Virus e altri aggressori informatici: uno schema di prevenzione

di Stefano Toria (MC0170 su MC-Link)

Siamo arrivati a delineare, negli scorsi articoli, uno schema degli elementi costitutivi del rischio-virus. Naturalmente ogni esposizione di un rischio presuppone la proposta di un metodo di protezione dal rischio, o quantomeno di valutazione dell'entità del rischio stesso. Come si vedrà, non è possibile dare un valore attendibile alla probabilità di essere «infettati»; per contro, è piuttosto semplice mettere in atto alcune misure preventive che minimizzano l'incidenza di un'eventuale aggressione da parte di un virus, o di un cavallo di Troia o simili programmi

Virus informatici e comportamenti a rischio

Si è detto negli scorsi articoli che molta parte della fortuna dell'argomento «virus» nella stampa di informazione trae origine dall'associazione, del tutto errata ma di forte impatto psicologico, tra i programmi virus e l'agente causale dell'AIDS. Capita nuovamente l'occasione di ripetere che i due fatti non hanno nulla in comune tra di loro se non il modo di trattarne, e proprio perché l'argomento di questo capitolo è il comportamento a rischio in relazione alla diffusione dei virus informatici.

La stampa, la televisione e le affissioni stradali hanno ormai instillato nel grande pubblico non soltanto la nozione, ma anche alcuni dettagli sui comportamenti a rischio per l'AIDS. La minore rilevanza sociale del fenomeno ha fatto sì che mancasse un'informazione altrettanto dettagliata sui virus informatici, tanto che molti comportamenti gravemente rischiosi per la diffusione di eventuali programmi aggressori vengono ancora tenuti con leggerezza.

In questa prima parte della trattazione dei metodi di protezione (la seconda sarà pubblicata sul numero di settembre) si esamineranno tali comportamenti a rischio, al fine di delineare il comportamento che un utente di personal computer deve tenere per ridurre al minimo la probabilità di ricevere un programma virus, per massimizzare la probabilità di accorgersene per tempo nel caso in cui, nonostante ogni precauzione, dovesse comunque contrarre un virus.

Si descriverà quindi ciò che è stato definito da un commentatore statunitense il «safe hex», che tradotto in italiano (codice esadecimale «sicuro») perde l'assonanza fonetica con il «safe sex», il «sesso sicuro» consigliato come difesa dall'AIDS.

Si delineerà infine uno schema di protezione, con le misure fondamentali da prendere per garantirsi una tutela ottimale contro il rischio dei virus.

Il virus, si è detto, è un programma. In quanto tale, si avvale degli stessi supporti utilizzati dagli altri programmi, cioè principalmente dei dischi. Ma un virus non può svilupparsi di propria iniziativa dal nulla, come taluni filosofi e scienziati dell'antichità ipotizzavano riguardo a particolari forme di vita. Un programma virus deve necessariamente avere un creatore, che scrive le specifiche di comportamento del virus, lo realizza materialmente a mezzo di un compilatore o assemblatore, lo utilizza per infettare un programma altrimenti innocuo, e quindi diffonde quest'ultimo programma con il suo carico occulto costituito dal virus. Chiunque riceva questo programma e lo esegua, si infetta. Ecco pertanto definito il primo comportamento a rischio: eseguire programmi provenienti dall'esterno. E la relativa contromisura di sicurezza consiste in: non eseguire programmi provenienti dall'esterno.

Chiunque abbia una pur minima dimestichezza con un computer comprende immediatamente che un'applicazione rigida di questo criterio equivale, per molti utenti, a spegnere il computer e utilizzarlo soltanto come soprammobile. Sono ben pochi i proprietari di personal computer che non acquistano o non ottengono da «fuori» nemmeno un programma, che lavorano esclusivamente con programmi sviluppati autonomamente, realizzati peraltro in linguaggio macchina in quanto vigerebbe anche il divieto di acquistare ed importare un compilatore. Applicare ciecamente alla lettera questo concetto equivale a terminare l'era del personal computer.

