Classificazione dei virus secondo le modalità di attacco

di Stefano Toria

Prende l'avvio da questo numero una rubrica focalizzata su uno dei più preoccupanti fenomeni riguardanti l'informatica personale: i virus. Ciascun articolo, realizzato in modo da fornire informazioni a un pubblico il più possibile vasto, si soffermerà sia sugli aspetti tecnici — laddove necessario — che su quelli pratici, mirando soprattutto a fornire delle linee di azione all'utente «medio», che non desideri approfondire eccessivamente i tecnicismi che stanno dietro al funzionamento dei virus, ma che voglia giustamente tutelare l'integrità del proprio patrimonio informativo dal rischio di danneggiamento che un virus può realizzare in breve tempo e senza che l'utente se ne accorga

Classificazione dei virus per modalità di attacco

Nel parlare di virus o vermi si fa frequente uso di termini come «attacco», «infezione», «penetrazione», «difesa», «vaccinazione», «eliminazione». Tale terminologia di origine medico-terapeutica è stata adottata per conseguenza della assimilazione tra virus informatici e virus biologici; l'operazione è tutt'altro che velleitaria, poiché molti concetti e molte prassi adoperati nel trattamento dei programmi virus trovano una corrispondenza logicamente congruente nel trattamento degli agenti patogeni del corpo umano.

Un virus può trasmettersi all'interno di un sistema solo ed esclusivamente se vengono eseguite le istruzioni del programma che gli fa da portatore. Questo concetto, sul quale non si insisterà mai abbastanza, significa che non è sufficiente che venga letta la directory di un dischetto, oppure che venga letto o stampato un file che si trova sul disco infetto, bensì è indispensabile che venga eseguito un programma. Questa condizione sovente porta gli utenti meno esperti a commettere degli errori, come nel seguente esempio: si supponga che un dischetto contenga, tra l'altro, due file: l'uno, READ.ME, è il breve testo introduttivo che il produttore del software si riserva di scrivere all'ultimo momento, subito prima di distribuire i dischetti; l'altro, README.EXE, è un programma realizzato per consentire una più agevole lettura del file READ.ME, ad es. con lo scorrimento delle pagine a piacimento dell'utente.

Nella situazione esemplificata il comando TYPE READ.ME, che provoca lo scorrimento del testo sul video, non ha alcuna conseguenza secondaria. La visualizzazione del file READ.ME a mezzo

del programma README.EXE potrebbe causare l'infezione del sistema, qualora quest'ultimo programma fosse infetto. Per l'utente inesperto non vi è praticamente alcuna differenza tra le due operazioni, poiché entrambe consistono nella «lettura del testo contenuto in READ.ME». Per contro, la differenza tra le due operazioni è fondamentale, poiché la prima si avvale di una funzione già residente nel personal computer (il comando TYPE), mentre la seconda utilizza un programma che proviene dall'esterno e che potrebbe pertanto essere fonte di infezione.

Il «Desktop» del Mac

Questa situazione è apparentemente ancora più complessa sui sistemi Apple Macintosh. Una caratteristica del sistema operativo di questa macchina agevola infatti la trasmissione di virus. Ciascun disco (fisso o removibile) contiene un file denominato «desktop», che descrive le caratteristiche del disco stesso e mantiene traccia del posizionamento sul video della «finestra» relativa al disco. Questo file contiene tra l'altro un breve programma eseguibile, utilizzato per le funzioni di modifica dell'aspetto della finestra relativa al disco. Trattandosi di istruzioni che vengono eseguite, vi è il presupposto perché un virus appositamente costruito infetti il desktop, come infatti si è verificato nel caso del virus WDEF.

La maggiore complessità a cui si accennava poc'anzi deriva dal fatto che molti utenti non sono a conoscenza dell'esistenza di questo breve programma contenuto nel desktop; venendo a conoscenza della presenza di un virus nel proprio sistema, possono ritenere di averlo contratto semplicemente introducendo un disco nel drive, poiché appunto ignorano che tale operazione determina l'esecuzione delle istruzioni contenute nel desktop.

La diffusione del contagio

Si tralascerà per il momento l'analisi del percorso che un virus può seguire per raggiungere e infettare un particolare sistema, rinviandola a una trattazione successiva.

Una volta raggiunto un elaboratore e ottenuto l'accesso, con la collaborazione attiva dell'inconsapevole proprietario o utente dello stesso elaboratore, il virus inizia la propria attività nel momento in cui viene eseguito il programma che gli fa da portatore. I virus si possono suddividere secondo il proprio comportamento in fase di propagazione.

