I virus di novembre: 855 e gli altri

Non tutti i virus portano con sè un carico distruttivo. Al contrario, una grande maggioranza di essi si limita a riprodursi senza causare altri danni.

I virus dannosi sono alcune decine; di essi la maggior parte poi attende, prima di scatenare i comportamenti distruttivi, il verificarsi di condizioni prestabilite.

Può trattarsi del trascorrere di un particolare intervallo di tempo dall'attivazione, oppure di un determinato numero di avvii del sistema.

Piuttosto frequente è la scelta di una data, che può avere un significato noto soltanto all'autore del virus come fu nel caso del virus «Michelangelo», che si attiva il 6 marzo per circostanze ignote, e che è stato battezzato col nome dell'artista perché per una coincidenza la data di attivazione del virus cade nell'anniversario della sua nascita; oppure un senso più generale, come nel caso di quei virus che si attivano di venerdì 13 (o di sabato 14 o giovedì 12, a seconda del senso di umorismo bacato dei rispettivi autori).

Il diffondersi di questa stupida abitudine ha portato al formarsi di un vero e proprio calendario dei virus.

Quasi in tutti i mesi è presente una data in cui l'uno o l'altro virus si scatena, e senza voler rifare degli allarmismi catastrofici come purtroppo hanno fatto i mezzi di informazione in occasione del 13 ottobre 1989 e del 6 marzo 1992 crediamo comunque utile cominciare a segnalare ai nostri lettori, mese dopo mese, quali sono le date «a rischio», insieme a poche, semplici istruzioni su come fare per evitare che il rischio si tramuti in un danno.

Il calendario di novembre e l'855

Nel mese di novembre è prevista l'attivazione dei seguenti virus:

Diskjeb (nei mesi di *ottobre, novembre* e *dicembre* intercetta le scritture sul disco e le corrompe);

Flower (l'*11 novembre* ricopre il programma infetto con un cavallo di Troia);

Hungarian-482 (il *7 novembre* scrive sul video la parola «Format...» e quindi procede alla formattazione del disco fisso);

Jerusalem Nov. 30 (come il normale Jerusalem ma si attiva il *30 novembre*);

Jerusalem Timor (id., ma per il *12 novembre*);

Kennedy (il *18* e *22 novembre* scrive sul video un messaggio in lingua svedese);

Maltese Amoeba (il *1 novembre* ricopre il contenuto del disco fisso).

Ma il virus contro il quale riteniamo di mettere in guardia i nostri lettori è soprattutto il «**Nov. 17**», noto anche come **855**. Come indicato dal nome, questo virus si attiva il 17 novembre; per la precisione si attiva in qualsiasi data compresa tra il *17* e il *30 novembre* inclusi.

Una volta attivato resta in attesa che l'utente abbia premuto 500 tasti (ad es. durante la scrittura di un testo), e quindi si scatena: identifica il disco attivo, e lo ricopre con dati a caso nei primi 8 settori. Nel caso di un disco fisso ciò comporterà la distruzione del boot sector e di una buona parte della File Allocation Table. Il contenuto del disco sarà probabilmente recuperabile, ma al prezzo di un lavoro specialistico che non è alla portata di tutti. Riteniamo di allertare i lettori, come abbiamo detto, per la semplice ragione che mentre questo articolo viene scritto stiamo assistendo a una vera e propria epidemia di questo virus. Un collaboratore della rivista ci ha fatto sapere di esserselo ritrovato per ogni dove.

Un'altra azienda con cui abbiamo rapporti ce lo ha segnalato. Ce ne sono state inviate almeno tre-quattro copie tramite MC-link. Noi stessi siamo riusciti a evitare che ci infettasse la rete. E non va dimenticato, comunque, che nel VSUM di Patricia Hoffman l'855 è riportato come «ampiamente diffuso a Roma nel dicembre 1991».

