Qualche lineetta di febbre...

Le signore, finalmente, se ne sono andate (se non capite di cosa sto parlando, occorre che leggiate la prima parte di questa minitelenovela) e finalmente posso aprire la porta. Il salotto è un vero campo di battaglia, bicchieri di carta e residui alimentari di vario genere sparsi dappertutto, ceneriere colme, "ma 'sta ggente 'a tene 'na casa da' loro?". Il computer in camera di Anja , dopo l'intervento, è sotto sedativi e dorme un sonno inquieto (ogni tanto vado a dare un'occhiata ove mai si staccasse la flebo!), anche se la febbre è calata. E io sto morendo di fame!

Accudita alla salute del bit, passiamo alla cura del corpo. La mia signora se ne va subito a letto, non senza pronunciare la fatidica frase "Anche fare del bene è faticoso!". E finalmente sono padrone del campo. Frigorifero, a noi! Recupero da "Avvisi ai naviganti" la mia favolosa ricetta del "Panino atripaldese" (burro, pomodoro, insalata, mortadella, gorgonzola e una spruzzata di pepe); il panino fresco non l'ha, ma nel pomeriggio ho comprato un "tortano con i cicoli" che parla da solo e l'uso come materia prima della pietanza. Telepiù sta trasmettendo "Reazione a catena" con Keanu Reeves (come dice Sergio Donati, chissà se ci è o ci fa), mi metto comodo e, complice l'insonnia, si godo un paio d'orette di piacevole serata. Voi, lettori cari e affezionati, leggetevi la parte finale riguardante i virus.

di Raffaello De Masi

Terza parte

Riassumendo...

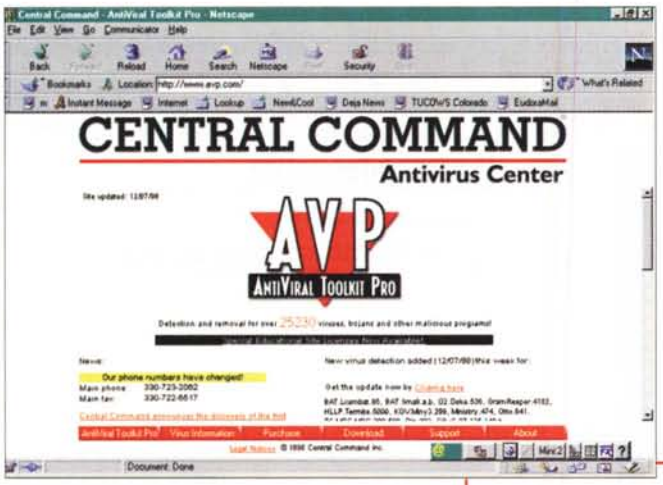
Beh, siano alla stretta finale, dove raccoglieremo i pezzi sparsi e daremo le medicine adatte. Quanto è grande il pericolo dei virus? Possiamo dire che è direttamente proporzionale al livello di guardia che useremo nelle nostre procedure quotidiane. Certo, la tecnica del backup può dare una certa garanzia diminuendo il pericolo di un disastro totale in caso d'attacco da virus, ma poiché anche le copie possono, a nostra insaputa, essere infette, occorrono altre misure di prevenzione.

Se il livello di difesa è basso, un virus ben progettato può trasmettersi pressoché senza dare sintomi da un virus all'altro. In tempi sufficientemente lunghi, un buon virus può infettare praticamente ogni computer di un'organizzazione o di un network, e con essi le eventuali copie di backup. Se l'implementatore del virus ha creato un agente potente ed efficace, le modifiche negli "ammalati" possono essere così sottili e irrilevanti da essere quasi impossibile rilevarle prima del collasso generale. Sovente piccole discrepanze, lievi imperfezioni dei dati, errori nel contenuto di una pagina di wp che si confondono meravigliosamente con quelli di battitura, imperfezioni che sono sovente confuse con errori dell'operatore o altri fattori casuali, stringhe di caratteri casuali comparse all'improvviso, messaggi d'attenzione come "disco pieno" o "operazione illegale". Queste piccole incongruità, che talvolta vengono addirittura patite con rassegnazione ("tanto Windows o Word o WordPerfect sono pieni di bug"), possono mascherare il periodo di latenza prima dell'attacco. Certo, non vogliamo contraddirci con quel che abbiamo detto nella prima parte; nella maggior parte dei casi non vogliono dire nulla, ma vuoi vedere che... Di esempi d'utenze anche grandi messe in ginocchio da un attacco, trascurato, di virus n'è piena la cronaca.