I parassiti

Virus parassiti sono quelli che si trasmettono utilizzando come veicolo un programma eseguibile (.COM o .EXE, in alcuni casi anche .OV*). La prima fase del contagio consiste nella identificazione di un programma candidato all'infezione.

Nella seconda fase il virus infetta il programma prescelto posponendogli una copia di se stesso, e modificando opportunamente le prime istruzioni del programma in modo da determinare l'esecuzione di se stesso. Allo stesso tempo, il virus «si identifica» in qualche modo, così da essere in grado di riconoscere la propria presenza in un particolare programma e non ripetere l'infezione in seguito.

Appartengono a questa categoria virus come l'Amstrad, il Christmas Tree, il Cookie, il DataCrime. Tutti questi virus si propagano ogni volta che viene eseguito il programma portatore, facendo

Origine e breve storia dei virus

Uno dei segreti più gelosamente custoditi dai diretti interessati riguarda l'identità delle persone che hanno realizzato la maggior parte dei virus in circolazione. Secondo le classificazioni più recenti le varianti assommano a 481, quindi si può stimare che almeno due-trecento persone abbiano speso una parte del proprio tempo nello sforzo di realizzare programmi aventi il fine di distruggere risorse e informazioni e di far perdere tempo.

Questa segretezza, che certamente trae origine dal timore di giustificate azioni legali — oltre che di comprensibili, seppure meno giustificate, azioni «di fatto» — rende difficile il lavoro di ricostruzione della storia dei programmi aggressori, e l'identificazione dell'origine di tali programmi. Tuttavia un primo impulso allo sviluppo di questo genere di programmi è provenuto dagli studi sulla modifica automatica del software, in particolare in contesti distribuiti.

Il primo virus fu sviluppato nel novembre 1983 con fini dimostrativi, nell'ambito di una ricerca finanziata da una delle principali società costruttrici di elaboratori e inserita in un più generale progetto di studio della sicurezza dei sistemi informativi. L'obiettivo della ricerca era dimostrare come le possibilità di un attacco al patrimonio informativo di un'azienda non fossero limitate a quelle tradizionalmente prese in esame negli studi sulla sicurezza, e cioè l'attacco fisico, la conoscenza illegittima di password, la modifica al codice sorgente etc.. L'esperimento, perfettamente riuscito, dimostrò anzi che predisponendo opportunamente il programma aggressore era possibile attaccare qualsiasi sistema. Il virus sperimentale, sviluppato in otto ore da un esperto, impiegava meno di mezzo secondo per replicarsi infettando un altro programma, che diventava a sua volta portatore del virus.

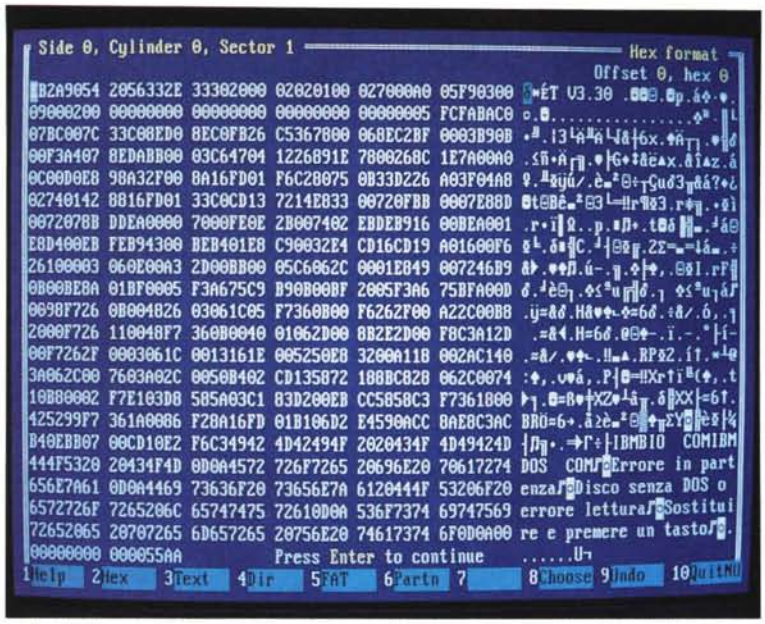
Pochi mesi dopo, nel luglio 1984, si dimostrò come il modello Bell-LaPadula (un sistema di sicurezza all'epoca ritenuto tra i più affidabili) fosse del tutto inadeguato a tutelare un sistema informativo dal rischio di un attacco virale.