Eppure l'unico comportamento rischioso, che può portare all'importazio-

ne di un virus nel proprio computer, consiste nell'eseguire programmi nuovi; la probabilità di infettarsi eseguendo un nuovo programma sarà maggiore o minore in funzione della maggiore o minore affidabilità della fonte del programma, come si vedrà tra breve.

Rischio e prevenzione

L'apparente assurdità del consiglio di non eseguire programmi provenienti da fuori, cioè programmi nuovi, nasconde il fatto che il concetto di per sé contiene alcuni elementi di saggezza. Non si dovrà evitare del tutto di utilizzare programmi di provenienza esterna, si dovrà sorvegliare il comportamento del computer prima, durante e dopo l'introduzione di un nuovo programma. È questa la principale e prima misura di sicurezza, che ne implica un'altra a monte: l'utente che desidera tutelarsi dal rischio di un virus deve necessariamente possedere una conoscenza operativa del proprio personal computer e del sistema operativo che lo governa. Dovrà essere in grado di intraprendere alcune specifiche azioni organizzative per disporre dati e programmi eseguibili in modo ottimale, al fine di minimizzare lo sforzo richiesto per mantenere aggiornate le copie di sicurezza, di cui si parlerà più avanti, e per ricostruire un sistema infetto, come si è visto nell'articolo pubblicato sullo scorso numero.

Alcune misure di prevenzione sono state ampiamente e ripetutamente invocate: ad esempio, non utilizzare soft-

Il software antivirus

ovvero: perché non abbiamo ancora pubblicato recensioni

Lo sviluppo del fenomeno virus ha fatto nascere e crescere rigogliosamente una nuova branca di software: i programmi antivirus.

In sintesi i programmi antivirus si possono dividere in due categorie: quelli che contribuiscono all'identificazione di un virus qualora esso abbia avuto occasione di infettare un particolare sistema, e quelli che prevengono l'infezione.

Quasi tutti i programmi antivirus, di entrambi i generi, fanno uso delle stringhe di ricerca alle quali si è accennato altrove in questo articolo. Il concetto di stringa di ricerca è piuttosto semplice: il virus viene analizzato e ne viene estratta una sequenza di caratteri sufficientemente lunga per consentire un'identificazione univoca del virus, tale cioè da poter essere riscontrata esclusivamente in quel programma e non in qualsiasi altro programma esistente, ma allo stesso tempo sufficientemente breve da consentire un rapido confronto con tutti i programmi presenti su un disco fisso, senza richiedere ore di tempo.

Il compromesso tra questi due requisiti è ciò che distingue, in ultima analisi, i programmi antivirus. Alcuni di essi tentano di massimizzare la velocità di scansione, a scapito dell'accuratezza. I ricercatori che hanno contribuito alla loro realizzazione hanno cioè utilizzato delle stringhe troppo brevi, che danno luogo a una serie di falsi allarmi. L'utente tenderà dopo qualche tempo a minimizzare l'importanza delle segnalazioni date dal programma, che diviene automaticamente inutile.

Altri programmi, più accurati, richiedono tempi eccessivamente lunghi per la scansione di un intero disco fisso, oppure si lasciano sfuggire le varianti meno note di alcuni virus.

Il compromesso perfetto non esiste. Peraltro stiamo riconsiderando l'effettiva utilità del software di scansione anche in funzione del materiale che abbiamo ricevuto in redazione.

I lettori rammenteranno che nel numero di maggio abbiamo annunciato la proposta di costituire un laboratorio antivirus, e a questo scopo invitavamo chiunque fosse in possesso di un programma sospetto ad inviarcene una copia per poter avviare l'attività del laboratorio.

Abbiamo ricevuto molte segnalazioni, delle quali ringraziamo i lettori in attesa di poter riportare un'analisi accurata di quanto ricevuto. Tuttavia una prima considerazione si impone immediata, in attesa di poterne trarre delle conclusioni più rigorose. Buona parte delle persone che ci hanno scritto segnalano «nuovi virus», che non vengono riconosciuti dai programmi in loro possesso. Non ci è stato possibile sottoporre a scansione tutti i dischi ricevuti, ma in alcuni casi abbiamo effettivamente riscontrato che i programmi da noi utilizzati (ViruScan di J.McAfee e Norton Antivirus) non danno alcuna segnalazione di presenza di virus.

