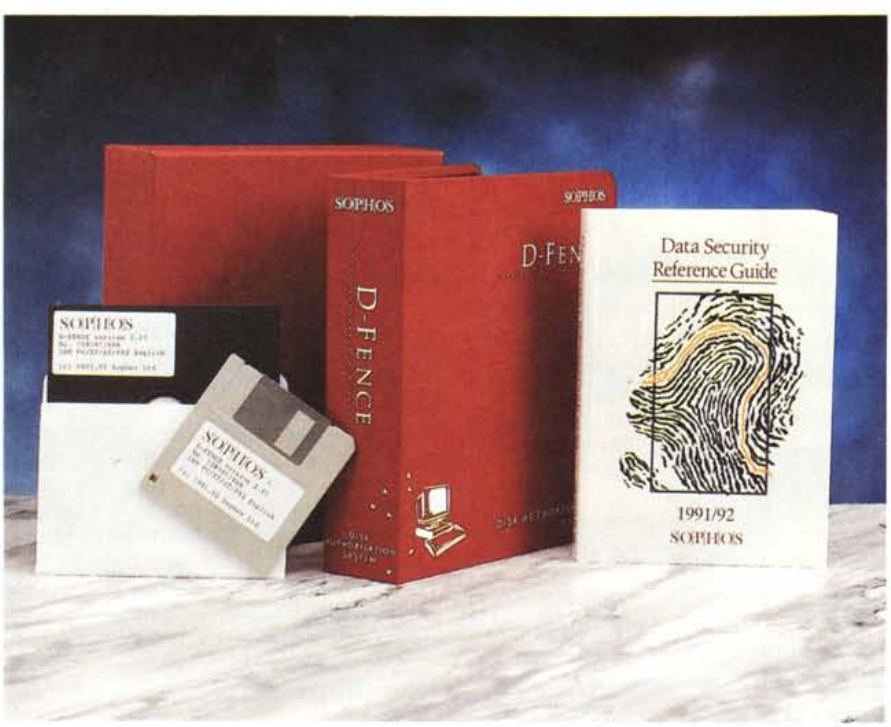
D-Fence

di Stefano Toria

Abbiamo intestato la rubrica di questo mese a un prodotto non specificamente progettato per la difesa dai virus ma genericamente destinato a proteggere il patrimonio informativo dell'azienda dalle interferenze dovute a programmi non autorizzati.
Negli articoli che formano questa rubrica in realtà andiamo al di là dell'esame di un prodotto: nel mese di novembre infatti abbiamo preso parte a una conferenza dedicata ai virus, e ne diamo il resoconto in un apposito riquadro; nel corso della stessa conferenza abbiamo avuto modo di intervistare John McAfee; infine, «a grande richiesta» come si legge nei cartelloni dei circhi, diamo uno sguardo al di fuori del mondo Ms-Dos per vedere che genere di problema costituiscano i virus per chi possiede un Macintosh

Sfatato il mito secondo cui i principali responsabili della diffusione dei virus sarebbero i sistemi telematici, e che la sola presenza di un modem in un PC costituirebbe un rischio, rimane la realtà: ciò che determina la circolazione dei virus è lo scambio di dischetti. Questa realtà è confermata da tutte le indagini statistiche che sono state effettuate nel mondo, non ultima una ricerca condotta da SecurityNet, della quale parliamo nel riquadro dedicato a una conferenza svoltasi lo scorso 6 novembre.

Qual è allora la prima norma di sicurezza? Controllare lo scambio di dischetti, ovviamente. E proprio al controllo dello scambio di dischetti è destinato il prodotto che esaminiamo questo mese. Non è un programma direttamente volto a identificare e eliminare i virus, ma costituisce in un certo senso una misura a monte: D-Fence, quando installato correttamente su tutti i PC dell'azienda, impedisce fisicamente l'uso di dischetti estranei. Il nome del prodotto di per sé è un gioco di parole molto significativo: in inglese si pronuncia allo stesso modo della parola «defense», che significa «difesa», ma «fence» significa anche «steccato, recinzione», e in effetti l'uso di D-Fence in un'azienda crea una sorta di steccato, all'interno del quale possono circolare esclusivamente dischetti opportunamente certificati e predisposti, e ogni scambio con l'esterno è sottoposto al controllo di un sistema-cancello. Nessun dischetto certificato per l'uso interno è leggibile al di fuori, e nessun dischetto non certificato può essere letto all'interno.