Come difendersi

È senz'altro più semplice e facile prevenire questo rischio che curarne gli effetti. In questo caso i virus che abbiamo elencato sono tutti noti e riconosciuti da tutti i programmi antivirus più diffusi. Ecco una semplice procedura di controllo:

— avviare il PC con il disco originale del DOS protetto contro la scrittura e preparare un dischetto di sistema;

— trasferire su questo dischetto una copia del programma antivirus che si usa comunemente, prelevandolo dall'originale che dovrà anch'esso rimanere protetto;

— proteggere il dischetto così ottenuto e utilizzarlo per i controlli;

— il giorno precedente la data di attivazione di ciascuno dei virus elencati inserire nel computer il dischetto protetto contro la scrittura, accendere il computer e attendere che si sia avviato; quindi eseguire il programma di ricerca e identificazione di virus.

Se la ricerca dovesse dare esiti positivi per qualsiasi virus, si dovrà annotare (o meglio stampare) le indicazioni fornite dal programma, spegnere il computer e assicurare che non venga acceso da nessuno, ad esempio rimuovendo il cordone di alimentazione e coprendo il foro per l'inserimento del cordone con del nastro adesivo, finché non si sarà predisposta la procedura di eliminazione dell'infezione, eventualmente avvalendosi della collaborazione di un consulente.

Stefano Toria

Pro-memoria

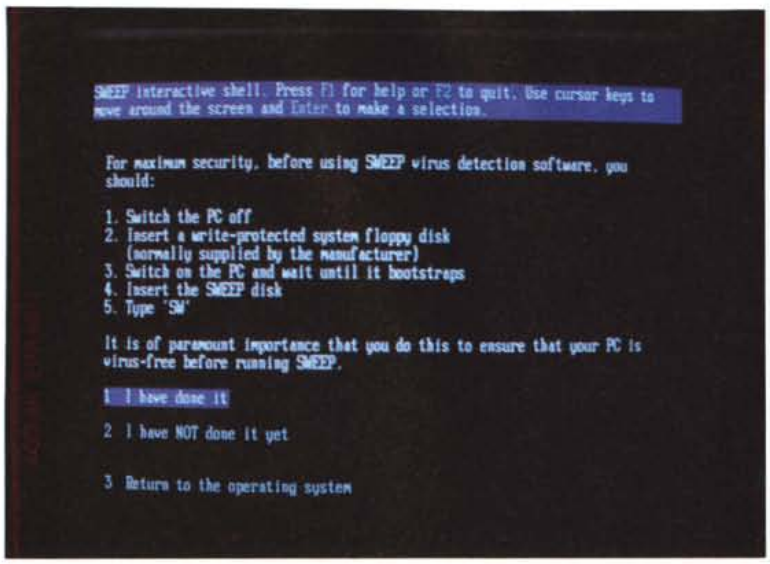
Le informazioni in questa pagina sono destinate a tutti i lettori in possesso di un personal computer Ms-Dos. Esperti o principianti, tutti sono esposti al rischio.

Vi ricordiamo che i più diffusi programmi shareware antivirus sono reperibili su MC-link: F-PROT (FP-205.ZIP), ViruScan (SCAN97.ZIP) e VIRex (VIRX25.ZIP) possono essere tranquillamente prelevati via modem dagli abbonati a MC-link, oppure su altri sistemi telematici.

