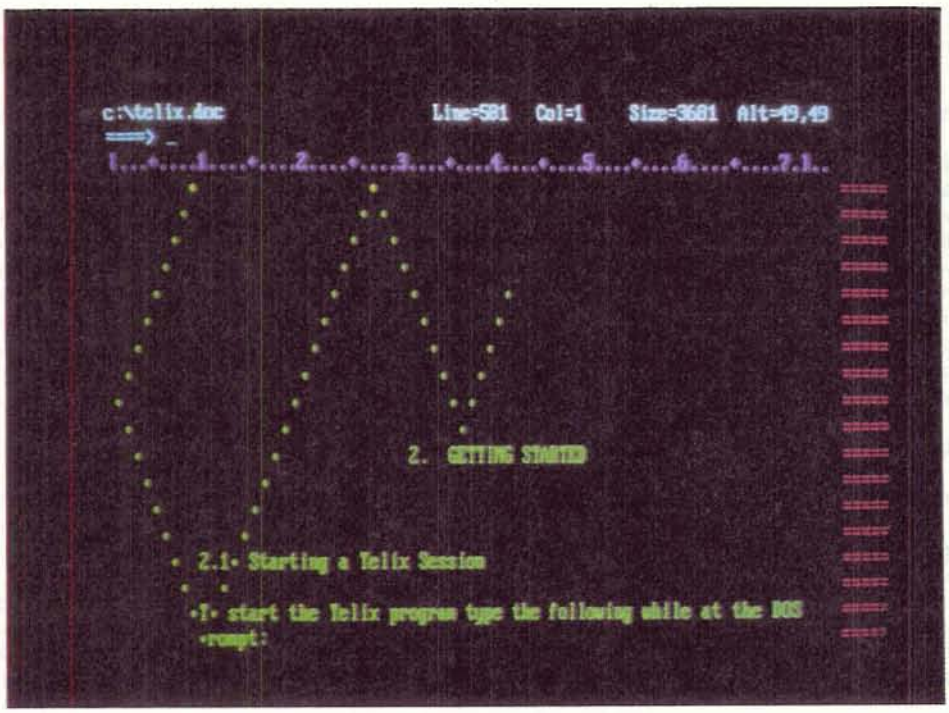
Panoramica sui virus del computer

di Stefano Toria (MCØ17Ø)



Tra i problemi che si pongono a chi si occupa di sicurezza di sistemi informativi, un posto di rilievo è occupato dai *virus*: termine introdotto nel 1983 da Len Adleman (un collaboratore di Fred Cohen, che fu il primo a teorizzare il funzionamento di un virus [2]).

Il problema virus è rilevante nella definizione e nella gestione della sicurezza dei sistemi informativi basati su personal computer, sicurezza che tuttavia non è limitata alla protezione dai virus o dagli altri analoghi fattori di rischio, cioè dai programmi aggressori. Non è questa la sede per una più ampia trattazione dell'argomento della sicurezza dei personal computer e si rimanda quindi ai numerosi testi disponibili.

Questo articolo si propone tre scopi: dare una definizione dei diversi tipi di programmi aggressori e descriverne il comportamento; esaminare in dettaglio i virus, con una serie di esempi tratti dall'ambiente Ms-Dos; fornire una indicazione di massima del rischio costituito dai virus e di come tutelarsi.

Definizione di «virus», «cavallo di Troia», «verme»

Si definisce virus un programma che ha la capacità di riprodursi introducendo una copia di se stesso in un altro programma, il quale diviene a sua volta portatore di virus. Possiamo rappresentare il funzionamento di un virus utilizzando una simbologia che si avvicina ai più comuni linguaggi di programmazione. Un esempio di struttura di un virus è riportato in figura 1 [2].

Il funzionamento del virus è semplice. La prima operazione eseguita dal programma è il tentativo di infettare un programma-oggetto non ancora infetto. Il programmatore che realizza il virus sceglie un proprio criterio per stabilire se un programma è già stato infettato. Nell'esempio abbiamo usato un criterio banale, e cioè che ogni programma infetto deve iniziare con una riga che

```
program virus :=
{1234567;

subroutine infetta-programma-oggetto :=
  {loop: file = programma-oggetto-a-caso;
  if prima-riga-di-file = 1234567
        then goto loop;
  anteponi virus a file;
  }
main-program :=
  {infetta-programma-oggetto;
  goto fine;
  }

fine: }
```

Figura 1
Esempio di virus.

contiene «1234567». Una volta accertato che il programma scelto è incontaminato, il virus lo infetta anteponendo una copia di se stesso al programma. In questo modo, quando quel programma verrà eseguito, saranno eseguite per prime le istruzioni del virus: il programma così infettato è diventato esso stesso un portatore di virus e a sua volta infetterà altri programmi.

Per contro, se il programma scelto a caso dovesse risultare già infetto, la procedura di infezione proseguirebbe con la ricerca di un altro programma da contaminare.

Si potrebbe obiettare che l'esempio dato non è completo in quanto è indefinito il comportamento del virus nel caso che nel sistema su cui il programma portatore viene eseguito non vi siano programmi incontaminati; ma lo scopo di questa trattazione non è di istruzioni per guastatori informatici.

Al termine della procedura di infezione, il virus passa il controllo al programma portatore (goto fine).

Il concetto di virus in sé non comporta alcun elemento qualitativo. Tuttavia, è grande il rischio che un virus sia a sua volta portatore di un «cavallo di Troia».

Si definisce *cavallo di Troia* un programma aggressore che nasconde la sua presenza dietro le apparenze di un programma innocuo o dichiaratamente utile. A differenza del virus, il cavallo di Troia non ha alcuna capacità di riprodursi.

La possibile struttura di un programma (ad es. una rubrica telefonica) che contiene un cavallo di Troia è rappresentata in figura 2. Apparentemente si tratta di un normale programma che gestisce una rubrica telefonica, ma in realtà al termine della esecuzione di ciascuna funzione del menu, viene eseguita una routine nascosta (il cavallo di Troia) la quale controlla se una data condizione si è verificata; potrebbe trattarsi dello scadere di una data prestabilita, oppure di un numero predeterminato di esecuzioni del programma che contiene la routine. In ogni caso, se la condizione si verifica (if innesco), allora la routine compie il danno che il programmatore aveva predisposto (then danneggia).

Tutto questo accade all'insaputa dell'utente, a cui viene consegnata una versione compilata del programma, e che non è quindi in grado di rendersi conto del rischio che corre in quanto ovviamente non vede per intiero la struttura logica del programma stesso. Accade quindi quasi sempre che l'utente scopra che un dato programma contiene un cavallo di Troia soltanto dopo che questo ha svolto l'azione dannosa prevista.

