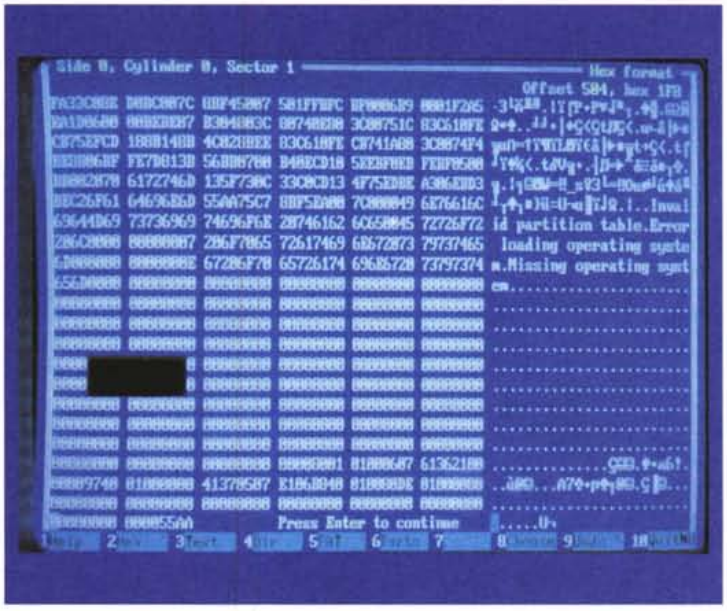
Tipologie di virus

Abbiamo pensato di dare ai prossimi dieci articoli, fino alla fine del 1994, la struttura organica di un vero e proprio corso sui virus. Non è ovviamente possibile corredare il corso con delle esercitazioni pratiche, per esempio di disassemblaggio di virus, ma crediamo che anche una semplice esposizione organica come quella che proporremo ai lettori possa essere utile

di Stefano Toria



Un virus è un programma come tutti gli altri. Questa affermazione ormai è stata ripetuta tante volte, eppure accade spesso di incontrare utenti che credono che un virus sia chissà cosa di miracoloso e magico. Invece si tratta semplicemente di un programma, o di una parte di programma, che ha la particolare caratteristica di essere capace di produrre una copia di se stesso senza che l'utente debba fare qualcosa di particolare. Anzi, il virus è in grado di duplicarsi senza che l'utente se ne accorga.

Un'altra caratteristica essenziale di un virus è che deve essere in grado di intercettare il percorso eseguibile, che è quella sequenza di istruzioni che il PC esegue dal momento in cui viene acceso. Seguiamole passo per passo, allo scopo di meglio comprendere i punti di attacco di un virus e quindi le vulnerabilità del nostro PC.

– La ROM

Quando il PC passa dallo stato di «spento» allo stato di «acceso» la memoria, i registri, etc. si trovano in una condizione indeterminata. Per poter determinare con certezza la sequenza di avvio, i progettisti della Intel che hanno realizzato il microprocessore 8086 e successivi hanno stabilito che la transizione da spento a acceso determinasse un particolare tipo di condizione, per la quale viene iniziata l'esecuzione di un programma che si trova all'indirizzo di memoria FFFF:0000.

Questo indirizzo deve ovviamente corrispondere a una ROM, il cui stato al momento dell'accensione è certo e predeterminato. La ROM del PC contiene quindi una serie di programmi specializzati tra cui quello che viene eseguito all'atto dell'accensione.

La funzione del programma in ROM è di predisporre variabili e registri in modo da consentire l'avvio della fase successiva: la ricerca di un disco e la lettura dello «stadio» successivo.

– Il master bootstrap

La sequenza di avvio del PC IBM «prima versione» prevedeva una ricerca di un drive per dischetti o di un disco fisso; qualora la ricerca non avesse effetto il programma in ROM «ricadeva» nel ROM-BASIC, un interprete Basic incorporato nella ROM. Si trattava di un retaggio architetturale del vecchio Apple II, dal quale la IBM mutuò alcune soluzioni progettuali. Ormai nessun PC è più dotato di ROM-BASIC, anche se l'architettura delle macchine più recenti mantiene lo spazio relativo a queste ROM per motivi di compatibilità.