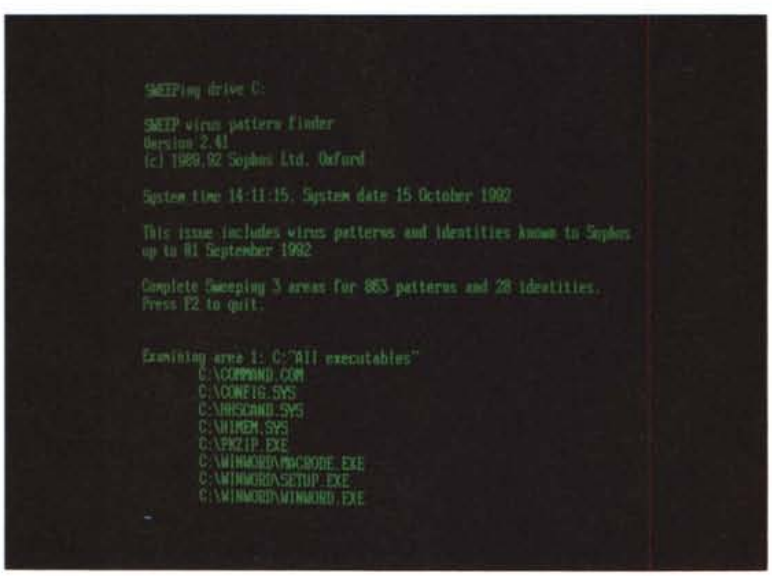
Per chi preferisca un programma commerciale possiamo raccomandare lo stesso Sweep, di cui in questo numero pubblichiamo la recensione, oppure il Dr. Solomon's AntiVirus Toolkit, del quale abbiamo parlato alcuni mesi fa.

Tenete comunque presente che i programmi di ricerca e identificazione di virus debbono essere mantenuti aggiornati, come ben sanno i lettori che seguono regolarmente questa rubrica; non si può pensare di acquistare oggi un prodotto e continuare a utilizzarlo per sempre senza aggiornarlo.

Ci impegneremo a mantenere aggiornati i lettori di MCmicrocomputer mese per mese.



Lo Shell interattivo SW.EXE chiede all'utente se sta seguendo la procedura corretta.



Sweep in cerca di virus...

da 3.5" manca dello sportellino per chiudere il foro di protezione.

È una piccola attenzione da parte del produttore, ma piuttosto significativa; come abbiamo già detto in occasione della presentazione di un altro prodotto resta ovviamente possibile scrivere sui dischi intagliando la tacca sul 5.25" o chiudendo con del nastro il foro del 3.5", ma ci auguriamo che nessuno sia così sciocco.

I dischetti contengono soltanto quattro file: il programma SWEEP.EXE, uno shell interattivo SW.EXE, un lungo testo descrittivo con le caratteristiche dei virus conosciuti VIRPATS.LST e le Sophos Utilities, un programma di utilità per funzioni ausiliarie sui dischi, SU.EXE.

Il manuale è breve, quasi telegrafico, ma non fa rimpiangere volumi più corposi: in 78 pagine c'è tutto quello che occorre, dalla preparazione alla descrizione delle funzioni del sistema. Sfogliando le prime pagine del manuale e avviando SW ci si accorge che alla Sophos hanno le idee ben chiare su come si fa la protezione antivirus, e hanno cercato di guidare anche l'utente più inesperto nel compiere i passi fondamentali. Già nella prima pagina del testo infatti l'utente apprende che il controllo della presenza dei virus richiede un dischetto di sistema protetto contro la scrittura. Anzi, il controllo della presenza dei virus *conosciuti:* chi ha scritto il manuale ci tiene a non generare equivoci sulle effettive possibilità del programma.

La prima schermata che compare all'avvio del programma è ancora più esplicita: prima di avviare il programma bisogna spegnere il computer, inserire un dischetto di sistema protetto dalla scrittura, accendere il computer, attendere che abbia completato il bootstrap, inserire quindi il dischetto di Sweep e dare nuovamente il comando SW. L'utente è invitato a controllare di aver eseguito questi passi ed eventualmente a tornare indietro per eseguirli.

A caccia di virus

Una volta rispettate le procedure di sicurezza si può entrare nel cuore del programma. Si è detto che SW è uno shell interattivo; in realtà il programma che svolge le funzioni di controllo è SWEEP.EXE, che viene richiamato da SW con gli opportuni switch per lo svolgimento delle diverse funzioni.