E allora, nella puntata di chiusura dell'argomento, qualche raccomandazione, qualche abitudine da acquisire o da evitare, insomma qualche buon consiglio che, al contrario della sorte che subiscono quelli non richiesti, vorremmo fossero ascoltati.

Miti e leggende sui virus

Passare dalla noncuranza alla psicosi è facilissimo. Ho conosciuto una persona a riguardo che, dopo essere stata



Antivirus toolkit Pro e Anyware Anti-Virus, due pacchetti shareware giunti ambedue alla versione 3.

colpita (pesantemente) dal famigerato Jerusalem, non accetta un dischetto sconosciuto neppure sotto la minaccia di una pistola.

L'area della cattiva informazione a proposito dei virus è, probabilmente, ampia quanto l'area, almeno dei virus stessi. Come dicevamo prima, si passa dalla completa noncuranza a una fobia incontrollata, cose che, in ambedue i casi possono produrre gravi danni, comparabili a quelli dei virus stesso.

Con la tecnica della " catena di sant'Antonio", certe comune credenze a proposito dei virus si sono sparse a macchia d'olio, rapidamente, del mondo informatico, creando disinformazione, e, talora, vere e proprie psicosi da caccia all'untore. Vediamo qualcuna di queste leggende metropolitane dell'informatica, cercando di dire, se possibile, una parola definitiva su certe assurde e strane credenze:

✔ il virus possono riprodursi spontaneamente: l'affermazione è del tutto errata, visto che il virus non può far nulla, letteralmente, fino a che un programma o un file infetto vengono lanciati, o un computer viene fatto partire da un disco infetto;

✔ il virus può propagarsi anche tra computer funzionanti sotto sistemi operativi diversi: l'affermazione era, sino a poco tempo fa, del tutto in consistente. Un virus di Windows non può certo attaccare un Mac o un sistema Unix; ma la comparsa, ultimamente, di macro virus che usano come veicolo file di Word ed Excel ha portato a infezioni trasmesse da computer a computer funzionanti sotto sui diversi sistemi operativi. C'è da precisare, in ogni caso, che queste macro colpiscono, ovviamente, solo i file prodotti con applicazioni riferibili allo stesso tipo (per esempio wp; tanto per intenderci, un macrovirus CAP non può certo infettare un computer che fa girare solo pacchetti grafici);

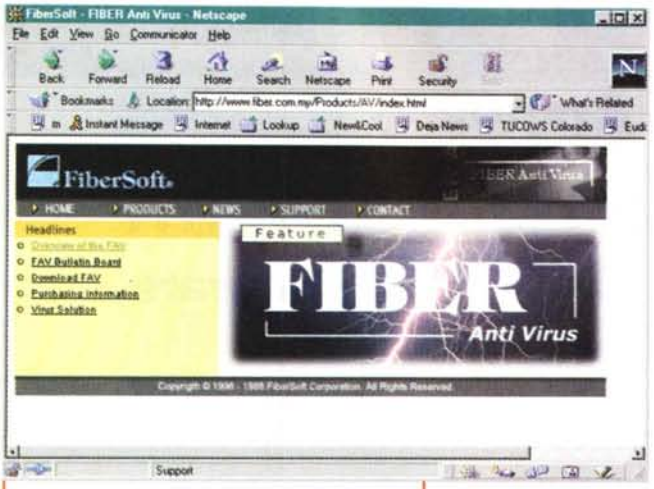
✔ il virus può infettare dischetti protetti da scrittura: l'affermazione è falsa. I dischetti (o altre unità di memoria, come cartucce o nastri) protetti manualmente dalla scrittura non possano essere colpiti; non è vero, però, il contrario. Un dischetto " sporco" anche se protetto da scrittura, può infettare il computer su cui viene letto;

✔ non tutti i virus sono pericolosi: l'affermazione è priva di significato oltre che di senso. Qualunque virus, per il fatto di riprodursi, può in teoria cancellare dati presenti sulla memoria di massa e, anche nei casi più benigni, resta sempre, sul disco, come ospite non invitato e non richiesto (che, solo per il fatto di esserci, occupa spazio che potrebbe servirsi per altri scopi);

✔ solo i programmi copiati contendono virus: l'affermazione è non vera. Sebbene il maggiore veicolo di trasmissione dei virus siano i dischetti passati di mano in mano, ci sono numerosi esempi di

Avast 32, un eccellente pacchetto dotato delle più raffinate opzioni; il prezzo è molto allettante.

e-safe, che, dopo l'acquisizione da parte di Aladdin ha subito un'efficace cura di aggiornamento e ringiovanimento; interessante l'area antivandalismo.



