Il percorso dell'infezione

Accesso di un virus in un sistema e riconoscimento della sua presenza

di Stefano Toria

Si è visto negli articoli precedenti quali sono le caratteristiche che permettono di stabilire che un particolare programma fa parte della categoria dei virus, e tra queste la disposizione a replicarsi e a sfuggire all'identificazione.
Questo articolo analizza i possibili percorsi che un programma aggressore può seguire nel perseguimento del proprio obiettivo. La conoscenza di tali percorsi è fondamentale per determinare la vulnerabilità di un determinato sistema, cioè la possibilità che il sistema divenga un obiettivo per un particolare virus, in modo da poter stabilire le eventuali misure di sicurezza per evitare che ciò accada

Esecuzione di un programma

L'accesso di un virus in un sistema si verifica nel momento in cui viene eseguito il programma che lo ospita. Durante questa fase vengono eseguite anche le istruzioni che compongono il virus, solitamente all'insaputa dell'utente, e si compiono le operazioni previste dall'ignoto programmatore che ha realizzato il programma maligno. La prima nozione da chiarire consiste quindi nella definizione del concetto di esecuzione di programma.

Il sistema MS-DOS agisce sotto il controllo di un programma supervisore, detto «shell» o CLI (Command-Line Interpreter), che comunemente è costituito dal programma COMMAND.COM distribuito assieme al sistema, ma che può essere sostituito da altri analoghi programmi che svolgano la stessa funzione. Questo programma supervisore interpreta i comandi scritti a tastiera e pertanto costituisce il principale mezzo di dialogo tra utente e sistema operativo. Con una certa approssimazione, si può scindere il comportamento dello shell nelle seguenti fasi:
— presenta il prompt (solitamente del tipo C> oppure C:\>), attende che l'utente scriva una stringa di caratteri sulla tastiera e accetta tale stringa;
— analizza la stringa separandola nei suoi elementi, prende il primo elemento e lo interpreta come un comando;
— tenta di eseguire il comando verificando, nell'ordine, se si tratti di un comando «interno» cioè contenuto nello stesso sistema, oppure se esista un file binario con nome uguale al comando ed estensione .COM, oppure .EXE, oppure se esista un file di testo contenente comandi del sistema (.BAT); in ognuno di questi casi, verranno eseguite rispettivamente le istruzioni corrispondenti alla funzione interna del sistema operativo, oppure quelle contenute nel file con estensione .COM o .EXE, oppure quelle del batch interpreter;
— se l'esecuzione del comando fallisce, il sistema lo segnala all'utente.

L'esecuzione di un comando dell'utente darà quindi luogo in ogni caso all'esecuzione di uno o più programmi binari. Nell'ipotesi più semplice verrà eseguito il solo COMMAND.COM, come ad esempio nel caso in cui l'utente scriva un comando che consiste in una funzione interna come SET, ECHO o PROMPT, oppure qualora richieda l'esecuzione di un batch che contenga soltanto comandi di questo genere. Altrimenti il DOS caricherà in memoria un file binario e darà inizio alla sua esecuzione, durante la quale potrà essere disposto il caricamento di ulteriori file, che verranno a loro volta eseguiti e così via.

Lo schema qui riportato descrive il comportamento dello shell una volta che il sistema MS-DOS sia stato correttamente caricato all'accensione dell'elaboratore. Ma anche durante la fase di avvio del sistema si dà luogo all'esecuzione di programmi e in particolare:
— all'atto dell'accensione, quando il microprocessore riceve il primo impulso elettrico, viene eseguito un particolare programma previsto dal costruttore e memorizzato in una ROM. Questo programma, detto POST (Power-On Self Test, ossia autodiagnostico all'accensione) procede al controllo di tutte le funzioni del sistema, segnalando eventuali

Ecco come appare il PC prima di incontrare il virus.