Il modello Bell-LaPadula essenzialmente consiste in una formulazione che assegna livelli crescenti di riservatezza alle informazioni e di autorità agli utenti, i quali possono accedere soltanto alle informazioni al proprio livello di autorità o a quelli inferiori. L'esperimento del luglio 1984 dimostrò come un virus avesse la possibilità di trasmettersi verso i livelli più alti di protezione, e l'utente apparentemente più limitato e controllato, quello cioè con il più basso livello di autorità, fosse invece quello che aveva la maggiore possibilità di danneggiare l'integrità del sistema mediante un virus.

La diffusione degli esiti di questi primi esperimenti suscitò la curiosità dei più esperti utenti di personal computer, i quali tentarono — a volte con successo — di replicare sui propri sistemi i programmi-virus creati negli ambienti di prova. Senza alcun apparente collegamento tra di loro, tra il 1985 e il 1986 due gruppi di persone, l'uno in Israele, l'altro in Pakistan, svilupparono dei programmi dotati della proprietà di replicarsi autonomamente, utilizzando come supporto i normali file eseguibili del sistema operativo MS-DOS (.COM o .EXE) oppure il boot sector, cioè quel settore di disco che contiene l'immagine del sistema operativo, e che viene letto ed eseguito all'atto dell'avvio della macchina, oppure quando viene premuto il pulsante di reset, oppure quando l'utente preme simultaneamente i tasti Ctrl-Alt-Del.

Dal programma israeliano, denominato «Suriv» (è la parola «virus» scritta da destra a sinistra), ebbe origine quel ceppo di virus attualmente noto come «Jerusalem», di cui esistono diverse varianti.

Il programma pakistano è attualmente noto come «Brain». Nonostante siano passati cinque anni dalla data del rilascio, continuano a verificarsi casi di infezione da Brain; questo fatto di per sé dovrebbe far riflettere sulla pericolosità del fenomeno virus.



Il boot sector di un floppy disk da 3,5".

divenire a sua volta portatore ciascuno dei programmi contagiati. In questo modo l'utente può inconsapevolmente trasportare il virus su altri elaboratori, contribuendo attivamente alla diffusione dell'infezione.

I parassiti residenti

Un caso particolare di virus parassiti è costituito da quei programmi che rimangono residenti in memoria dopo essere stati eseguiti la prima volta. La tecnica adottata da questi programmi consiste nel fare uso di una particolare funzione del DOS detta «Terminate and Stay Resident», abbreviato in TSR. Un programma TSR installa una copia di se stesso in memoria, allo scopo di rimanere sempre pronto per l'esecuzione. Fanno parte della categoria dei TSR numerosi programmi di utilità, tra i quali alcuni sono anche piuttosto noti (e ovviamente *non* sono virus) come il Sidekick della Borland. Lo stesso DOS fa uso di funzioni TSR, ad esempio nella esecuzione dei comandi Mode e Print e nella definizione delle funzioni della tastiera (keybit o simili).

La funzione TSR, se utilizzata da un virus, lo rende ancora più pericoloso. Un virus parassita non residente, una volta raggiunto un sistema, vivrà una fase iniziale di sviluppo piuttosto lento, con la curva di diffusione che cresce in forma esponenziale man mano che riesce a raggiungere e contaminare sempre più programmi, e quindi a diffondersi attaccando quei programmi che l'utente esegue più frequentemente; dopo la fase di più ampia diffusione si raggiungerà una situazione di saturazione, in cui tutti i programmi disponibili sono stati infettati. Per contro, la diffusione di un virus parassita residente non ha un avvio lento dato che l'esecuzione del programma virale non dipende dalla esecuzione di uno specifico programma portatore, in quanto questo è già stato eseguito e ha lasciato una traccia permanente in memoria, pronta ad attivarsi secondo quanto è stato specificato dal programmatore. Questa attivazione avviene sovente in congiunzione con la richiesta di comuni funzioni del DOS: l'apertura di un file, la lettura di un dato sul disco, la copia di un file da un disco a un altro. Si intuisce come in questo caso la diffusione del virus sia inizialmente molto più rapida proprio perché è lo stesso DOS a divenire idealmente portatore del virus, e le funzioni del DOS vengono eseguite in continuazione nell'ordinaria attività di un utente di personal computer.