Come funziona

Il principio di funzionamento di D-Fence è relativamente semplice: quando viene installato sul disco fisso D-Fence modifica il primo settore fisico del disco, che come noto contiene il master boot record e la tavola delle partizioni. Il contenuto del settore viene trasferito altrove e la tavola delle partizioni viene codificata; il boot record viene quindi sostituito da un diverso programma, che costituisce la base del sistema D-Fence.

D-Fence si avvale di una tecnica molto simile a quella utilizzata da una particolare categoria di virus, in quanto alla richiesta di esaminare il primo settore fisico del disco viene presentata l'immagine di quello che il settore dovrebbe essere e non l'effettivo contenuto del disco. Peraltro la serietà della ditta produttrice e la disponibilità di documentazione garantiscono l'assoluta sicurezza di questa procedura, in tutti i sensi:

D-FENCE

Sophos Ltd., 21 The Quadrant, Abingdon Science Park, Abingdon, Oxon OX14 3YS, Gran Bretagna. Tel. (0044 235) 559933. Fax (0044 235) 559935.
Rappresentante esclusivo per l'Italia:
TELVOX Teleinformatica sas, Via F.lli Cairoli 4-6, 40121 Bologna. Tel. (051) 252784. Fax (051) 252748.
Prezzi di listino:

Singola licenza	*L. 48.000*
Quantitativo minimo ordinabile n. 10 licenze	*L. 480.000*

infatti se si cerca di scavalcare la protezione avviando il PC da un normale dischetto di sistema ci si ritrova con un disco C del tutto illeggibile.

Analogamente agisce D-Fence sui dischetti: questi ultimi mancano del master boot record, ma la installazione di D-Fence sul dischetto dà luogo alla codifica della root directory e della FAT (file allocation table); in mancanza della chiave di decodifica di queste due aree vitali del dischetto, esso non è utilizzabile in modo normale.

Come si usa

D-Fence arriva su due dischetti, uno da 5,25" e l'altro da 3,5". Come già abbiamo avuto occasione di vedere in altre occasioni, i dischetti sono permanentemente protetti contro la scrittura.

La installazione di D-Fence è semplicissima: basta inserire il dischetto del programma e lanciare il programma DFENCE dal dischetto. L'utente potrà scegliere tra cinque opzioni: installazione e disinstallazione di D-Fence su un PC, installazione e disinstallazione su un dischetto (cioè certificazione per uso interno e liberazione per l'uso esterno),

I virus del Macintosh

Questa rubrica esiste ormai da due anni. Da un mese all'altro abbiamo cercato di fornire ai lettori una serie di informazioni sulla struttura dei virus, sul modo di combatterli e su quanto accade nel mondo. E quasi sempre i riferimenti concreti che abbiamo fatto sono stati presi dal mondo Ms-Dos. Esiste una duplice ragione per questa scelta: innanzitutto i virus per Ms-Dos sono molti di più di quelli scritti per il Macintosh; in secondo luogo la lotta ai virus su ques'ultima piattaforma è resa molto più agevole dalla struttura del sistema. Il problema dei virus in ambiente Macintosh è quindi molto meno preoccupante di quanto non lo sia per i possessori di computer Ms-Dos.

Ma rimane comunque un problema. Vediamo di delineare brevemente gli aspetti principali dei virus per Macintosh.

