La protezione antivirus in un sistema informativo complesso

di Stefano Toria

Ci auguriamo che i lettori di questa rubrica abbiano finalmente assimilato i principi basilari della protezione dai virus. Gli stessi principi possono essere adottati per tutelarsi contro qualsiasi rischio di danni a carico del patrimonio informativo. Negli ultimi mesi abbiamo ripetuto spesso quali sono questi principi: salvataggi frequenti e regolari e marcatura degli eseguibili.
Peraltro il problema della protezione si complica quando sia necessario tutelare non un singolo computer o un insieme ristretto di sistemi, ad esempio tre-quattro personal computer concentrati in una stanza, ma decine o centinaia di computer localizzati negli uffici di un ente di grandi dimensioni. I gradi di libertà del sistema aumentano talmente da rendere praticamente quasi ingestibile la sicurezza. Tuttavia qualcosa si può fare: vediamo cosa

La possibilità di entrare in contatto con un virus costituisce un serio problema per qualsiasi utente di personal computer. Il problema si ingigantisce quando non si tratta di un utente individuale con un solo computer, o con alcuni computer installati in un piccolo ufficio, ma di una organizzazione di dimensioni considerevoli, con centinaia o migliaia di addetti ciascuno dei quali sia dotato del proprio computer. Il rischio cresce in modo esponenziale, come pure il livello di complicazione di tutte le procedure, sia di prevenzione che di recupero da un'infezione una volta che si sia verificata.

Le quattro fasi dell'infezione

In un sistema organizzativo di grandi dimensioni le quattro fasi dell'infezione possono essere osservate ed analizzate con chiarezza e dettaglio.

Infezione locale della memoria

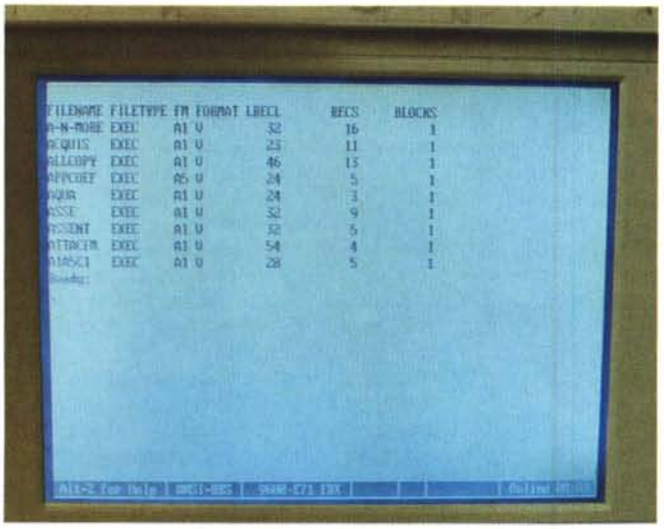
Il virus che entra in contatto con un sistema, per effetto dell'esecuzione del programma che ne fa da portatore, come prima azione si colloca nella memoria del computer. Questo non vuole necessariamente dire che diviene residente, ma semplicemente che il programma viene eseguito e mette in atto le proprie capacità di replicarsi. Alcuni virus si replicano più volte al secondo, altri sono più lenti e attendono circostanze favorevoli che possono verificarsi dopo minuti, ore o addirittura giorni.

Se fosse possibile identificare e bloccare un virus in questa fase, nessuna infezione si propagherebbe. Purtroppo però questa identificazione precoce è pressoché impossibile, per una serie di ragioni che vanno dall'abilità con cui alcuni virus si celano all'osservazione, alla scarsa dimestichezza dell'utente con il proprio computer, che rende difficoltosa — se non impossibile — una interazione tra uomo e macchina al livello necessario per identificare il problema all'origine e rimuoverlo.

