Gli antivirus in rete

Marzo uguale Michelangelo. Questo stupido virus è ai primi posti nella classifica della diffusione, secondo le ultime statistiche. Niente di più facile che lasciarsene infettare, basta lasciare nel drive A: un dischetto infetto e poi accendere il computer. Ma niente di più facile che difendersene: basta partire da un dischetto di sistema pulito e protetto, poi fare una scansione con un qualsiasi programma antivirus, anche vecchio, purché non più vecchio di un anno, un anno e mezzo (ovviamente un programma recente è molto meglio). Se si dovesse riscontrare il Michelangelo sul proprio disco fisso, si fa presto a toglierlo: basta un bel FDISK /MBR (una funzione non documentata del DOS 5) e siamo a posto

di Stefano Toria

Affrontiamo questo mese un tipo di programma antivirus che da qualche tempo ha fatto la sua comparsa sul mercato. Considerato che il problema dei virus assume particolare rilevanza quando non è una sola la macchina soggetta al rischio di infezione, e che il controllo antivirus effettuato direttamente sulle macchine a rischio comporta alcuni inconvenienti che ormai ben conosciamo (l'utente non ha voglia di farlo, anche se lo fa dimentica di partire da un disco di sistema pulito e protetto, etc.) alcuni produttori hanno pensato di delegare la funzione di controllo antivirus al server della rete locale.

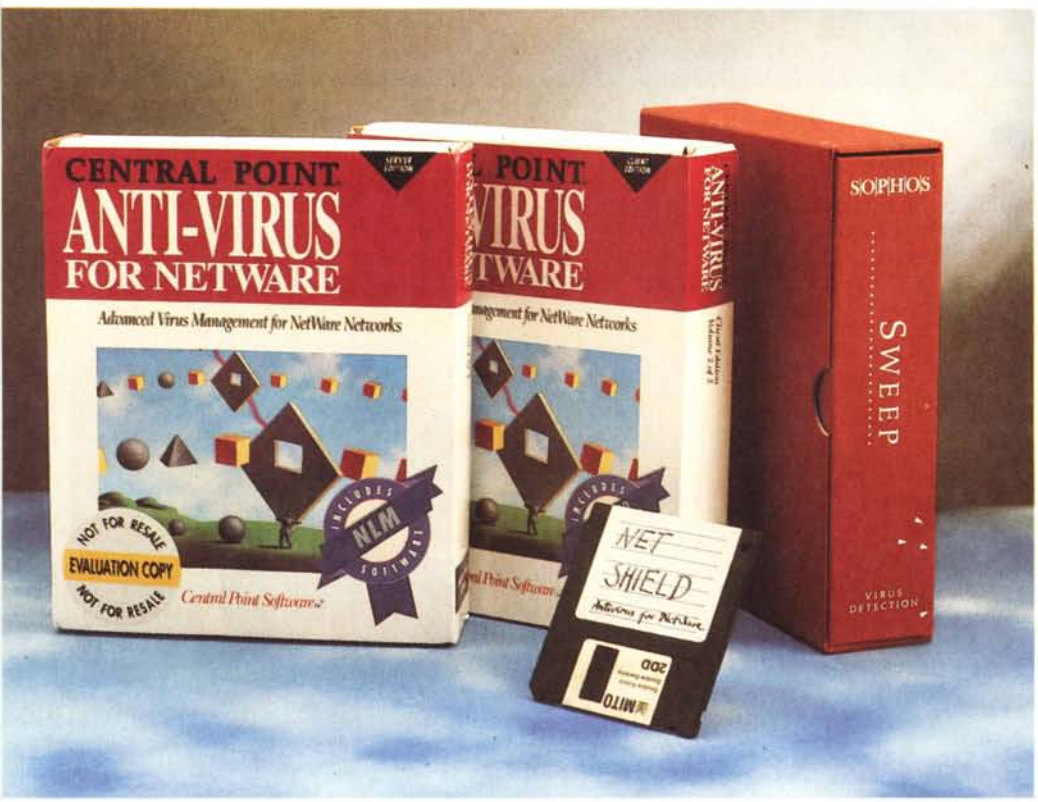
La soluzione ovviamente non è universale; è applicabile soltanto laddove una rete locale esista e dove il software di rete sia di tipo compatibile con i programmi antivirus per rete attualmente disponibili sul mercato. Tuttavia, se correttamente utilizzata, può dare risultati interessanti: vediamo come.

Quando si parla di «antivirus» genericamente, senza specificare a cosa ci si riferisce, quasi sempre si fa riferimento ai programmi di scansione. In realtà gli strumenti software a disposizione di chi deve difendersi dai programmi aggressori sono molti, ne abbiamo esaminati alcuni nel corso della vita di questa rubrica e i lettori avranno familiarizzato con essi.

Però rimane il fatto che i programmi di scansione restano i favoriti nei gusti del pubblico, sostanzialmente per la loro facilità di uso e perché non sono necessarie complesse procedure di installazione per utilizzarli.

Lo svantaggio della scansione, lo abbiamo ripetuto diverse volte, consiste nel fatto che è facile che un virus riesca a ingannare questo tipo di programmi, se l'utente non prende opportune precauzioni. E la pratica ci mostra quanto poco l'utente sia disposto a dar retta a chi consiglia queste precauzioni: spesso tutto ciò che egli chiede è di sapere quale sia «il migliore antivirus», per poterlo installare residente e dormire tranquillo. Almeno, così egli crede. Quando poi viene qualcuno che gli spiega in termini comprensibili le tecniche di stealth e di tunneling, allora accade spesso che sul viso del nostro utente si dipinga un'espressione tra lo stupito e l'incredulo, quasi che gli si stia cercando di rifilare un mito urbano come la storia dei coccodrilli nelle fogne di New York.