Fiber antivirus, il pacchetto meno costoso del gruppo. Efficace, ma con non molte opzioni aggiuntive.

Inoculan, un vecchio prodotto ben noto in ambiente Windows; molto diffuso tra piccole dotate di network.

McAfee, che rivaleggia, in popolarità con NAV, offre un supporto all'utente di ottima qualità e protezione su diverse piattaforme.

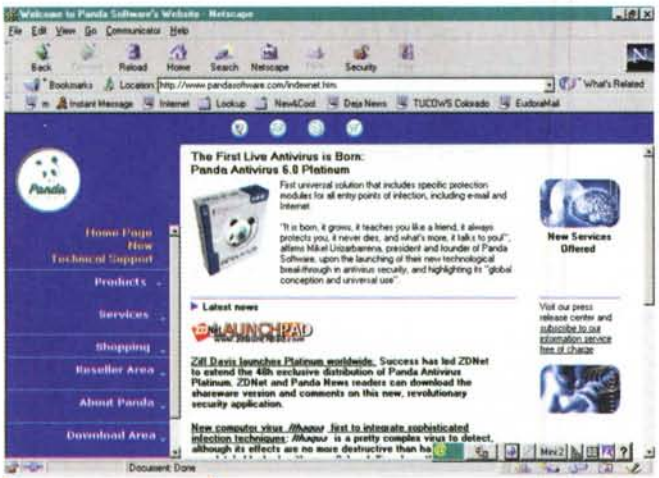
infezioni trasmesse in maniera anche disastrosa, da produttori di software che hanno messo in commercio applicazioni infette. In questi casi, sovente, accadono infezioni disastrose, in quanto ben difficilmente un dischetto originale viene sottoposto alle comuni pratiche di verifica da infezione;

✔ la maggior fonte di virus sono la posta elettronica e i collegamenti a Internet: sembrerebbe un'affermazione plausibile, e invece, almeno in parte, non lo è. Se è vero che è molto facile trasferire virus nei collegamenti persona a persona (attenzione, quando si scambiano file attached; la posta in formato di solo testo non può trasportare infezioni) è altrettanto vero che il downloading di file da BBS e da siti che distribuiscono shareware generalmente non comporta eccessivi pericoli (tutti i file qui ritrovati vengono controllati prima di essere messi a disposizione del pubblico; è questa un'operazione di precipuo interesse per il distributore, visto che, in caso di infezione in questi termini, la cosa si tradurrebbe in un vero e proprio disastro per il distributore stesso). Inoltre, virus che attaccano i settori di boot (come il famoso Michelangelo, Valkyrie, o Form) non sono trasmissibili via Internet;

✔ l'uso di un buon antivirus garantisce la completa protezione della nostra

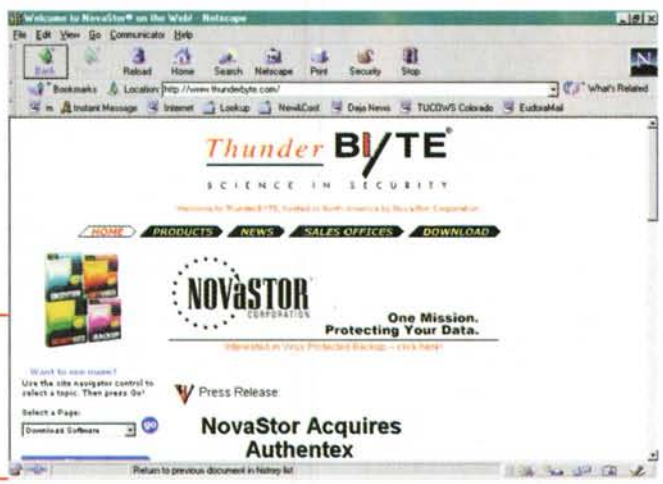
Caratteristiche principali degli antivirus commerciali disponibili

