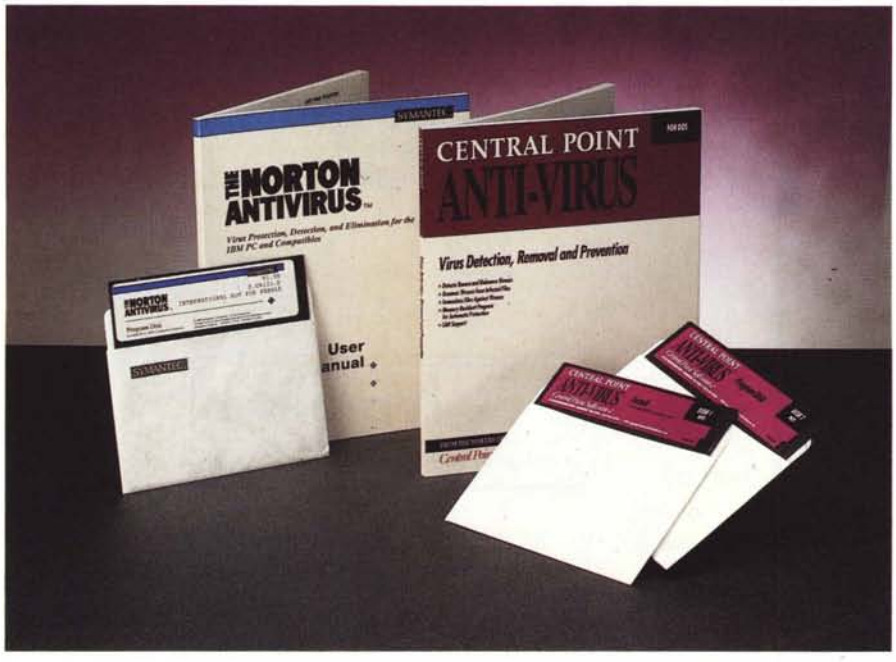
Com'è fatto un programma antivirus

di Stefano Toria

Riprendiamo da questo mese alcuni argomenti tecnici, allo scopo di familiarizzare i lettori con gli strumenti di cui potranno servirsi per difendersi dal rischio di aggressione da parte di un virus. Abbiamo più volte ripetuto che non esiste una unica misura di protezione che garantisca la certezza assoluta; una protezione adeguata si ottiene mettendo in atto un insieme di misure, senza affidarsi completamente a nessuna. Una di queste misure è l'utilizzo sensato di un programma antivirus; in questo articolo e nei prossimi approfondiremo l'argomento

Un mercato che rende

Dopo il battage pubblicitario che ha ricevuto il fenomeno dei virus, grazie al modo in cui la stampa d'informazione lo ha trattato (fra il divertito e il terrorizzato, due atteggiamenti che non denotano certo profonda conoscenza del fenomeno stesso) il grande pubblico ha quantomeno acquisito la nozione dell'esistenza di una particolare categoria di programmi che si chiamano «virus», unitamente all'idea che si tratti di qualcosa da cui difendersi. È quindi nata, e si è sviluppata rapidamente, la domanda di un nuovo prodotto: un «antidoto» al virus. È anche cresciuta rapidamente l'offerta di simili prodotti, come era ovvio che accadesse. L'utente si trova quindi nella necessità di scegliere un prodotto tra una gamma ormai piuttosto vasta, con la difficoltà di non essere in grado di valutare immediatamente le capacità effettive del programma. Abbiamo già accennato in passato a questa difficoltà; cercheremo in questo articolo di gettare un po' di luce sul funzionamento di un programma antivirus.



Perché un antivirus?

I lettori di questa rubrica ne avranno probabilmente fin sopra i capelli di sentirsi ripetere ogni volta che debbono fare le copie dei propri dati (anche questo mese ce lo siamo lasciato sfuggire un paio di volte). Potranno quindi legittimamente chiedersi: ma non stiamo già a posto avendo fatto le copie? A cosa ci serve adesso un'altra misura di difesa?

Le copie dei dati sono indispensabili, è vero. Sono l'unica possibilità di salvezza dopo l'attacco distruttivo di un virus, dopo che un disco fisso si è distrutto per l'errore del tecnico che stava riparando il computer, o dopo che uno sbalzo di tensione ha reso illeggibile buona parte del contenuto dello stesso disco.