Alla categoria dei virus parassiti residenti appartengono molti tra quelli più noti, tra cui l'Alabama, il Cascade, il Dark Avenger, il Fish.

Virus in sovraimpressione

Una terza tipologia di virus che attaccano i file eseguibili è costituita da quei programmi che vanno a sovrapporsi alle legittime istruzioni del programma vittima. La tecnica è simile a quella adottata dai parassiti, salvo che il virus non si replica copiando se stesso in coda al programma che intende infettare, o in un'altra zona disponibile; le istruzioni del virus vengono trascritte in una parte del programma che contiene altre istruzioni, con il risultato che quasi sempre il programma infetto non può essere disinfettato in quanto parte di esso è andata perduta.

Appartiene a questa categoria il Lehigh, uno tra i primi virus ad essere stati identificati e analizzati.

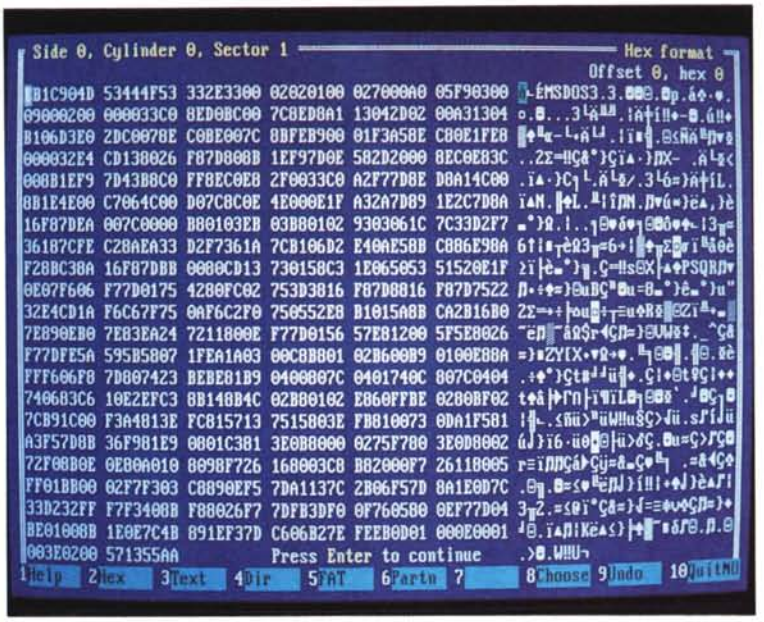
Il boot sector

È in crescita anche il numero di virus che fanno uso del *boot sector* come veicolo per il trasporto dell'infezione. Ogni disco formattato dall'MS-DOS o dal Pc-DOS contiene, in una posizione prestabilita, un breve programma detto «boot» o «bootstrap». Questo programma può svolgere due distinte funzioni, a seconda di come il disco è stato predisposto: se si tratta di un disco di sistema, utilizzabile cioè per l'avvio del sistema operativo, il boot costituisce il primo stadio della partenza del sistema stesso, e le istruzioni che lo compongono vengono prelevate dal PC all'atto dell'accensione per essere eseguite. Solitamente il boot procede alla ricerca e al prelievo della parte centrale del sistema operativo, contenuta in alcuni file predefiniti; i file vengono caricati in memoria e il sistema prende l'avvio. Se per contro non si tratta di un disco di sistema, il boot consisterà in un semplicissimo programma che scrive sul video un avvertimento all'utente, segnalando il fatto che ha inserito nel drive un disco che non contiene il sistema operativo e invitandolo a rimuoverlo e ad inserirne uno corretto.

In entrambi i casi si tratta di programmi che vengono eseguiti, con modalità

Prossimamente...

Gli argomenti che saranno affrontati nel prossimo futuro comprenderanno i criteri per il riconoscimento della presenza di un virus in un sistema, l'identificazione del virus colpevole dell'infezione e la recensione di uno tra i più diffusi prodotti software sviluppati appositamente per la difesa dalle aggressioni virali.



Lo stesso boot sector modificato a seguito dell'infezione da «Ping Pong».