Purtroppo non si tratta di miti, ma di una realtà che ogni giorno peggiora. Secondo uno dei più seri e affermati laboratori esteri con cui siamo in contatto ogni mese vengono scoperti e identificati circa 150 nuovi virus. La maggior parte di essi sono banali, ma cresce il numero di virus pericolosi, appositamente costruiti per rimanere ben nascosti (stealth, tunneling e polimorfismo) e per nuocere il più possibile (formattazione di singole tracce «strategiche»).



L'«oggetto magico»

Quando poi si cerca di convincere l'utente a non servirsi di un programma residente perché intrinsecamente non è in grado di offrire sicurezza, e a utilizzare per contro un programma non residente dopo aver avviato il sistema con quello che abbiamo scherzosamente definito «oggetto magico», cioè un dischetto di sistema *pulito* e *protetto contro la scrittura*, allora ecco che l'utente si ribella: ma che pensiamo che lui non abbia altro da fare? lui ci deve lavorare, col computer, non perdere tempo a fare questi giochetti (ovviamente il fatto che lui provi regolarmente tutti i videogame che gli porta il suo amico trafficone non ci riguarda: pensiamo a impicciarci degli affari nostri). Tutte queste belle cose che gli stiamo raccontando sono teoria, andranno bene forse per le installazioni militari, ma lui non ci tiene mica i segreti di stato sul suo computer. Tutto quello che vuole è di essere protetto contro i virus: invece di fargli perdere tempo con le nostre chiacchiere, vediamo di dargli questo programma residente, altrimenti diciamogli chiaro e tondo che non glielo vogliamo dare e lui vedrà di rivolgersi a qualcun altro.

Peggio per lui. Gli auguriamo di non incontrare mai un Michelangelo (a proposito, vi ricordate che questo mese il nostro simpatico amico si attiverà nuovamente? avete pensato a fare una scansione del vostro disco, per vedere se per caso non ve lo siete buscato in tutto questo tempo in cui non se ne è parlato mai? Se leggete questo articolo prima del giorno 6, vi consigliamo di dare un'occhiata per vedere come state messi). Perché il suo programma antivirus residente può fare ben poco per lui, se le cose si mettono male. Gli antivirus residenti controllano il sistema soltanto nel momento in cui vengono eseguiti, cioè bene che vada all'inizio del caricamento dei device definiti nel CONFIG. SYS. Ma se il sistema è stato infettato da un virus da boot sector come il Michelangelo, è il virus ad essere eseguito, subito prima dell'antivirus. E se il Michelangelo ha infettato il sistema la sera del 5 marzo, quando il mattino seguente l'utente va ad accendere il suo computer si ritrova il disco formattato prima ancora che il programma antivirus, su cui l'utente riponeva erroneamente la sua fiducia, abbia modo di accorgersi di nulla. Così il nostro incauto amico, sul cui computer non c'erano segreti di stato ma semplicemente il risultato del suo lavoro, magari durato mesi o anni e quasi certamente senza copie di backup, si ritrova all'improvviso in condizione di dover ripartire da capo: gli ultimi mesi del suo lavoro sono spariti in un istante, è come se non fossero mai esistiti.

È chiaro che abbiamo descritto un caso limite, ma la sicurezza serve proprio per i casi limite. Dal 31 marzo 1992, giorno in cui ho ritirato la mia nuova auto, ho fatto quasi trentamila chilometri, nei quali non è successo nulla. Mia moglie ed io indossiamo sempre le cinture di sicurezza, e nostra figlia di due anni e mezzo viaggia sul suo seggiolino omologato, con una cintura a quattro punti. Il caso limite è che veniamo coinvolti in un gigantesco tamponamento a catena; non me lo auguro e senz'altro non mi accadrà mai, però le cinture continuiamo a indossarle. Sono inutili e scomode e danno fastidio, specie in questo periodo a mia moglie che è quasi al termine della gravidanza e che ogni volta cerca di evitare di mettersi la cintura (ma io la costringo a mettersela lo stesso). Abbiamo intenzione di avere cura di questa macchina, di tenerla a lungo e di continuare a indossare, spero inutilmente, le fastidiosissime cinture di sicurezza.

Per portare l'utente di personal computer a comportarsi in modo sicuro ci vuole tempo e un'adeguata formazione. Ma non sempre ciò è possibile, o desiderabile. Sarebbe opportuno sottrarre all'iniziativa dell'utente i controlli, come prima misura precauzionale, laddove ciò risulti possibile.

La diffusione delle reti locali

Negli ultimi anni si è parlato molto di reti locali. Ogni anno ci sentiamo ripetere che questo sarà l'Anno della Rete Locale; effettivamente questa tecnologia si è notevolmente diffusa, soprattutto negli ultimi cinque anni. Nelle aziende e negli enti di grandi dimensioni è da tempo una realtà operante; anche piccole società e studi professionali con due o tre computer stanno installando le loro piccole reti, magari con un 486 che fa da server e un paio di stazioncine per fare word processing, in modo che l'avvocato titolare dello studio possa buttare giù lo schema della comparsa, i procuratori aggiungano fatti e circostanze e dopo i ritocchi finali la segretaria possa metterla in bella copia, magari con un programma di DTP e una stampante laser. Ciascuno, ovviamente, sul proprio computer.

La praticità delle reti locali sta nel fatto che dati e programmi rilevanti possono essere mantenuti su un sistema unico, più facile da gestire e da controllare; se il software di rete è stato scelto opportunamente e le cose sono state fatte bene, gli utenti potranno accedere soltanto a quelle parti del server a cui hanno diritto ad accedere secondo la funzione di ciascuno, e soltanto per quelle operazioni che è loro compito svolgere (lettura della directory, creazione di file, modifica di file esistenti, cancellazione di file, lettura, scrittura, etc.).