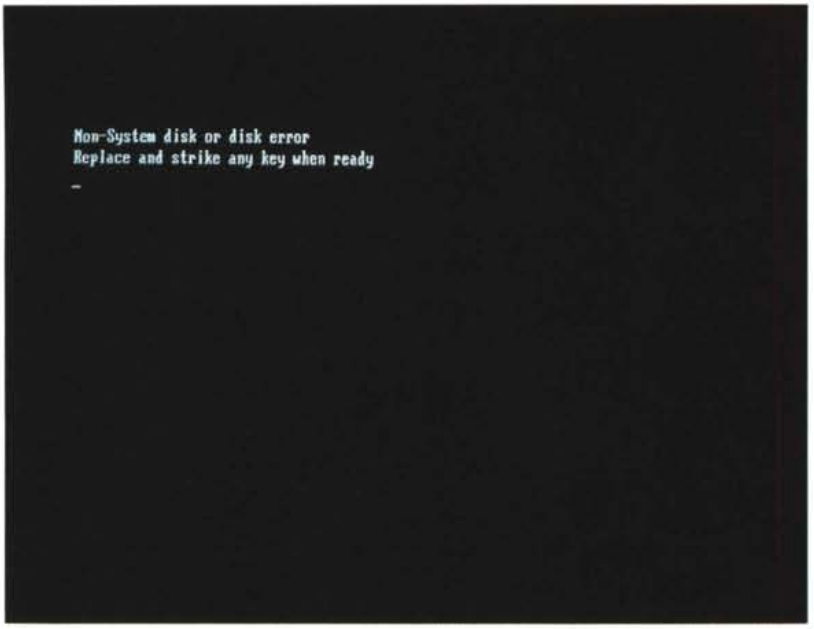
Il resto della sequenza è rimasto tuttavia invariato: dopo le operazioni di predisposizione e di avvio il programma in ROM esegue la scansione delle unità A: e C: per verificare se risultano esistenti e se contengono un supporto valido e leggibile. Scartiamo per ora l'ipotesi che sia presente un dischetto (ne riparleremo tra poco) e consideriamo cosa succede con il disco fisso.

La ROM va a leggere il primo settore della prima traccia del primo cilindro del primo disco fisso, la carica in memoria e – poiché si tratta di istruzioni eseguibili, in linguaggio macchina – passa il controllo del microprocessore all'indirizzo in cui ha caricato il contenuto di questo settore.

Parte così il «secondo stadio» della procedura di avvio; una fase rapidissima, che ha il solo scopo di determinare in quali e quante partizioni è suddiviso il disco fisso, e di lasciare residente in memoria un microscopico programma che ha solo e unicamente la funzione di trasformare le richieste dei programmi che verranno caricati in seguito, in modo da tenere conto dell'eventuale partizionamento del disco, descritto in una apposita tabella che si trova anch'essa all'inizio fisico del disco.

– L'avvio del sistema operativo

L'ultima operazione svolta dal programma di master bootstrap consiste nella determinazione di quale sia la «partizione attiva», cioè quella che contiene il sistema operativo da avviare, e nel leggere il primo settore di questa partizione, caricarne in memo-



ria il contenuto e avviarne l'esecuzione. Nel caso del DOS il programma di avvio consiste in un sistema in embrione, che è in grado di leggere la directory principale, identificare due file che solitamente sono i primi due dell'elenco, sono nascosti e hanno nomi standard (IBMBIO.COM e IBMDOS.COM oppure IO.SYS e MSDOS.SYS), e caricarli in memoria.

– Il «nucleo» e CONFIG.SYS

I due file appena caricati procedono con l'avvio del DOS, quindi cercano e leggono un file di testo che si chiama CONFIG.SYS e contiene istruzioni per la ulteriore configurazione del sistema: allocazione di aree, caricamento di dispositivi software di interfaccia, definizione e caricamento dell'interprete dei comandi. Solitamente quest'ultimo non verrà specificato, e in questo caso verrà preso per default il nome \COMMAND.COM

– L'interprete dei comandi

È quella componente del sistema che fa da interfaccia tra l'utente e il sistema stesso; l'utente impartisce dei comandi a tastiera e l'interprete li esegue. Normalmente consiste in un programma che si chiama COMMAND.COM ma può avere nomi diversi, vuoi perché l'utente gli ha cambiato nome, vuoi perché è installato un diverso interprete come ad es. 4DOS.

– AUTOEXEC.BAT

Quando viene richiamato per la prima volta, COMMAND.COM va in cerca di un file nella directory principale, che contiene una sequenza di istruzioni e comandi che l'utente può utilizzare per meglio configurarsi l'ambiente operativo.

Al termine dell'esecuzione dell'AUTOEXEC il controllo passa solitamente all'utente.