L'utente non lo sa, ma questo dischetto, contenente una copia artigianale di un noto programma, è infetto dal virus Datacrime IIB, uno dei più pericolosi virus in circolazione.

difetti che ne possano pregiudicare l'uso, e procede quindi all'esecuzione della fase successiva;
— dopo il POST viene eseguito il «bootstrap» che consiste nel caricamento da disco delle funzioni elementari del sistema operativo. La sequenza più comune di bootstrap consiste nella scansione dei dispositivi a disco installati nell'elaboratore, per ricercare le istruzioni che compongono tali funzioni elementari. Viene acceduto prima il drive per floppy disk (solitamente il drive A:), quindi il secondo drive per floppy disk se presente (il B:), quindi il disco fisso. Se uno dei drive per floppy disk contiene un disco, ne viene letta una particolare zona detta «boot sector», che riporta le istruzioni per il caricamento del nucleo del sistema operativo. Se per contro nessun drive per floppy disk contiene un disco, la sequenza procede fino al raggiungimento del disco fisso. Su quest'ultimo la zona che viene acceduta è la tavola delle partizioni, che descrive il modo in cui è ripartito lo spazio sul disco fisso, e quale sia la partizione attiva, quella cioè da cui dovrà essere caricato il sistema operativo. La tavola delle partizioni contiene anche un programma per l'accesso alla partizione attiva, che viene quindi acceduta per mezzo di tale programma. Dal boot sector della partizione attiva viene prelevato ed eseguito il programma di caricamento del nucleo del sistema operativo;
— in qualsiasi modo si sia raggiunto il boot sector, questo determina il caricamento l'avvio del nucleo del DOS, e l'esecuzione di COMMAND.COM che rimane residente in memoria fino allo spegnimento del sistema o fino alla successiva sequenza di bootstrap.

Esecuzione di programmi e di virus

Nelle fasi descritte qui sopra, ogni esecuzione di programmi o istruzioni può comportare l'esecuzione e la replicazione di un virus, oppure lo scatenarsi dell'azione distruttiva dello stesso, oppure le due cose simultaneamente. È importante che l'utente abbia ben chiare le modalità di esecuzione dei programmi, anche solo secondo lo schema semplificato proposto qui sopra, poiché ogni volta che si parla di «esecuzione» di programmi egli dovrà far riferimento a tutte le fasi qui sopra descritte, e non soltanto al caricamento di un file binario con estensione .COM o .EXE.

Ad esempio, molti possessori di personal computer sanno che un dischetto «di sistema» contiene le istruzioni atte a «far partire» il sistema operativo; ma pochi sanno che anche i dischetti non «di sistema» contengono un analogo programma, memorizzato nella stessa posizione e cioè nel boot sector, e che questo programma serve soltanto a scrivere sul video il messaggio «Disco non di sistema — sostituire e premere un tasto quando pronti». Un virus che si trasmetta avvalendosi del boot sector può quindi infettare anche un dischetto non di sistema, e questo dischetto, ancorché non sia in grado di avviare il DOS, può comunque trasmettere l'infezione qualora l'utente lo dimentichi inavvertitamente chiuso dentro il drive all'atto dell'accensione della macchina (è accaduto anche all'autore di questo articolo).

Quando viene eseguito un programma che porta in sé un virus, come si è detto, viene eseguito anche il virus. Esso determinerà l'azione da svolgere, a seconda di come è stato progettato, e in alcuni casi procederà alla propria replicazione, ai danni di un programma finora indenne che diventa a sua volta portatore di virus.

Questo è un punto molto importante: qualsiasi programma, su qualsiasi supporto si trovi (disco fisso o dischetto) può divenire portatore di virus in qualsiasi momento. Alcuni virus restano residenti in memoria dopo la loro esecuzione, sfruttando la funzione TSR (Terminate and Stay Resident) del DOS. Una volta residente, un virus potrebbe intercettare tutti i comandi passati allo shell dall'utente, riconoscere le richieste di esecuzione di programmi e procedere all'infezione di tali programmi; di fatto, sono molti i virus che agiscono in questo modo. Per conseguenza, se un elaboratore si infetta con uno di questi virus, è sufficiente inserire per pochi istanti un dischetto nel drive — il tempo di eseguire un programma in esso contenuto — perché tale dischetto si infetti e diventi a sua volta portatore del virus.

Il percorso del virus

Si è visto quindi come un virus sia composto da istruzioni di programma, come tali istruzioni abbiano bisogno di un programma portatore per trasmettersi da un sistema a un altro, come il programma portatore debba essere eseguito su un sistema perché questo si infetti, e come l'infezione possa trasmettersi da un programma a un altro.