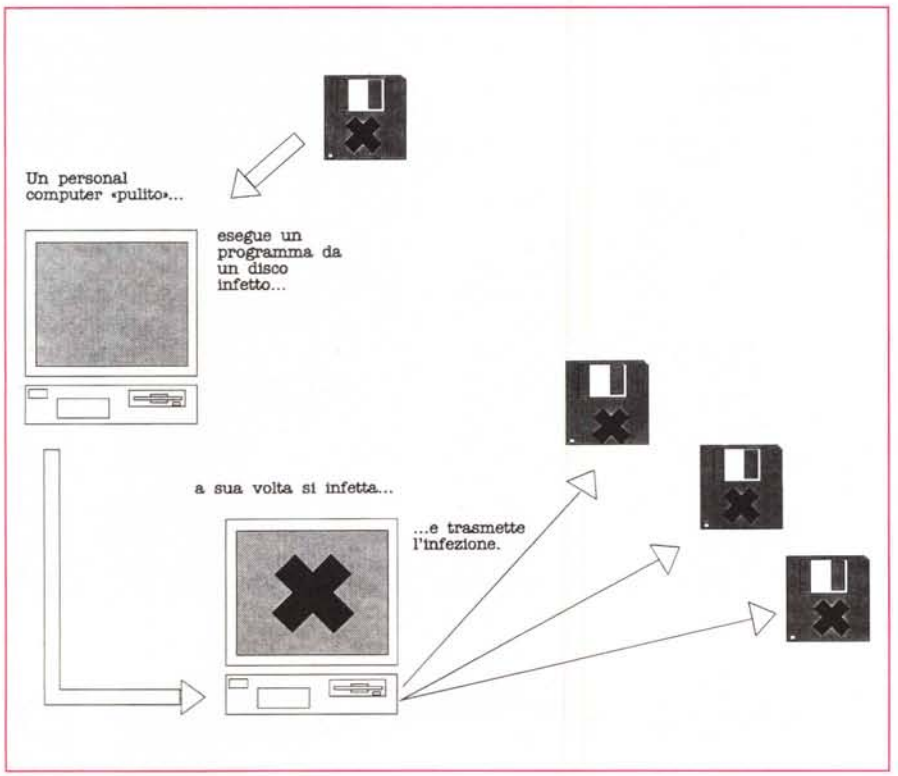
diverse rispetto a quelli contenuti nei file .COM e .EXE ma con gli stessi effetti ai fini di questa trattazione: il boot infatti può essere infettato esattamente come avviene a un programma contenuto in un file.

Nella maggior parte dei casi noti il boot sector viene sostituito con uno diverso, contenente il virus, e l'originario boot sector viene riposto in una diversa zona del disco, per essere eseguito dopo che è stato eseguito il virus. Dopo l'infezione quindi il disco rimane un disco di sistema, ma contiene anche il virus. Alla successiva richiesta di caricamento del sistema operativo dal disco infetto il PC svolgerà le operazioni in questa sequenza:

— caricamento del boot sector che contiene il virus;
— esecuzione del virus, che quasi sempre rimarrà residente;
— caricamento, ad opera del virus, del boot sector originario prelevato dalla posizione in cui era stato memorizzato;
— caricamento del sistema e avvio del funzionamento, apparentemente normale, del computer.

L'utente può non avvedersi subito della presenza del virus, ma questi rimane latente e procederà ad infettare, con lo stesso metodo, tutti i dischi che l'utente inserirà nel drive.

Si avvalgono del boot sector come veicolo di propagazione alcuni tra i più noti virus diffusi nel mondo, tra cui il Ping Pong, il Brain, il Den Zuk, il Disk Killer.



La tavola delle partizioni

Un caso particolare di infezione di un boot sector è costituito da quei virus che infettano la tavola delle partizioni. In un personal computer IBM o compatibile i dischi fissi vengono gestiti suddividendoli in zone di ampiezza prestabilita, a piacimento dell'utente o con vincoli particolari a seconda della versione di sistema operativo che viene utilizzata. Un disco può contenere anche una unica partizione, nel qual caso la strutturazione è praticamente invisibile all'utente, ma su ciascun sistema dotato di disco fisso sarà presente una tavola delle partizioni.

L'avvio del sistema da un disco fisso, anziché da un disco removibile, richiede una fase in più. Infatti il primo programma ad essere prelevato dal disco è quello che gestisce le partizioni; esso determina quale sia la partizione da cui deve essere caricato il sistema operativo, in base a quanto è stato stabilito in sede di installazione del computer, e quindi procede con le fasi già descritte, leggendo il boot e proseguendo nell'avvio del sistema.