Il problema di rendere sicura una struttura informatica basata su una rete locale è quindi più circoscritto: gli utenti possono infettarsi i propri computer come preferiscono, purché sia salvaguardata l'integrità del server. È sufficiente quindi una scansione periodica del server perché l'intero sistema sia sicuro.

Automatico è bello

Ma andiamo un passo più avanti. Spesso accade che un server sia gestito da una persona con una sufficiente preparazione tecnica. Questo è vero senz'altro nelle grandi strutture, che probabilmente nel proprio organigramma prevedono espressamente la gestione dei sistemi informativi. Forse è meno vero in un piccolo studio professionale come quello che abbiamo descritto sopra, ma anche in questo caso vi sarà una figura tecnica di riferimento: installare una rete locale non è particolarmente complesso, ma è al di fuori della portata dell'utente completamente a digiuno di tecnica.

È facile che il tecnico sia sensibile al problema della difesa dai virus, e che quindi abbia installato il server in condizioni di sicurezza anche fisica: ad esempio, staccando il cavo del drive A: per impedire che vengano letti dischetti non autorizzati, e riservandosi di controllare personalmente e preventivamente tutti i dischetti da inserire direttamente nel server. Se questa precauzione viene correttamente progettata e applicata, sarà praticamente impossibile che il server venga infettato da un virus da boot sector.

Rimane la possibilità che il server si infetti perché una delle stazioni cliente, a sua volta infetta, esegua un programma sul server trasmettendogli l'infezione. Una prima misura di prevenzione consiste nel fare buon uso dei dispositivi di sicurezza offerti dal software di rete, ma spesso questi non sono sufficienti.

Bene, questo è uno dei casi in cui un antivirus residente può risultare efficace: poiché le misure fisiche di sicurezza saranno sufficienti a impedire che il sistema si infetti a monte del CONFIG. SYS, si potrà installare un antivirus sotto forma di device driver, mettendolo come

primo device nella configurazione. In questo modo tutti i tentativi di infettare i programmi residenti sul server potranno essere bloccati alla radice o quantomeno identificati in fase estremamente precoce, in modo da prendere per tempo gli opportuni provvedimenti.

I server senza il Dos

Ma non sempre è possibile applicare una misura così semplice. Molte strutture di rete locale fanno uso di software che non va eseguito sotto Ms-Dos. Il caso più classico è quello del Novell NetWare, uno tra i più diffusi software di rete locale. Il NetWare prevede due diverse strutture di rete: una di dimensioni ridotte, con un unico server che è una macchina Dos con opportuni dispositivi software; una di dimensioni teoricamente illimitate, in cui può essere presente più di un server, e in cui i server sono macchine dedicate esclusivamente a questa funzione, con un apposito sistema operativo (il NetWare, appunto) che non è il Dos e che con il Dos non ha niente a che vedere. Soltanto in questo modo è possibile garantire prestazioni accettabili in un contesto in cui decine, forse centinaia di persone possono richiedere i servizi di un unico sistema. Il NetWare, residente sul server, coopera con gli appositi programmi residenti sui sistemi cliente, che estendono le capacità del Dos mettendolo in condizione di accedere alle risorse del server.

Ma il NetWare non è l'unico caso di server non-Dos. Si vanno diffondendo le reti basate su server Unix, oppure in cui la funzione di server viene svolta da un sistema Vax della Digital, su cui gira il sistema operativo VMS. Anche in questi casi i sistemi cliente montano opportune estensioni del Dos per consentire il dialogo con il software che fa da server sul sistema Unix o VMS.

La scansione sotto Windows: una pessima idea

Sono apparsi già da tempo diversi programmi di scansione fatti apposta per l'ambiente Microsoft Windows. La struttura dei vari prodotti offerti sul mercato varia da una semplice shell scritta per far girare sotto Windows uno scanner Dos, fino a un prodotto completo in grado di funzionare autonomamente e di offrire protezione contro i virus in ambiente Windows.

L'idea è piaciuta al mercato, che si sta orientando sempre di più verso prodotti facili da utilizzare e dotati di accattivanti interfacce grafiche, colorate e multiformi.

Nella realtà, dal nostro punto di vista si tratta di una pessima idea, che anziché accrescere il livello di sicurezza dell'utente si limita ad accrescere i volumi di fatturato di chi offre queste soluzioni, lasciando l'utente nello stato in cui si trovava. Se non peggio: illudersi di essere al sicuro è peggio che sapere di non esserlo.

La ragione di questa affermazione è presto detta. Sappiamo che gli autori di virus non sono rimasti fermi ad osservare lo sviluppo delle tecniche messe in atto da chi scrive programmi antivirus per combattere il dilagare di questo fenomeno: si sono dati attivamente da fare e hanno inventato delle tecniche, note come «stealth» e «tunneling», per cercare di mettere in atto delle misure di schermatura dei virus, in modo da mascherarne la presenza dopo che si è verificata una infezione, cosicché il periodo di latenza in cui il virus ha modo di infettare altri sistemi sia il più lungo possibile e il virus si diffonda quanto più possibile.

Un virus che riesce a infettare un sistema e a mettere in atto in modo efficiente una manovra di camuffaggio riuscirà anche a sfuggire ai tentativi di identificazione, perché ogni richiesta di lettura di qualsiasi cosa dal disco verrà intercettata dal virus che sarà in grado di decidere cosa effettivamente restituire come risultato della richiesta di lettura.