Una caratteristica comune ai virus e ai cavalli di Troia è di avere bisogno di un programma portatore. Nel caso del virus, qualsiasi programma può divenire portatore quando viene contaminato. Nel caso del cavallo di Troia, l'immissione nel programma portatore deve, invece, essere effettuata da parte del programmatore che lo realizza.

La situazione purtroppo più frequente è quella in cui coesistono un virus e un cavallo di Troia (v. fig. 3).

In questo caso il programma svolge due funzioni distinte: quella di infezione tipica del virus, e il controllo del verificarsi della condizione che dà l'avvio all'azione dannosa, tipica del cavallo di Troia.

Esiste una terza tipologia di programma aggressore: è quella detta *verme*. Si definisce verme un programma che si riproduce in una rete di sistemi di elaborazione, trasmettendo una copia di se stesso a uno o più sistemi collegati e avviandone l'esecuzione [3]. Esso svolge la propria azione esclusivamente in un sistema distribuito. Un verme, attivato su uno dei nodi di una rete, si avvale delle funzioni di comunicazione con gli altri sistemi della rete per avviare l'esecuzione di una copia di se stesso su ciascuno dei sistemi collegati. Ciascuno dei vermi così originati svolgerà poi la stessa operazione, causando la propagazione di un programma che può sfuggire al controllo dei gestori di ciascuno dei sistemi collegati in rete. La situazione ipotizzata è potenzialmente disastrosa. Un esempio basti a confermare questa affermazione: il 2 novembre 1988 Robert T. Morris Jr., uno studente della Cornell University statunitense, attivò un verme su uno degli elaboratori del MIT, passando per una delle connessioni tra il MIT e la Cornell. Sfruttando alcune particolarità del sistema Unix, nel giro di otto ore il verme di Morris si propagò su circa 6.000 sistemi collegati alla rete DARPA Internet, causando ral-

Figura 2
Esempio di cavallo di Troia.

```
program rubrica :=
{

subroutine danneggia :=
  {qualsiasi danno si voglia compiere}

subroutine innesco :=
  {if condizione-prestabilita
        then return(true);
        else return(false);
  }

main-program :=
  {loop: presenta menù;
  if scelta-fine then goto fine;
  esegui funzione scelta;
  if innesco then danneggia;
  goto loop;
  }

fine: }
```

```
program bad-virus :=
{01234567;

subroutine infetta-programma-oggetto :=
  {loop: file = programma-oggetto-a-caso;
  if prima-riga-di-file = 01234567
        then goto loop;
  anteponi virus a file;
  }

subroutine danneggia :=
  {qualsiasi danno si voglia compiere}

subroutine innesco :=
  {if condizione-prestabilita
        then return(true);
        else return(false);
  }
main-program :=
  {infetta-programma-oggetto;
  if innesco then danneggia;
  goto fine;
  }

fine: }
```

Figura 3
Virus portatore di cavallo di Troia.

lentamenti e in molti casi interruzione del servizio sui sistemi colpiti. Il costo degli effetti di questo verme è stato stimato in quasi cento milioni di dollari tra ore di lavoro specialistico per l'identificazione e la eliminazione del verme su tutti i sistemi colpiti e disservizi all'utenza degli stessi sistemi. Morris è stato condannato a tre anni di arresto, una multa di $10.000 e 400 ore di lavoro a favore della collettività [4] [9].

L'utente di personal computer e i virus

Vedremo più avanti che esistono diverse decine di tipi di virus, e la lista è destinata ad allungarsi. Prima di esaminare i modi in cui il problema si pone in concreto, esaminiamo in breve alcuni principi generali.

1. *Diffusione di virus*: un virus si diffonde quando viene eseguito il programma portatore. È specificamente richiesta l'esecuzione di un programma: non si può diffondere un virus semplicemente perché viene listata la directory di un disco, oppure perché viene stampato il file che contiene le istruzioni del programma, a meno che la stampa del file di istruzioni non venga effettuata eseguendo un programma presente sullo stesso dischetto, e che questo programma non sia portatore di virus. In genere, comunque, l'unica possibilità perché un virus si diffonda è che venga eseguito il programma che lo contiene. Questo include anche il sistema operativo: che sia il Dos oppure il Finder, se si preleva il sistema operativo da un disco che non è quello che viene comunemente utilizzato per questa operazione, si deve considerare la possibilità che esso sia infetto.

2. *Latenza del virus*: un virus può raggiungere uno specifico sistema in diversi modi ma sempre per esecuzione del programma che lo trasporta. Una volta che si sia impiantato in un sistema, esso agirà secondo le modalità previste da chi lo ha realizzato. In particolare, è possibile che per un certo periodo il virus non dia alcuna manifestazione della propria presenza. Questa latenza non è dovuta al caso ma spesso si tratta di un artificio voluto da chi ha realizzato il virus; per un dato periodo il virus si limita a replicarsi, attaccando uno o più programmi ogni volta che viene eseguito. Se il portatore del virus è uno dei moduli del sistema operativo (ad esempio COMMAND.COM per il Dos) le infezioni saranno molte e ripetute. In questo modo il virus può diffondersi anche piuttosto rapidamente, sia sullo stesso sistema ospite che anche su altri sistemi, se l'utente del sistema infetto distribuisce ad altri copie di dischetti infetti.

3. *Attivazione del virus*: si è detto che il caso più frequente è quello dell'abbinamento di un cavallo di Troia a un virus. Allo scadere del periodo di latenza, l'esecuzione di un programma portatore del virus scatena gli effetti del cavallo di Troia. Questi possono essere i più disparati: dalla scrittura di messaggi sul video, alla formattazione del disco fisso del sistema ospite.

4. *Protezione dal virus*: nella maggior parte dei casi, a tutt'oggi, la protezione è realizzata esclusivamente *a posteriori*. Dopo che un virus ha colpito con gli effetti del cavallo di Troia che conteneva, l'utente cerca in qualche modo di ricostituire il proprio patrimonio di informazioni. Il danno può essere più o meno grande, a seconda del tempo che richiede tale ricostituzione; un danno limitato nel caso che l'utente avesse effettuato di recente un back-up dei propri dischi; danni più ingenti quando i dati debbano essere ricostruiti manualmente. Inoltre, un sistema già colpito da un virus può reinfettarsi, e anche questa eventualità dovrà essere tenuta in considerazione.