Per poter prevenire l'infezione del proprio elaboratore è quindi essenziale comprendere quali possano essere i percorsi che un virus può seguire per raggiungere una determinata macchina.

Si consideri il procedimento di installazione di un nuovo elaboratore, appena acquistato. Il rivenditore fornisce abitualmente l'elaboratore, che si supporrà dotato di disco fisso, con un corredo di manuali e dischi che costituiscono la dotazione software di base per il funzionamento dell'elaboratore. Poiché in questi articoli si prende sempre ad esempio l'ambiente MS-DOS, i manuali e i dischi riguarderanno questo sistema operativo, e si tratterà normalmente di una copia originale sigillata della opportuna versione del sistema. Avvalendosi di tale copia, l'utente procederà alla installazione del sistema operativo sul disco fisso dell'elaboratore, nelle note fasi di definizione della tavola delle partizioni, formattazione di ciascuna partizione (o dell'unica partizione se ne viene definita una sola), trasferimento del sistema operativo.

Al termine di queste operazioni l'utente è in grado di accendere l'elaboratore senza inserire alcun disco nel drive,

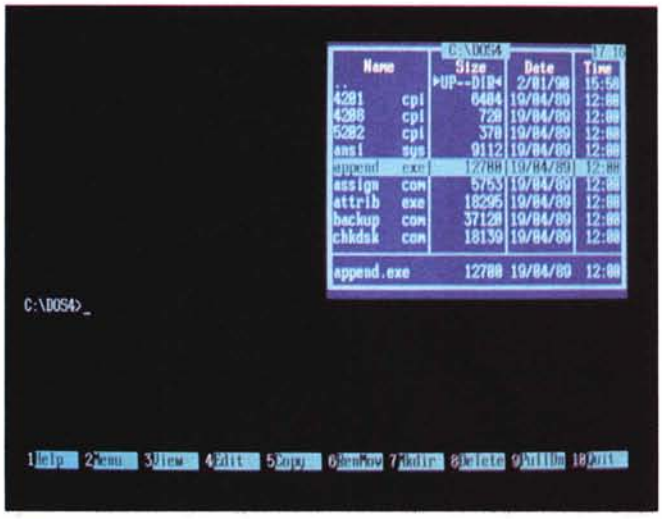
in quanto il sistema operativo risiede sul disco fisso. Inizierà quindi l'installazione di uno o più programmi applicativi, che avrà acquistato insieme all'elaboratore o separatamente ma di cui comunque si presume sia dotato, in quanto un elaboratore con il solo sistema operativo e senza alcuna applicazione può svolgere ben poche funzioni.

Ciascun programma applicativo si presenta anch'esso come un insieme di manuali e dischi, da cui l'utente installa il programma che successivamente rimane residente sul disco fisso.

Successivamente, durante il normale uso del sistema, l'utente richiederà continuamente l'esecuzione di programmi, che possono essere sia parte del sistema operativo (DOS), sia parte di applicazioni residenti sul disco fisso, sia applicazioni prelevate da dischetti appositamente inseriti di volta in volta nel drive.

In ognuna delle operazioni elencate (installazione del sistema operativo, installazione di applicazioni, esecuzione di programmi da disco fisso o da dischetti) uno o più programmi provenienti dall'esterno ottengono l'accesso all'elaboratore. Se uno di tali programmi è portatore di virus, tale virus può quindi esplicare la propria azione sull'elaboratore, replicandosi e determinandone l'infezione.

È quindi essenziale verificare le fonti di tutti i programmi che si eseguono, in quanto ciascuno di essi può contenere un virus. I più pericolosi sotto questo punto di vista sono quei programmi che presumibilmente sono passati per molte mani. La diffusa abitudine di ricorrere alla pirateria del software aumenta la probabilità di incorrere in un programma infetto. Normalmente infatti i programmi venduti legittimamente vengono sottoposti a un controllo di qualità, minore o maggiore a seconda della serietà del produttore del software, delle dimensioni della sua struttura, della professionalità della sua organizzazione. Tali programmi vengono generalmente riprodotti in appositi centri di riproduzione, in grado di produrre grandi volumi di copie in tempi ridotti. Tutto il procedimento è sottoposto a controlli, e pertanto i dischetti che vengono rinchiusi nelle buste sigillate che poi arrivano all'utente sono normalmente da ritenersi indenni da infezione. Sarà cura dell'utente controllare l'integrità dei sigilli quando acquista un programma: tale integrità garantisce l'acquirente contro la possibilità che i dischetti siano già stati utilizzati, con la possibilità — come si è visto — che si siano infettati.