Soltanto una analisi accurata del materiale che ci è stato inviato, e del suo comportamento, consentirà di stabilire se effettivamente i programmi contengono del codice che si autoriproduce; in attesa di poter condurre tale analisi ci esprimiamo nel senso di una riserva nei confronti dei programmi di scansione, anche dei migliori, in considerazione del loro limite implicito dato dal fatto che un programma di scansione non può riconoscere un virus sconosciuto all'équipe di ricercatori che ha realizzato tale programma.

Nessun programma antivirus dovrà mai essere utilizzato come unica misura di protezione nel caso in cui un personal computer contenga dati rilevanti o difficili da sostituire.

Un ulteriore limite dei programmi antivirus è implicito nel concetto stesso del programma.

Un utente è in grado di valutare i meriti e i demeriti di una qualsiasi applicazione, confrontando più programmi diversi per scegliere quello che meglio lo soddisfa.

Con i programmi antivirus questo non è possibile in quanto alla maggior parte degli utenti è preclusa la possibilità di mettere alla prova l'unica caratteristica veramente rilevante di questi programmi, cioè la loro accuratezza.

A meno che l'utente non sia in possesso di un vasto campionario di virus, egli non potrà mai essere certo del fatto che il programma riconosce effettivamente tutti i virus che afferma di riconoscere, e dovrà sempre fidarsi della parola di chi ha sviluppato il programma. (Personalmente tremiamo all'idea di un utente in possesso di così tanti virus).

È per questa ragione che finora non abbiamo pubblicato, in questa colonna, recensioni di programmi antivirus.

Senza un campionario di almeno trecento-trecentocinquanta virus non è possibile dare un giudizio sulle prestazioni di un antivirus.

Rinnoviamo quindi l'invito ai nostri lettori perché ci facciano pervenire i programmi che ritengono sospetti.

Le segnalazioni e i programmi possono essere inviate in redazione; rammentiamo che nulla dovrà essere indicato sulla busta, ma all'interno dovrà essere presente l'indicazione «Laboratorio antivirus». I programmi possono essere inviati anche a mezzo di MC-Link, indirizzandoli alla filebox di MC0100 (MCmicrocomputer) o MC0170 (Stefano Toria).

I contributi ritenuti più interessanti verranno ricompensati con un abbonamento omaggio alla rivista.

ware la cui fonte non sia più che certa. A questo proposito giova precisare in che modo deve essere valutata la fonte di un programma. Infatti si potrebbe essere portati a valutarla in funzione di caratteristiche personali o soggettive: mi fiderò più o meno ciecamente di una persona a seconda di quanto intimamente io conosca questa persona, da quanto tempo, etc. Ora, se questi criteri possono essere adottati con sicurezza nella maggior parte dei rapporti interpersonali, ad esempio nell'accettare in pagamento un assegno, non si può dire altrettanto nel caso del ricevimento di un programma da una persona, la quale può essere massimamente affidabile, onesta e bene intenzionata, ma del tutto inesperta di informatica e in particolare delle problematiche dei virus. Si deve cioè evitare di basare le proprie valutazioni sulle caratteristiche individuali della persona da cui si riceve un programma, dimenticando che tale programma può essere giunto a questa persona dopo un lungo giro di mani, le quali possono essere non altrettanto affidabili delle sue — ed egli può non avere le conoscenze tecniche necessarie ad avvedersi della presenza di un virus inserito da mani ignote.

In difetto di maggiori informazioni, pertanto, si dovrà prendere l'abitudine di diffidare inizialmente di ogni programma che non provenga da una fonte legittimabile.

Questo non vuol dire che non si dovranno utilizzare programmi a meno che non siano stati acquistati direttamente presso il produttore, anche perché chi ha seguito questa serie di articoli rammenterà il caso del programma «Freehand», distribuito inavvertitamente dalla Aldus Corp. (un serio e stimato produttore di software) completo di un virus.

La raccomandazione che si dà a chi riceve un programma da un amico, un conoscente o che acquista un programma da una fonte non sicura è di prestare particolare attenzione a ciò che il programma effettivamente fa sul proprio personal computer, consci del fatto che esso può contenere un virus — sebbene non è affatto detto che lo contenga. Si vedrà più avanti quali siano le attività da sorvegliare.