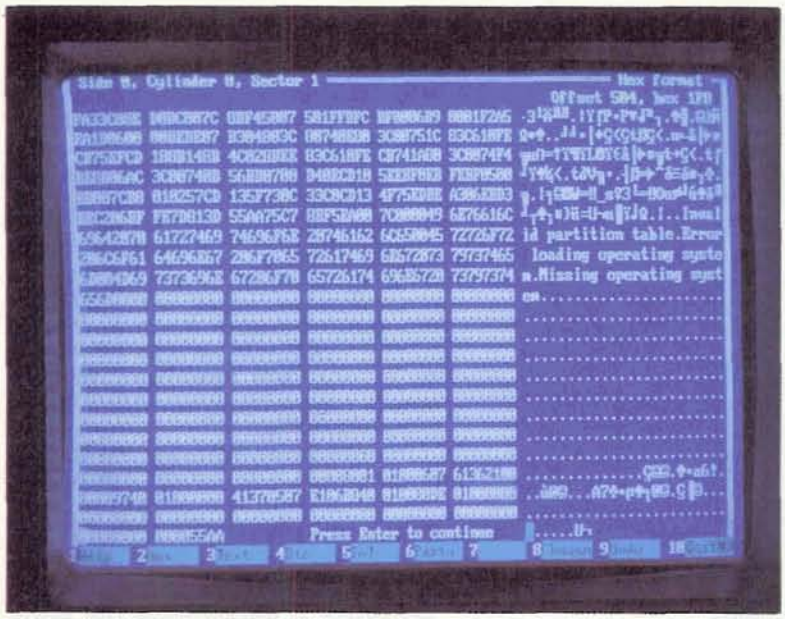
Più avanti presenteremo uno schema di protezione elementare, ma tuttavia tale da garantire una sufficiente tutela dal rischio di danneggiamento del patrimonio informativo.

Struttura e descrizione dei virus maggiormente diffusi

Nel mese di febbraio 1989, un articolo pubblicato sulla rivista «Computerworld» a firma di John McAfee, presidente della «Computer Virus Industry Association», faceva riferimento ai sei virus più diffusi, precisando nel contempo che il numero di virus noti, pari a sette nel febbraio 1988, era salito nel frattempo ad oltre 30 [10].

Prendeva così avvio quella che possiamo definire «epidemiologia informatica», la quale ha mutuato dalla scienza medica buona parte della terminologia. Come la microbiologia, infatti, distingue tra «ceppi» e «varianti» di virus biologici, anche per i virus informatici si adottano gli stessi termini per definire rispettivamente un determinato tipo di programma-virus, identificabile dal suo comportamento, e le varianti successivamente sviluppate a partire dal tipo originario.

L'avere mutuato queste denominazioni ha costituito allo stesso tempo un vantaggio e uno svantaggio. Il vantaggio consiste nell'avere a disposizione una terminologia già consolidata, senza la necessità di svilupparne una *ex novo*. Lo svantaggio è dato dal fatto che l'uso di questa terminologia, spesso citata a sproposito da persone non correttamente informate né in medicina né in informatica, ha determinato una confusione nel pubblico il quale, sottoposto a un bersagliamento di informazioni sull'AIDS da un lato e sui virus informatici dall'altro, può aver assimilato tra di loro due fatti totalmente estranei quali la diffusione di un problema che riguarda la sicurezza delle informazioni e la diffusione, ben più grave e preoccupante, di



Gli effetti del virus «Jerusalem» sono ben visibili rispetto all'immagine originaria.

una patologia umana attualmente incurabile.

L'elenco completo dei virus noti nell'ambiente Ms-Dos, pubblicato sul numero di agosto del «Virus Bulletin», comprende 93 diversi ceppi virali esaminati o in corso di studio, più altri 18 di cui si ha notizia, ma che non è ancora stato possibile esaminare. I numeri coincidono più o meno con quelli riportati da altre liste, ma poiché ciascun ricercatore adotta un proprio criterio di classificazione, accade che alcuni considerino ceppi autonomi quelli che per altri sono varianti, e viceversa. Tuttavia si può tranquillamente affermare che esistono oltre 110 tipi diversi di virus conosciuti.

Non esiste ancora una tassonomia ufficiale dei virus, e pertanto accade che lo stesso programma sia conosciuto con nomi diversi. In molti casi i nomi derivano dagli effetti apparenti del virus (è il caso di «PingPong», «Cascade», e altri), oppure dai messaggi che il programma scrive sul video («Datacrime», «Den Zuk», etc.), o ancora dalla provenienza geografica del virus o dal luogo di prima identificazione («New Zealand», «Jerusalem», «Lehigh»). Un diverso criterio di denominazione fa uso della dimensione in byte del virus, stabilita come incremento della lunghezza del programma portatore in seguito all'infezione. Questo criterio viene utilizzato a volte in aggiunta al precedente, altre volte in alternativa; in questo modo, il virus Datacrime è noto anche come 1280 e il Traceback come 3066, mentre i virus 405 e 800 non hanno altro nome all'infuori della propria lunghezza.

L'esame di un virus richiede che il programma portatore sia confrontato con una versione non infetta dello stesso programma, per isolare quelle che presumibilmente sono le istruzioni che costituiscono il virus. Si procede quindi a disassemblare il virus per studiarne il comportamento e stabilire tre cose: il meccanismo di riproduzione, il criterio di attivazione degli eventuali effetti dannosi (se il virus contiene un cavallo di Troia), e quale sia il danno che l'eventuale cavallo di Troia può compiere. Si cerca quindi di identificare una stringa unica di ricerca, detta «firma», che consenta di distinguere il virus oggetto di studio da tutti gli altri possibili programmi: in questo modo diviene possibile determinare se un programma generico è infetto da un dato virus controllando se all'interno del programma sospetto è presente la firma specifica di quel particolare virus.

Il primo virus di cui si ebbe notizia in Italia fu il **PingPong.** Sembra che sia stato sviluppato da un ignoto studente del Politecnico di Torino, e anche se un rappresentante dello stesso Politecnico, in un convegno sui virus tenutosi lo scorso anno a Milano, avrebbe affermato il contrario, il virus è noto all'estero come «Italian virus».