I punti di attacco

Il percorso eseguibile, a cui abbiamo accennato prima e che un virus deve poter intercettare per poter agire, consiste nella lunga sequenza di istruzioni macchina che vengono eseguite a partire da quella all'indirizzo FFFF:0000 fino al prompt C:\> nonché tutte quelle che vengono eseguite su richiesta dell'utente, perché avrà scritto "win excel" oppure "wolf3d" o qualsiasi altro comando.

Un programma entra nel percorso eseguibile su precisa disposizione dell'utente nel momento in cui questi dà il relativo comando di esecuzione.

Ma non sempre un programma entra nel percorso eseguibile per volontà esplicita dell'utente; ci sono anzi casi ben precisi in cui questo non accade. Vediamone uno.

Il dischetto traditore

Nel descrivere la sequenza di avvio del PC abbiamo volutamente sorvolato su quello che accade all'accensione del sistema se nel drive A: è presente un dischetto.

Vediamolo meglio adesso: il programma contenuto nelle ROM verifica prima la presenza di un dischetto nel drive A:, poi passa a leggere il C:. Ma se nel drive A: c'è un disco, allora scavalca la doppia fase master boot - boot di partizione e legge semplicemente e direttamente il settore di boot dal dischetto. I dischetti non prevedono partizionamento, infatti, per cui non è necessario leggere alcuna tavola di partizioni; in caso di presenza di un dischetto partono direttamente le fasi successive: lettura del settore di boot, lettura dei file nascosti, scansione del CONFIG.SYS eccetera.

Un momento. Tutto questo va bene se il disco è di sistema; ma se non lo è? Sappiamo bene la risposta a questa domanda: se il dischetto che si trova in A: al momento dell'avvio non è di sistema, non è stato cioè formattato con il comando FORMAT A: /S o simili, allora riceviamo il messaggio ben noto: «Disco non di sistema - sostituire e premere un tasto».

Ma qui viene il bello: quasi tutti gli utenti sono convinti che a emettere questo messaggio sia un programma contenuto nel PC, o per essere più precisi non si pongono nemmeno il problema di chi sia a scrivere questo messaggio.

Invece è importantissimo saperlo, è essenziale anzi, perché il messaggio VIENE SCRITTO DA UN PROGRAMMA CHE SI TROVA NEL SETTORE DI AVVIO DEL DISCHETTO STESSO.

Nessuno ci fa particolarmente caso, ma può capitare che il messaggio appaia in inglese («Non-system disk - Replace and press any key»). In altri casi può apparire in altre lingue, e allora sì che l'utente ci fa caso.

Il messaggio apparirà nella lingua prevista nella versione di DOS con cui il dischetto è stato formattato, ovviamente; ma il motivo per cui ci interessa tanto questo messaggio, e il programma che lo scrive sul video, è che questo programma costituisce il più formidabile e efficace veicolo di infezione per il nostro PC.

Infatti è facilissimo far eseguire questo programma senza nemmeno accorgersene: basta accendere il PC tenendo un dischetto infilato nel drive A:.

E questa è la prima operazione da NON FARE MAI: come scrivevamo nello scorso numero, e abbiamo scritto diverse altre volte, il PC va acceso senza dischetti nel drive. Il dischetto si potrà inserire solo dopo che il DOS sarà andato su regolarmente. Ma questa per tanti utenti è una sottigliezza, una particolarità a cui nemmeno si fa caso, oberati come si è da tanti altri pensieri e preoccupazioni.

E per questo motivo sono tanto diffusi i virus come lo Stoned, il Form, lo Spanish Telecom e il Flip, che utilizza-

Come si fanno le copie di sicurezza

Uffa, che noia. Ancora con queste maledette copie di sicurezza. Sì, ancora con le copie di sicurezza: poiché costituiscono l'unico metodo per avere la certezza di ripartire dopo un guaio, ad esempio dopo un'infezione massiccia ad opera di un virus, vale la pena di spendere qualche parola per spiegare bene, ancora una volta, come vanno fatte.

Regola numero uno: comprarsi uno streamer. Progettare di fare le copie di sicurezza sui dischetti equivale a progettare di non farle, perché ci sono poche cose più noiose del perdere il proprio tempo davanti a una macchina che ogni tanto chiede un nuovo dischetto, come un bambino piccolo che fa i capricci perché vuole il biscotto.