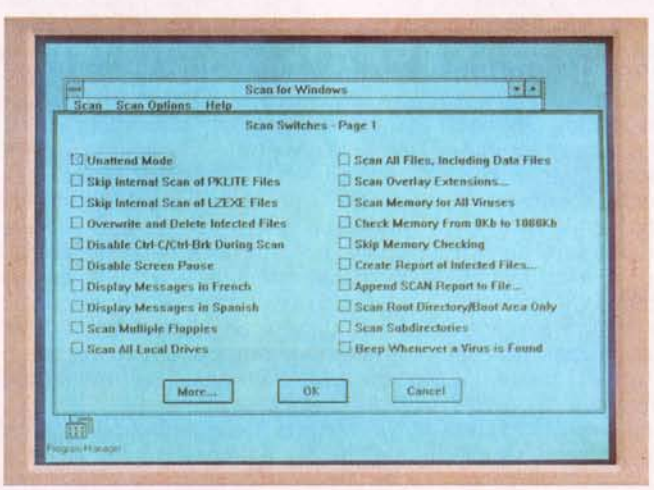
Un virus del genere non ci mette niente a prendere dal disco un programma infetto da una copia di se stesso, modificarla in memoria in modo da farlo apparire sano, e offrirlo a chi ha chiesto di leggerlo, ad esempio un programma antivirus. La presenza dell'infezione nel programma rimane quindi del tutto nascosta.

Per sconfiggere queste misure di camuffaggio esiste un solo sistema, efficace nel 100% dei casi senza alcuna possibilità di eccezione: avviare il sistema operativo (il Dos) da un dischetto che sia garantito al 100% esente da infezione.

Questa misura di sicurezza è talmente importante ai fini della difesa dai virus da giustificare la spesa, invero ridotta, dell'acquisto di una nuova copia originale del Dos, qualora l'utente non sia in grado di procurarsi in altro modo un originale *sicuramente non infetto*. Di questo originale dovrà essere fatta una copia, che sarà quella di cui l'utente si servirà nei controlli; l'originale andrà riposto e mai più utilizzato.

Inoltre, per evitare che il disco di sistema pulito si infetti qualora dovesse essere inavvertitamente eseguito un programma infetto dal disco fisso, lo stesso dischetto di sistema dovrà essere inserito protetto contro la scrittura. Questo è un blocco fisico, non aggirabile in alcun modo da nessun programma.

Infine, durante il controllo del sistema non dovrà essere eseguito alcun programma dal disco fisso, ma soltanto



Menu di scansione di un programma di antivirus in ambiente Windows.

È plausibile affermare che il caso di un server controllato dal Dos sia l'eccezione più che la norma. In questa situazione quindi sembrerebbe impossibile demandare al server il controllo antivirus. Ma in realtà, lungi dal costituire un handicap, l'assenza del Dos offre un importantissimo vantaggio.

A caccia di virus, senza il Dos di mezzo

Abbiamo detto e ripetuto fino alla nausea che i programmi di scansione vanno usati dopo aver avviato il sistema con un dischetto pulito e protetto. Rammentiamo ancora una volta la ragione di questa raccomandazione: perché se si avvia il sistema dal disco fisso non si può avere la certezza che all'atto dell'esecuzione del programma di scansione non vi sia alcun virus residente in memoria. Se il sistema fosse infetto da uno stealth virus, ad esempio dal 4096, il controllo antivirus darebbe esito negativo, perché il 4096 si interpone tra il programma antivirus e il disco, «disinfettando» al volo i programmi infetti quando un programma chiede di leggerli e facendoli così apparire «puliti» mentre in realtà rimangono infetti.

Questo accade perché il virus, per infettare il sistema, ha avuto la possibilità di essere eseguito: al momento opportuno è il virus ad avere il controllo del sistema, sono le istruzioni del virus quelle che il microprocessore 80x86 esegue e che hanno la possibilità di controllare le varie parti fisiche della macchina.

Peraltro i virus sono scritti avendo in mente il Dos. Tutte le tecniche di camuffaggio (stealth, tunneling, polimorfismo) dipendono strettamente dalla presenza del sistema operativo Dos, su un personal computer IBM o compatibile. Un programma infetto da un virus, trasportato su un sistema diverso, perde anche la sua natura di programma: diventa una

i programmi di scansione, preventivamente trasferiti sulla copia del disco di sistema in condizioni di assenza di virus. Ogni esecuzione di programmi dal disco fisso costituisce un rischio: poiché si sta cercando di verificare se il disco è infetto non si può sapere in anticipo se l'infezione si trova proprio in quel programma che si sta per eseguire. Ripetiamo: non dovrà essere eseguito alcun programma dal disco fisso durante il controllo antivirus dopo l'avvio da un disco di sistema pulito e protetto.

È chiaro quindi che non ha senso fare i controlli sotto Windows. Prima di arrivare a Windows infatti ci sono diversi programmi che vengono eseguiti dal disco fisso, ciascuno dei quali potrebbe essere infetto. Li ricapitoliamo in breve:

— al termine del POST il Bios legge il Master Boot Record dal cilindro 0, traccia 0, settore 1 del primo disco fisso: questo potrebbe essere infetto, p. es. da uno Stoned o da un Michelangelo;

— il programma di gestione delle partizioni stabilisce la partizione attiva e legge il Partition Boot Record (il primo settore della partizione): questo potrebbe essere infetto, p. es. da un Form o da un Ping Pong;

— il «primo stadio» del Dos va a cercare i file di sistema che contengono la parte residente del Dos, generalmente con i nomi IO.SYS e MSDOS.SYS, e li carica in memoria: questi potrebbero essere infetti da uno dei diversi virus che attaccano i .SYS;

— viene acceduto e letto il file CONFIG.SYS e vengono eseguiti i comandi di configurazione che contiene, caricando via via in memoria i diversi device driver specificati dall'utente: ciascuno di questi device driver potrebbe essere infetto; in particolare dovrà essere caricato, su un sistema 286 o 386 con memoria estesa o espansa, il gestore della memoria, anch'esso potenzialmente infetto;