Si tratta di un virus che infetta il boot sector, cioè il settore iniziale di un disco, che contiene l'immagine del programma di caricamento del sistema operativo. Il virus occupa l'intero boot sector e un cluster nell'area dati, il quale viene marcato nella prima copia della File Allocation Table (FAT) come «bad cluster». Il virus si installa agganciando la funzione Int 13H del BIOS, che gestisce l'input/output su disco, si attiva ad ogni richiesta di lettura da disco, e controlla periodicamente (per circa un secondo ogni mezz'ora) se deve essere attivata l'immagine sul video. L'immagine consiste in una «pallina» (il carattere 07H) che si sposta diagonalmente sul video, «rimbalzando» contro i

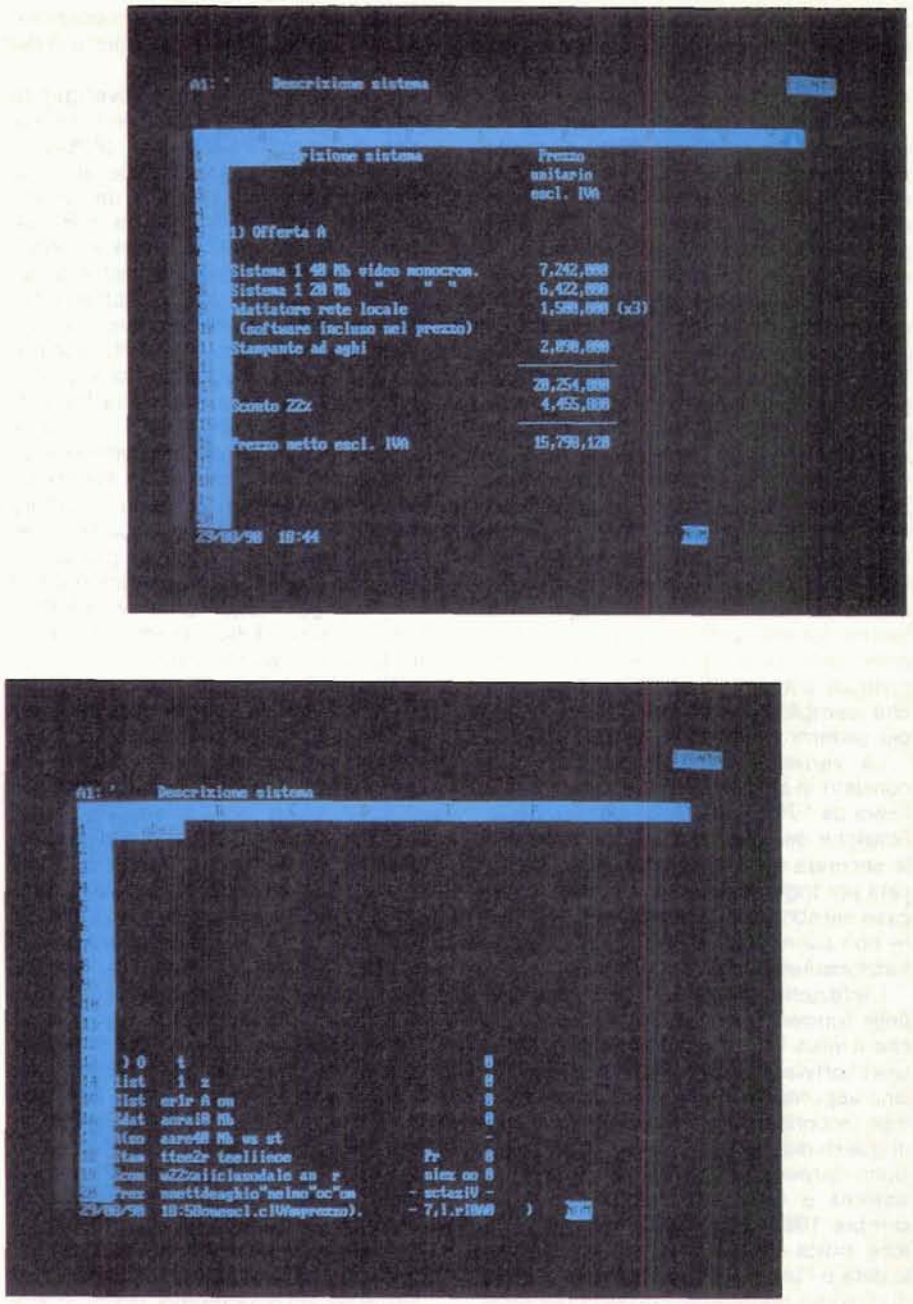
bordi e contro determinati caratteri. All'infuori del periodo di attivazione dell'immagine, tuttavia, il virus è permanentemente in controllo del sistema, poiché intercetta la funzione di lettura da disco e, in determinate condizioni, si riproduce trasferendo una copia di sé su dischi non infetti.

La versione originale del PingPong contiene un errore che ne rende impossibile il funzionamento sui microprocessori 80286 e 80386. Su queste macchine, l'attivazione del virus causa un loop infinito che blocca il sistema. Una variante del virus è stata modificata in modo da funzionare anche su macchine 286 e 386.

Il virus **Lehigh** fu identificato alla Lehigh University nel novembre 1987. Si trasmette utilizzando come portatore lo shell del sistema Ms-Dos, COMMAND .COM, di cui sfrutta uno spazio disponibile (lo stack) e che pertanto non cresce in dimensione. Ad ogni esecuzione di COMMAND.COM (e quindi ad ogni comando dato al Dos tramite la tastiera o da un file batch) il virus si attiva per tentare l'infezione di una nuova copia di COMMAND.COM, ad esempio in un dischetto appena inserito nell'unità A o B. Dopo la quarta infezione, il virus distrugge il contenuto del disco contenuto nell'unità centrale. La distruzione viene effettuata riscrivendo i primi 32 settori successivi al boot sector. Dato il ristretto tempo intercorrente tra l'infezione e la distruzione dei dati, è probabile che il Lehigh passi inosservato all'utente. Esiste una variante del Lehigh che si attiva dopo dieci infezioni anziché quattro.

Il virus **Yale** o **Alameda** fu isolato al Merritt College di Alameda, California, nel 1987. Si compone di un boot sector, e infetta soltanto dischi removibili da 5'' 1/4 contenuti nell'unità A. Anche questo virus blocca il funzionamento di macchine 286 e 386; si replica in occasione di un warm boot (Ctrl-Alt-Del), trasferendo una copia di se stesso sul boot sector del disco contenuto nell'unità A, ma soltanto se si tratta di un disco da 5'' 1/4», 360 Kb. Il virus contiene le istruzioni per la formattazione della traccia 39 testina 0, ma sembra che tali istruzioni non vengano mai attivate.

Un caso interessante di virus è il **Brain**. Si tratta di uno dei virus più comunemente osservati, ma non è questa la particolarità che lo rende interessante; la peculiarità di questo virus consiste in due caratteristiche: è stato il primo virus di cui siano stati identificati gli autori, avendo essi lasciato il proprio nome e indirizzo tra le istruzioni del virus (Brain Computer Services, 730 Nizam block, Allama Igbal Town, Lahore, Pakistan), ed è anche il primo virus che sia stato scritto in modo da tentare di sfuggire deliberatamente all'identificazione. Si tratta anche di uno tra i primi virus di cui si ebbe notizia, dato che le prime manifestazioni della sua presenza risalgono al 1986.



Il virus «Cascade»: l'immagine originaria ed al termine della «caduta» dei caratteri.

Il Brain consiste in un boot sector e tre cluster (6 settori) marcati «bad clusters» nella FAT. Il primo di questi settori contiene l'immagine dell'originario boot sector del disco; la versione originale di questo virus colpisce soltanto i dischi removibili da 5'' 1/4, 360 Kb.