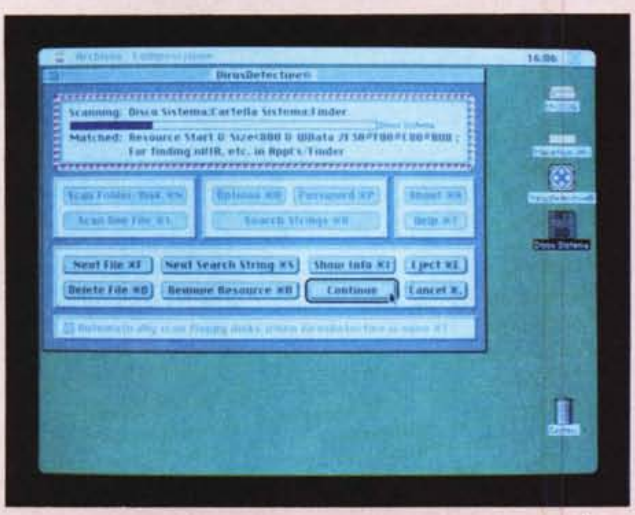
Innanzitutto sul Mac le tipologie dei virus differiscono rispetto a quelle per il Dos: non esistono virus di boot sector e virus parassiti; la struttura dei dischi e dei file eseguibili sul Mac è completamente diversa rispetto a quella del Dos, e un eseguibile per Mac è un oggetto complesso suddiviso in più parti dette «risorse». Quasi sempre un virus sul Mac aggiungerà una risorsa al file a cui si attacca, scegliendone un tipo che venga eseguito prima del codice centrale dell'applicazione. In questo modo il meccanismo di infezione è per così dire garantito dal sistema operativo: quando l'applicazione viene caricata verrà eseguito per primo il virus, il quale ovviamente per prima cosa farà una copia di se stesso dentro un altro eseguibile, e la trasmissione dell'infezione è assicurata.

L'operazione di formattazione di un dischetto determina la scrittura sul disco stesso del cosiddetto «desktop», una struttura che mantiene traccia della forma, dimensione e posizione della finestra del disco sulla scrivania del Mac. Il desktop viene «eseguito» ogni volta che il dischetto viene inserito nel drive, in quanto contiene parti di codice che gestiscono l'apertura e il posizionamento della finestra. Questo codice è quasi sempre il veicolo principale scelto dai virus per trasmettersi, dato che sono pochi gli utenti Macintosh che sono a conoscenza di questa particolarità e pertanto nessuno fino a poco tempo fa considerava pericoloso il semplice inserimento di un disco nel drive. L'operazione più semplice e frequente diventava quindi la più pericolosa. Tuttavia l'apertura del desktop e l'esecuzione del codice in esso contenuto sono operazioni facili da intercettare, e qualsiasi programma antivirus è in grado di controllare un dischetto quando viene inserito e prima che il suo desktop venga eseguito, bloccando l'operazione se il desktop risulta infetto.

Ma il maggior punto di forza del Mac sta nella complessità della sua struttura. Stealth, tunneling, companion, termini tristemente noti a chi si occupa di virus per Ms-Dos, sono pressoché sconosciuti nel Mac. Mettere le mani nel sistema è un'operazione relativamente semplice per chi conosca un minimo la struttura del Dos; sul Mac è un'operazione rischiosa, riservata a chi abbia una grande esperienza del sistema, e non è detto che si possa uscire indenni dal manomettere le variabili interne che controllano il funzionamento del Macintosh. Sono quindi ben poche le tecniche a disposizione degli autori di virus, ed è comprensibile che i virus conosciuti in ambiente Mac siano a tutt'oggi meno di quaranta, contro i circa millecinquecento del Dos.

Per concludere questo quadro idilliaco va aggiunto il fatto che, a differenza di quanto avviene nel mondo Dos dove i battibecchi tra ricercatori sono all'ordine del giorno, i ricercatori antivirus per il Mac sono una comunità ristretta e compatta, in cui collaborazione e scambio di informazioni sono concetti fondamentali da sempre. Ogni volta che esce un nuovo virus lo scopritore lo passa a tutti i colleghi ricercatori, ci si scambiano rapidamente le informazioni sul disassemblaggio, e in breve tempo si giunge ad avere disponibili le nuove versioni dei prodotti antivirus.

st



Il virus «nVIR» identificato da Virus Detective e da Disinfectant.

o applicazione di D-Fence su device driver particolari, ad es. per dischi SCSI o esterni.

Inoltre è possibile adottare un particolare codice di identificazione, che renda impossibile all'interno del gruppo l'uso di dischetti anche certificati da D-Fence ma nell'ambito di un diverso gruppo di utenza.

Una volta installato, D-Fence è completamente trasparente all'utente per l'uso quotidiano del computer. L'utilizzo di dischetti esterni al gruppo dà luogo a un «Errore generale», mentre non ci è stato possibile determinare alcun con-

Intervista a John McAfee

Nato in Gran Bretagna ma residente in California, laureato in matematica, John D. McAfee è indubbiamente il primo personaggio che viene in mente quando si parla di virus. Si deve a lui il primo prodotto di ampia diffusione per la lotta ai virus in ambiente Ms-Dos.

