avviato in presenza di un virus stealth può anche fallire completamente il proprio scopo, contribuendo magari anche alla ulteriore diffusione del virus. Molti virus stealth, infatti, se viene richiesta la lettura di un file infetto, intercettano la risposta del sistema in modo che il file appaia non infetto: in tal caso il controllo di integrità darebbe esito positivo e l'utente avrebbe fallito il proprio scopo.

Per questa ragione è assolutamente indispensabile accertarsi che non vi siano virus residenti in memoria prima di avviare un controllo di integrità, pena l'inutilità del controllo, nella migliore delle ipotesi, o un danno ancora superiore, nella peggiore.

Inoltre, a differenza dei programmi di scansione, i programmi di controllo di integrità non possono essere utilizzati su un sistema già infetto per determinare le cause dell'infezione e possibilmente curarla.

Infine non è possibile, o non è agevole, il controllo di integrità su sistemi

F-PROT offre un buon sistema di ricerca euristica dei virus.

in cui gli eseguibili variano frequentemente. Oggi non sono più in uso, grazie al Cielo, programmi come una vetusta rubrica telefonica che mi è capitata tra le mani qualche tempo fa, in cui i numeri di telefono vengono memorizzati NELL'IMMAGINE BINARIA DEL FILE ESEGUIBILE cioè all'interno del file .COM (orrore!). Ma un'azienda che sviluppa software troverebbe assai disagevole l'uso di un programma di controllo di integrità, dato che i file eseguibili cambiano continuamente.

Allora, quale scegliere?

Per un utente che abbia un singolo personal computer, sul quale magari non siano presenti dati di rilevanza planetaria, la scelta ricadrà quasi certamente su un programma di scansione. Il mercato ne offre attualmente un centinaio: quale scegliere?

Diversi enti, organizzazioni e persone si sono proposti come certificatori di programmi antivirus. Tra questi probabilmente la più nota al grande pubblico è Patricia Hoffman, autrice della controversa lista di virus «VSUM» all'interno della quale si trova una scheda di valutazione dei principali antivirus. In realtà la valutazione non è molto imparziale, ma costituisce una buona base di partenza.

Altre valutazioni sono quelle proposte dal Virus Bulletin, una rivista molto autorevole, e da centri universitari.

Come abbiamo avuto occasione di scrivere più volte la valutazione di un antivirus è piuttosto difficile. Se lo si prova contro i vari campioni di Cascade, Form, Stoned e Tequila l'unico risultato che si ottiene è di scartare eventualmente quegli antivirus (posto che esistano) scritti talmente male da non riuscire a riconoscere nemmeno questi vecchi e diffusissimi virus.

L'utente in realtà non dispone di un mezzo efficace per valutare un antivirus. L'unico modo per avere una valutazione attendibile è di rivolgersi a un esperto di fiducia, e in ogni caso di mantenere costantemente aggiornato il proprio antivirus. L'ideale è di aggiornarlo una volta ogni mese, e un prodotto che non offra un piano di aggiornamento a ritmo ravvicinato va senz'altro scartato a priori. Il migliore antivirus è quello che riconosce il virus che ha infettato il mio computer, altrimenti sono soldi buttati. MC

Stefano Toria è raggiungibile tramite MC-link alla casella MC0170 e tramite Internet all'indirizzo MC0170@mclink.it.