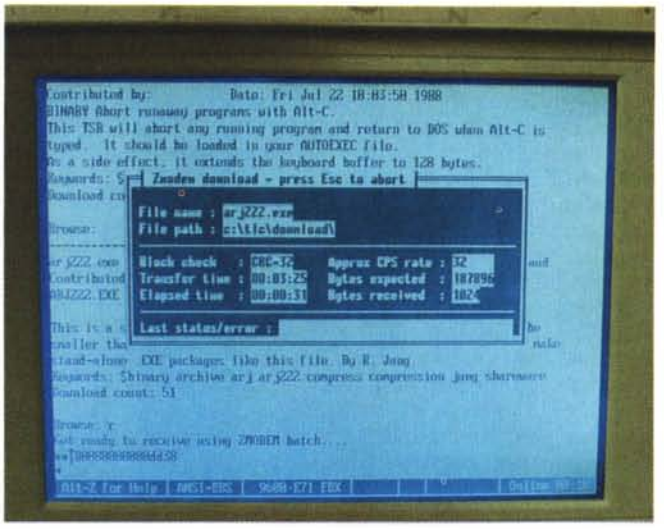
Infezione locale degli archivi su disco

Poiché è estremamente raro che un'infezione venga rilevata nel corso della prima fase, in quasi tutti i casi il virus riesce a passare alla seconda fase, cioè alla propria diffusione nell'ambito del sistema colpito.

I collegamenti alle reti locali possono causare una rapida diffusione dell'infezione nella struttura informatica aziendale.



Le reti geografiche e i collegamenti con i mainframe non costituiscono pericolo...



...a meno che non vengano utilizzati per trasferire programmi eseguibili.

Man mano che il programma portatore viene eseguito più e più volte, vengono infettati in sequenza sempre più programmi, i quali a loro volta diventano portatori di virus esattamente come quello originario, infettano altri programmi che trasmetteranno l'infezione in una catena esponenziale.

Al termine di questa fase tutti i programmi eseguibili contenuti nei dischi del sistema colpito sono portatori di virus.

Identificare un virus in questa fase è relativamente più semplice; utilizzando un opportuno programma di scansione (servendosi della versione più recente possibile) si possono rintracciare tutti i programmi infetti. Esiste, seppure remota, la possibilità di essere stati colpiti da un virus nuovo, non ancora conosciuto e pertanto non riconosciuto dal programma di scansione. A parte questa possibilità tuttavia la ricerca della presenza di un virus a mezzo di un programma di scansione dà risultati accettabili.

Rimane comunque il problema della disinfezione del sistema colpito; ma se l'utente ha seguito almeno la prescrizione dei backup frequenti non avrà problemi nel formattare a basso livello il proprio disco fisso, reinstallare tutti i programmi e riprendere dal backup tutti gli archivi non eseguibili.

Si tratta comunque di un lavoro lungo, che fa perdere ore e talvolta giorni di tempo. Se ne è già parlato in passato, e si rimanda pertanto agli articoli precedenti per una descrizione dettagliata del procedimento di disinfezione di un sistema colpito da un virus.

La transizione del virus a questa fase, inoltre, può comportare a volte la perdita parziale o totale dei dati. Se il virus viene identificato prima dell'attivazione delle funzioni distruttive che dovesse eventualmente contenere, il problema non si pone; ma se ciò non dovesse accadere, e il virus avesse modo di cominciare a far danni, allora sarebbe possibile e anzi piuttosto probabile che l'utente sia costretto a ricostruire una parte dei propri archivi, o nella peggiore delle ipotesi a ricostruirli tutti.

Infezione degli archivi condivisi

La tecnologia informatica ha messo da tempo a disposizione degli utenti la possibilità di condividere archivi e applicazioni su reti di personal computer. Le reti locali sono una realtà quotidiana in molte aziende, è anzi estremamente improbabile riscontrare la presenza di almeno due o tre computer in un'azienda senza che vi sia anche un collegamento tra i sistemi per poter condividere le stesse applicazioni o gli stessi archivi di dati.

Questa importante struttura costituisce un ulteriore elemento di rischio di diffusione di un virus. Infatti, data la natura delle reti locali, che attribuiscono a ciascun sistema risorse comuni con la disponibilità delle risorse proprie, è possibile che un virus migri da un disco locale su un disco condiviso, o che addirittura scelga come proprio obiettivo i programmi eseguibili residenti su dischi condivisi dalla rete.