Se vengono acquistati o prelevati più programmi allo stesso tempo dalla stessa fonte, sarà consigliabile metterne in uso uno per volta, tenendo d'occhio il funzionamento del proprio computer per qualche giorno. Nel caso in cui non si verifichino fatti tali da far sospettare l'introduzione di un virus, si potrà mettere in uso il programma successivo, e così proseguendo. Per contro, se si dovesse rilevare che il programma ha introdotto un virus, si dovrà procedere alla disinfezione come è stato descritto nello scorso articolo.

Se il consiglio vale per i programmi ricevuti da chi si conosce personalmente, ancor di più ha valore per i programmi prelevati da un BBS. Si deve precisare, per dovere di corretta informazione, che non si è a conoscenza di una sola infezione contratta prelevando un programma da un BBS, il che depone a favore della professionalità dei SysOp (i gestori dei BBS), i quali controllano personalmente uno per uno tutti i programmi inviati dagli utenti o prelevati da altri sistemi prima di metterli a disposizione del pubblico. Tuttavia il problema teoricamente esiste, e nulla impedisce che un programma prelevato da un BBS contenga un virus.

In questo caso non è possibile alcuna valutazione personale sul gestore o sull'utente che ha inviato il programma, che saranno senz'altro delle degnissime persone ma sconosciute all'utente che intende prelevare il programma. Pertanto si dovranno applicare tutte le misure di sicurezza descritte, senza affidarsi alla nomina di professionalità di uno specifico sistema.

Le attività da sorvegliare nel periodo di «quarantena» di un nuovo programma riguardano essenzialmente gli accessi ai dischi. Ciascun utente, dopo qualche tempo, dovrebbe sviluppare il senso dei tempi delle principali funzioni svolte dal proprio computer, ad esempio per avviare un programma del quale si chieda l'esecuzione. Tempi eccessivamente lunghi, come si è visto, possono rivelare il fatto che un programma sta facendo più di quanto dichiara di fare: potrebbe essere in corso l'infezione di uno o più altri programmi eseguibili, o addirittura potrebbe essersi avviata l'azione dannosa contenuta in un virus maligno.

Oltre ai tempi si dovranno tenere d'occhio anche le dimensioni dei programmi eseguibili. Si è visto come molti virus si appendano ai programmi eseguibili, incrementandone le dimensioni. Prima di eseguire un nuovo programma sarà opportuno prendere nota delle dimensioni di alcuni eseguibili frequentemente utilizzati, primo fra tutti COMMAND.COM negli ambienti MS-DOS. Sarà opportuno identificare anche un eseguibile di tipo .EXE frequentemente eseguito e annotarne le dimensioni. Dopo una o più esecuzioni del programma sotto quarantena si potrà provare ad eseguire altri programmi, quindi far ripartire l'MS-DOS da un dischetto pulito e protetto, ed esaminare nuovamente le lunghezze dei file. Se non corrispondono, si è senz'altro verificata un'infezione ai danni dei file che sono aumentati di dimensione. Peraltro, se corrispondono non si può affermare con certezza che non vi sia stata infezione; potrebbe essersi infatti trattato di un virus che ricopre parte dell'eseguibile, o che infetta il boot sector o altre sezioni del disco fisso.

Programmi di scansione e copie di sicurezza

Una ulteriore misura di prevenzione consiste nell'adozione di un programma di scansione o di schermo antivirus. Di questi programmi ne esistono diverse decine ormai, più o meno noti e più o meno costosi. Un programma di scansione antivirus esamina rapidamente il contenuto di tutti i programmi eseguibili incontrati sul disco, alla ricerca di particolari sequenze di caratteri, ciascuna delle quali identifica univocamente un virus in quanto è stato verificato che è riscontrabile unicamente in quel particolare virus.

L'utente dovrà procurarsi una copia recente del programma di scansione o di schermo, e provvedere ad aggiornare periodicamente la copia in suo possesso sostituendola con una più recente. Data la rapidità con cui cresce il numero di virus noti, utilizzare una vecchia versione di un programma di scansione equivale quasi a non utilizzarne per niente.