	Dr SolomonÕs Anti-Virus 7.79	Dr SolomonÕs Anti-Virus Toolkit for Windows 95 7.79	eSafe Protect 1.02	F-Prot Professional 3.01	IBM Anti-Virus 3.0.1	InocuLAN AntiVirus 5.0 for Windows 95
Prezzo di listino	**$49.95**	**$125.00**	**$49.00**	**$49.95**	**$49.00**	**$69.00**
Creazione del disco di recupero	Si	Si	Si	Si	Si	Si
Scansione durante l'installazione	Si	Si	Si	No	Si	Si
Scansione dei settori di boot	Si	Si	Si	Si	Si	Si
Creazione di copia del record di boot	No	No	Si	Si	No	Si
Scansione di file compressi	Si	Si	Si	Si	Si	Si
Scansione della memoria	Si	Si	Si	Si	Si	Si
Scansione programmata	No	Si	Si	Si	Si	Si
Scansione dei file al lancio	Si	Si	Si	Si	Si	Si
Scansione in background	Si	Si	Si	Si	Si	Si
Riconoscimento e cancellazione di macrovirus	Si	Si	Si	Si	Si	Si
Risultati dell'analisi su schermo e su report	Si Si	Si Si	Si Si	Si No	Si Si	Si Si
Update diretto da Internet	Si	No	Si	Si	Si	Si
Update automatico	Si	No	Si	Si	No	Si



Panda Antivirus, forse il pacchetto shareware più noto alla piccola utenza. Si tratta di un prodotto affidabile e aggiornato.

Dalla Romania, terra di illustri implementatori di virus, una risorsa per combattere i cattivi; la libreria (14.000 stringhe) però non è proprio al top!



Thunderbyte di Novastor. Aggiornato ai primi di dicembre, la nuova versione gode di significative migliorie, che la mettono al pari dei pacchetti più noti.

macchina e del nostro network: affermazione vera a certe condizioni. Innanzi tutto è consigliabile adottare almeno un paio di prodotti antivirus diversi, questo per compensare eventuali piccole differenze nelle librerie. Ma la cosa più importante è il continuo aggiornamento della libreria stessa, visto che anche il miglior pacchetto antivirus è inutile se non ha i mezzi per riconoscere il suo nemico. Alcuni programmi (es F-Secure) incorporano metodi euristici capaci di individuare attività di virus non ancora conosciuti, ma la loro azione si fermerà qui, visto che non sapranno "estirpare" l'intruso. Perciò, l'unico sistema, che poi non costa quasi nulla, è quello di mantenere aggiornato il file di riferimento dell'antivirus stesso;

✔ un virus può distruggere un computer: falso. Nonostante le ricorrenti notizie riguardo a fatti del genere. non si è ancora a conoscenza di un solo caso di hard disk rovinato o di monitor bruciato da un virus. Il terribile e disastroso CHI, che pur rende inservibile un computer, in pratica cancella solo il BIOS, per cui una nuova riscrittura dello stesso (purtroppo non realizzabile con metodi casalinghi; ecco il motivo della credenza che questo virus distrugga i banchi di memoria) riporta in condizioni normali la macchina, senza alcun vero danno fisico;

McAfee VirusScan 4	Norton AntiVirus 4.0	PC-cillin 3.0	ThunderByte Anti-Virus Utilities 8.03a	Vet Premium Anti-Virus 9.6	ViruSweep 1.0	Datafellows Fsecure 4.0	Command Antivirus (client & server)
$49.00	**$49.95**	**$44.95**	**$99.95**	**$65.00**	**$39.95**	**$ 125,00**	**$ 150,00**
Si	Si	Si	Si	Si	Si	Si	Si
Si	Si	Si	Si	Si	Si	Si	Si
Si	Si	Si	Si	Si	Si	Si	Si
No	Si	Si	Si	Si	Si	Si	Si
Si	Si	Si	Si	No	Si	Si	Si
Si	Si	Si	Si	Si	Si	Si	Si
Si	Si	Si	No	No	Si	Si	Si
Si	Si	Si	Si	Si	Si	Si	Si
Si	Si	Si	Si	Si	Si	Si	Si
Si	Si	Si	Si	Si	Si	Si	Si
Si Si	Si Si	Si Si	Si Si	Si Si	Si Si	Si Si	Si Si
Si	Si	Si	Si	Si	Si	Si	Si
Si	Si	Si	Si	Si	Si	Si	Si

A proposito di qualche virus curioso

Nella non lunga, ma affollatissima storia di questi nemici esiste una casistica d'aneddoti e una cronologia commentata interessante e non priva di spunti divertenti. Ecco quindi qualche descrizione di virus famosi, per un motivo o per un altro, o che si sono dimostrati interessanti per certe loro caratteristiche. La maggior parte delle descrizioni è dovuta a Mikko Hypponen, un big hunter di virus attualmente in forze alla DataFellows, casa che produce l'antivirus presentato sulle pagine della rivista nella sezione "Prove".