— al termine del caricamento dei device driver viene caricata ed eseguita la shell, normalmente COMMAND.COM ma comunque specificabile dall'utente: trattandosi di un normale eseguibile potrebbe essere infetto da uno delle centinaia di virus che infettano i file eseguibili: uno tra tutti come esempio, il Dark Avenger;

— quando la shell prende il controllo, cerca ed esegue un batch che si chiama AUTOEXEC.BAT, in cui l'utente ha specificato una serie di istruzioni da eseguire automaticamente. Molte di queste istruzioni possono consistere nel caricamento e nell'esecuzione di programmi, che possono eventualmente rimanere residenti (es. KEYB.COM, DOSKEY.COM): anche questi potrebbero essere infetti;

— al termine dell'esecuzione dell'AUTOEXEC.BAT l'utente si ritrova il prompt C:\> e, per avviare Windows, scriverà il comando WIN dando luogo all'esecuzione di WIN.COM, anch'esso potenzialmente infetto;

— se ipotizziamo che a questo punto l'utente si fermi e come prima cosa esegua il controllo antivirus con lo specifico programma di scansione per Windows, possiamo facilmente renderci conto di come un eventuale virus abbia avuto decine di opportunità per assumere il controllo del sistema prima che l'utente arrivasse all'inizio del controllo.

Qualcuno potrebbe obiettare: benissimo, allora facciamo un dischetto di sistema pulito e protetto come dici tu, ci mettiamo sopra anche Windows e l'antivirus, e facciamo partire sia il Dos che Windows dal dischetto pulito, così andiamo sul sicuro. Benissimo, in teoria non fa una grinza. Ma in pratica innanzitutto è improbabile che su un solo dischetto, sia pure da 1,44 Mb, ci entrino sia il Dos, sia Windows 3.1 nella versione minima per l'avvio, sia l'antivirus.

Ma la risposta all'obiezione è un'altra. La ragion d'essere dei programmi antivirus per Windows, nella mente degli uomini di marketing delle società che li producono, è che dovrebbero rendere la vita più semplice all'utente. Lui sta lì che lavora con i suoi Excel, WinWord, PageMaker, Corel Draw e quant'altro, e ogni tanto fa partire il programmino antivirus, che in background gli dà un'occhiata al sistema mentre lui continua a lavorare, senza tutte queste storie di dischetti puliti. Ma abbiamo detto che questa è una illusione di sicurezza, non una vera sicurezza. La vera sicurezza si ottiene avviando il Dos da un dischetto pulito e protetto.

E visto che si deve far partire tutta la baracca da un dischetto allora tanto vale usare un antivirus per Dos e non per Windows: già è una perdita di tempo dover avviare il sistema da un dischetto per controllare se ci sono virus, non si vede perché si dovrebbe triplicare la perdita di tempo per far caricare anche Windows *(da dischetto!)* prima di poter scandire il disco fisso. E facciamola da Dos, 'sta scansione, che abbiamo altro da fare che perdere tempo con i giochetti. Ma stavolta sul serio.

Stefano Toria

sequenza di byte e null'altro. Sto scrivendo questo articolo su un Apple Macintosh (microprocessore Motorola 68020, perfettamente incompatibile con l'Intel 80386 SX contenuto nel mio notebook Tandon); poco fa ho prelevato dei programmi via modem, tra cui un paio di programmi che mi servono per la macchina Dos. Se ne stanno lì seduti sul disco fisso del Mac, in attesa che io li sposti su un dischetto e li trasporti sulla macchina Dos. Se nel frattempo cercassi di eseguirli, il mio Mac non sarebbe in grado di farlo.

I programmi li ho presi da un sistema Unix, un Sun con una versione custom dello Unix. Anche là i programmi erano semplici sequenze di byte, non diverse nella struttura e nella natura da un testo o da un'immagine GIF. Non avrei mai potuto eseguire i miei programmi Dos su quel Sun.

Ma anche se si fosse trattato di un 386 o un 486 con la propria versione di Unix (come le macchine del nostro MC-link) non sarebbe cambiato nulla: le istruzioni Intel contenute nel mio programma Dos potrebbero teoricamente essere eseguite dal microprocessore, ma non possono essere eseguite sotto Unix, perché i due sistemi non sono compatibili. Il virus, scritto per il Dos, non saprebbe dove cominciare a mettere le mani, se per avventura venisse eseguito sotto Unix. E lo Unix, inflessibile nella sicurezza al contrario del Dos, interromperebbe immediatamente l'esecuzione di un programma così clamorosamente «intruso».

È facile comprendere dove stiamo andando a parare: su un sistema che non sia il Dos i programmi eseguibili scritti per il Dos non sono altro che sequenze di byte. La scansione, effettuata su uno di questi sistemi, dovrà semplicemente consistere nell'andare a verificare se sono presenti determinate sequenze di byte, eventualmente disposte secondo criteri particolari nel caso dei virus polimorfi. Non è necessario preoccuparsi di stealth e tunneling, quando la ricerca di virus viene effettuata su programmi eseguibili sotto Dos ma appoggiati su elaboratori gestiti da altri sistemi operativi.

Un caso particolare: i Netware Loadable Module (NLM)

Il NetWare è un sistema particolarmente sicuro, che offre diversi livelli di sicurezza. L'accesso al sistema è controllato da password, e a ciascun nominativo di utente è associato un complesso di restrizioni. A ciascun file poi è assegnato un insieme di attributi e di privilegi. Alcuni di questi sono analoghi agli attributi associati ai file Dos, ma a differenza di questi ultimi, che sono semplici «flag» facili da scavalcare, attributi e privilegi dei file su un server NetWare sono ben più rigidi.