Carismatico e controverso, sicuro di sé e delle proprie opinioni anche quando vanno (in tutto o in parte) controcorrente, McAfee ha fondato e dirige un'azienda — la McAfee Associates — praticamente quasi monoprodotto: i programmi della serie VIRUSCAN sono stati venduti in oltre sei milioni di esemplari nel mondo, e si calcola che più del doppio siano le copie effettivamente in circolazione.

Abbiamo intervistato John McAfee nel corso della «1992 Computer Virus Solutions Conference», che per la prima volta ha portato ufficialmente nel nostro paese l'inventore della scansione antivirus.

* * *

***L'**accusa principale che viene fatta a VIRUSCAN riguarda una presunta minore acuratezza nella identificazione dei virus, da cui deriverebbe una minore affidabilità nella funzione di rimozione dei virus. Cosa risponde a questa affermazione?*

Direi che si sta verificando una transizione nel mondo dei virus: stiamo assistendo al passaggio dall'azione specifica contro particolari ceppi virali a un'azione generalizzata di classificazione di virus. Mi spiegherò con un esempio: la medicina conosce oltre 3.000 virus capaci di determinare il comune raffreddore, eppure se vado da un medico per farmi curare questi non cercherà di identificare con certezza quale di questi virus è responsabile del mio raffreddore: farà la sua diagnosi in base ai sintomi e poi mi dirà di prendere il dato farmaco, di bere molti liquidi, stare al caldo e riposare. Riportando l'esempio al nostro settore dovremo fare qualcosa di analogo, perché al momento i virus in ambiente Ms-Dos sono soltanto 1.400 ma il numero cresce in progressione geometrica: tra due anni ne avremo 25.000 e fra tre anni 100.000; allora sarà impossibile identificare ciascuno dei centomila diversi ceppi. E quand'anche fosse possibile sarebbe un'informazione inutile.

***M**olti ricercatori e professionisti della sicurezza concordano sul fatto che la rimozione dei virus dai programmi eseguibili non sia una pratica affidabile, e che piuttosto è preferibile reinstallare i programmi infetti.*

Qual è la sua opinione?

Non sono assolutamente d'accordo. Secondo me la comunità di ricerca si sta dividendo tra ricercatori puri e ricercatori applicati. Ora i ricercatori puri diranno che certo, è molto meglio reinstallare perché si ha la certezza del 100%. Ma non è fattibile in pratica. Prendiamo ad esempio un caso che ci è capitato, di una grande azienda del sud-est (degli USA, NdR) che è stata colpita da un virus molto semplice sui propri 2.000 computer, nei quali sono risultati infetti oltre 50.000 programmi. Se avessimo pensato di reinstallare quei 50.000 programmi avremmo speso decine di milioni di dollari. Abbiamo scelto per contro di rimuovere i virus, con un risultato positivo nel 99,5% dei casi. È stato molto meglio dover reinstallare 1/200 delle applicazioni infette che doverle reinstallare tutte.

In secondo luogo la maggior parte dei virus possono essere rimossi con un'affidabilità pari al 100%. Senz'altro i virus parassiti (quelli che infettano i file eseguibili, NdR) sono i più facili da rimuovere.

***N**on sempre.*

Ovviamente dipende dal virus e dal meccanismo di rimozione che viene utilizzato. Ma i nostri clienti sono esclusivamente aziende, e nella pratica quotidiana in azienda la rimozione è l'unica possibilità. Nel caso di utenti individuali forse i ricercatori hanno ragione, se si hanno venticinque programmi infetti è meglio reinstallarli. Ma sui grandi numeri non è pensabile.

Inoltre molti prodotti antivirus offrono una funzione generica di disinfezione che richiede una installazione preventiva e successivamente consente di rimuovere qualsiasi virus. SCAN ad esempio ha le funzioni /AF e /AG, che raccolgono informazioni finalizzate alla rimozione di eventuali successive infezioni. Il vantaggio consiste nel fatto che al momento della installazione si sa perfettamente com'è fatto il file integro, e in seguito è facile ripristinarlo al suo stato primitivo.