Il file APPEND.EXE è ora infetto e contiene una copia di Datacrime IIB. Poiché esso viene eseguito nell'AUTOEXEC. BAT di questo PC, ogni volta che l'utente accende la macchina o la resetta corre il rischio di perdere definitivamente tutti i propri file. Infatti il Datacrime IIB esegue una formattazione a basso livello di una sezione del disco; a volte il disco risulta danneggiato in modo non rimediabile né dall'utente, né dal servizio di assistenza, ed è necessario inviarlo al laboratorio del costruttore per la riconfigurazione.

Chi acquista, o in altro modo si procura, software non originale si sottopone al rischio che tale software sia infetto. Le riproduzioni non autorizzate di software vengono effettuate solitamente senza alcun controllo, da parte di normali utenti di personal computer e non di centri specializzati. In alcuni casi si tratta di utenti non particolarmente esperti: ci si passa le copie «sprotette» dei più diffusi programmi applicativi così come ci si passa l'ultimo libro pubblicato, o la copia su cassetta dell'ultimo disco uscito. E una copia di un programma, eseguita su un sistema infetto, è quasi certamente infetta anch'essa.

Un notevole impulso alla diffusione dei virus proviene dai programmi per videogiochi. Tali programmi hanno una grande circolazione, quasi sempre essendo riprodotti dagli stessi utenti che se li trasmettono analogamente alle altre applicazioni.

Infine, i testi e gli articoli sulla sicurezza citano sempre invariabilmente BBS e gruppi di utenza come potenziali mezzi di diffusione di virus; anzi, alcuni utenti sono arrivati a ritenere pericoloso il semplice possesso di un modem collegato al proprio personal computer, tanto si è insistito sul rischio del prelievo di software da sistemi telematici. Questo è vero in teoria, in quanto sia i BBS che i gruppi di utenza hanno come scopo anche la diffusione del software di pubblico dominio; ma nella realtà non si è a conoscenza di alcun caso di infezione da virus proveniente da un BBS, anche e soprattutto per la grande professionalità dimostrata da chi gestisce questi sistemi.

Riconoscimento dell'infezione

Il virus, seguendo i percorsi più disparati, raggiunge quindi un determinato sistema e lo infetta. Come si è visto nello scorso articolo, l'infezione si può concretare in diversi modi, ma in ogni caso l'effetto è lo stesso: l'elaboratore contiene, in aggiunta a tutti i programmi che conteneva in precedenza, anche un nuovo programma, non previsto né conosciuto dal suo legittimo utente, che entrerà in azione al verificarsi di una data condizione, ed eseguirà un'azione prestabilita. Nel frattempo, non appena gliene viene data l'occasione, si replica; se l'utente fa uso di programmi su dischetto e li porta con sé per eseguirli su elaboratori altrui, il virus ne approfitta per avvalersene come portatori e proseguire la propria diffusione.

L'utente si accorgerà immediatamente che qualcosa non va se il virus mette in atto la sua carica distruttiva. Alcuni virus sono scritti con lo scopo di nuocere gravemente, ad esempio distruggendo il contenuto del disco fisso del sistema che li ospita (uno di questi è il

Ultim'ora
Scoperto l'autore di uno tra i virus più diffusi

È indonesiano l'autore del virus «Den Zuk». Questa informazione, che è giunta dopo che l'articolo di questo mese era stato già predisposto in redazione, proviene da Fridrik Skulason, una delle massime autorità mondiali sui virus.

Nel prossimo numero verrà approfondita la notizia, e si accennerà brevemente a come sono stati identificati i pochi autori di programmi aggressori noti alla comunità di ricerca.