✔ Virus Mange-Tout; il nome è francese, e significa onnivoro. E' un virus residente in memoria che deve la sua fama al fatto che, inconsapevolmente, diverse case produttrici che distribuivano alla clientela floppy vuoti preformattati immisero sul mercato grandi quantità di dischetti infetti. Sebbene sia un virus piuttosto vecchio (1995) e ormai ben noto anche nelle sue varianti, è interessante in quanto ben costruito e capace di rimanere criptato in memoria fino al momento dell'azione. Il trigger che lo scatena è l'assenza di digitazione alla tastiera per un'ora; a questo punto il virus viene decifrato attraverso una complessa procedura e attraverso la gestione degli interrupt 08h, 09h and 21h (clock, tastiera and DOS). Il virus infetta allora gli exe contenuti nella directory su cui si è installato, e successivamente, passa alle altre. Curioso il fatto che sia stato segnalato, per la prima volta, in Cina.

✔ Virus Alameda, chiamato altre volte Yale; è interessante perché si tratta forse del più vecchio virus prodotto (data di prima comparsa aprile 1987). Si replicava ogni volta che veniva usata la combinazione Ctrl-Alt-Del. L'interesse termina qui, visto che ha importanza solo storica; è stato scritto probabilmente, utilizzando un assembler A86.

✔ Virus Murphy: sebbene non sia un virus ben progettato, lo nominiamo in quanto si tratta di uno dei pochi di cui si conoscono gli autori, Lubomir Mateev Mateev e Iani Lubomirov Brankov, bulgari. Il virus prende il nome dal messaggio:" Hello, I'm Murphy. Nice to meet you friend. I'm written since Nov/Dec. Copywrite (c)1989 by Lubo & Ian, Sofia, USM Laboratory". Il virus si attiva in maniera del tutto casuale. Se ne conoscono circa trenta varianti diverse.

✔ Virus Suriv 1: origine israeliana. Sconosciuto l'autore. E' importante in quanto si tratta del primo tentativo di virus che poi darà origine al temibile Jerusalem. Il primo aprile il computer infetto mostra il seguente messaggio: " APRIL 1ST HA HA HA YOU HAVE A VIRUS".

✔ Virus CASINO: origine Malta. Virus altamente distruttivo, residente su file .COM. Cancella, tra l'altro, la FAT. Curioso il suo funzionamento: al momento dell'azione il virus invita a partecipare a un gioco; se si vince non accade nulla, altrimenti il danno è fatto.

✔ Virus DotKiller: origine Polonia. E' un virus piuttosto rozzo e primitivo, facile da trovare e distruggere, ma è curioso in quanto il suo unico effetto è quello di cancellare tutti i punti (intesi come segni di interpunzione) dallo schermo.

✔ Virus Eliza: origine sconosciuta. Da citare perché si tratta probabilmente di un virus prodotto da ragazzini inesperti. Non funziona alla perfezione, in quanto cancella file infetti dallo stesso virus e, sovente, cancella lo stesso file unicamente infettato sul disco.

✔ Virus ENET-35: origine Spagna o SudCalifonia. Lo citiamo perché, come quello del vaiolo, è stato definitamente dichiarato estinto, visto che non ne esistono esemplari se non quelli nelle mani dei ricercatori.

✔ Virus Finnish: origine Finlandia. Interessante perché probabilmente è il virus che si propaga con la maggiore velocità conosciuta. Ciononostante non procura alcun danno, tranne che occupare lo spazio libero sul disco. E' facilmente removibile e non colpisce in alcun modo file e programmi.

✔ Virus BombTrack: origine Belgio. Uno dei virus più distruttivi mai conosciuti. Si tratta di un virus polimorfico estremamente complesso, ma che fortunatamente contiene diversi bug che lo rendono facilmente riconoscibile. Su certi tipi di file esercita un'azione invalidante, impedendo la loro esecuzione sebbene il codice non sia stato attaccato.