Se pensiamo di lasciar perdere la disinfezione possiamo anche arrenderci ai virus perché passeremmo il 100% del nostro tempo a reinstallare i programmi infetti.

***V**i sono però alcuni virus, mi viene in mente ad esempio il Voronezh, che infettano in modo sporco. E non è possibile ripristinare gli eseguibili allo stato precedente l'infezione.*

Èun po' vero, ma fortunatamente questi virus tendono ad avere poca diffusione. Se un virus per infettare un programma lo distrugge, rendendone impossibile il ripristino, è altamente probabile che l'utente stesso si accorga ben presto che qualcosa non va e il virus viene identificato in tempi molto brevi. Voronezh è un buon esempio: non si diffonde molto rapidamente, e non c'è motivo di preoccuparsene. Il problema più grande sono i virus che infettano in modo «pulito», perché possono sfuggire all'attenzione dell'utente. Se un virus infetta in modo sporco non avrà vita molto lunga. Certo, i teorici diranno che no, che si deve guardare anche al Voronezh perché è un problema anch'esso: in realtà secondo me è un non-problema.

Stiamo spendendo il 99% del nostro lavoro per risolvere l'1% del problema. È più utile applicarsi al rimanente 99% del problema. Niente sarà mai perfetto: non è possibile costruire un caveau bancario perfetto perché non appena lo si sarà costruito arriverà il ladro perfetto che troverà il modo di aprirlo. Non è il caso di preoccuparsi di tenere fuori il ladro perfetto: è sufficiente tenere fuori tutti gli altri. Lo stesso discorso si applica ai virus: non dobbiamo mirare al 100% ma ad ottenere soluzioni pratiche e utili. Se cerchiamo il 100%, tanto vale che diamo via tutti i nostri computer e torniamo all'abaco.

***I**n primavera il Mutation Engine, la scorsa estate il Commander Bomber. Pensa che stiamo raggiungendo il limite della tecnologia della scansione?*

(NdR: il «Commander Bomber» è l'ultimo prodotto di Dark Avenger; è un virus dal meccanismo di infezione assolutamente inedito che rende più difficile la sua identificazione. Inoltre nel corpo del virus è contenuta la stringa [DAME] che ha fatto ritenere ai ricercatori che Dark Avenger abbia l'intenzione di combinare questo virus con il Mutation Engine per ottenere un virus non scandibile)

Assolutamente no. Qualsiasi scanner iden-

flitto tra D-Fence e i più diffusi programmi, compresi quelli che accedono al disco con modalità particolari. Né Windows, né le Norton Utilities, né PCTools o altri programmi di utilità hanno fatto rilevare nulla di particolare.

Inoltre la presenza di D-Fence non dà luogo ad alcun degrado di prestazioni, il che è facile da intuire dato il modo in cui il programma funziona.

Data Security Reference Guide

Nella confezione del prodotto, incluso nel prezzo, si trova un pratico manualetto che descrive in modo semplice e

tifica il Mutation Engine, e qualsiasi scanner identifica il Commander Bomber.

***E** se Dark Avenger li mettesse insieme?*

Non ci preoccupa affatto. Dopotutto è soltanto software. Sono anni che la gente predice la fine della tecnologia della scansione. All'inizio vennero fuori i virus crittati, e si disse che gli scanner non li avrebbero riconosciuti. Storie. Poi si disse che gli scanner non avrebbero potuto riconoscere i virus a crittografia multipla come il V101. Storie. Poi è venuto fuori il Mutation Engine, e nessuno sarebbe stato in grado di riconoscerlo. Storie! Un virus è un programma, e in quanto tale dovrà pur compiere qualche azione. Basta ottenerne una copia e disassemblarla, vedere come funziona e invertire il procedimento. Ogni volta che c'è stato uno sviluppo di questo genere, il mondo gli è stato appresso senza troppi problemi.

Non esisterà mai un virus che non può essere identificato. Certo, se qualcuno scrive un virus può dire che il suo virus non può essere identificato con la tecnologia corrente, e può anche avere ragione. Ma certamente la comunità dei ricercatori non ha intenzione di chiudere bottega: appena qualcuno viene in possesso del virus si trova un modo di identificarlo. Sta riscuotendo un notevole successo l'analisi numerica nella ricerca dei virus; e non esiste alcun modo di scrivere un virus che possa sfuggire all'analisi numerica, perché qualsiasi cosa il virus faccia dovrà avere una funzione comune. La si può nascondere come si vuole, farla in mille pezzi o codificarla un milione di volte: sarà sempre possibile riscontrare al suo interno delle stringhe comuni, e l'analisi numerica sarà sempre in grado di trarre fuori le stringhe comuni dal corpo del virus.