Datacrime). Un'azione di questo genere non può sfuggire nemmeno al più disattento e inesperto degli utenti, e qualora tale utente sia anche imprevidente, e non abbia una copia recente del contenuto del disco fisso, si ritroverà di punto in bianco senza più nemmeno un dato e senza la possibilità di ricostruire ciò che ha perduto. Anche in altri casi il virus farà notare la propria presenza; ad esempio, un virus che si sovrapponga a un programma eseguibile, rendendolo ineseguibile, non sfuggirà all'attenzione nel momento in cui l'utente cerchi di eseguire il programma infetto.

In altri casi il comportamento del virus è più subdolo, ed esso può restare latente in un sistema anche molto a lungo prima di essere identificato. Questi sono i virus più pericolosi, in quanto a un lungo periodo di latenza corrisponde una lunga fase di replicazione e di corruzione di un numero via via sempre crescente di programmi; inoltre, cresce la probabilità che l'utente porti con sé un programma infetto su un floppy disk, determinando la trasmissione del virus in altri ambienti.

L'ideale sarebbe quindi che l'utente si avveda della presenza di un virus prima che questo possa minimamente agire sull'elaboratore; addirittura, prima ancora di eseguire un nuovo programma l'utente dovrebbe essere certo della innocuità del programma. Questo non è possibile in assoluto; tuttavia si può raggiungere un ragionevole grado di certezza, avvalendosi dei programmi c.d. di «scansione». Tali programmi esaminano i file che sono potenziali portatori di virus (.COM, .EXE, boot sector, etc.) in cerca degli elementi identificativi dei virus già noti. Se viene riscontrata la presenza di uno di tali elementi in un programma, viene attirata l'attenzione dell'utente, che dovrà decidere cosa fare del programma sospetto. Se nessun programma viene segnalato come sospetto, non per questo è esclusa la presenza di un virus: semplicemente è esclusa la presenza di uno dei virus noti a chi ha sviluppato il programma di scansione, e alla data in cui tale programma è stato sviluppato. Per questo motivo è indispensabile non distruggere un virus, ma farlo pervenire il più presto possibile al più vicino (e più fidato) centro di ricerca antivirus, perché la conoscenza di tali programmi è una delle migliori armi per la lotta contro i virus. Inoltre è altrettanto importante che qualora si faccia uso di programmi di scansione antivirus ci si procuri sempre la copia più recente.

Si è detto che in mancanza di segnalazioni da parte di un programma di scansione si può ritenere che un determinato programma o dischetto sia immune da infezioni da uno dei virus noti. Ma non è impossibile che un programma porti un virus che non sia ancora noto alla comunità di ricerca, sia perché si tratti di un virus di nuova realizzazione, sia perché sia una nuova variante di un virus già noto. Nessun programma di scansione può quindi offrire una garanzia di sicurezza pari al 100%.

Alcuni virus poi sono scritti con il preciso intento di nascondersi. Esistono delle tecniche ben precise, messe a punto da ingegnosi quanto ignoti programmatori, che consentono a un virus di sfuggire all'identificazione anche da parte dei più abili programmi di scansione.

In questi casi occorre considerare una caratteristica che praticamente tutti i virus condividono. Si è visto come un virus esamini un programma potenzialmente portatore e, nel caso in cui determini che esso non è infetto, procede a replicarsi utilizzando tale programma come portatore. Un virus dovrà quindi essere in grado di determinare se un programma già lo ospita, e dopo essersi replicato a spese di un programma, dovrà segnalare il fatto di essersi installato, a beneficio di una eventuale successiva esecuzione di se stesso che dovrà quindi scartare il programma già infetto nella fase di ricerca di un bersaglio per la replicazione.

Tutte queste operazioni modificano il programma portatore. Nel normale funzionamento di un elaboratore, generalmente accade che i dati vengano modificati mentre i programmi restano invariati. (Si deve sottolineare che questi esempi prendono in esame l'uso che un utente medio fa di un elaboratore. Nel caso di chi sviluppa software, invece, è più frequente la modifica ai programmi che non quella ai dati). Quindi, una qualsiasi modifica a un programma deve far insospettire. Ma il solito utente

Il «laboratorio biologico»: un invito ai lettori

Come si accenna altrove in questo articolo, l'unico modo per debellare un programma maligno e — se possibile — per prevenirne l'azione è di conoscere approfonditamente questo programma. È intenzione di MCmicrocomputer costituire un laboratorio di ricerca per raggiungere una conoscenza approfondita dei programmi aggressori. Una pronta e tempestiva informazione sui virus consente una migliore prevenzione contro i rischi specifici; inoltre, è essenziale che le recensioni dei prodotti software venduti per la difesa dai virus riportino il comportamento di tali prodotti in presenza di effettivi virus, per stabilire se un determinato prodotto possa generare falsi allarmi o, per contro, si lasci sfuggire un vero virus.