Ma la misura di prevenzione più importante consiste nell'effettuare regolarmente le copie di sicurezza. Questa è un'operazione trascurata dalla maggior parte degli utenti di personal computer in quanto noiosa, ripetitiva, apparentemente improduttiva e difficile da eseguire. Eppure sono sufficienti pochi semplici accorgimenti operativi per rendere quasi automatico il lavoro di esecuzione delle copie; un'accurata pianificazione e un investimento iniziale di tempo consentono di ottenere copie perfettamente funzionali in breve tempo. Riportiamo uno schema valido per sistemi MS-DOS, ma facilmente adattabile anche ad altri sistemi.

1) Organizzare i file sul proprio disco fisso in modo da ottenere delle directory distinte che contengano i programmi e i dati separatamente. Anche se l'uso di un sistema di backup incrementale (v. più avanti) rende parzialmente superflua questa raccomandazione, è tuttavia indispensabile avere la massima chiarezza possibile nell'organizzazione del proprio disco fisso; a questo fine la prima misura da prendere

è proprio la separazione fisica tra programmi e dati. In questo modo oltre tutto si rende più semplice il passaggio da una versione di un programma alla successiva, in quanto la disinstallazione di un programma si riduce alla semplicissima operazione di rimuovere (con un del *.*) tutti i file presenti nella directory che contiene il programma.

2) Procurarsi un programma di backup/restore che consenta un'operazione più flessibile delle funzioni «spartane» BACKUP e RESTORE contenute nel DOS. In particolare, il programma deve fare uso dell'indicatore «archivio» che il DOS attiva su tutti i file che crea o modifica. Il programma dovrà prevedere la disattivazione dell'indicatore per i file che vengono trasferiti nella copia di sicurezza, e la possibilità di copiare soltanto i file che hanno l'indicatore attivato. L'ideale sarebbe acquistare un dispositivo di backup rapido (nastri di vario genere, dischi ottici) che quasi sempre si accompagnano a un software appositamente sviluppato che contiene queste ed altre utili funzioni; tuttavia il costo di un simile dispositivo lo mantiene fuori della portata di una parte degli utenti.

3) Effettuare una copia totale di tutte le directory che contengono dati. Archiviare i supporti della copia (dischetti, nastri, dischi ottici) con un foglietto che riporti indicazioni precise sulle circostanze della copia (data, ora, directory copiate).

4) Stabilire una procedura per l'esecuzione periodica delle copie dei file modificati. La cadenza di esecuzione di tali copie dipenderà dalla periodicità di aggiornamento dei dati: se variano quotidianamente in maniera significativa, le copie dovranno essere fatte tutti i giorni; se le variazioni sono settimanali, sarà sufficiente una copia alla settimana, etc. In queste fasi di copia periodica dovranno essere trasferiti soltanto i nuovi file, o quelli modificati dall'ultima copia; al termine dell'operazione tutti gli indicatori di archivio dovranno essere spenti. Una copia di questo genere (c.d. «incrementale») abitualmente non richiede più di cinque-dieci minuti in un sistema utilizzato normalmente da una sola persona che ne faccia un uso personale per videoscrittura, gestione piccoli archivi, grafica o programmazione.

Le copie incrementali dovrebbero essere tutte conservate, almeno da una copia completa all'altra (v. appresso). Se i backup vengono effettuati su dischetti da 1.44 Mb, è possibile che tali copie non richiedano più di uno-due dischetti per volta; se si utilizza un'unità a nastro probabilmente si potranno effettuare diverse decine di copie sullo stesso supporto prima di arrivare a riempirlo.

5) Stabilire in anticipo due giornate l'anno da dedicare a una copia completa del sistema, in cui verrà ripetuta l'operazione effettuata all'inizio. Le copie complete dovranno essere tutte conservate, per poter avere una situazione storica dell'andamento delle modifiche effettuate sui propri dati.