Non vogliamo fare moralismi né permetterci di giudicare nessuno, ma chi spende cifre di tutto rispetto per mettere insieme un sistema, magari un 486 DX2 da 66 MHz, con disco fisso da 600 Mb, XGA, CD-ROM, scanner a colori, stampante laser da 600 dpi, SoundBlaster a 16 bit, e modem/fax, può senz'altro permettersi di spendere qualche centinaio di migliaia di lire in più per comprarsi una piccola unità a nastro.

Non serve niente di particolare o di grandioso: basta un piccolo streamer da collegare alla porta parallela, tra il PC e la stampante. Sarebbe opportuno che l'unità sia in grado di scrivere, su un unico nastro, un quantitativo di Mb superiore alla capacità del disco; ma se si organizza bene la struttura del disco non è nemmeno indispensabile.

Anche i possessori di laptop e notebook possono usare uno streamer da porta parallela: anzi, per questo tipo di macchine le copie di sicurezza sono assai più importanti, perché il rischio di beccarsi un virus è rilevante ma è molto più rilevante il rischio di farsi sfuggire di mano il notebook mentre si scendono le scale di corsa.

Una volta acquistato e installato lo streamer molti utenti fanno le copie semplicemente trasferendo tutti i file dal disco fisso al nastro. Ma non è così che si fa.

La pratica migliore consiste nell'organizzare il proprio disco fisso ad albero: un primo ramo che distingue tra programmi e dati, e poi all'interno di ciascun ramo una distinzione per programmi o per categorie di dati. Ecco un esempio:

```
\
\BIN
\BIN\WINDOWS
\BIN\EXCEL
\BIN\WORDPERF
\BIN\CORELDRW
\BIN\SCANNER
\BIN\SBPRO
\BIN\FS5
\DATA
\DATA\740-92
\DATA\740-93
\DATA\TESTI
\DATA\TESTI\LETTERE
\DATA\TESTI\MC-LINK
...
```

I programmi di gestione degli streamer offrono generalmente due funzioni fondamentali per una buona esecuzione delle copie: il trasferimento di una directory con tutte le directory subordinate, e la copia incrementale.

In questo modo è sufficiente fare la copia di \BIN per trasferire con un sol colpo tutti gli eseguibili, e averne una copia di riserva da cui riprenderli, già installati, se qualcuno di essi dovesse infettarsi o comunque alterarsi. Questa copia dovrà essere eseguita una sola volta, dopo aver installato correttamente tutto il software dai dischi originali; i nastri utilizzati per le copie dovranno essere messi da parte e utilizzati soltanto in occasione di un problema nei programmi, quale ad esempio una cancellazione accidentale o un'infezione da parte di un virus, nei quali casi si potrà ricorrere alla copia di sicurezza per ripristinare il programma o i programmi soggetti all'incidente: in questo modo si riprenderà a lavorare assai più rapidamente che se si dovesse ripetere l'installazione anche di un solo programma.

Facendo la copia di \DATA invece si trasferiscono in una sola volta tutti i dati.

Per questi ultimi, che presumibilmente si modificheranno con frequenza, sarà opportuno iniziare con una copia integrale, il primo giorno, facendola seguire nei giorni successivi da copie «incrementali», nelle quali vengono trasferiti soltanto i file che risultano modificati dopo l'ultima esecuzione di una copia.

Di tanto in tanto (ogni mese, ogni due mesi) è opportuno rifare una copia integrale, soprattutto per riflettere la situazione degli eventuali file rimossi, perché le copie incrementali non segnalano il fatto che l'utente ha rimosso un determinato file.