In questo caso il virus viene messo direttamente a disposizione di tutti i computer che hanno accesso ai programmi che lo contengono. Poiché inoltre i programmi posti a disposizione di una rete saranno quasi sempre programmi di largo uso (trattamento di testi, grafica, compilatori, programmi di utilità, programmi di sistema) l'infezione può espandersi con grande rapidità e raggiungere in breve tempo tutti i sistemi collegati alla rete, che possono essere anche diverse centinaia.

Una volta che l'infezione ha raggiunto gli archivi condivisi, diviene praticamente incontrollabile. In breve tempo si infettano tutti i computer dell'organizzazione, e se l'identificazione del virus è possibile in breve tempo con un opportuno programma di scansione, non è altrettanto semplice la disinfezione. Se la procedura di disinfezione non viene effettuata in modo radicale, bloccando ogni attività del sistema informativo fino al termine dell'operazione di controllo e pulizia di tutti i dischi di tutti i computer collegati alla rete, allora in qualsiasi momento una qualsiasi delle stazioni di lavoro in rete può ridare inizio all'infezione. E si ricomincia daccapo.

Infezione dei supporti rimuovibili

Dopo che l'infezione si è trasmessa a un computer, da questo si allargherà anche a tutti i supporti rimuovibili che vengono utilizzati su di esso. La diffusione può avvenire in due modi: per contaminazione diretta, nel caso in cui un virus scelga come bersaglio della propria replicazione un programma eseguibile contenuto in un dischetto; questo dischetto, tolto dal sistema su cui si è infettato e trasportato altrove, è veicolo

di infezione; se invece viene conservato nei pressi del sistema da cui è stato infettato, può diventare la causa del riprodursi dell'infezione anche a seguito di una procedura di disinfezione che non tenga conto appunto della eventualità che il virus sia rimasto residente su supporti rimuovibili.

L'altra modalità di diffusione consiste nella copia di un programma infetto, generalmente a scopi di backup. In questo modo possono infettarsi supporti che generalmente vengono utilizzati soltanto per archiviazione e non per il diretto prelievo di programmi da eseguire: dischi rigidi rimuovibili, nastri in cartuccia o in bobina, dischi WORM, e qualsiasi altro supporto su cui il computer sia in grado di scrivere.

Un supporto che contiene anche un solo programma infetto può vanificare tutto il lavoro di disinfezione dei computer dell'azienda. E un solo computer infetto, a sua volta, può trasmettere l'infezione a centinaia di supporti rimuovibili, prima che l'infezione venga identificata e curata. Molti di questi supporti, ad esempio i dischetti, sono facilmente trasportabili, possono diffondersi rapidamente, e sono divenuti oggetti di uso talmente comune che è facile che non vi si faccia più nemmeno caso. È facilissimo, e di fatto è avvenuto spesso, che un singolo dischetto contenente un programma infetto finisca sotto una pila di carte, per riemergere soltanto in occasione di una «pulizia di primavera» della scrivania, magari molti mesi dopo che l'infezione è stata curata e che le precauzioni messe frettolosamente in atto in quell'occasione sono state dimenticate.

Un solo computer è soggetto a un rischio di questo genere, è anzi estremamente probabile che ciò si verifichi. Si può immaginare che proporzioni catastrofiche possa assumere un'infezione quando le centinaia o migliaia di computer installati in una grande azienda, tutti infettati per via della diffusione di un virus tramite gli archivi condivisi in rete locale, si mettono a loro volta a infettare i supporti rimuovibili, quei dischetti la cui facilità di circolazione è stata ed è alla base della grande diffusione dell'informatica personale. Il numero di supporti infetti e di programmi portatori di virus può raggiungere in breve tempo una dimensione da capogiro. Se l'identificazione e la cura del virus per qualche ragione dovesse ritardare, si arriverebbe in tempi relativamente brevi a una situazione in cui la probabilità di identificare e rimuovere con successo la totalità delle copie dell'infezione è praticamente zero.