I prodotti della Central Point Software per la prevenzione dei virus.

Il tallone di Achille del NetWare consiste nella necessità della esistenza di un «super-utente», in grado di controllare e gestire il sistema e stabilire le restrizioni e i privilegi per gli altri utenti. Normalmente questo super-utente ha il nome di «Supervisor», e nessuna restrizione si applica a chi accede a un server con l'identità di super-utente: può fare tutto ciò che vuole. Se un super-utente accede alla rete da un PC infetto, infetterà tutto ciò che incontra.

A partire dalla versione 3 del NetWare è stata introdotta una importante modifica. Mentre in precedenza il server era una scatola nera, configurabile dal gestore della rete, ma sempre e soltanto nell'ambito delle possibilità standard, con la nuova versione viene introdotto il concetto di NetWare Loadable Module (NLM). Un NLM corrisponde più o meno a ciò che un TSR è per il Dos: un programma scritto da terze parti, fatto in modo da interferire con l'ordinario funzionamento del sistema operativo in modo da estenderne la funzionalità.

Da qualche mese a questa parte non meno di cinque produttori di programmi antivirus hanno presentato sul mercato dei prodotti specifici per NetWare, cioè degli NLM. Il vantaggio di questo tipo di prodotti, come abbiamo visto, consiste essenzialmente nel fatto che il controllo sui programmi eseguibili viene del tutto sottratto all'utente, viene eseguito automaticamente e in un contesto in cui nessun virus può interferire per trarre in inganno il programma di controllo.

Il NetWare è un sistema operativo multitasking: per poter offrire risorse a centinaia di utenti deve essere in grado di eseguire più operazioni simultaneamente, ad esempio l'inoltro di un file a un utente, la ricezione di un altro file da un altro, il controllo della password di chi chiede di entrare, l'invio di una stampa alla stampante locale e magari il backup di un volume. Tutte queste operazioni vengono eseguite in modo non-preemptive, cioè senza interferenza del sistema: ogni task decide se e quando rilasciare il controllo al sistema operativo.

Una delle operazioni che possono es-

sere eseguite in un task è l'esecuzione di un NLM. Servendosi di un NLM apposito è possibile eseguire due diversi tipi di scansione:
— una su richiesta, per sottoporre a verifica l'intero server e determinare se si è verificata o meno infezione su qualsiasi programma eseguibile;
— una «al volo», su tutto ciò che entra o esce dal server nel momento stesso in cui si cerca di farlo entrare o uscire.

In quest'ultimo caso (più difficile da realizzare tecnicamente, ma assai più efficace) si riesce di fatto a prevenire l'infezione, o a rilevarla immediatamente dopo che si è verificata e quindi prima che possa spargersi. Di fatto questa modalità di scansione equivale alla installazione di un antivirus residente sui sistemi cliente, ma con un grado di protezione ben più consistente.

Di questi prodotti abbiamo avuto occasione di esaminarne tre. Ecco le nostre impressioni in sintesi.

Central Point Anti-Virus for NetWare

Annunciato lo scorso novembre in Italia, è ora disponibile il prodotto antivirus per NetWare che completa la gamma dei prodotti Central Point per la ricerca di virus.

CPAV per NetWare consiste in due confezioni incellofanate assieme, delle quali l'una contiene il modulo NLM con le relative istruzioni, l'altra gli eseguibili da installare sui sistemi cliente.

I prodotti della linea CPAV in realtà erano già da tempo predisposti per l'uso in ambiente NetWare. Già lo scorso anno avemmo l'occasione di verificare l'esistenza di questa funzione sulla rete NetWare che congiunge i vari uffici della Technimedia. In quell'occasione fu Massimo Truscelli a consultarmi perché, dopo aver trovato un virus Form su uno delle centinaia di dischetti che entrano in redazione per centomila motivi (e che vengono tutti regolarmente verificati), aveva notato sul server una segnalazione in merito al rilevamento del virus.

Le versioni più recenti dei tre prodotti (CPAV per Dos, per Windows, per NetWare) sono tutte in grado di comunicare tra di loro. Inoltre la nuova versione per NetWare consente di gestire con semplicità anche reti dalla struttura molto complessa. In presenza di più server infatti è sufficiente aggiornare la versione installata su uno di essi perché esso provveda a trasmettere agli altri server la versione aggiornata, determinando un allineamento pressoché istantaneo.

In occasione del rilevamento di un virus il modulo NLM aggiorna un file di log, visibile dal supervisore, e può intraprendere diverse azioni a seconda di come viene configurato: può inviare un messaggio al supervisore servendosi di una funzione di mail ovvero comporre, su un modem collegato al server, il numero del cercapersone («Teledrin») della persona che dovrà occuparsi del problema.