È per questa ragione che la recensione del ViruScan di John McAfee, anticipata nel numero precedente, non viene riportata su questo articolo ma verrà pubblicata sul prossimo. Stiamo trattando con uno dei principali centri di ricerca europei per l'acquisizione di una copia di ciascuno dei virus in loro possesso. In seguito, l'attività del laboratorio antivirus fornirebbe il supporto necessario per la recensione dei nuovi prodotti segnalati nel campo della lotta ai programmi aggressori.

La costituzione del laboratorio è uno scopo meno semplice da raggiungere di quanto sembri, per tre ragioni:

— molti programmi maligni sono scritti con l'obiettivo di sfuggire il più possibile all'individuazione, per diffondersi il più possibile e causare il maggior danno possibile prima di essere scoperti; disassemblare e analizzare un programma di questo genere si è dimostrato, in alcuni casi, un compito tutt'altro che banale;

— è indispensabile una buona collaborazione con la ristretta comunità internazionale che opera in questo settore della ricerca informatica, e che — per ragioni più che comprensibili — è estremamente diffidente e cauta nell'ammissione di nuovi membri; MCmicrocomputer si sta adoperando in questa direzione, per conquistare la fiducia delle persone che contano nella ricerca antivirus;

— infine, per poter analizzare un programma occorre ovviamente esserne in possesso.

È su quest'ultimo punto che MCmicrocomputer chiede l'assistenza e la collaborazione dei suoi lettori. Chiunque sia in possesso di un programma sospetto, è invitato a spedirlo in redazione, su un dischetto di qualsiasi formato (5,25" o 3,5", bassa o alta densità), in busta chiusa, con il proprio cognome, nome e indirizzo, unitamente all'indicazione «Laboratorio antivirus», all'interno della busta. È importante che nulla venga indicato esternamente alla busta.

Chi fosse dotato di modem e abbonato a MC-Link, potrà inviare il file incriminato direttamente in filebox a MC0100 (MCmicrocomputer) o a MC0170 (Stefano Toria); questo metodo non potrà essere utilizzato, ovviamente, per i virus che si trasmettono tramite boot sector o tavola delle partizioni, ma soltanto per i virus parassiti che si avvalgono di un file binario come veicolo per il trasporto dell'infezione.

I contributi più interessanti e utili, a giudizio della redazione, verranno compensati con un abbonamento gratuito a MCmicrocomputer.

medio non si mette certo a controllare ciascun programma ogni volta che accende l'elaboratore, anche perché tale controllo è obiettivamente difficile e inoltre alcuni virus fanno in modo che tale controllo dia comunque esito negativo, e così facendo rendono più problematica la loro identificazione.

Esistono dei sistemi che tengono traccia delle modifiche fatte ai file, su specifica dell'utente che può richiedere il controllo routinario di gruppi di file. Tali controlli, che si avvalgono di sofisticate tecniche algebriche, sono tuttavia piuttosto lunghi e richiedono notevoli risorse, tanto da costituire quasi una ultima ratio, un procedimento da adottare quando i dati contenuti in un elaboratore sono molti e molto importanti e il rischio della loro perdita parziale o totale sia notevolmente superiore al costo che comporta il controllo routinario dei file eseguibili.

In ogni caso, l'utilizzo combinato di un programma di scansione e di un programma di controllo delle modifiche ai file garantisce una probabilità molto prossima al 100% di identificare un virus prima che abbia modo di agire.

Nei testi e negli articoli sui virus si suggerisce agli utenti di «tenere d'occhio eventuali comportamenti anomali del sistema», con il risultato che una società di consulenza statunitense, specializzata in problemi di sicurezza di sistemi informativi e in particolare in virus, è stata interpellata da un cliente che riportava apparentemente problemi di virus in una rete locale e ha riscontrato semplicemente una serie di falsi contatti negli spinotti che collegano i monitor alle unità centrali.