Inoltre lo stesso processo di rimozione del virus è irto di pericoli. Non ci sono due computer al mondo in cui le directory siano strutturate allo stesso modo. I dati e i programmi contenuti nei dischi di ciascun computer sono organizzati in un modo che riflette il modo di lavorare dell'utente. Anche in situazioni aziendali altamente standardizzate si riscontra comunque un elevato livello di personalizzazione delle organizzazioni dei dati. Non è possibile curare l'infezione di mille computer allo stesso modo: occorre agire in mille modi diversi. E la procedura può richiedere giorni, talvolta mesi. In tutto questo tempo gli archivi condivisi debbono restare fermi, intoccabili, perché possono diventare veicolo di reinfezione dei sistemi già curati; sempre che questi non si reinfettino da soli, a causa di un disco sbucato fuori dal fondo di un cassetto.

Come comportarsi

L'enfasi che viene qui posta sugli effetti dell'infezione e sulle difficoltà della cura è dovuta al fatto che quasi sempre l'infezione viene rilevata soltanto dopo che si è diffusa, anzi dopo che il virus ha cominciato a causare danni. Come in molti casi, si chiudono le stalle dopo che i buoi ne sono scappati. Non è certo la politica più efficiente per tutelare l'investimento in sistemi informativi, tuttavia si deve essere certi di compierla correttamente, per non renderla del tutto vana o — peggio ancora — perché il rimedio non diventi peggiore del male.

Innanzitutto l'identificazione e la cura di un'infezione deve essere affidata esclusivamente a personale veramente competente. I sedicenti «esperti», che agiscono per mettersi alla luce agli occhi dei dirigenti dell'azienda, possono fare più danno che altro. Inoltre sarebbe bene affidare l'intera operazione a consulenti esterni, che non abbiano alcun rapporto con l'azienda. Si pensi a cosa queste persone debbono fare: andare a mettere le mani approfonditamente in tutti i computer dell'azienda, con la possibilità di accedere a informazioni più o meno riservate o anche (cosa spesso tollerata *pro bono pacis* o come forma indiretta di retribuzione) su fatti personali dei singoli utenti delle macchine. Se queste operazioni vengono affidate a persone interne all'azienda è facile che si creino situazioni di tensione, attriti o gelosie, che possono anche compromettere il buon esito dell'operazione.

La prima cosa che l'addetto alla disinfezione dovrà fare consisterà nel fermare tutte le attività di elaborazione su tutti i sistemi colpiti. Questo è un imperativo categorico, per quanto disastrosi possano sembrarne gli effetti. La maggior parte delle informazioni in molte aziende viaggia attualmente sui computer; fermarli equivale a fermare l'azienda. Di volta in volta l'esperto potrà suggerire delle azioni di rimedio, decidendo se e in che modo limitare le fermate; ma è imperativo che sia soltanto una persona a decidere quali computer possono essere accesi e quali debbono restare spenti.

Il consulente dovrà quindi tracciare la mappa degli scambi informativi in azienda, per esaminare il percorso che l'infezione possa aver seguito, determinare le priorità nella disinfezione e stabilire in che misura l'infezione si possa essere trasmessa ai supporti rimuovibili. Procederà quindi con le disinfezioni, regolandosi caso per caso a seconda della quantità e tipologia delle informazioni contenute nei sistemi, della presenza ed eventuale aggiornamento dei backup, dell'esistenza o meno dei supporti originali dei programmi.

Questa operazione, apparentemente «liquidata» in un breve paragrafo, può durare anche dei mesi e comportare problemi difficili o impossibili da sormontare senza perdite parziali o totali di informazioni. In ogni caso, anche se l'esperto riesce a recuperare tutte le informazioni, l'azienda avrà comunque sofferto un danno, quantomeno a causa delle fermate e per il compenso che dovrà corrispondere al consulente.

L'attività di disinfezione dovrà essere opportunamente corredata da un'opera di formazione diretta a tutti gli utenti dei computer. La formazione ideale sarà distinta in due fasi: una all'inizio del lavoro, in cui il consulente spiegherà a tutto il personale dell'azienda che cosa si accinge a fare, perché lo farà e come ciascun addetto può aiutarlo e rendergli più agevole il lavoro nell'interesse comune; al termine della disinfezione verrà fornito un minimo di cultura di base sui virus, sulla loro azione e sul loro effetto e — la cosa più importante di tutte — sulle misure di sicurezza. Dovrà essere spiegato il comportamento da tenere quando si eseguono programmi di provenienza incerta, e soprattutto si dovrà mettere in guardia ciascun utente contro i rischi di reinfezione, soprattutto da supporti rimuovibili.