Il dispositivo di schermatura per impedirne l'identificazione è piuttosto ingegnoso: qualsiasi richiesta di servizio al sistema operativo che possa determinare la lettura del boot sector viene ridiretta verso quel settore in cui il virus ha depositato la copia del boot sector originario. Pertanto, l'utente ritiene di vedere il settore 0 della traccia 0 ma in realtà vede il contenuto di una diversa zona del disco, mentre gli viene nasco-

sto il vero boot sector, che contiene le istruzioni del virus (peraltro facilmente identificabili in quanto contengono in chiaro la dicitura «(c)Brain»).

Un virus piuttosto diffuso è il **Cascade**. Di questo programma esiste anche una versione non infettiva (che pertanto non è un virus), che manifesta gli stessi effetti sul video. Anche questo virus possiede una caratteristica singolare, in quanto contiene le istruzioni per identificare se l'elaboratore su cui viene eseguito è una macchina IBM o meno; se si tratta di un PC IBM, o di un XT o AT o PS/2, non viene eseguita alcuna infezione, su diverse macchine, invece, il programma procede all'infezione come vedremo tra poco. Questo particolare comportamento del virus fa riflettere sulle sue possibili origini. Potrebbe essere il primo sintomo di una «guerra batteriologica» tra concorrenti sul mercato dell'informatica, ma in ogni caso, anche volendo limitare al massimo le ipotesi futurologiche, è la prima indicazione della possibilità che i virus siano costruiti con un preciso obiettivo, anziché semplicemente per colpire quanti più sistemi riescono a raggiungere.

La versione originale del Cascade consiste in due varianti, l'una da 1701 e l'altra da 1704 byte. Nella prima l'identificazione dei sistemi IBM non funziona; la seconda è stata leggermente modificata per togliere alcuni errori, ma in ogni caso sembra che l'ignoto programmatore non sia riuscito a ottenere il corretto funzionamento del controllo.

L'infezione avviene senza fare uso delle funzioni del Dos, forse per evitare che il virus venga identificato dai dispositivi software di protezione che controllano appunto le intercettazioni agli interrupt (accenneremo più avanti ad alcuni di questi dispositivi). In ogni caso, l'infezione avviene soltanto se la data di sistema è compresa fra ottobre e dicembre 1988, oppure se l'anno è 1980 (che indica che l'utente non ha inserito la data e l'ora e che l'elaboratore è privo di orologio perpetuo). Portatori del virus sono tutti i file .COM, ivi incluso COMMAND.COM.

Una volta installato, Cascade verifica nuovamente la data: e al di fuori del periodo indicato, quindi prima dell'ottobre 1988 e dopo il dicembre dello stesso anno, attiva la modifica dei dati sul video. Questa modifica, che ha valso il nome al virus, consiste nel trasportare verso il basso i caratteri presenti sullo schermo, che sembrano quindi «cadere» e «ammucchiarsi» sul bordo inferiore del video.

Il virus non ha alcun altro effetto sui dati; esiste tuttavia una variante che si attiva unicamente nei mesi tra ottobre e dicembre di qualsiasi anno ad eccezione del 1993, e che formatta la traccia 0 del primo disco fisso incontrato.

Il virus noto come **Dark Avenger** fa parte di un gruppo di virus che si presumono sviluppati in Bulgaria. (Abbiamo già trattato, in un precedente articolo, l'argomento della «fabbrica dei virus» che sembra essersi instaurata in Bulgaria). Il funzionamento del Dark Avenger è piuttosto complesso. Si tratta di un virus che si avvale come portatori di file .COM e .EXE, aumentandone la lunghezza di 1800 byte. Una volta installato, il virus intercetta alcune tra le principali funzioni del Dos, tra cui la Int 21H che svolge molti dei servizi relativi ai file. Anche operazioni apparentemente innocue come la copia di un file da un disco a un altro, o da una directory all'altra, oppure il semplice cambio del nome di un file, possono provocare l'infezione. Questa caratteristica rende il Dark Avenger estremamente infettivo ed è la causa della grande diffusione che ha avuto questo virus.

L'attività del virus procede con l'infezione di qualsiasi programma oggetto che riesce a raggiungere, sia .COM che .EXE. Ad ogni infezione riuscita il programma incrementa di una unità un contatore. In un caso su sedici, inoltre, dopo l'infezione il virus punta casualmente a un settore dell'area dati del disco da cui è stato prelevato il programma portatore; se poi il contatore è arrivato a 15, prima di riportarlo a 0 il virus distrugge il contenuto del settore appena selezionato. Questa azione può provocare la perdita di informazioni.

Tra le istruzioni del virus sono leggibili anche delle frasi, le quali, però, non vengono mai scritte sul video. Il creatore del virus fa riferimento a se stesso come «Dark Avenger» (il «Vendicatore Oscuro», da cui il nome del virus); inoltre c'è una citazione da un album di un gruppo musicale inglese, e il nome di battesimo di una persona non meglio identificata.

Un altro virus piuttosto comune è il **Den Zuk** (in olandese: la ricerca). Sembra che sia originario dell'Indonesia, ed è noto sin dal settembre 1988. Il portatore dell'infezione è il boot sector dei dischetti da 5'' 1/4, 360 Kb, il quale viene ricoperto con le istruzioni di avvio del virus anche se il disco soggetto all'infezione non contiene sistema; il resto del virus è contenuto nella traccia 40, normalmente non utilizzata. Quando viene effettuato il boot da un disco infetto, compare la scritta violetta «DEN ZUK», nei modi grafici CGA, EGA o VGA; la scritta si forma entrando simultaneamente da destra e da sinistra, e scompare rapidamente.

Il virus sopravvive a un warm reboot; la versione originaria del programma non aveva effetti dannosi, e anzi sembra che sia stato scritto a scopi utili. Infatti oltre a procedere all'infezione dei dischi non infetti, il Den Zuk provvede anche alla ricerca (da cui il nome) e alla eventuale rimozione dei virus dei ceppi Brain e Ohio.

Il criterio seguito dal realizzatore del Den Zuk sembra essere stato che gli utenti per lo più non possiedono le cognizioni tecniche sufficienti ad avvedersi del fatto che il proprio sistema è stato contaminato da un virus, che nella maggior parte dei casi non prestano sufficiente attenzione a questa possibilità ed è quindi opportuno che se ne occupi qualcuno al loro posto.