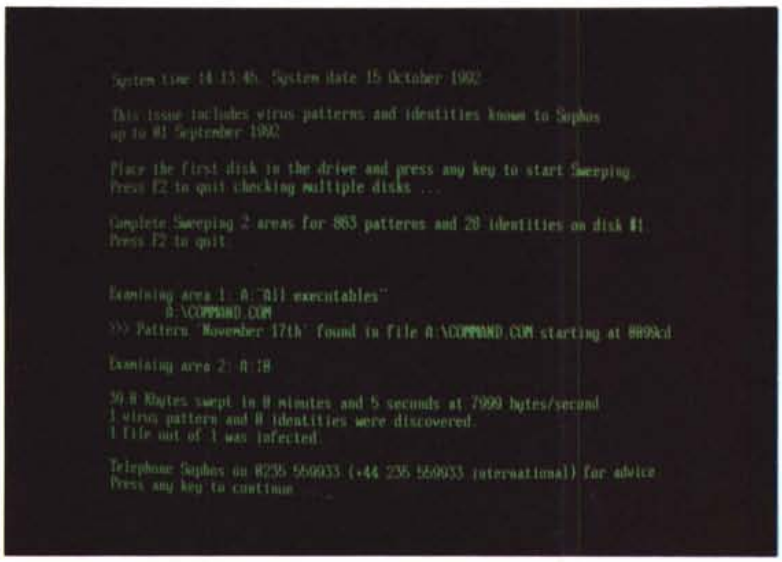
Tre comandi separati consentono di passare al setaccio tutti gli hard disk installati sul proprio elaboratore, oppure uno o più dischetti, o infine tutti i drive di rete che risultano presenti all'atto della esecuzione.

La scansione e la ricerca di virus di per sé non presenta novità sostanziali rispetto alle analoghe funzioni di altri programmi. È rapida e affidabile, e ha identificato tutti i virus del nostro test set in poco più di tre minuti.

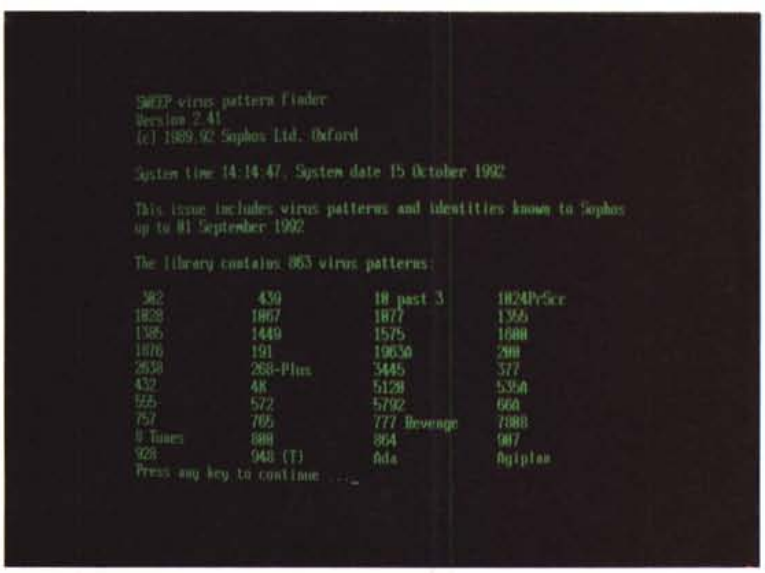
Lo shell che gestisce Sweep consente la scelta di una serie di caratteristiche che determineranno le modalità di esecuzione della ricerca. In particolare esistono due diversi modi di scansione, denominati «Quick» e «Complete». La scansione rapida, adottata ormai da molti programmi per via dell'enorme quantitativo di virus oggi in circolazione, permette di limitare la ricerca di ciascun virus a quella zona dove ci si aspetta di trovare quel dato virus. In termini di sicurezza la procedura è accettabile, e può essere adottata con successo da quegli utenti che hanno fretta ma che non vogliono rinunciare ai controlli. Chi invece abbia requisiti di sicurezza ad alto livello dovrà per contro optare per una scansione completa.