Ciascuna copia dovrà essere verificata immediatamente dopo la sua esecuzione. Poiché il fine delle copie è di consentire all'utente di dormire sonni tranquilli a fronte non soltanto del rischio di essere attaccato da un virus, ma anche del semplice rischio di un guasto, è indispensabile che egli sappia di poter fare affidamento sulle copie. Per qualsiasi evento — virus, rottura di disco fisso o inavvertita rimozione di un file — l'utente deve confidare nel fatto che è sufficiente prendere il supporto che contiene l'ultima copia e riportare su disco ciò che è andato distrutto. In particolare, in caso di attacco da parte di un virus l'utente deve poter tranquillamente effettuare una formattazione a basso livello del disco fisso, senza preoccuparsi dei propri dati se non per quelle modifiche fatte successivamente all'ultima copia di sicurezza effettuata. MC

Un po' di tecnica: i virus «nascosti»

Una tecnica di guerra utilizzata sin dall'antichità consiste nell'introdursi di soppiatto nel territorio nemico per attaccarlo dall'interno, o per compiere azioni di sabotaggio.

Determinante ai fini della riuscita di questo genere di azioni è una buona mimetizzazione, che in alcuni popoli in determinate epoche storiche ha raggiunto livelli di particolare sofisticazione.

Anche oggi, in presenza di una massiccia introduzione della tecnologia nella pratica bellica, la mimetizzazione riveste particolare importanza, anche se l'occhio da ingannare non è più soltanto quello dell'uomo ma quello ben più attento dei dispositivi elettronici di identificazione: primo fra tutti il radar.

Ecco quindi lo sforzo profuso dai centri di ricerca per realizzare dispositivi, principalmente aerei, a prova di identificazione. Una categoria di aerei incursori è stata denominata «Stealth» (lett. «soppiatto») proprio per questa capacità di sfuggire all'identificazione dei radar della contraerea.

Nella terminologia della ricerca antivirus, sono stati definiti «stealth» quei virus che mettono in atto qualche forma di mimetizzazione per sfuggire all'identificazione da parte dei programmi di scansione. Abbiamo tradotto questo termine con «nascosto».

Il primo virus nascosto di cui si abbia notizia è uno tra i primi virus ad essere stati riconosciuti: si tratta del Brain. Questo virus intercetta l'INT 13H, una funzione del DOS utilizzata per leggere un settore sul disco.

Se il virus — residente in memoria — riconosce che il settore letto è il boot sector, in risultato alla richiesta di lettura viene passato l'originario boot sector, non infetto, in luogo di quello effettivamente registrato all'inizio del disco; in questo modo l'utente può essere tratto in inganno, vedendo che il boot sector contiene ciò che dovrebbe contenere, e il virus gli tiene nascosto il fatto che in realtà il boot sector è stato modificato.

Aggirare questa tecnica di mimetizzazione è piuttosto semplice. È sufficiente avviare il sistema partendo da un dischetto sicuramente pulito e leggere il boot sector del disco incriminato; poiché il virus sicuramente non sarà residente in memoria, il settore restituito dall'operazione di lettura è il «vero» boot sector, e non quello mantenuto dallo stesso virus per ingannare l'utente.

Nel caso di un virus parassita, che si trasmette cioè attaccandosi a un programma eseguibile, la mimetizzazione è più difficile perché il virus dovrà soddisfare due condizioni:

1) non dovrà essere visibile (ad es. mediante il comando DIR) un aumento nella lunghezza del file;

2) un programma che legga il file eseguibile contenente il virus deve ottenere soltanto il contenuto del file originario, senza il virus.

Alcuni virus implementano un dispositivo di mimetizzazione che rispetta molto efficientemente entrambe le condizioni. Tra di essi i più significativi sono il «Number of the Beast» e il 4K (Frodo).

Tra le due condizioni indicate, la seconda è di gran lunga la più difficile da implementare.

Mentre molti virus sono in grado di nascondere l'aumento di lunghezza dei file che li ospitano, più difficile è nascondere l'effettiva presenza del codice virale.

Esistono tecniche particolarmente sofisticate, che per ovvie ragioni non è opportuno descrivere in dettaglio; i due metodi attualmente utilizzati richiedono che il virus mantenga da qualche parte una copia del contenuto originario del file infettato, per poterlo offrire «disinfettato» all'esame, per esempio a un programma di scansione.