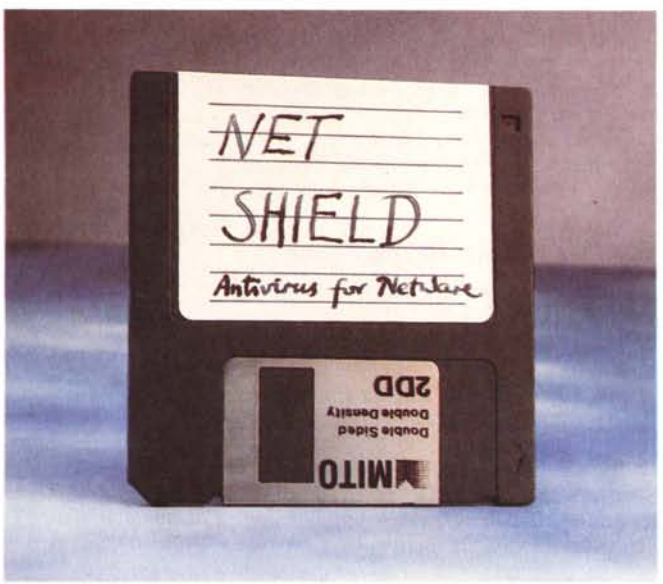
Il sistema offre anche una funzione di rilevamento generico di «comportamento virale», cioè un monitor di attività sospette. Ogni volta che un programma chiede di accedere a un file eseguibile sul server (un'operazione che normalmente è riservata al Dos) il monitor verifica le intenzioni del programma, e se risultano sospette lo segnala in un file di log. A nostro avviso si tratta di una funzione estremamente soggetta al rischio di falsi positivi, che non andrebbe utilizzata se non come misura di supporto e soltanto laddove si è certi che mai nessun utente avrà bisogno di effettuare modifiche a un eseguibile.

Le capacità di identificazione dei virus, verificate sul campione standard che ormai utilizziamo da tempo, risultano buone; non abbiamo condotto prove in merito ai tempi perché non avrebbero senso. CPAV per NetWare infatti, essendo un NLM, gira sul server e quindi non ostacola in alcun modo il normale funzionamento dei sistemi cliente. Con questo Anti-Virus per NetWare la Central Point ha sviluppato un prodotto di qualità accettabile, con forse un po' troppa attenzione all'interfaccia a scapito della sicurezza. Infatti per accedere alle funzioni di controllo del prodotto occorre servirsi di una stazione cliente, su cui dovrà essere eseguito un apposito programma peraltro molto ben curato nell'interfaccia. Ma ogni volta che il supervisore accede alla rete corre il rischio di essere un formidabile veicolo di infezione; avremmo preferito vedere una scarna e monotona interfaccia riga-per-riga sulla console del server, esente dal rischio di infezione diretta, piuttosto che una bellissima interfaccia grafica su una workstation che può benissimo infettarsi.

McAfee NetShield

Secondo l'affermata strategia aziendale della McAfee Associates anche questo prodotto viene distribuito come shareware, esattamente come i corrispondenti programmi che fanno parte della serie VIRUSCAN. La versione che abbiamo esaminato è stata prelevata direttamente dall'elaboratore della McAfee Associates, effettuando una richiesta di FTP sulla rete Internet tramite MC-link.

Il programma arriva sotto forma di un archivio .ZIP contenente, oltre al modulo eseguibile, anche i soliti file che accompagnano i prodotti di McAfee: elenco dei virus riconosciuti, lista degli agenti autorizzati, programma VALIDATE.COM con la relativa documentazione, informazioni sul forum McAfee su CompuServe, e ovviamente la documentazione del programma. La documentazione è scritta in modo coerente e sintetico, secondo la tradizione della McAfee Associates. Le istruzioni sono poche e chiare: l'installazione del prodotto consiste semplicemente nel copiare i file NETSHLD.NLM (l'eseguibile) e VIR.DAT (le «firme» dei virus) sulla directory SYS:SYSTEM e



Il dischetto e «domestico» perché il programma di McAfee NetShield è distribuito anche tramite BBS.

nell'inserire il comando LOAD NETSHLD nell'AUTOEXEC.NCF. Quando il NetWare viene riavviato verrà caricato il modulo NETSHLD, che offrirà al supervisore diverse opzioni, controllabili dalla console del server. Il sistema è gestito tramite una serie di menu, rigorosamente eseguibili soltanto dalla console. Sembra che sia stato fatto un certo sforzo per conciliare le esigenze di una interfaccia gradevole e della massima sicurezza. Poiché non è necessario svolgere le funzioni di controllo da un sistema cliente, ma si deve per forza utilizzare il server, non potrà mai accadere che il supervisore infetti il server durante una sessione di gestione di NetShield.

NetShield offre le funzioni di scansione «al volo» e a tempi prestabiliti (giornalieri, settimanali, mensili). Il gestore può scegliere tra diverse azioni che NetShield potrà svolgere ogni volta che viene scoperto un virus: rimuovere il file infetto, lasciarlo dove si trova, trasferirlo in una diversa directory. Viene inoltre mantenuto un file di rapporto su tutte le operazioni compiute.

Alla prova di identificazione di virus risulta che NetShield si comporta come gli altri prodotti shareware della McAfee: una buona capacità di rilevamento di virus, ma una certa imprecisione nella corretta identificazione del ceppo e della variante, con una tendenza determinata a raggruppare i virus per «famiglie» (si veda a questo proposito l'intervista a John McAfee, che abbiamo pubblicato lo scorso dicembre).

NetShield quindi è un prodotto accettabile, ma rischia di vedersi sorpassare sul mercato da prodotti con un marketing più aggressivo, soprattutto nel nostro Paese. La formula dello shareware, assai gradita agli utenti finali soprattutto se hobbisti, è per contro piuttosto mal vista dai professionisti dell'informatica, specie dagli uomini di azienda, che hanno assorbito acriticamente le informazioni (spesso errate e comunque quasi sempre approssimate) sulla presunta scarsa affidabilità di BBS e shareware.

Sophos Sweep for NetWare

Abbiamo avuto occasione di parlare della Sophos alcuni mesi fa, in occasione della recensione di due prodotti della dinamicissima casa di Abingdon. In quell'occasione, quando ci occupammo di Sweep per Dos, facemmo notare che si tratta di un prodotto dalle ottime caratteristiche tecniche, assai semplice nella struttura e nell'interfaccia, e destinato (anche per ragioni di prezzo) a un pubblico di fascia alta.