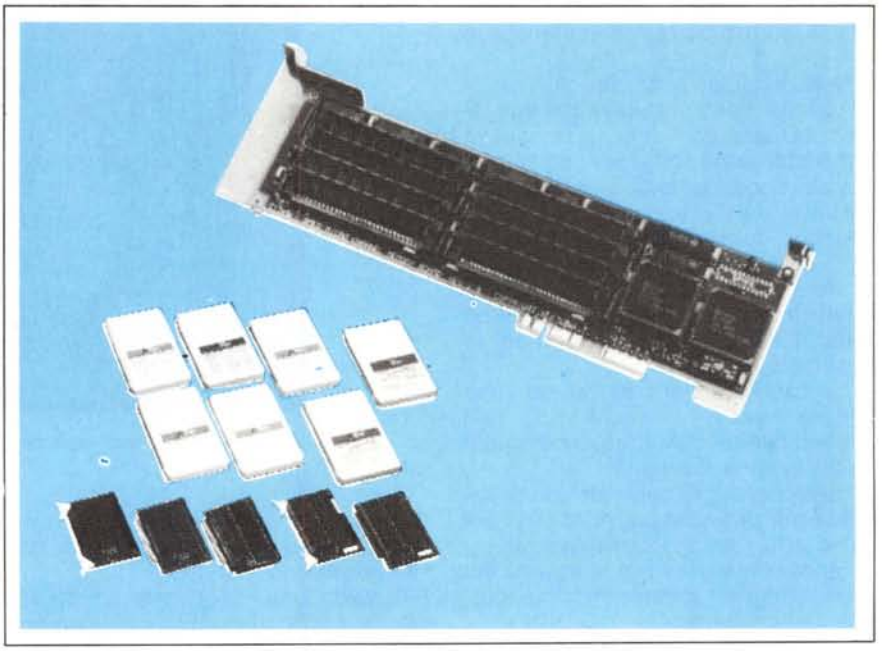
Alcuni virus, tra i quali il più noto è lo Stoned, utilizzano il programma di gestione delle partizioni come veicolo per l'infezione. Tali virus sono in grado di distinguere se il disco che stanno trattando è un disco fisso, che debba essere infettato nella tavola delle partizioni, o un dischetto di cui dovrà essere infettato direttamente il boot.

MC

SISTEMI & TECNOLOGIE srl
PRESENTA

ESPANSIONI DI MEMORIA

IBM
COMPAQ
EPSON
NEC
AST RESEARCH INC.
TOSHIBA
HYUNDAI
AT&T
ZENITH
WYSE
Acer
HEWLETT PACKARD
MITSUBISHI ELECTRONICS
SAMSUNG



I marchi summenzionati sono tutti registrati dalle rispettive case

ESPANSIONI PER TUTTI I PORTATILI
TOSHIBA

MEMORIE:
Da 1 Mb T1000SE/XE;
Da 2 Mb T1000SE/XE; 1200XE; 1600; 3100e; 3200SX; 5100; 5200; 3100SX;
Da 3 Mb T3200;
Da 4 Mb T3100SX; 3200SX;
Da 8 Mb T5200

DISCHI RIGIDI "PALMARI" REMOVIBILI INTERNI:
Da 20 Mb e 60 Mb da 2,5", 21 msec.; Perso 194 gr. alloggiamento: 5,25"/3,5" dim. disco: 80x125x20 mm.

DISCHI RIGIDI "PALMARI" REMOVIBILI ESTERNI A BATTERIE RICARICABILI PER PORTA PARALLELA:
Da 20 Mb, 60 Mb e 120 Mb da 2,5"; 21 msec.; dim. disco: 80x125x20 mm.; dim unità esterna: 109x50x19 7 mm.

DISCHI RIGIDI INTERNI:
20 Mb T1000+, 1200+, 3100e;
40 Mb T1600, 3100e;
100 Mb T5100, 5200.

UNITA' D'ESPASIONE PER N. 1 SCHEDA FULL SIZE:
T1100+; 1000SE/XE; 1200; 1600; 3100e; 3100SX; 5100.

ALIMENTATORE PER USO IN AUTO (PRESA ACCENDISIGARI).

KIT BATTERIE PER ALIMENTAZIONE LAPTOP.

FLOPPY ESTERNO MULTIDRIVE 2: 5,25" DA 1,2 mB/36kb.

P.ZZA MATTEOTTI, 2 - 20020 ARESE (MI) - TEL. (02) 9380212/3/4 - FAX 9380214