L'utente può richiedere a Sweep la generazione di un rapporto, che può essere rigenerato ex novo di volta in volta oppure incrementato, per mantenere la storia dei controlli effettuati su ciascun computer e risalire — qualora se ne presenti la necessità — alle origini di un problema che si dovesse riscontrare successivamente.

È interessante notare come Sweep non offra alcuna funzione di rimozione



... trovato!



L'elenco dei virus noti a questa versione di Sweep.

dei virus dai programmi infetti. Tale funzione infatti è ritenuta controproducente dalla Sophos; questa opinione ci è stata confermata personalmente dal dr. Jan Hruska, direttore tecnico della Sophos, che abbiamo incontrato a Roma lo scorso maggio in occasione di un convegno. L'unico modo veramente affidabile per rimuovere un virus consiste nel rimuovere il programma che lo contiene e installare nuovamente la versione originale del programma stesso. Chi segue questa rubrica da qualche tempo potrà rendersi conto quanto siamo d'accordo con questa impostazione.

La rimozione dei programmi infetti può limitarsi alla semplice cancellazione (come fa ERASE); se lo desidera, l'utente può richiedere la sovrapposizione di dati non significativi sulle informazioni che costituivano il file, per evitarne ad es. il recupero da parte di dipendenti «smanettoni».

È interessante e utile la possibilità offerta da SW di generare un batch file per l'avvio di Sweep con i parametri scelti, per non dover ogni volta passare per lo shell e richiedere nuovamente le stesse funzioni.

Altre funzioni del programma hanno scopo informativo: la lista dei virus conosciuti dalla versione corrente del programma, e l'elenco delle aree del computer che verranno sottoposte a ricerca e identificazione di virus.

Il manuale

Normalmente nella recensione di un programma il manuale viene quasi dato per scontato. Non è così nel caso di Sweep, il cui manuale è uno strumento prezioso complementare al programma stesso. Si divide in quattro sezioni: la prima dedicata all'avvio rapido, la seconda contenente la descrizione dettagliata delle singole funzioni di Sweep; segue un capitolo su come trattare le infezioni e la descrizione delle Sophos Utilities.

Il comportamento da tenere in caso di infezione viene trattato in modo sintetico ma senza tralasciare alcuna informazione indispensabile. I passi descritti possono essere tranquillamente seguiti da qualsiasi utente, anche inesperto.

L'autore del manuale tende da un lato a rassicurare l'utente che dovesse essere vittima di un'infezione, dall'altro a suggerire una serie di norme pratiche per fronteggiare l'emergenza e ridurne al minimo gli effetti: limitare o escludere gli accessi alla rete, impedire lo scambio di dischetti, proteggere fisicamente tutti i supporti attivando il meccanismo di protezione dalla scrittura, procedere alla eliminazione del virus e alla neutralizzazione degli effetti della sua eventuale attivazione.

L'utente viene avvisato della possibilità di una reinfezione successiva alla disinfezione, e vengono fornite altre indicazioni di corredo, tra cui la necessità (per i soli cittadini britannici) di informare il *Computer Crime Unit* di New Scotland Yard. La normativa britannica infatti, come abbiamo accennato nello scorso numero in occasione del convegno del Virus Bulletin, considera esplicitamente reato la creazione e la diffusione di virus.

Prezzi e politica commerciale

Sweep non è esattamente un prodotto economico. I prezzi riportati dal listino, e confermati dall'importatore italiano, sono di diversi ordini di grandezza superiori rispetto a prodotti analoghi che abbiamo esaminato in passato.