I teorici dicono che il limite del software di scansione potrà essere raggiunto. La mia risposta è: dimostratelo, portatemi a vedere un virus che non si riesce a identificare con la scansione.

Nella pratica abbiamo già fatto la prova di combinare il Commander Bomber con tutti i tipi di Mutation Engine: non c'è alcun problema nell'identificare i virus che ne vengono fuori.

***S**i parla molto della tecnica del controllo dell'integrità come alternativa valida alla scansione.*

Non sono assolutamente d'accordo. È stato dimostrato anni fa che il controllo dell'integrità non costituisce una soluzione valida al problema dei virus. È presto detto: per controllare l'integrità è necessario leggere dal disco l'oggetto da controllare, e siccome non si può leggere con il microscopio la superficie del disco si dovrà usare una funzione di accesso, e la funzione di accesso è il punto debole di questa tecnica. Se io sono un virus, mi metto lì a tenere d'occhio la funzione di accesso e non appena qualcuno mi chiede di leggere un oggetto infetto io lo leggo, lo disinfetto al volo e glielo passo in memoria e il controllo di integrità fallisce il proprio scopo.

***Q**uesto è vero. Ma infatti i programmi di controllo di integrità si basano sull'assunto che vengano installati su un sistema pulito, e questa è la loro debolezza. Ma se in seguito il controllo di integrità viene effettuato avviando il sistema operativo da un dischetto pulito, si è al sicuro.*

È vero anche questo. Ma in questo modo si impone sull'utente un requisito poco realistico.

***E**ppure anche per la scansione si raccomanda di avviare il sistema da un dischetto pulito.*

Non è vero. Non conosco alcuno scanner che lo richiede.

***P**erò un virus nascosto («stealth») residente in memoria può ingannare gli scanner.*

Solo se si tratta di un virus nascosto mai visto prima, nel qual caso si tratta di un nuovo virus. E come con tutti i nuovi virus, prima o poi ne veniamo in possesso di una copia. D'altra parte quando viene creato un virus non si diffonde istantaneamente in cento milioni di computer: occorrono mesi, a volte anni prima che divenga una minaccia. Lo Stoned, ad esempio, che oggi è il virus più diffuso nel mondo, ci ha messo due anni per raggiungere una diffusione apprezzabile, eppure noi tutti ne avevamo copie già da tempo.

Ma quando un virus nascosto viene nelle mani dei ricercatori perde questa sua segretezza, perché la prima cosa che faranno gli scanner sarà di cercarne la presenza in memoria. Non c'è modo di nascondersi in memoria, perché per prendere il controllo della macchina un programma deve trovarsi in chiaro, almeno quattro o cinque istruzioni debbono essere in chiaro. E per questa ragione non è indispensabile far partire il sistema da un dischetto pulito prima di passare uno scanner.

Sarà poi cura dello scanner segnalare eventualmente la presenza di un virus, e suggerire all'utente di spegnere il sistema e riavviare da un dischetto pulito: ma si tratterà dell'eccezione e non della norma, come avviene invece con il controllo dell'integrità. E vorrei invitare chiunque a convincere 10.000 utenti in azienda a spegnere ogni giorno la propria macchina, inserire un dischetto pulito e fare il controllo di integrità: posso garantire che non lo farà quasi nessuno.

***E**ppure SCAN, con le sue funzioni /AV e /CV, offre una forma di controllo di integrità. Peraltro ci sarebbero delle obiezioni da fare sul modo in cui è implementato, perché aggiungendo i codici di convalida a un file eseguibile che già di per sé controlla la propria integrità si rischia di far saltare il controllo.*

È vero che le funzioni /AV e /CV servono al controllo di integrità, ma non si tratta certo della funzione principale di SCAN. Quanto all'aggiunta dei codici, se qualcuno ha problemi può scegliere di non farli aggiungere in coda agli eseguibili ma di farli memorizzare in un file a parte.