Sarà inoltre opportuno far seguire questa formazione, ad alcuni mesi di distanza, da un «follow up», che potrà eventualmente ripetersi, per verifiche e aggiornamenti e per tenere desta l'attenzione del personale sul rischio virus.

Infine ciascuna azienda, a seconda del valore attribuito al proprio patrimonio informativo, potrà prendere le opportune misure contrattuali nei confronti dei propri dipendenti, nei limiti e nell'ambito delle possibilità di contrattazione offerte dalla normativa sul lavoro e dalle relazioni sindacali, per scoraggiare ed eventualmente sanzionare i comportamenti più marcatamente a rischio ai danni delle informazioni aziendali.

MC

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

rcp

SE VOLETE SAPERE COME CAMBIA L'INFORMATICA, CHIEDETELO AL VOSTRO EDICOLANTE.

Lui sa qual è il mensile di informatica sulla cresta dell'onda: ***MCmicrocomputer****, la rivista che ogni mese vi guida attraverso i cambiamenti e le novità del mondo degli strumenti del futuro, con un team di professionisti che non vi lasciano mai soli nel grande mare dell'informatica.*
La più diffusa, completa, autorevole rivista di informatica.

technimedia

Technimedia - Roma, via Carlo Perrier 9 - tel. 06.4180300

HD SCSI CONTROLLER PER A2000

SYNTHESIS HARDITAL 0-8 MB	L. 240000
PER OGNI MB AGGIUNGERE	L. 100000
SERIE II GVP 0-8 MB	L. 410000
PER OGNI MB AGGGIUNGERE	L. 100000
A2091 COMMODORE 0-2 MB	L. 280000
PER OGNI MB AGGIUNGERE	L. 100000
ADSCSI ICD	L. 240000
DATA FLYER	L. 170000

HARD DISK SCSI

QUANTUM 52 MB-11ms	L. 440000
QUANTUM 80 MB-11ms	L. 790000
QUANTUM 105 MB-11ms	L. 890000
QUANTUM 210 MB-11ms	L. 1210000

HD SCSI PER A500

SYNTHESIS HARDITAL 0-8MB	
CON QUANTUM 52 MB-11ms	L. 580000
PER OGNI MB AGGIUNGERE	L. 100000
A 590 COMMODORE 0-2MB/20MB	L. 620000
PER OGNI MB AGGIUNGERE	L. 100000

HD IDE PER A500/1000/2000

DOTTO HARDITAL	L. 150000

HD IDE-ATBUS PER DOTTO

PRAIRIETEK 20MB-2,5"	L. 490000
PRAIRIETEK 40MB-2,5"	L. 790000
QUANTUM 40MB-3,5"	L. 420000

ESPANSIONI PER A2000

SYNTHESIS HARDITAL 2MB L. 340000
4MB L. 520000-6MB L. 700000-8MB L. 840000
SUPEROTTO HARDITAL 2MB L. 280000
4MB L. 460000 - 8MB L. 780000
A2058 COMMODORE 2MB L. 790000

ESPANSIONI PER A500

SYNTHESIS HARDITAL 2MB L. 380000 4MB L. 580000-6MB L. 740000-8MB L. 880000
INSIDER 05 HARDITAL 512 KB L. 59000
CON CLOCK L. 74000
INSIDER 1 HARDITAL 1MB PER A500 PLUS L. 99000
INSIDER 2 HARDITAL 2MB L. 259000
INSIDER 4 HARDITAL 4MB L. 390000