Con questo non si vuole dire che non è necessario nemmeno un minimo di attenzione. Ma per l'appunto ne basta un minimo: non occorre divenire degli Sherlock Holmes costantemente con la lente d'ingrandimento all'occhio, ma non dovrebbero nemmeno sfuggire dei particolari eclatanti: ad esempio, un programma che normalmente si avvia subito, pochi istanti dopo che si è premuto l'invio alla scrittura del comando di esecuzione, e che invece all'improvviso comincia a richiedere diverse decine di secondi per l'avvio; oppure un programma che ha sempre funzionato e che smette di funzionare; o ancora, un programma che non ha mai dato problemi di memoria e che improvvisamente comincia a segnalare scarsezza o totale mancanza di spazio in memoria RAM.

Non è detto che tutti questi sintomi corrispondano a dei virus, ma vale senz'altro la pena che l'utente si soffermi un attimo a pensare al proprio comportamento in tempi recenti: ha eseguito programmi nuovi provenienti dall'esterno? ha installato nuovo software, magari di provenienza non del tutto legale? ha consentito ad altri di utilizzare il suo elaboratore, con programmi propri? Se la risposta anche a una sola di queste domande è affermativa, conviene indagare più a fondo su quanto possa essere accaduto.

MS

Nel prossimo numero

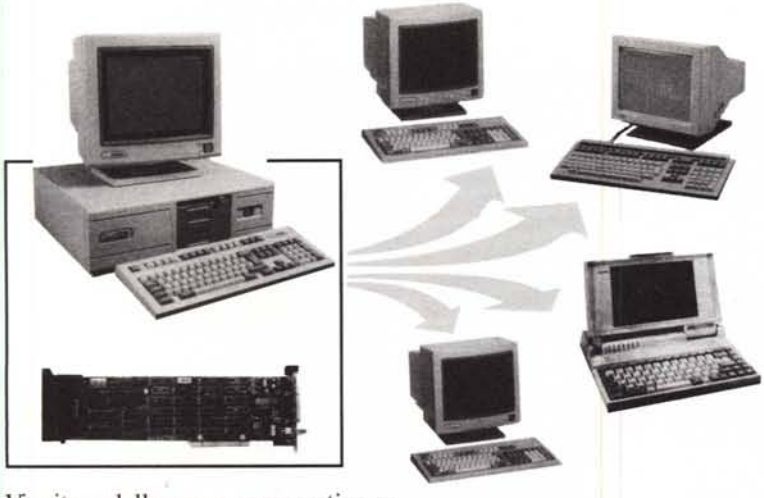
Saranno esaminati nel prossimo articolo i principali metodi di «cura» da adottare quando si riscontri, sul proprio personal computer, la presenza di un virus.

386MULTIWARE ALLOY

Invece di una rete o altri sistemi operativi complicati...

MULTIUTENZA DOS con MW.386,

il sistema che non si siede all'aumento di numero di utenti e che puoi installare e gestire da solo.



Vincitore delle prove comparative su
PC-MAGAZINE e MICRO-SYSTEMES FRANCIA

Incluse nel pacchetto:
- posta elettronica
- collegamento tramite modem
- spooling di stampa
- task-view: visione e controllo dell'attività degli altri terminali
- training mode: per le scuole, tutti i terminali vedono in tempo reale l'attività del professore
- BUS: ISA, EISA, MCA
- MW. 386/M: multitasking, monoutente 8 programmi DOS che possono girare contemporaneamente
- MW. 386/E : multitasking, multiutente fino a 5 utenti, 40 programmi DOS che possono girare contemporaneamente, (5 utenti x 8 programmi)
- MW. 386: multitasking, multiutente fino a 21 utenti, 168 programmi DOS che possono girare contemporaneamente, (21 utenti x 8 programmi)
- MULTINODE: connessione MW. 386/NOVELL per multitasking in ambiente NOVELL.

SOFCO s.r.l. 20154 MILANO - Via Borgese, 14
Tel 02/336.00.958 - Fax 02/336.00.962