Mentre si può in parte concordare sulla premessa, non possiamo assolutamente condividere la conseguente linea di azione dell'ignoto programmatore. Il motivo è semplice: una volta sviluppato e messo in circolazione un programma autoreplicante, cioè un virus, non si può prevedere quale uso verrà fatto di tale programma; lo dimostra il fatto che esiste una variante del Den Zuk che dopo un dato numero di warm reboot procede alla formattazione del disco da cui è avvenuto l'ultimo reboot, il cui contenuto va quindi irrimediabilmente perduto.

Il programma «benigno» è divenuto «maligno» per volontà di qualcuno che certamente non è l'originario realizzatore.

Tra la fine di settembre e l'inizio di ottobre dello scorso anno, si è molto parlato di virus in seguito alla scoperta del **Datacrime**. Questo che è uno dei più maligni tra i virus noti, esso rimane latente fino al giorno successivo al 12 ottobre, limitandosi ad infettare tutti i files .COM ad eccezione di quelli il cui nome contiene una «D» in settima posizione, e quindi anche COMMAND .COM. Nel 1989 il 12 ottobre, che negli Stati Uniti corrisponde al «Columbus Day» (la data della scoperta dell'America), cadeva di giovedì, e pertanto il giorno successivo era un venerdì 13.

Molto è stato detto a sproposito sull'origine, sul funzionamento e sullo scopo di questo virus, anche perché — come si è detto — il virus è particolarmente aggressivo.
Quando si attiva, sul video compare la scritta
DATACRIME VIRUS
RELEASED: 1 MARCH 1989
e viene avviata la formattazione a basso livello del disco fisso.

Per la caratteristica data di attivazione, il virus Datacrime è stato erroneamente chiamato anche «Venerdì 13»;

questo è invece uno dei nomi con cui è noto un altro diffusissimo virus, il **Jerusalem**. Il virus, originario di Israele da cui il nome, infetta sia i .COM che gli .EXE; questi ultimi, a causa di un errore nel meccanismo di replicazione, vengono infettati ripetutamente. L'effetto più direttamente visibile del Jerusalem è la trasposizione di un gruppo di caratteri sul video: tutto ciò che si trova tra la riga 5 colonna 5 e la riga 16 colonna 16 viene spostato in alto di due righe, lasciando uno spazio vuoto in basso. Un altro effetto visibile della presenza del virus è dato dal rallentamento che l'elaboratore subisce mezz'ora dopo l'infezione.

Tuttavia, se l'infezione avviene quando la data del sistema è posta al giorno 13 in un mese in cui tale giorno cade di venerdì, il virus cancella dal disco ogni programma di cui l'utente chiede l'esecuzione.

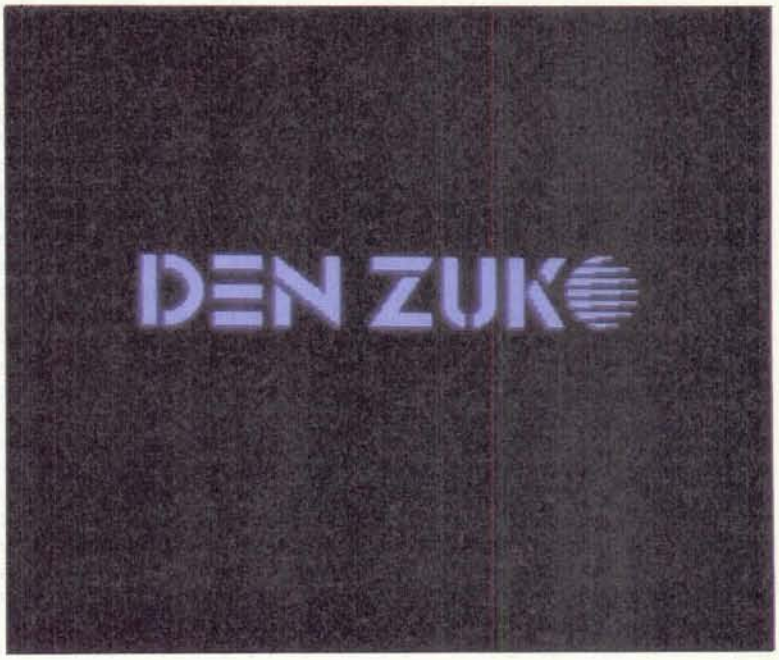
La variante **Jerusalem-B** è probabilmente il virus più diffuso in assoluto. In molti casi non si trasmette ai file .EXE, mentre sembra che aggredisca i .SYS e i segmenti di programma oggetto (.OVL e simili).

Il virus Jerusalem e le sue varianti discendono da tre versioni di uno dei primi virus sviluppati, il **Suriv**. Questo virus è interessante in quanto sembra in grado di autoaggiornarsi: quando un programma portatore viene aggredito da una versione di Suriv che riscontri la presenza di una versione precedente, tale versione viene rimossa e sostituita con la più recente [7].

L'ultimo virus che tratteremo è il **New Zealand** o **Stoned**. Il veicolo che questo virus utilizza per propagarsi è il boot sector, con una particolarità: nel caso dei dischi fissi viene infettato il master boot record, quello che contiene la tavola delle partizioni in cui il disco stesso è suddiviso.

Apparentemente il virus non è stato progettato per danneggiare, limitandosi a scrivere sul video «Your PC is now stoned» (il tuo PC ha fumato hashish); tuttavia l'autore — uno studente di Wellington — si è preoccupato di non danneggiare alcuna area di disco che possa contenere dati, ma non ha tenuto conto della possibilità che un disco contenga oltre 360 Kb di memoria.

Infatti, il boot sector originario viene sostituito con quello tipico del virus, e viene archiviato nella traccia 0, testina 1, settore 3, che in un dischetto da 360 Kb è il settore finale della directory, che raramente conterrà riferimenti a file; ma in un disco da 1,2 Mb lo stesso settore è il terzo della directory, ed è probabile che in questo caso il virus risulti distruttivo (se il disco contiene più di 32 file).



Il virus «Den Zuk», originariamente prodotto come strumento di identificazione ed eliminazione di altri virus, è stato poi reso distruttivo da un ignoto hacker.

Come difendersi

L'aspetto più grave del problema virus consiste nel fatto che la comunità mondiale degli utenti di personal computer si rifiuta di affrontare il problema. Disinformati dalla stampa non specializzata, gli utenti minimizzano il problema anche perché in molti casi gli effetti dei virus si limitano ad azioni infantili, risibili, poco dannose: scritte poco serie quali «Your PC is now stoned», oppure «palline» che rimbalzano, caratteri che «cadono» in fondo al video, musichette, e cose simili.

A nostro parere, invece, i virus costituiscano un problema molto grave e urgente, per due ragioni: perché esistono virus estremamente distruttivi e maligni e in ogni caso non è impossibile costruirne e dare loro ampia diffusione; e perché gli stessi utenti che minimizzano il problema non soltanto non sono in grado di riconoscere l'assalto di un virus da una loro manovra errata, ma probabilmente non sanno nemmeno quali sono i comportamenti che possono portare ad essere vittime dell'assalto di un virus.