ESPANSIONI CHIP RAM PER A500 E A2000

MEGA AGNUS HARDITAL 2MB DI CHIP RAM L. 349000

ESPANSIONI PER A3000

RAM ZIP 1MBX4-2MB L. 190000-4 MB L. 320000-8MB L. 620000

I MONITOR

COMMODORE 1084S	L. 450000
PHILIPS 8833	L. 430000

LE STAMPANTI

1230 COMMODORE	L. 315000
1550 COLOR COMM.	L. 410000

I PERSONAL COMPUTER IBM COMPATIBILI

HAR286-16 L.M.21 MHZ-CPU 286 A 0 WAIT STATE-1 MB RAM-1 DRIVE 1,44 MB 3,5"-2 SERIALI 1 PARALLELA-CASE CON DISPLAY DESK TOP O MONITOWER CON ALIM DA 200W-CONTROLLER PER 2 FD E 2 HARD DISK IDE AT BUS-SCHEDA VGA 800X600- TASTIERA ESTESA DA 102 TASTI-DR.DOS 5.0 CON MAN. ITALIANO A CORREDO. L. 690000

HAR 286-20. COME SOPRA MA CON CPU 286/20 L.M. 26MHZ L. 730000

HAR 386-SX16. COME SOPRA MA CON CPU 386 SX16 L. 849000

HAR 386-SX20. COME SOPRA MA CON CPU 386 SX20 L. 899000

HAR 386-25 L.M. 33MHZ-CPU 386/25 A 0 WAIT STATE-4 MB RAM-1 DRIVE 1,44" MB 3,5"- 2 SERIALI 1 PARALLELA 1 GAME-CASE CON DISPLAY DESK TOP O MINITOWER CON ALIM. 200W-CONTROLLER PER 2 FDD E 2 HARD DISK IDE AT-BUS-SCHEDA VGA 800X600-TASTIERA ESTESA 102 TASTI. DR. DOS 5.0 E MANU. ITALIANO A CORREDO. L. 1390000

HAR 386-33 L.M. 56MHZ. COME SOPRA MA CON CPU 386/33 E 64KB CACHE L. 1590000

HAR 486-33-SX20 L.M. 92MHZ COME SOPRA MA CON CPU 486SX20 L. 1690000

HAR 486-33 L.M. 151MHZ. COME SOPRA MA CON CPU 486/33 L. 1990000

NOTEBOOK CPU 386/20-LCD DISPLAY RETROILLUMINATO CON RISOL. VGA 640X480-1MB RAM- 1 HD 20MB-1 DRIVE 1,44" MB-CON ALIM. BATTERIE, BORSA TRASPORTO. L. 2990000

COME SOPRA MA CON HD DA 60MB L. 3490000

ACCESSORI E PERIFERICHE

MOTHER BOARD-286-16 L.M.20MHZ	L. 179000
MOTHER BOARD-286-20 L.M.26MHZ	L. 210000
MOTHER BOARD-386-SX16 L.M.21MHZ	L. 349000
MOTHER BOARD-386SX20 L.M.26MHZ	L. 419000
MOTHER BOARD-386/25 L.M.33MHZ	L. 570000
MOTHER BOARD-386/33 L.M.56MHZ	L. 749000
MOTHER BOARD-486SX20 L.M.92MHZ	L. 890000
MOTHER BOARD-486/33 L.M.151MHZ	L. 1340000
MOTHER BOARD-486/50 L.M.230MHZ	L. 1690000
COPROCESSORE INTEL 80287 10/12/16/20MHZ	L. 190000
COPROCESSORE INTEL 80387SX20MHZ	L. 290000
COPROCESSORE INTEL 80387/33MHZ	L. 430000
DRIVE 1,2 MB-5,1/4"	L. 125000
HARD DISK 40MB-17ms IDE AT-BUS	L. 390000
HARD DISK 130MB-17ms IDE AT-BUS	L. 720000
HARD DISK 210MB-15ms IDE AT-BUS	L. 1190000
CONTROLLER PER 2 HD AT-BUS	L. 29000
CONTR. 2FDD+2HD+2SER+1PAR+1GAME	L. 49000
MONITOR 14" VGA B/N SCH.PIATTO	L. 190000
MONITOR 14" SUPER VGA COLORI TRISCAN 1024X768	L. 549000
MONITOR 19" SUPER VGA COLORI TRISCAN 1024X768	L. 1590000
SCHEDA VGA 256 K 800X600	L. 89000
SCHEDA VGA 1024X768 1MB	L. 190000
MOUSE	L. 40000
HANDY SCANNER 200/300/400 DPI	L. 290000
HANDY SCANNER COLORI	L. 840000