Ma la ricostruzione di un disco fisso è un'operazione che porta via tempo, che può dare risultati non del tutto precisi e che in ogni caso è preferibile evitare se possibile. Inoltre la sicurezza offerta da una regolare procedura di copia è direttamente proporzionale alla frequenza con cui la procedura viene svolta: l'unico caso in cui l'utente è tutelato al 100% è quando il virus attacca e distrugge esattamente dopo che l'utente ha terminato di fare la copia più recente. Se soltanto il virus aspetta il giorno dopo è probabile che l'utente abbia nel frattempo svolto qualche lavoro, che andrà perduto in quanto non sarà stato trascritto sulla copia effettuata il giorno precedente.

È quindi sempre preferibile evitare, se possibile, di dover ricostruire il disco: un buon programma antivirus correttamente installato e utilizzato, pur con i suoi limiti (che vedremo in questo articolo), fornisce una protezione sufficiente a stroncare sul nascere le più probabili infezioni ad opera dei virus più dif-

fusi. Nel caso in cui l'utente dovesse essere poi «contagiato» da un virus che passa le maglie del controllo dell'antivirus, ci saranno sempre le copie di sicurezza a cui ricorrere come extrema ratio.

Che cosa fa un antivirus

L'attività svolta da un programma antivirus può essere riassunta in tre semplici punti: prevenire l'infezione, impedire che un qualsiasi programma esegua funzioni pericolose, identificare l'infezione una volta che si è verificata. Non tutti i programmi svolgono tutte e tre queste azioni, che vediamo ora in maggiore dettaglio.

Prevenzione

Appartengono a questa categoria i programmi che si prefiggono lo scopo di identificare un programma sospetto prima che abbia modo di attaccare il suo bersaglio (programma eseguibile, boot sector, master boot sector). L'identificazione può avvenire in varie maniere, essenzialmente riconducibili all'esame del contenuto di un programma prima della sua esecuzione, alla ricerca della eventuale presenza di sequenze di istruzioni che facciano sospettare la presenza di un virus.

Questa funzione si definisce «scansione». Si tratta della più comune modalità di difesa dai virus; parte dall'assunto che sia possibile identificare con certezza un programma, distinguendolo da qualsiasi altro programma che sia mai stato scritto, in base alla presenza di una particolare sequenza di istruzioni. Chiariamo meglio questo concetto con un esempio.

Di per sé la parola «libro» non fa venire in mente alcun testo specifico: è una parola di uso comunissimo. Anche la sequenza di parole «il libro e» risulta del tutto anonima. Ma se estendiamo la sequenza e diciamo «galeotto fu il libro e chi lo scrisse» chiunque è in grado di riconoscere univocamente il canto V dell'Inferno.

Potremmo pensare di scrivere un programma fatto più o meno in questo modo:

▼

```
program cerca :=
{ for (parola := 1 to ultima-parola)
  { if gruppo-di-8-parole [parola] = "galeotto fu il libro e chi lo scrisse"
      then goto trovato;
  }
  goto fine;
  trovato: print "Inferno - Canto V";
  fine: }
```

Un simile programma, oltre ad essere riduttivo, avrebbe anche l'inconveniente di identificare erroneamente come canto V anche il presente articolo, dato appunto che contiene le parole utilizzate come sequenza di ricerca. Ma sarebbe sufficiente estendere di qualche parola la sequenza, aggiungendo le prime due-tre parole del verso successivo, «quel giorno più». Resterebbe comunque il fatto che, poiché il programma contiene la sequenza di parole utilizzata come identificazione, una scansione effettuata sul testo stesso del programma darebbe un risultato falsamente positivo. Ma sarebbe semplice modificare il programma in modo da arrivare al punto in cui il risultato positivo si ottiene esclusivamente dal programma stesso, dal canto V dell'Inferno e da nessun altro testo. Una ulteriore piccola modifica potrebbe far escludere il risultato positivo se il programma si accorgesse che sta eseguendo una scansione di se stesso, e in questo modo il procedimento diverrebbe perfettamente funzionale.