Si pensi ad esempio ad un virus biologico, che colpisca quindi gli esseri viventi, che sia infettivo al 100% e si trasmetta in occasione di qualsiasi contatto fra gli organismi, rimanendo latente — ma infettivo — per una settimana, senza manifestazioni visibili, e quindi uccidendo istantaneamente il proprio ospite, con una mortalità anch'essa pari al 100%. Qualora un virus del genere dovesse realmente svilupparsi, in breve tempo resterebbero in vita soltanto gli abitanti di pochi remoti villaggi, tagliati fuori dal flusso mondiale delle comunicazioni: il resto dell'umanità sarebbe rapidamente e totalmente cancellato.

Un virus informatico con analoghe caratteristiche potrebbe mettere in ginocchio buona parte delle attività che comportano il trattamento di informazioni. Ma senza giungere a esemplificazioni estreme, è necessario che si stabilisca la mentalità secondo cui un programma che ottiene in qualche modo l'accesso a un sistema di elaborazione di dati, senza che il legittimo utente del sistema ne sia a conoscenza, è comunque un aggressore e un fattore di rischio: anche se poi lo stesso programma si limita a far rimbalzare una pallina sul video.

Cosa deve fare un utente, per evitare che il proprio personal computer sia aggredito da un programma sconosciuto? Fino a poco tempo fa la risposta era: «Non utilizzare alcun programma che non sia stato regolarmente acquistato in scatola sigillata, ed eseguire regolarmente una copia dei propri dati». La situazione adesso è leggermente cambiata, da quando la Aldus Corporation, uno dei principali produttori mondiali di software, ha distribuito inavvertitamente una nuova versione di un proprio prodotto (il Freehand) infetto da un

virus. Come questo sia stato possibile, verrà esaminato in un prossimo articolo in cui verranno dettagliatamente esaminati i percorsi che l'infezione può seguire nel diffondersi.

È importante tuttavia che ogni utente salvaguardi il proprio patrimonio informativo tenendo presente una semplice regola: ***nessun programma, da qualsiasi fonte provenga, è sicuramente immune da contaminazione virale.*** Questa norma vale per i programmi di uso professionale come per quelli di uso domestico; vale per il software acquistato in negozio e maggiormente per quello copiato in modo più o meno legale. Vale anche per il software prelevato da BBS e gruppi di utenza.

Ciò significa che non si deve utilizzare nessun nuovo programma? Certamente non è questo il senso della nostra affermazione; l'utente deve apprendere non a scartare i nuovi programmi che gli vengono sottoposti, ma a sperimentarli in modo responsabile. In una grande azienda, che può permettersi il costo, dovrà esistere un «ambiente sterile», costituito da uno o più personal computer dedicati esclusivamente alla sperimentazione dei nuovi programmi. L'utente individuale, che non può permettersi di acquistare un secondo personal computer su cui sperimentare i programmi, dovrà seguire alcune elementari norme di sicurezza, che qui riportiamo in sintesi.

1) Cercare di acquisire un minimo di dimestichezza con il proprio elaboratore, e con ciò che esso contiene, in modo da farne un uso razionale e non cieco. Senza dover divenire un programmatore, l'utente può informarsi su come funziona il proprio computer, come vengono registrati i dati sui dischi, che convenzioni e che nomi vengono utilizzati, etc..

2) Strutturare le informazioni nel proprio elaboratore in modo da mantenere ben separati e distinti i programmi e le informazioni su cui tali programmi operano. Per questa operazione gli utenti meno esperti potranno richiedere l'assistenza di uno specialista; tuttavia è essenziale che dati e programmi restino sempre e comunque separati e rapidamente identificabili per le operazioni qui di seguito descritte. Inoltre, per tutelarsi dalla possibilità che il proprio sistema sia colpito da un virus che si trasmette attraverso il boot sector e quindi attraverso il sistema operativo, si dovrà conservare un dischetto contenente una copia sicuramente «pulita» del sistema operativo, possibilmente ottenuta da un disco originale e sigillato. Tale dischetto non dovrà mai essere utilizzato per nessun motivo, salvo per il recupero da un'infezione virale. Inoltre dovrà essere conservato protetto contro la scrittura, e la protezione non dovrà mai essere rimossa, con l'avvertenza che la disponibilità di un simile dischetto in molti casi è l'unica possibilità di recupero da un attacco distruttivo di un virus.

3) Eseguire regolarmente la copia su dischi removibili del contenuto del disco fisso. Questa operazione non dovrà essere eseguita in blocco sull'intero disco, ma separatamente per ciascun raggruppamento di file (dati o programmi); in questo modo le copie successive alla prima richiederanno tempi inferiori, in quanto non è necessario ripetere le copie di ciò che presumibilmente rimane invariato (i programmi) ma sarà sufficiente copiare ciò che varia periodicamente (i dati). Inoltre, se per qualsiasi ragione è necessario prelevare il contenuto delle copie, è facilitata l'identificazione di ciò che si cerca.

4) Le copie debbono essere eseguite secondo criteri che consentano di massimizzare il risultato minimizzando il tempo per ottenerlo. È necessario poter disporre di più versioni successive degli stessi dati; non si dovrà pertanto riutilizzare lo stesso gruppo di dischetti per sovrapporre alla precedente una nuova copia, ma si dovranno usare a rotazione due o tre serie diverse di dischetti, ciascuna delle quali dovrà essere corredata della indicazione della data in cui vi è stata registrata una copia; i dischetti da utilizzare saranno sempre quelli che portano la data più vecchia. Se si dispone di un programma di copia di sicurezza che consente le copie c.d. incrementali, ossia dei soli dati aggiunti o modificati dopo l'ultima copia, sarà preferibile farne uso.

5) Prima di provare un nuovo programma, conviene fare una copia extra, e tenere strettamente sotto controllo il funzionamento del sistema: al primo verificarsi di comportamenti inconsueti (modifiche al video, rallentamenti, inattesa attività del disco fisso o dell'unità di lettura del disco removibile, etc.) si dovrà interrompere il lavoro, spegnere completamente l'elaboratore, inserire il disco «pulito» precedentemente predisposto, riaccendere e ripristinare tutto il sistema allo stato della copia effettuata prima della installazione del nuovo programma. Possibilmente si dovrà procedere alla riformattazione dell'intero disco fisso, e alla ridefinizione della tavola delle partizioni.