L'unico metodo veramente efficiente per l'identificazione di un virus nascosto comporta l'uso di un algoritmo di controllo del contenuto dei file eseguibili. Di questo argomento si tratterà più diffusamente in un prossimo articolo.

E.GI.S.COMPUTER

VENDITA AL MINUTO E PER CORRISPONDENZA
UNICA AD UNIRE PRODOTTI DI ALTA QUALITA' A PREZZI CONTENUTISSIMI
VIA CASTRO DEI VOLSCI 40/42 M COLLI ALBANI - 00179 ROMA - TEL. 06/7810593-7803856
CONTATTATECI GARANTIAMO QUALITA' CORTESIA COMPETENZA
TUTTI I NOSTRI PRODOTTI SI INTENDONO GARANTITI 12 MESI - PREZZI IVA ESCLUSA
ORARIO 9.30 - 13.00 / 16.30 - 19.30 GIOV. POM. CHIUSO - SAB. MATTINA APERTO
POSSIBILITA' ANCHE DI VENDITA RATEIZZATA (SOLO PER ROMA)

MS DOS COMPUTER

AT 16 MHZ 1MB FD 1,44MB DUAL TASTIERA 101 DESK TOP PARALL. E SERIALE	650.000
AT 27 MHZ 1MB, FLOPPY 1,44MB, VGA 800x600, TASTIERA 101, DESK TOP, PARALLELA, SERIALE, HD 40MB, JOYSTICK	1.200.000
386 SX 20 MHZ, 1MB, FLOPPY 1,44MB, VGA 800x600, TASTIERA 101, DESK TOP, PARALLELA, SERIALE, HD 40MB	1.700.000
386 35 MHZ, 1MB, FLOPPY 1,44MB, VGA 800x600, TASTIERA 101, DESK TOP, PARALLELA, SERIALE, HD 40MB	2.300.000
386 54MHZ, 64 CASH, 2MB, FLOPPY 1,44MB, VGA 800x600, DESK TOP, TASTIERA 101, PARALLELA SERIALE, HD 40MB	2.500.000
486 117MHZ, 4MB, FLOPPY 1,44MB, VGA 1024, DESK TOP, TASTIERA 101, PARALLELA, SERIALE, HD 40MB	3.950.000
PORTATILE NOTEBOOK 286 VGA, HD 20, FD 1.44MB, KG. 2.6	2.600.000
PORTATILE NOTEBOOK 386 SX, HD 20MB, FD 1.44MB, FD EXT 1.2 MB, VGA, KG. 2.6	3.500.000
PORTATILE NOTEBOOK 286, 21 MHZ, FD 1.44MB, HD 40MB, VGA - VERYDATA -	3.150.000

ATTENZIONE ! SUI NOSTRI PREZZI NON VI SONO SGRADEVOLI SORPRESE: SI INTENDONO PER MACCHINE COMPLETE DI TUTTO

CONTATTATECI PER QUALSIASI CONFIGURAZIONE PERSONALIZZATA, SAPREMO ACCONTENTARVI !!