✔ Virus Goldbug: origine USA. Si tratta di un virus polimorfico mutante altamente distruttivo, che, per una serie di circostanze, a distanza di tanto tempo ancora non chiarite, fu distribuito a un gran numero di persone attraverso una copia pirata di DOOM II. Si tratta di un virus realizzato da esperti, visto che il suo modo di attacco è molto differenziato e specialistico, in base al punto da cui parte l'infezione. Gli specialisti hanno studiato molto bene questo virus, visto che si tratta di un punto di partenza per diverse altre piattaforme di infezione.

✔ Virus Macedonia: origine sconosciuta, ma prevedibile. Non fa null'altro che mostrare, ogni tanto, il messaggio politico "Macedonia to macedonians!". Beh, auguri!

✔ Virus Michelangelo: origine non sicura. Troppo noto per raccontarne. Lo citiamo solo per invitare gli utenti a stare attenti alla data del 6 marzo (anniversario della nascita di Michelangelo Buonarroti, ecco perché!). Beh, se siete stati infettati, avete poche chance di recuperare i file colpiti.

✔ Virus Virogen: origine sconosciuta. Si tratta di un semplice virus che offre il messaggio:(c)1993 VG Enterprises.* Congratulations, You have recieved the privelge of being infected by the * Offspring I v0.05. * . E niente altro! Beh, più educati di così?

E l'elenco potrebbe continuare, come immaginerete, a lungo. Ma non importa. Fate un salto su WWW e potrete vederne di altrettante, egualmente divertenti. Ma mi raccomando, munitevi di un antivirus.

✔ il virus può essere eliminato solo formattando l'HD; errato anche questo! Oggi la disinfezione eseguita attraverso un buon pacchetto garantisce l'eliminazione completa del virus e molto raramente si giunge alla formattazione completa delle memorie di massa;

✔ le infezioni colpiscono solo gli altri: affermazione che si commenta da sé. Nessuno è davvero protetto da un'infezione, se appena può esistere un banalissimo scambio di floppy.

Concludendo

"Lavati bene le mani", raccomandava il mio papà quando si andava a tavola, "e mi raccomando, col sapone!", aggiungeva! Beh, laviamo bene anche i nostri floppy, e, quando navighiamo in Internet, un po' d'attenzione a dove mettiamo i piedi non guasta certo. E, per ogni evento, compriamo un buon antivirus, o almeno scarichiamone qualcuno; come dicevamo nelle puntate precedenti, ce ne sono di commerciali, molto buoni, che applicano il concetto di demo time-limited in maniera molto elastica. Ne possiamo approfittare fino al momento di metterci in regola con i pagamenti. L'unica vera cura sta proprio lì; quindi scegliete fra quelli che vi proponiamo, sperando di non averne dimenticato qualcuno!

Beh, il film è finito, ma le cose non si mettono per niente bene. Il computer dorme ormai un sonno tranquillo da convalescente, ma il fatto è che a me è venuta un'acidità di stomaco che mi pare di aver inghiottito una tanica di cherosene! Che sia stato quel panino leggero che mi sono fatto? O, per l'amor di Dio, a furia di parlare di virus, vuoi vedere che me ne sono beccato uno gastrointestinale?. Quasi quasi, per combattere il male ab imo, mi faccio un altro panino col dischetto delle Norton in mezzo. Chissà!

MC

Dealer o Leader?

MC-link Point. L'offerta Internet da Leader

Se avete il pallino per gli affari c'è un'offerta di connettività ad Internet da proporre ai vostri clienti, che vi farà fare molta strada. Basta diventare MC-link Point. Insieme al kit di installazione che leva ogni preoccupazione di configurazione, potrete offrire ai vostri clienti la serenità di un'assistenza che li segue ovunque. E molte certezze in più. **A partire** dal supporto di un provider nazionale come MC-link, da più di 12 anni al fianco di grandi aziende e piccoli utenti con tecnologie e prodotti avanzati. **Per continuare** con una rete capillare estesa in oltre 110 città in Italia e 1200 nel mondo. **E finire** con un'offerta completa e qualificante che presenta molti punti di forza: Kit di abbonamento bimestrale o annuale; connessione RTC anche in X2 e ISDN; spazi web e domini; connettività Internet e Intranet dedicata per le aziende. **Diventate** anche voi MC-link Point, potrete usufruire di un'agile rapporto commerciale e un completo supporto di merchandising. Contattateci scoprirete che differenza corre tra essere un Dealer e un Leader.

MC-link point

MC-link Point, il punto che fa la differenza.

R.C.P. associati

Per saperne di più telefonate al (06)418921 o inviate una e-mail a: point@mclink.it