Un listino di questo genere si giustifica considerando la natura del prodotto, che si rivolge alle aziende e alle organizzazioni di grandi dimensioni, piuttosto che al privato o al piccolo professionista.

In Italia Sweep viene utilizzato da aziende dei settori finanziario e industriale e nella pubblica amministrazione. Peraltro i prezzi di listino hanno valore di puro riferimento, e la casa madre lascia ampio spazio ai rappresentanti nella determinazione delle condizioni economiche.

Può accadere quindi, come è accaduto in contesti del tutto particolari in Italia, che un'azienda acquisti a prezzo pieno di

Le prove dei prodotti antivirus vengono effettuate in redazione su un PC Unibit 286 a 12 MHz con 640 Kb di RAM, scheda Hercules e video monocromatico, disk controller St-506, disco fisso Seagate da 60 Mb e drive per floppy da 3,5" 1.44 Mb.

Sul disco fisso sono installati i seguenti virus (il numero tra parentesi indica il numero di campioni differenti per i virus di cui sono presenti più copie e/o varianti):

512, 855, 1244, 1381, 1554, 4096, AIDS, AIDS-II, Alabama, Ambulance, Amoeba (2), Anarkia, Anthrax, Anti-Pascal (2), Anti-Pascal II (3), Attention, Bebe, Burger (3), Cascade, Crash, Dark Avenger (2), Darth Vader (3), Datacrime (2), Datacrime-2, Destructor, Devil's Dance, Fish 6, Flip, Fu Manchm, Icelandic (2), Invader, Jerusalem, JoJo, JoJo-2, June 16 th, JW2, Kennedy, Leprosy, Liberty, Lisbon (2), Lozinsky, Murphy, Nomenklatura, Ontario, Oropax, Plague, Pogue, Polish 529, Saturday 14th, September 18th, Smack, Stupid, Suomi, Suriv-A, Sverdlov, Taiwan (3), Taiwan-3, Traceback, Typo-712, USSR-600, V801 (2), Victor, Violator, Old Yankee Doodle.

La collezione sperimentale di MCmicrocomputer, utilizzata per questa prova, contiene inoltre tre virus da boot sector: Stoned, Ping-Pong e Michelangelo.

listino una licenza d'uso del programma ricevendo l'autorizzazione a riprodurre il programma stesso in tante copie quante ne sono necessarie all'interno dell'azienda, senza che sia richiesto il pagamento di ulteriori registrazioni.

Se a questa particolarissima politica di site licensing si unisce la grande capacità e la disponibilità dello staff tecnico della casa madre, a disposizione 24 ore al giorno per fornire consulenza telefonica su qualsiasi genere di problema con i virus, diviene del tutto accettabile e anzi conveniente quello che all'apparenza è un prezzo esorbitante. MC

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

Computer Viruses and Anti-Virus Warfare

Scrivere libri sui virus è di moda, negli ultimi tempi.

Molti autori più o meno noti si sono dedicati a questa attività, sicuramente redditizia; alcuni di essi avevano cose molto interessanti da dire, altri meno, ma tutti hanno trovato il loro posto nel mercato, affamato di notizie, curiosità e sensazioni su uno degli argomenti scottanti del momento.

L'autore del libro che presentiamo questo mese è Jan Hruska, di cui abbiamo parlato nel corpo dell'articolo. Direttore tecnico della Sophos Ltd., esperto di sicurezza informatica e consulente a tempo pieno, Hruska è una figura di primo piano nella ricerca e nella lotta contro i virus.

Il volume, di cui è uscita nel mese di settembre la seconda edizione, è molto ben curato; chiaro, preciso e semplice fornisce una serie di informazioni utili sia a chi voglia approfondire particolari aspetti del fenomeno virus sia a chi per la prima volta si avvicina al problema, per necessità o curiosità.