***Q**uindi lei crede che sia una buona idea andare a fare modifiche in un eseguibile.*

Tutti lo fanno. Sono pochi i programmi eseguibili che si autoverificano: abbiamo installato oltre sei milioni di copie del nostro sistema in aziende di tutto il mondo, e i problemi riscontrati nell'aggiunta dei codici di convalida sono stati inferiori all'1%. Certo, i teorici diranno che non è una buona idea modificare i file eseguibili, ma a me non interessa.

Mi interessa la realtà, non la teoria. Nella realtà non ha mai costituito un problema. Se dovesse diventare un problema, allora si potrà passare alla versione che memorizza i codici di convalida in un file.

Stefano Toria

conciso i principali problemi di sicurezza a cui va incontro un utente di personal computer o l'amministratore di un sistema informativo aziendale. In realtà il volume ha un chiaro scopo promozionale, poiché per ciascun problema viene presentata la soluzione offerta dalla Sophos Ltd.; ma la lettura del manuale è di per sé istruttiva e utile, anche se non si ritenga di acquistare nessuno dei prodotti proposti. Infatti il dichiarato fine propagandistico del testo nulla toglie alla correttezza della presentazione, che fa del manuale una ottima guida di riferimento alla problematica della sicurezza.

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

1992 Computer Virus Solutions Conference

Organizzata da una società australiana e promossa in Italia da Ultimobyte, l'agente italiano per i prodotti della McAfee Associates, si è tenuta il 6 novembre a Milano una conferenza breve nella durata ma molto intensa nel programma. La notorietà dei relatori e il livello delle relazioni presentate ne hanno fatto un evento significativo al fine di tracciare un quadro della situazione, non tanto per chi dei virus fa argomento di studio teorico quanto per chi si confronta con la realtà quotidiana del problema.

La relazione di apertura del convegno è di John McAfee. Profeta e guru per gli uni, abile manipolatore di media per gli altri, McAfee è tuttavia un protagonista della prim'ora della lotta contro i virus. I suoi prodotti sono utilizzati da più di sei milioni di aziende nel mondo, oltre che da innumerevoli privati.

Nella sua presentazione introduttiva McAfee descrive le principali tipologie dei virus conosciuti. È un preludio indispensabile in un convegno che tratta di virus, data la eterogeneità del pubblico e l'impossibilità di determinare in anticipo il livello di preparazione tecnica degli uditori. (Diverso è il caso delle conferenze riservate agli sviluppatori di prodotti antivirus, in cui una relazione preliminare di questo genere è del tutto assente).

La relazione successiva è tenuta da Christoph Fischer, che già nel convegno di settembre scorso a Edimburgo aveva presentato il prodotto realizzato dal Micro-BIT Virus Centre dell'Università di Karlsruhe. Ulteriormente affinato e messo a punto, il database del Micro-BIT sarà presto a disposizione del pubblico per fornire informazioni collegate ai virus.

Dopo la pausa per il caffè due relazioni hanno tratteggiato alcuni aspetti della realtà italiana: Carlo Sarzana di Sant'Ippolito, magistrato di Cassazione e addetto all'Ufficio Legislativo del Ministero di Grazia e Giustizia, ha presentato lo schema di disegno di legge (ddl) contenente modificazioni e integrazioni alla normativa penale, in tema di criminalità informatica. Molto probabilmente il ddl verrà presentato alle Camere entro la fine dell'anno, e la sua approvazione consentirà all'Italia di trovarsi finalmente allineata con la disciplina prevista in altri Paesi della CEE.

Il ddl copre con ampio respiro la tecnologia attuale, dai sistemi di elaborazione propriamente detti alle reti telematiche, al software, al patrimonio informativo; si propone il fine di delineare alcune nuove figure di reato particolarmente rilevanti nel settore informatico e risulta particolarmente rilevante la scelta di modificare il codice penale anziché creare una legge penale speciale, poiché indicherebbe la volontà del legislatore di integrare il reato informatico nel quadro dei reati di rilevanza sociale generale.

Tra i diversi reati informatici previsti dal ddl spiccano la frode informatica, il falso informatico, il sabotaggio informatico; quindi l'accesso e l'intercettazione non autorizzati, la riproduzione non autorizzata di programmi informatici e la utilizzazione non autorizzata di un elaboratore. Guerra agli hacker, quindi, anche sul fronte legislativo.