Tornando ai virus e ai programmi eseguibili, è evidente come sia possibile estrarre da un programma «A» una sequenza unica di istruzioni in linguaggio macchina tale da consentire di affermare che qualsiasi programma eseguibile che contiene la sequenza data è inequivocabilmente il programma «A».

Peraltro la pratica è un po' più complessa della teoria, e la progettazione e realizzazione di questi programmi, per non parlare della continua manutenzione di cui abbisognano grazie alla continua attività di sviluppo di nuovi virus da parte dei soliti ignoti, sono attività di tutto rispetto.

Un programma di identificazione preventiva di virus si prefigge lo scopo di attrarre l'attenzione dell'utente su un virus prima che questo abbia la possibilità di essere eseguito. Teoricamente si tratta della migliore difesa possibile:

Michelangelo: la nuova catastrofe?

Tra la fine di gennaio e i primi di febbraio molti quotidiani, tra cui il «Corriere della Sera», riportarono in cronaca l'annuncio di una possibile nuova catastrofe analoga a quella annunciata per il venerdì 13 ottobre 1989, mai verificatasi in realtà. Stavolta la data del destino è il 6 marzo, ma un'attenta analisi del virus fa dubitare che possa succedere niente di così tragico.

Cominciamo dal nome: il virus è stato battezzato «Michelangelo» non dal suo autore, ma da un ricercatore che ha notato l'identità tra la data di attivazione del virus medesimo, determinata in fase di disassemblaggio, e la data di nascita di Michelangelo Buonarroti, il 6 marzo 1475. Siamo propensi a ritenere che si tratti di una coincidenza.

Per il resto, da un punto di vista tecnico il «Michelangelo» ricorda da vicino lo «Stoned».

Si trasmette servendosi del master boot record, si installa residente in memoria, aggancia l'INT 13H e se riscontra la sua presenza sul disco fisso, oppure all'atto di un boot da un disco fisso infetto, si attiva e procede alla verifica della data. Qualora la data corrisponda al 6 marzo il virus procede con la distruzione di tutti i dati sul disco infetto: l'operazione viene eseguita ricoprendo le tracce 0 e 1 (sui dischetti) oppure da 0 a 3, scrivendo su tutti e 9 i settori di un dischetto da 360K, o sui primi 14 settori di un dischetto di alta capacità, oppure sui primi 17 settori di un disco fisso. Il valore utilizzato per ricoprire i settori prescelti per la distruzione viene prelevato da una precisa locazione della memoria, che tipicamente conterrà un valore pari a 0.

Questa operazione quasi certamente causerà un danno irrimediabile al contenuto di un disco fisso, costringendo l'utente a riformattarlo e a ripartire dalle copie di sicurezza (avete fatto le copie di sicurezza dei vostri dati?

Mettete giù la rivista e provvedete a farle subito).

Per liberarsi da questo virus, una volta identificata la sua presenza in memoria, è sufficiente far ripartire il DOS da un dischetto sicuramente «pulito», quindi eseguire il comando «FDISK» per riscrivere sul disco fisso le istruzioni di avvio del sistema.

nessuna infezione è possibile se il virus non viene eseguito, quindi intercettarlo prima dell'esecuzione significa spuntargli le armi. Nella pratica l'identificazione preventiva funziona soltanto con quei virus già noti e analizzati dai ricercatori, quindi non può essere utilizzata come unica misura di sicurezza.

Ma vediamo più in dettaglio come funziona la scansione. Un programma di scansione antivirus per essere considerato efficace ed efficiente non può limitarsi a un dispositivo di ricerca corredato da un database di sequenze di identificazione (che per comodità chiameremo «firme»). Il programma dovrà essere estremamente ottimizzato, poiché dovrà essere eseguito ogni volta che viene ordinata al sistema operativo l'esecuzione di un programma; il sovraccarico di lavoro richiesto dalla scansione dovrà essere minimo. Cercare individualmente ciascuna firma partendo da ciascun singolo byte di un programma eseguibile porterebbe a un sovraccarico intollerabile, se si pensa che già adesso le firme a disposizione dei ricercatori superano abbondantemente il migliaio. Il programma dovrà sapere dove andare a cercare ciascuna firma, e accelerare la ricerca limitandola alle zone in cui è più verosimile trovarle.