Molto apprezzabile è il fatto che l'autore non si abbandona mai al sensazionalismo, a quel desiderio di *épater le bourgeois* di dubbio gusto che si ritrova in altri testi. I virus sono un problema, d'accordo; ma i programmi che possono arrecare danno ai dati non sono sempre e soltanto virus (e comunque, aggiungeremmo noi, fa più danno un notebook che cade malamente per terra).

Particolare attenzione viene dedicata alla illustrazione del meccanismo di propagazione dei virus; la precisione tecnica non cede mai il passo alla chiarezza espositiva, e concetti intrinsecamente complessi come la distinzione tra un virus attivo in RAM e un supporto infetto, oppure la classificazione di virus (parassiti, da boot sector, multipartiti) vengono affrontati tranquillamente in modo accessibile e comprensibile.

Anche la struttura interna dei virus viene descritta facendo uso di semplici concetti ed esempi, segnalando dove opportuno quali sono i comportamenti a rischio che possono determinare la trasmissione dell'infezione da questo o quel tipo di virus.

Un intero capitolo è dedicato all'analisi e alla smentita di voci fatte circolare da persone poco esperte o deliberatamente disinformative.

Segue una lunga e dettagliata analisi delle procedure di difesa e recupero dalle infezioni; Hruska copre in dettaglio tutte le fasi della protezione dai virus, dalle attività preliminari e preparatorie (una sana politica di copia di sicurezza, la preparazione di un dischetto di sistema protetto contro la scrittura, la definizione di un piano di emergenza) alla prevenzione attiva, fino al recupero dei programmi infetti e al trattamento degli eventuali danni causati dai virus.

Sono quindi brevemente descritte le diverse tipologie di programmi antivirus, con le indicazioni per l'utente che deve scegliere quale acquistare; l'ultimo capitolo fornisce informazioni dettagliate sulle particolarità del comportamento dei virus nelle reti, e sugli appositi strumenti per difendersene in un contesto distribuito.

Il testo si conclude con delle appendici di natura tecnica, di cui la più lunga (oltre 70 pagine) riporta una breve descrizione e l'impronta identificativa di tutti i virus conosciuti alla data di pubblicazione del testo.

Si tratta di un volume la cui lettura è senz'altro suggerita a chi sia interessato a una sintesi dei fatti e delle procedure riguardanti i virus, senza rinunciare alla chiarezza e alla completezza.

Dr. Jan Hruska
Computer Viruses and Anti-Virus Warfare
(Second Revised Edition)
Ellis Horwood Ltd., 1992
ISBN 0-13-036377-4

LA MOSTRA

OLTRE ALLE PIÙ PRESTIGIOSE AZIENDE ITALIANE, CONSIDEREVOLE PRESENZA DI CASE STRANIERE CHE PRESENTANO UNA PANORAMICA COMPLETA DELLE SOLUZIONI PIÙ INNOVATIVE NEI SETTORI: **HARDWARE, SOFTWARE, TELEMATICA E TELECOMUNICAZIONI, SERVIZI DI INFORMATICA E DI ASSISTENZA TECNICA, ATTREZZATURE PER L'UFFICIO, ARREDAMENTO, CARTOTECNICA.**

I CONVEGNI

"L'OSSERVATORIO DI ROMAUFFICIO" UN MOMENTO D'INCONTRO SU TEMI DI PARTICOLARE INTERESSE ED ATTUALITÀ CONFRONTATI CON ESPERIENZE DIRETTE DI OPERATORI ED UTENTI QUALIFICATI.

con il patrocinio
della Regione Lazio
Assessorato Industria
Commercio e Artigianato

15ª MOSTRA CONVEGNO
DELLE TECNOLOGIE
E DELLE SOLUZIONI
PER L'AZIENDA

6-10 MARZO
FIERA DI ROMA
ORE 9.30-19.00

PROMOSSA DALL'ISTITUTO MIDES
INFORMAZIONI: TEL. 06/6875575

ROMAUFFICIO '93

IL NOCCIOLO DELLA SOLUZIONE