Analoghe considerazioni valgono anche per la versione per NetWare. L'installazione, se possibile, è ancora più semplice di quella degli altri prodotti che abbiamo visto: è sufficiente copiare un solo file dal disco di distribuzione alla directory SYS:SYSTEM e inserire il comando LOAD nella sequenza di attivazione del server, e il gioco è fatto.

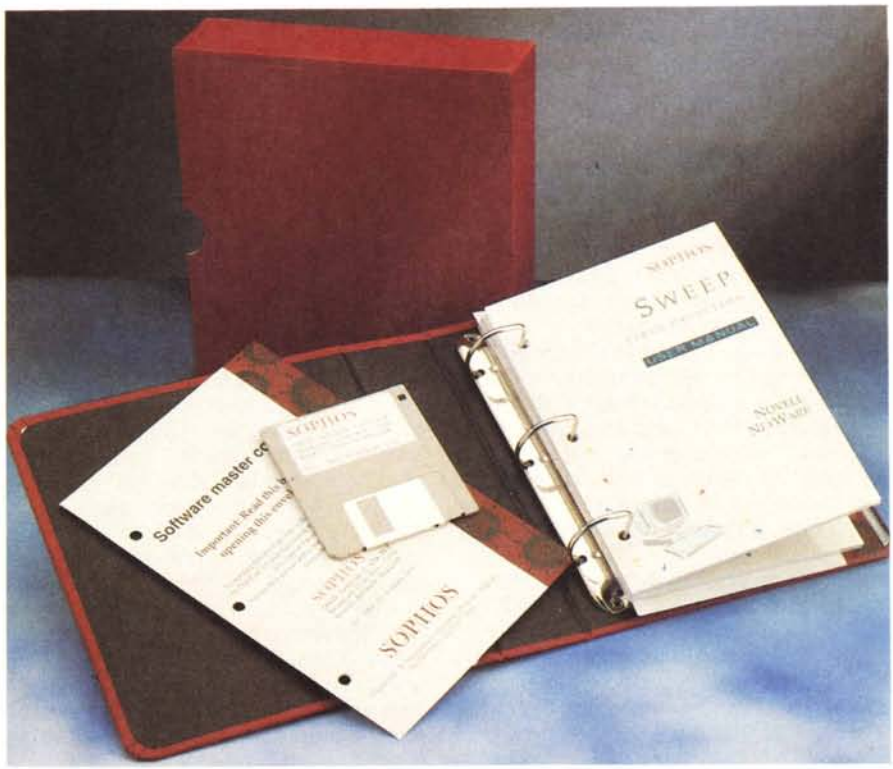
Per scelta esplicita della Sophos, Sweep for NetWare non è stato dotato di una funzione di scansione «al volo», poiché la versione 3 del sistema operativo NetWare non consente di farlo in modo perfettamente pulito. In attesa della versione 4, che offrirà questa possibilità, gli utenti di Sweep dovranno accontentarsi della possibilità di effettuare una scansione continua in background. Certo, l'identificazione preventiva sarebbe meglio, ma anche con il metodo adottato da Sweep è possibile un rilevamento precoce e un rapido contenimento delle infezioni. Il sistema è estremamente semplice da utilizzare, le opzioni sono poche e chiare e possono essere gestite esclusivamente dalla console del server.

Con l'acquisto di Sweep for NetWare si acquista anche una site license per la corrispondente versione Dos del prodotto, con la possibilità di sottoporre a verifica anche tutte le singole stazioni cliente collegate alla rete.

Ottime le capacità di corretta identificazione del campionario di virus.

MC

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



Il pacchetto Sophos Sweep per NetWare.

Central Point Anti-Virus for Netware

Produttore:
Central Point Software, 15220 Greenbrier Pkwy - Beaverton, OR 97006 USA.
Tel. (001) 503-690-8088.
Distributore:
OPC-LAN
Milano - Tel. (02) 2870083
Prezzi *(IVA esclusa):*
Central Point Anti-Virus per netware *L. 1.590.000*
Central Point Anti-Virus per DOS *L. 230.000*

Netshield

Produttore:
McAfee Associates, Inc., 3350 Scott Blvd, Bldg 14 - Santa Clara, CA 95054-3107, USA.
Tel. (001) 408-988-3832.
Distributore:
Ultimobyte Editrice Srl
Via Aldo Manuzio, 15 - 20124 Milano.
Tel. (02) 6555306
Prezzi:
NetShield 2-5 *L. 600.000 Server*
NetShield 16-20 *L. 420.000 Server*
NetShield 51-100 *L. 370.000 Server*

Sweep for Netware

Produttore:
Sophos Ltd., 21 The Quadrant, Abingdon Science Park - Abingdon, Oxon 0X14 3YS, Gran Bretagna. Tel. (0044235) 559933.
Distributore:
Telvox Teleinformatica Sas
Via F.lli Cairoli, 4/6 - 40212 Bologna.
Tel. (051) 252784
Prezzi: *(IVA esclusa):*
Sweep 1 coppia di PC *L. 737.500*
Sweep 25 coppie *L. 1.237.500*
Sweep oltre le 25 coppie *L. 2.237.500*

Più di settecento pagine, novemilacinquecento prodotti hi-fi con relativi prezzi (che sono aggiornati mese per mese su AUDIOREVIEW), seimilacinquecento foto, cinquanta pagine di articoli monografici che svelano tutto ciò che è necessario sapere prima di scegliere ogni singola parte del vostro impianto hi-fi. Tutto questo è AUDIOGUIDA HI-FI: l'alta fedeltà al gran completo. Ideale per ascoltare bene, indispensabile per acquistare meglio.

Indispensabile volume d'ascolto.

technimedia
Pagina dopo pagina, le nostre passioni.

AUDIOGUIDA HI-FI '92/'93. Una sonora lezione.