Ciascun virus infatti si comporta in modo univoco e quasi sempre è possibile prevedere in quale zona di un file infetto si potrà riscontrare il corpo del virus. È inutile cercare all'inizio di un file un virus che si attacca esclusivamente alla fine degli eseguibili. Per citare Alan Solomon, uno tra i più noti ricercatori antivirus, «uno non va a cercare un autobus di Londra in fondo all'oceano Atlantico».

I più noti programmi di ricerca preventiva (VSHIELD di McAfee, Central Point Antivirus, Norton Antivirus) impiegano pochi secondi nella ricerca e identificazione della presenza di virus.

Monitoraggio delle funzioni pericolose

Si tratta di un'operazione semplice ma di scarsa efficacia. Si basa sull'assunto che un programma dannoso debba necessariamente servirsi, per nuocere, di una funzione del sistema operativo scelta tra quelle che agiscono sui dischi (lettura, scrittura, formattazione). Si è quindi pensato di sviluppare dei programmi che, installandosi residenti in memoria e intercettando tutte le chiamate al sistema operativo, lascino passare soltanto quelle innocue (es. richiesta di data e ora), segnalando all'utente quelle che comportano qualche rischio e richiedendo l'autorizzazione dello stesso utente per eseguirle. Si diceva che si tratta di una misura scarsamente efficace poiché assieme alle eventuali richieste illegittime di un virus verrebbero bloccate quelle del tutto legittime

Cinta e bretelle: ovvero non esageriamo nelle precauzioni

Ci è pervenuta con la posta una lettera di un lettore che, con un tono piuttosto allarmato, ci mette in guardia contro un particolare antivirus, accusato di essere portatore di un bel po' di virus.

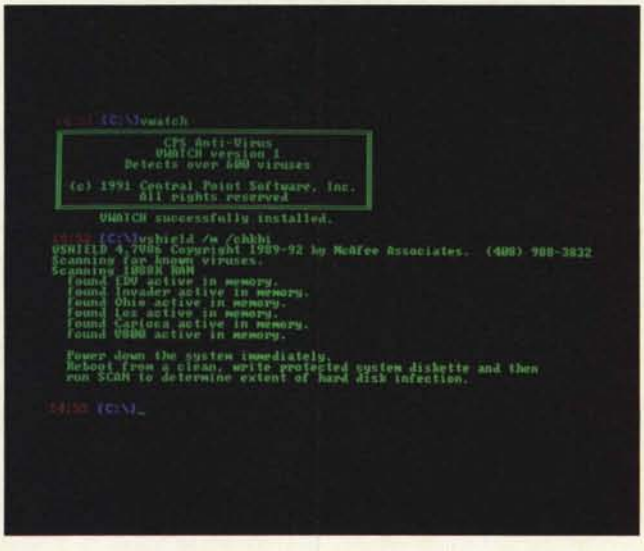
Il lettore, di cui rispettiamo il desiderio di non apparire con il proprio nome, afferma di aver verificato una utility antivirus residente (del tipo progettato per identificare i virus prima che possano introdursi nel sistema) servendosi di un'altra analoga utility: quest'ultima avrebbe riscontrato, in presenza dell'altra, ben cinque virus presenti in memoria.

I programmi incriminati sono il Central Point Antivirus e il VSHIELD, una delle utility di McAfee. Il lettore ha caricato in memoria VWATCH, la porzione residente del CPAV, e quindi ha fatto scandire la memoria da VSHIELD, con il risultato visibile nella foto (noi abbiamo riscontrato più virus di quanti non ne abbia trovati il lettore perché abbiamo utilizzato una versione più recente di VSHIELD).

E allora? Dalli all'untore? Niente affatto. Rileggendo attentamente quanto abbiamo detto qui sopra a proposito dei programmi di scansione si comprenderà facilmente come è normale, anzi forse scontato, che un programma identifichi erroneamente come virus quello che in realtà è un diverso antivirus.