Non è qui il caso di trattare gli strumenti software che possono essere utilizzati per tutelarsi dall'aggressione dei virus. Si tratta di programmi che intercettano le normali funzioni del sistema operativo e controllano che nessun altro programma tenti a sua volta di intercettarle. Vi sono anche dei programmi di ricerca, che esaminano il contenuto di un disco per determinare se i programmi in esso contenuti sono portatori di uno dei virus conosciuti ed analizzati.

L'efficacia di questi programmi è relativa, in quanto possono essere molto utili per eliminare completamente gli effetti di un'infezione da parte di un virus conosciuto, ma poiché si basano sulla conoscenza di un virus per determinarne l'identificazione, sono ovviamente inutili per tutelare l'utente dall'aggressione da parte di virus di nuova realizzazione. In un prossimo articolo sarà approfondito l'argomento degli strumenti di difesa dai programmi aggressori.

Bibliografia

[1]: *Known IBM PC Viruses* — Virus Bulletin, 8/90
[2] F. Cohen: *Computer Viruses — Theory and Experiments* — Computers & Security 6 (1987) 22-35
[3] D. Ferbrache: *Wide and Local Area Network Worms* — Virus Bulletin, 1/90
[4] D. Ferbrache: *The Internet Worm — Action and Reaction* — Virus Bulletin, 6/90
[5] J. Hirst: *Virus Dissection: The Italian Virus* — Virus Bulletin, 11/89
[6] J. Hirst: *Virus Dissection: The Cascade Virus* — Virus Bulletin, 9/89
[7] J. Hirst: *Virus Dissection: Jerusalem Virus — The Early Days* — Virus Bulletin, 8/89
[8] P. M. Hoffman: *Virus Information Summary List* — 15/7/90, BBS file
[9] J. McAfee, C. Haynes: *Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System* — New York, NY, St. Martin's Press, 1989
[10] J. McAfee: *Managing the Virus Threat* — Computerworld 13/2/89, vol. XXIII n. 6
[11] T. Sirianni, S. Nueman: *The Dirty Dozen — An Abbreviated Trojan Alert List* — BBS file
[12] F. Skulason: *Virus Dissection: Dark Avenger* — Virus Bulletin, 2/90
[13] F. Skulason: *Virus Dissection: New Zealand — Causing Chaos Worldwide* — Virus Bulletin, 5/90
[14] S.R. White, D.M. Chess, C.J. Kuo: *Coping with Computer Viruses and Related Problems* IBM, Research Report Number RC 14405, 1989.

IMPORTAZIONE DIRETTA

GVH linea computer

PREZZI INGROSSO

SERVIZIO CASH CARRY EXPRESS

Gianni Vecchietti GVH - 40131 Bologna - Via Della Selva Pescarola, 12/8 - Tel. 051/6346181 - Fax 051/6346601

Se nella vostra città non trovate i nostri prodotti, rivolgetevi direttamente alla nostra sede di Bologna

ALA'S

COMPUTER CON SCHEDE MYCOMP CERTIFICATE

386 SX 16 (P9)

- Mainboard con CPU 80386 SX 16 MHz (21 MHz speed) - 8 slot di espansione - zoccolo 80387 - chip set INTEL o NEAT-Bios AMI o Phoenix
- 1 Mbyte RAM installate (espandibili 8 Mb)
- 1 Floppy drive 1,2 Mb TEAC
- 1 Floppy drive 1,44 Mb TEAC
- Scheda video VGA 16 bit 256K
- Scheda doppia seriale + parallela
- Scheda controller HD+FD AT bus 16 bit
- 1 Hard disk 40 Mby 28 mS Miniscribe o WD
- Involucro metallico desk top oppure mini Tower (Vedi foto)
- Monitor 14" monocromatico VGA 16 toni di grigio, base swivel. Antiriflesso.
- Tastiera estesa 101 tasti italiana
- Alimentatore switch 200 W
- Mouse Genius

Montato e collaudato compreso spese di trasporto

£ 2.450.000 +IVA

Opzione per monitor VGA colori 14" + L. 390.000

386 25 CH 64 K

- Main board con CPU 80386/25 MHz certificate chip set NEAT - Cache memory da 64 K
- Ram installate 4 Mbyte 70 nS
- 1 Floppy drive da 1,44 Mb
- 1 Floppy drive da 1,2 Mb
- 1 Hard disk 80 Mby 19 mS
- Scheda video VGA 16 bit 256 K
- Scheda doppia seriale + parallela
- Scheda controller HD+FD AT bus 16 bit HI-Speed
- Involucro metallico Tower da pavimento
- Monitor colore VGA 0,31 dp 14" antiriflesso
- Alimentatore switch 220 W
- Tastiera estesa 101 tasti italiana

Montato e collaudato compreso spese di spedizione

£ 5.450.000 +IVA

PC 286 12 M

- Main board 286/12 MHz Ø WS chip set G2
- 1 Mby installate
- 1 Hard disk 20 Mb 28 mS 3,5"
- 1 Floppy drive da 1,2 oppure 1,44 a scelta
- Scheda video VGA 16 bit 256 K OAK
- Scheda doppia seriale + parallela
- Scheda controller HD+FD AT bus
- Alimentatore switch 200 W
- Involucro metallico desk top da tavolo
- Tastiera estesa 101 tasti
- Monitor monocromatico VGA 16 toni di grigio, base swivel - antiriflesso

Montato e collaudato **£ 1.450.000** +IVA - Spese trasporto L. 30.000

Opzione per monitor VGA a colori + L. 390.000

STAMPANTI

STAR LC 10	L.	360.000
STAR LC 24/10	L.	550.000
NEC P2 Plus ..	L.	telefonare
Citizen Swift 24	L.	telefonare

ACCESSORI

Mouse F 302 Genius	L.	85.000
Handy Scanner HS4500	L.	290.000
Floppy disk 720K bulk (min. 50 pz.) .	L.	715

Co-processori IIT
80287/12 - 80287/16
80387SX - 80387/25
L. telefonare

A TUTTI I PREZZI VA AGGIUNTA IVA 19%

ESCLUSIVISTI DI ZONA

LA BOTTEGA ELETTRONICA
BOLOGNA - Via S. Pio V° 5 - Tel. 550761

ELECTRONIC CENTER
MODENA - Via Canaletto Sud, 276 - Tel. 315802

RED TELEMATICA
MANTOVA - Via Pilla, 29/A - Tel. 381159

PLAYER
FORLÌ - Via F.lli Valpiani 6/A - Roncadello - Tel. 31323

RIDEL
NAPOLI - Via Scipione Capece, 2 - Tel. 640268

GENERAL COMPUTER
SALERNO - Corso Garibaldi 56 - Tel. 237835

DUAL SOFT
TRIESTE - Via Valdirivio, 40/E - Tel. 631226

Rivolgetevi con fiducia ai nostri distributori troverete un vasto assortimento di prodotti GVH-MYCOMP