I COMPUTER AMIGA

AMIGA 500 CON GARANZIA COMM.ITALIA	L. 629000
COME SOPRA MA CON 1MB	L. 690000
COME SOPRA MA CON 2,5MB	L. 849000
AMIGA 500 PLUS CON 2.0 E 1MB RAM	L. 710000
CDTV COMMODORE	L. 1040000
AMIGA 2000 CON GAR. COMM. ITALIA	L. 1190000
COME SOPRA MA CON HD SCSI QUANTUM 52MB E 3MB RAM	L. 2190000
AMIGA 3000 25MHZ E HD QUANTUM 52MB	L. 4760000
COME SOPRA MA CON HD QUANTUM 105 MB	L. 5390000

I DISCHETTI

DISCHETTI SONY, BULK, DS-DD, DA 3,5"
1 L. 790 - 10 L. 690 - 100 L. 640 - 1000 L. 560

SCHEDE AUDIO-VIDEO

GENLOCK CARD A2300 COMMODORE	L. 390000
FLIKER FIXER A2000	L. 310000
FLIKER FIXER 500 INTERNA	L. 310000
MONITOR MULTISYNC 14" PER FLIKER FIXER	L. 490000
COLORBURST MAST PER A500/1000/2000	L. 990000

COMPUTER CENTER

PER ORDINAZIONI
E INFORMAZIONI:
VIA FORZE ARMATE 260
20152 MILANO
TEL 02 48016309/4890213
FAX 02 4890213

TUTTI I PREZZI
SONO IVA
COMPRESA

SHEDE ACCELERATRICI

BANG 2081/2 HARDITAL CON 68020 E 68881 A 16 MHZ PER A 500/2000 L. 290000

BIG BANG HARDITAL C ON 68030 E 68882 A 25MHZ E 2 MB RAM PER A500/2000 L. 990000

COME SOPRA MA CON 4MB L. 134000-CON 8MB L.1690000. CON CLOCK A 50 MHZ AGGIUNGERE L. 990000

A2630 COMMODORE CON 68030, 68882 A 25 MHZ E 2 MB RAM L. 1760000

COME SOPRA MA CON 4MB RAM L. 2050000

COMBO GVP CON 60030, 68882 A 22MHZ 1MB RAM E CONTR. HD L. 1540000

COMBO GVP CON 68030, 68882 A 33MHZ 4 MB RAM E CONTR. HD L. 2690000

SUPER BIG BANG HARDITAL CON 68030,68882 A 25MHZ E CONTR. HD L. 990000. PER OGNI MB DI RAM AGGIUNGERE L. 120000

COME SOPRA MA CON 68030 E 68882 A 52MHZ L. 1990000

FUSION FORTY RCS CON 68040, 4 MB RAM L. 3990000

PROCESSORI

68000 16 MHZ L. 29000-68010 L. 24000-68020 16 MHZ L. 140000-68030 25MHZ L. 230000-68030 50MHZ L. 390000-68040 25MHZ L. 800000

INTEGRATI AMIGA

KICKROM 2.0 PER A500/2000 L. 99000
8373 SUPER DENISE ECS L. 129000
8372A FAT AGNUS 1MB L. 120000
8372B FATTEST AGNUS 2MB L. 149000
5719 GARY L. 29000

GLI EMULATORI MS-DOS

AT ONCE VORTEX CON EM.VGA L. 329000
AT ONCE PLUS CON 512K CACHE CHIEDERE AT ONCE ADAPTER PER A2000 L. 120000
JANUS XT COMMODORE L. 560000
JANUS AT COMMODORE L. 849000

I DRIVE

ADRIVE-DA 3,5" ESTERNO PER A500/1000/2000 CON INTERRUTTORE E PASSANTE L. 119000
ADRIVE 2000-INTERNO PER A2000 COMPLETO DI KIT L. 99000
SUPERDRIVE-ESTERNO PER A500/1000/2000 CON TASTO COPIATORE E ANTIVIRUS L. 139000

HARDITAL

SHOW ROOM VIA G. CANTONI 12
20144 MILANO
FERMATA METRO PAGANO
TEL 02 4983457-4983462