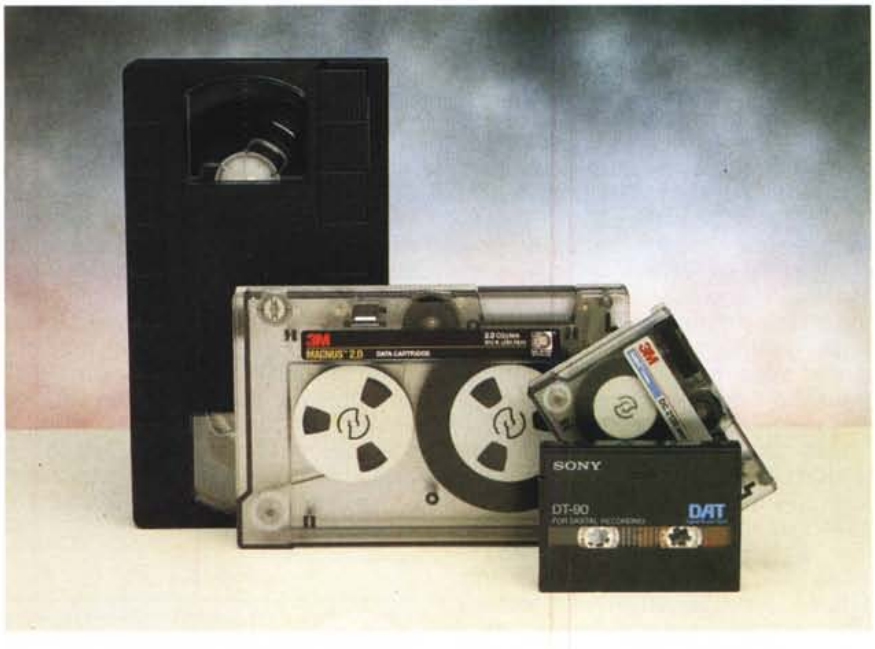
Ma la cosa più importante da fare dopo una copia di sicurezza è di verificare se funziona. Questa è una cosa che sono ben pochi a fare, anche tra coloro che - in un supremo sforzo di volontà - costringono se stessi a una regolare esecuzione delle copie.

Non c'è niente di peggio che perdere tempo a fare delle copie che al momento in cui servono risultano illeggibili.

Molti programmi di copia offrono una funzione di verifica della qualità della copia; è indispensabile utilizzarla ogni volta, ma anche simulare un recupero, copiando uno o più file dal nastro a una directory temporanea, e quindi confrontando (con il comando FC) il file ripristinato con l'originale: debbono risultare identici. Non è necessario fare tutti i giorni la doppia verifica, ma almeno una volta a settimana è utile farla. A scanso di sorprese.

Il mese prossimo vedremo come si organizza correttamente un ripristino di file dalle copie di sicurezza: dalla decisione di effettuare il ripristino al modo di eseguirlo.

Stefano Toria



no il settore di boot dei dischetti come mezzo, esclusivo o alternativo, di diffusione.

Definiremo quindi «virus di boot sector» quei virus che si servono del settore di boot per replicarsi; potremo poi distinguere tra virus di MBR, che sul disco fisso «attaccano» il settore di master boot, e di PBR, che si servono invece del partition boot record.

Il programma traditore

Ma il settore di boot non è il solo mezzo utilizzato dai virus per replicarsi e viaggiare. Un metodo alternativo consiste nel servirsi di un file eseguibile.

Il modo più facile è di scegliere come bersaglio un .COM, la cui struttura è semplicissima. Un file .COM consiste semplicemente in un'immagine della memoria; limitato a 64K in lunghezza, per poter essere «ospitato» interamente all'interno di un segmento di memoria, non contiene altro se non una sequenza di istruzioni riconoscibili ed eseguibili da parte del microprocessore.

Un virus ci mette poco a attaccare un .COM: basta che aggiunga in coda le istruzioni che lo compongono, aprendo il file per un'operazione di «append»; dovrà poi soltanto modificare la prima istruzione, per sostituirla con un «jump», che trasferisca l'esecuzione del programma alla prima istruzione del virus, e quindi accodare dopo l'ultima istruzione del virus un ulteriore «jump» alla prima istruzione valida del programma.

L'utente non si accorgerà quasi mai del minimo aumento nel tempo di esecuzione del programma; il virus sarà stato scritto in modo tale per cui ogni volta che viene eseguito va in cerca di una potenziale vittima per infettarla, oppure per rimanere residente in memoria in modo da infettare ogni programma che viene eseguito, oppure per avvalersi di altre tecniche di infezione.

Nel caso di un .EXE l'operazione è resa leggermente più complessa dal fatto che questi file iniziano con un'intestazione, lunga 512 byte, che contiene informazioni particolari per l'esecuzione del programma; ma l'infezione dei file .EXE è possibilissima, e sono centinaia i virus in grado di eseguirla.

Questo tipo di virus si chiama «parassita».

Due piccioni, etc.

Il veicolo tipico delle infezioni da virus di boot sector è il dischetto, dimenticato nel drive al momento dell'accensione.

Per i virus parassiti veicolo d'infezione è il programma, il file eseguibile, che può essere copiato da un dischetto, ma anche prelevato a mezzo di un modem (per esempio su un BBS il cui gestore sia poco attento ai controlli), o diffuso su una rete locale.