Per poter identificare il canto V dell'Inferno, tanto per avvalerci dello stesso esempio utilizzato nell'articolo, dobbiamo servirci di un programma che vada alla ricerca della frase «galeotto fu il libro e chi lo scrisse». Passando un qualsiasi testo al setaccio di questo programma si potrà verificare se si tratta o meno dei versi di Dante. Peraltro se sottoponiamo a questo programma il n. 116 di MCmicrocomputer ci verrà segnalato che si tratta del canto V dell'Inferno. Ma noi sappiamo bene che non è così; semplicemente il n. 116 di MCmicrocomputer contiene proprio quella frase che noi abbiamo adottato come criterio per stabilire se un testo consiste nel canto V dell'Inferno o meno.

Lo stesso può accadere se utilizziamo simultaneamente due antivirus. Un programma di scansione deve contenere le firme dei virus che si prefigge di identificare; sotto questo punto di vista nulla lo differenzia da un effettivo virus. Sta all'utente servirsi con criterio dei programmi antivirus, utilizzandone soltanto uno alla volta, poiché l'autore di un antivirus può progettare il proprio programma in modo da riconoscere se stesso ma non può e non deve abbassare la guardia davanti a nessun altro programma, pena il rischio di lasciar passare un autentico virus.



Un prodotto antivirus segnala la presenza di una infezione in un altro analogo prodotto: nessun falso allarme, è una incompatibilità del tutto legittima.

provenienti, ad esempio, da un comando di formattazione di dischetto o dalla modifica di un parametro interno a un file eseguibile; l'utente, confuso da una serie di segnalazioni di cui probabilmente non afferra il senso e la portata, finirebbe per rispondere affermativamente a tutte le richieste del programma di monitoraggio senza ragionarci su, annullandone per conseguenza l'efficacia.

Inoltre è possibile che un programma particolarmente malizioso scavalchi il protocollo standard di richiesta di servizi al sistema operativo, e vada a pasticciare direttamente nella memoria del computer in modo da rendersi invisibile al programma di monitoraggio.

Nel prossimo numero di MCmicrocomputer riprenderemo l'argomento del controllo delle funzioni pericolose che, pur fornendo un livello di protezione insufficiente se adottato come unica misura, può comunque presentare dei vantaggi in alcuni casi.

Identificazione

Una volta che il virus è riuscito a introdursi in un sistema è facile identificarne le tracce, se si sa cosa cercare e dove cercarlo. Non pretendiamo che nessun utente si trasformi in un esperto di linguaggio macchina e di codice esadecimale; il compito può essere tranquillamente delegato a uno dei tanti programmi di scansione disponibili sul mercato i quali, se sono in grado di identificare un virus che sta cercando di introdursi nel nostro elaboratore, ancor di più saranno capaci di scovarlo dopo che vi si è introdotto, sempre che vengano utilizzati correttamente.

Abbiamo visto come una delle tecniche adottate più di recente dagli autori di virus consista nel nascondere il codice eseguibile che compone il virus stesso. È uno sforzo compiuto nella deliberata intenzione di rendersi invisibili proprio ai programmi di scansione. Ma per eseguire con successo questa operazione è necessario che il virus assuma il controllo dell'elaboratore dall'inizio, cioè dall'accensione. Per impedire a un virus di installarsi prima dell'esecuzione del programma di scansione è quindi indispensabile, come abbiamo più volte ripetuto, avviare l'elaboratore con una copia di sistema operativo sicuramente esente da infezione. Soltanto in questo modo si otterrà che la memoria sia libera da programmi non autorizzati i quali potrebbero celare proprio ciò che l'utente sta cercando di portare alla luce, cioè le tracce dell'infezione da virus.

Il programma di scansione, correttamente avviato da un sistema operativo non contaminato, rileverà l'eventuale presenza di un virus. A questo punto i programmi infetti andranno fisicamente rimossi dal disco, non soltanto segnalati come non disponibili. Non dovrà essere utilizzato il comando ERASE ma una utility come la WIPEFILE delle Norton Utilities, o altre analoghe. Non dovrà restare sul disco alcuna traccia del virus. Questa procedura naturalmente vale per i virus di tipo parassita, che si trasmettono attaccandosi ai file eseguibili; per rimuovere i programmi che aggrediscono il boot sector o il master boot record è necessario in linea di massima riformattare il disco fisso.

MC

Stefano Toria è raggiungibile tramite MC-link alla casella MC0170.