PIASTRA AT 27MHZ	270.000
PIASTRA AT 16MHZ	150.000
PIASTRA AT 21MHZ	230.000
PIASTRA 386 SX 20MHZ	550.000
PIASTRA 386 28MHZ	850.000
PIASTRA madre 386/33 CACHE	1.350.000
PIASTRA 486/117 MHZ	2.600.000
HARDISK SEAGATE 124-20	280.000
HARDISK SEAGATE 157-40 AT BUS	390.000
HARDISK QUANTUM 40MB	550.000
HARDISK QUANTUM 80MB	700.000
HARDISK MAXTOR 80MB,17M/S 1"	650.000
HARDCARD 40MB per Amstrad e Amiga	546.000
CDROM INT. + CONTROLLER	630.000
HARD DISC TOSHIBA 105 MB	700.000
HARD DISC SEAGATE 130 MB	850.000
MONITOR DUAL 14" B/W	190.000
MONITOR EGA AMBRA	218.000
MONITOR VGA BIANCO	210.000
COLORE VGA 1024x768 0,28	590.000
COLORE VGA 800x600 0,31	550.000
COLORE VGA 640x480 0.39	510.000
COLORE MULTYSINCH	700.000
MULTISYNCH MITSUBISHI	924.000
MULTISYNCH NEC III D	930.000
MOUSE da Lire	50.000
MODEM INTERNO 1200	99.000
MODEM INTERNO 2400	227.000
MODEM ESTERNO 1200	168.000
MODEM ESTERNO 2400	252.000
MODEM 2400 EXT. MNP5	294.000
TAVOLETTA GRAFICA	400.000
CABINET DESK TOP	142.000
CABINET MONITOWER	243.000
DRIVE 360K	100.000
DRIVE 720K	100.000
DRIVE 1.2MB	129.000
FLOPPY 1,44MB	129.000
CGA/HERCULES	60.000
VGA 800 x 600	120.000
VGA 1024 x 768 + ZOOM	210.000
VGA 1M+ZOOM	250.000
TASTIERA 101 TASTI	71.000
PARALLELA + 2 SERIALI	50.000
CONTROLLER AT MFM	120.000
CONTROLLER AT BUS	40.000
SCANNER + OCR	299.000
FAX FENNER FFI	750.000

CENTRO ASSISTENZA E RIPARAZIONI IN 24 ORE DI OGNI DIFETTO.
VOLETE RICEVERE IMMEDIATAMENTE IL NOSTRO DETTAGLIATISSIMO LISTINO?
COLLEGATEVI DOPO LE 20.00 CON LA NOSTRA BBS. NE RIMARRETE ENTUSIASTI: TEL 06/7803856

NOVITÀ

SCHEDA SOUND BLASTER	290.000
GRUPPO 600 W SINUSOIDALE	850.000
GRUPPO 500 W TRAPEZOIDALE	500.000
STREAMING TAPE ARCHIVE 60 MB	800.000
MODEM 38.400 MNP8	1.600.000
SCANNER 256 TONI	550.000
SCANNER COLORI	700.000
DOS 4.01	150.000
DR DOS 5.0	135.000

COMMODORE

AMIGA 500	588.000
AMIGA 2000	1.260.000
COMMODORE 64 NEW	220.000
MONITOR PHILIPS DD 33 II°	378.000
DRIVE PER CBM 64	205.000
DRIVE EST. AMIGA	139.000
DRIVE INT. A2000	120.000
ESPANSIONE AMIGA 500	84.000
MONITOR CBM 1084S NEW	400.000
SCANNER AMIGA	336.000
MOUSE AMIGA	50.000
GENLOCK A 2301	340.000
GENLOCK AMIGA	470.000
DIGIVIDEO AMIGA	110.000
DIGIAUDIO AMIGA	110.000
ANTIFLICKERING	800.000
VIDEON 3.0	462.000
HD 2000 2090	714.000
HD A590 500	714.000
MIDI AMIGA	67.000

STAMPANTI

IMMEDIATAMENTE DISPONIBILE A
PREZZO IMBATTIBILE
QUALSIASI MODELLO
DELLE SEGUENTI CASE:

EPSON
STAR
CITIZEN
NEC

LINEA GVP AMIGA

HARD DISK GVP 500 20MB	798.000
HARD DISK GVP 500 40MB	1.050.000
HARD DISK GVP 2000 40MB	945.000
HARD DISK GVP 2000 105MB	1.245.000
CONTROLLER GVP 8MB+HD	400.000
AT ONCE	396.000

COPROCESSORI MATEMATICI
IMMEDIATAMENTE DISPONIBILI
A PREZZI ECCEZIONALI.

UN ESEMPIO:

80287/12	**190.000**
80387/25	**350.000**
80387/33	**490.000**

FLOPPY DISK

5 1/4 DSDD	462
5 1/4 HD MITO	1.680
3 1/2 DSDD	756
3 1/2 SSDD SONY	1.092
3 1/2 DSDD MITSUBISHI	1.261
3 1/2 HD	1.680

PREZZI IVA ESCLUSA - GARANZIA 12 MESI - RICHIEDERE IL NOSTRO CATALOGO CON 350 ARTICOLI