Qualcuno ha pensato di massimizzare le opportunità di diffusione del proprio virus, unendo la tecnica di infezione del boot sector a quella di infezione dei file. I virus di questo tipo si chiamano «multipartiti» e rappresentano una minaccia raddoppiata rispetto ai parassiti o a quelli di boot sector.

Di nascosto

Un altro tipo di virus sfrutta una particolarità del sistema MS-DOS. Quando l'utente scrive un comando, per esempio «win», questo viene interpretato da COMMAND.COM secondo una precisa sequenza di analisi. Innanzitutto verifica se il comando corrisponde a una delle funzioni interne allo stesso COMMAND.COM (dir, type, set, ver, copy, chdir, mkdir, rmdir, erase, cls eccetera). Se non corrisponde a nessuna di queste, l'interprete dei comandi va a cercare un file con il nome corrispondente al comando, e estensione ".COM"; nell'esempio, "WIN.COM". Se lo trova lo esegue; se non lo trova va a cercare un file corrispondente, ma con estensione .EXE ("WIN.EXE"); se non trova nemmeno questo cerca un file con estensione .BAT ("WIN.BAT"); se non trova neppure quest'ultimo, segnala che il comando non è riconosciuto.

Questa sequenza di priorità viene sfruttata da un tipo di virus che scrive una copia di se stesso in un file di tipo .COM, che viene registrato sul disco con l'attributo «hidden», nascosto, in modo che l'utente non lo veda quando lista i file contenuti nella directory. L'astuzia del virus consiste nel fatto che il nome attribuito al virus è lo stesso di un file .EXE presente nella stessa directory. Pertanto l'utente scriverà ad es. CONTAB, sapendo che esiste un programma CONTAB.EXE che serve a far partire il sistema di contabilità, e a sua insaputa verrà eseguito per primo CONTAB.COM, nascosto nella stessa directory, ma ben visibile al DOS che nel seguire la sua procedura di ricerca lo trova per primo. CONTAB.COM contiene il virus, che farà quello che deve fare (tipicamente fare una copia di se stesso con un altro nome, sempre corrispondente a un .EXE) e quindi avvierà esplicitamente l'esecuzione di CONTAB.EXE.

Questo tipo di virus è piuttosto poco diffuso, anche perché non è possibile trasferire un file «hidden» con il comando «copy»; in inglese viene definito «companion», che possiamo tradurre con «associato».

Senza rete

Ci sono stati poi alcuni casi isolati di autori di virus che hanno voluto fare vere e proprie acrobazie: dall'autore del DIR II che sfrutta il meccanismo di collegamento tra nome di file e inizio fisico del file, per far puntare gli eseguibili alla stessa posizione, che contiene il virus; all'autore del Batman, che sfrutta l'identità tra una particolare sequenza di istruzioni in linguaggio macchina e la rappresentazione ASCII dei caratteri che compongono la sequenza di istruzioni "@ECHO OFF <CR> <LF> REM" per ottenere un virus trasformista, che si presenta come .BAT ma può essere eseguito anche come .COM; non approfondiamo questi tipi di virus perché si tratta di curiosità piuttosto che di effettive minacce. MC

Stefano Toria è raggiungibile tramite MC-link alla casella MC0170 e tramite Internet all'indirizzo MC0170@mclink.it.

Una legge sui crimini informatici

Il 14 dicembre dello scorso anno il Senato ha approvato il testo di un disegno di legge che già il 29 luglio era passato al vaglio della Camera dei Deputati. Argomento: penalizzazione della criminalità informatica.

La legge, che porta il titolo «Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica», è il risultato di diversi anni di lavoro e di un notevole sforzo di sintesi di esperienze di altri Paesi che prima del nostro si erano dotati di strumenti normativi di questo genere.

Ben lungi dall'essere perfetta, la nuova legge ha già scontentato alcune categorie: ad esempio, chi si occupa di virus vede nella nuova normativa una possibilità di repressione indiscriminata dei ricercatori in buona fede assieme a chi i virus li scrive o li diffonde consapevolmente.

La normativa, che è entrata in vigore il 14 gennaio di quest'anno, è stata invece accolta con soddisfazione negli ambienti più sensibili al rischio delle intrusioni, come ad esempio le banche.

Il prossimo 3 marzo si terrà a Roma un convegno sui contenuti della legge. Organizzatore è il Club sul Computer Crime, una divisione dell'Ipacri, azienda leader nel settore dell'informatica bancaria.

Informazioni sul convegno possono essere richieste alla Segreteria del Club, telefono (06) 51894227, fax (06) 51894200.

Prodotti di Alta Qualità e Convenienza nei Prezzi
Professionalità ed Assistenza Qualificata

VENDITA AL MINUTO E PER CORRISPONDENZA
MERCE PRONTA CONSEGNA
RICHIEDETE IL NOSTRO LISTINO :
I NOSTRI PREZZI SARANNO IL VOSTRO GRANDE AFFARE !

EGiS COMPUTER

Competenza e cortesia a Vostra disposizione per consigliarvi nelle Vostre scelte

PAGAMENTO RATEIZZATO

Possibilità di pagamento rateizzato in ***tutta Italia*** *con evasione della pratica in un giorno* ***senza costi aggiuntivi*** **!**

UPGRADE SISTEMI

Entra nel nuovo ***Standard Vesa*** con valutazione del Tuo usato. Sostituzione in 24 ore

Piastre Madri

386 SX/40 SMT	164
386 DX/33 256k upg 486	293
386 DX/40	259
386 DX/40 128k upg 486 L.Bus	389
486 DLC/40	349
486 DX/33 256k Vesa Pentium	770
486 DX/40 128k Vesa Pentium	790
486 DX2/50 128k Vesa Pent.	870
486 DX/50 256k Vesa Pentium	1.039
486 DX2/66 256k Vesa Pent.	1.142
New IBM 66 MHz 64k Vesa	**825**
New IBM 99 MHz 64k Vesa	**Tel.**

Amiga

Amiga 600	460
Amiga 1200	568
Hard Disk A1200 - 130Mb	488
Hard Disk A1200 - 210Mb	699
Amiga 4000/030 HD	2.099
Amiga 4000 + 120Mb HD	3.529

Tutti gli accessori per Amiga

Schede VGA

800x600 256 Kbyte	49
1024x768 1 Mbyte	109
1280x1024 1 Mbyte da	136
1280x1024 1Mb TrueCol. da	170
1280 Vesa - Win. Acc.	159
1280 Vesa TrueColor exp.2Mb	199
Weitek 9000	800

Accessori

SoundBlaster Pro II DeLuxe	199
Multimed. Kit DoubleSpeed	890
Video Blaster	550
Video Spigot	580
LogiTech Scanner + OCR	280
LogiTech Scan. 256 + OCR	450
Scanner Colori TrueColor	590
Scanner da tavolo	790
Tavoletta Grafica 12x12	320
Fax TRL	650
Gruppo di Continuità 250W	399
Gruppo Continuità 1000W	950
ModemFax Poket - V42bis	259
ModemFax esterno - V32	420

Hard Disk

40 Mbyte	199
80 Mbyte	270
135 Mbyte	329
210 Mbyte	420
250 Mbyte	460
340 Mbyte	569
425 Mbyte	740
600 Mbyte	890
1.050 Mbte	1.590
CD ROM Mitsumi XA	390
CD ROM Sony XA D.S.	450
Tape BackUp 120 Mb	250
Tape BackUp 250 Mb	399

Monitor

VGA Monocromatico	180
VGA color 1024 da	350
VGA color 1024 0.28 da	399
VGA color 1024 low rad.	450
LARIS 15" col. 1280 NI	850
VGA 19"color 1024	1.299
Sony Trinitron 14" 0.25	950
Sony Trinitron 17" 0.25	1.790
Sony Trinitron 20"	3.290

Add - On

Local Bus Cache IDE	299
Local Bus Cache OPTI	259
Local Bus Vesa	89
Local Bus Cache Vesa	399

Tastiere Italiane e USA
Drive, Controller e Multi I/O
Porte Parallele, Seriali e Game,
Joystick e schede di ogni tipo
Mouse a partire da £ 19.000

SOFTWARE su CD

Vasto assortimento CD di tutte le marche:
Corel, MicroForum, Chestnut, Walnut Creek, ...
Titoli su ordinazione. **Servizio SCRITTURA CD !**

FLOPPY DISK

Dischetti 3.5 HD preformattati 1.44 Mb 840

Speciale STAMPANTI

9 aghi	9 aghi colori	24 aghi	InkJet	InkJet colori	Laser	Laser
259	**310**	**349**	**369**	**649**	**980**	**1.180**
IBIComp	Star LC100	CitizenSW200	Fujitsu B100plus	HP310	Texas	HP IV L

Citizen - OKI - Star - NEC - Epson - Hewlet Packard - Fujitsu

Macchine Complete :

Olivetti M290 350
386 Sx/40 579
386 DX/40 642
486 DLC/40 745

486 DX/40
128k Vesa - upg. *Pentium*
1.199

486 DX2/50
128k Vesa - upg. *Pentium*
1.279

486 DX/50
256k Vesa - upg. *Pentium*
1.540

486 DX2/66
256k Vesa - upg. *Pentium*
1.607

---------- **Eccezionale** ----------
486 IBM 66 MHz 64k Vesa
1.242
Nuovissimo 486 IBM 99 MHz
Telefonare !

NoteBook 386 Sx
2Mb - HD 60
1.499

***Sub*-NoteBook 386 Sx**
Texas - 2Mb - HD 80
2.200

NoteBook 486 SLC/25
SuperMate - 4Mb - HD 170
2.499

NoteBook 486 Sx/25
Texas **- Schermo Colori**
4 Mb - HD 120
3.699

Ogni computer è da ritenersi così configurato :
Piastra Madre in Cabinet Desk - 1 Mbyte RAM
Scheda Grafica VGA - Drive 1.44
2 Seriali - 1 Parallela - Game - Tastiera 101 tasti

Garanzia 12 Mesi , anche a domicilio

EGiS COMPUTER

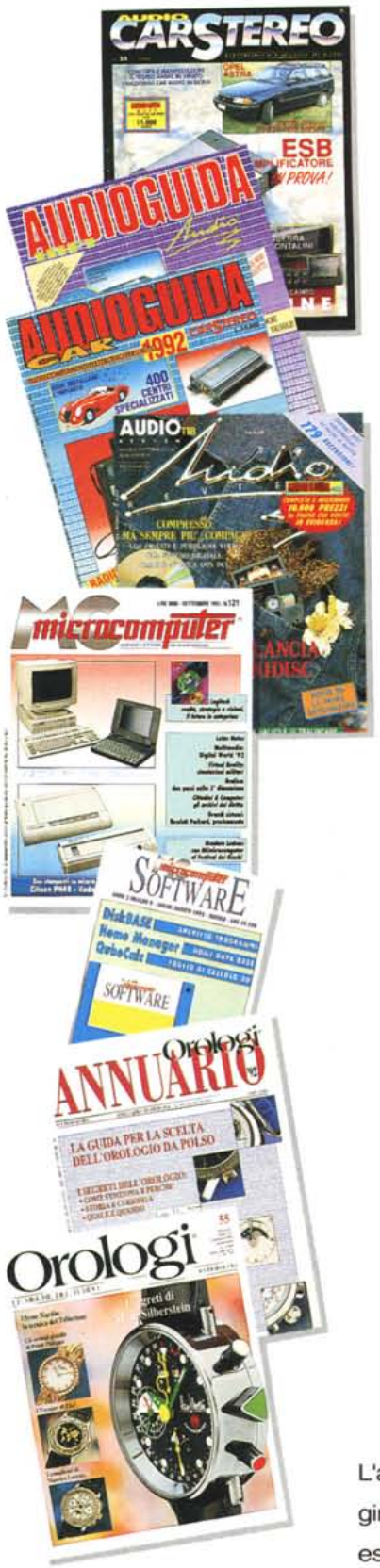
si trova a:

ROMA - Via Tuscolana 261 - 00181 (Metro Furio Camillo) - Tel. 06 / 7810593 - 7803856 (Fax)
FROSINONE - Via Cosenza 62 - 03100 - Tel. 0775 / 260499 (Fax)
UDINE (S. Daniele del Friuli - Zona tre Venezie) - Via Kennedy 31 - 33038 - Tel 0432 / 941078

Orari: 9:30 - 13:00 / 16:30 - 19:30 - Giovedì chiuso

Telefonateci per la Vostra Configurazione Personalizzata: Sapremo darvi il Meglio

IBICOMP Punto Vendita computer IBI*Comp* ***Distributore***



Le vostre passioni sono anche le nostre.

L'alta fedeltà, l'informatica, gli orologi: non hanno segreti per i nostri lettori. Migliaia di pagine di cultura, di tecnica, di attualità, di splendide immagini, di giudizi e consigli dei migliori esperti dei rispettivi settori, guide sicure per orientarsi nell'uso o nell'acquisto di ciò di cui avete bisogno, o di ciò che amate. Per chi vuole saperne di più: per cultura, per lavoro. O per passione.

technimedia

Technimedia. Pagina dopo pagina, le nostre passioni.