Alla relazione del Presidente Sarzana ha fatto seguito un altro intervento su un tema giuridico: l'Avv. Pietro Tamburrini ha descritto le possibilità di perseguire penalmente il danneggiamento di sistemi informatici altrui a mezzo di un virus. Risulterebbero applicabili per estensione alcune fattispecie di reato, ma nella pratica si incontrerebbero notevoli ostacoli nel colpire il comportamento di chi crea o distribuisce virus.

Potrebbe avere maggiore efficacia l'applicazione della normativa civile, soprattutto in materia di danneggiamento; si possono ipotizzare diversi casi, a seconda che l'introduzione del virus sia volontaria o accidentale, e che la persona che introduce il virus sia o meno legata da rapporti contrattuali con il danneggiato.

A questo proposito riportiamo una notizia, ricevuta successivamente alla data del convegno, e proveniente dalla Gran Bretagna. È stato condannato a un'ammenda di 500 sterline e al pagamento delle spese processuali pari ad ulteriori 500 sterline il Dr. Roy Booth, un docente della Newcastle University riconosciuto colpevole di estorsione per aver minacciato un'azienda statunitense, la Imec, di introdurre un virus in un programma costato 200.000 sterline se non gli fosse stato riconosciuto un controverso rimborso di spese.

Dopo la pausa per il pranzo il convegno riprende con una seconda relazione di McAfee, centrata stavolta sul problema della protezione delle reti locali. Sta prendendo piede l'idea di delegare al server, anziché alle singole stazioni cliente, il controllo sui file eseguibili per il rilevamento della presenza dei virus. McAfee ha illustrato i sostanziali vantaggi di questa opzione, legati soprattutto al fatto che il controllo antivirus viene sottratto all'iniziativa del singolo utente e centralizzato sotto il diretto controllo dell'amministratore della rete.

Jan Terpstra, dipendente della IBM dal 1980 e moderatore per diversi anni della conferenza internazionale sui virus nella rete Fidonet, è coordinatore delle attività del CERT (Computer Emergency Response Team) della IBM. L'idea del CERT, promossa dalla IBM in collaborazione con alcune Università statunitensi tra cui la Carnegie-Mellon, è applicabile in qualsiasi realtà aziendale di dimensione superiore alle poche unità. Non è indispensabile assumere personale specializzato o formare costose risorse interne: quasi sempre in un'azienda che abbia alcune decine di dipendenti è possibile identificare un gruppo di almeno due persone che abbiano autonomamente sviluppato conoscenze avanzate in campo tecnico, a cui sia possibile delegare — eventualmente dopo una limitata formazione specifica — il compito di primo intervento in caso di emergenze informatiche, salvo il richiedere ove necessario l'intervento di personale esterno specializzato.

Fulvio Berghella è il responsabile di SecurityNet, un network informativo di cui già abbiamo avuto occasione di parlare. Tra i 200 soci di SecurityNet vi sono principalmente banche, ma anche industrie ed enti statali. Berghella ha presentato la situazione italiana: un'azienda su due ha subito un'infezione da virus nei primi nove mesi dell'anno; nel solo mese di settembre si sono riscontrati più incidenti che nell'intero 1991. Particolarmente diffusi sono i virus Flip, Form, 855 seguiti dai soliti Cascade (170X), Ping Pong e Stoned. Pollice verso ai tecnici esterni venuti in azienda per riparare o installare computer: sono risultati responsabili dell'infezione nel 35,5% dei casi, mentre i videogiochi usati più o meno lecitamente sono colpevoli soltanto del 17% dei casi. Quasi il 29% è da attribuire al software introdotto abusivamente dai dipendenti, mentre lo scambio di dischetti tra aziende ha causato il 10,5% dei casi rimanenti.

Termina la giornata dedicata ai virus una spumeggiante presentazione di Jim Lynch, responsabile della clientela internazionale della McAfee Associates. Lynch ha tratteggiato il profilo dei futuri prodotti antivirus, sconsigliando di attendersi l'apparizione del Prodotto Perfetto e Definitivo e fornendo alcune indicazioni su come scegliere i prodotti antivirus: evitare di seguire gli slogan e affidarsi alle prove imparziali condotte da organismi provati e attendibili.

Stefano Toria

CD-ROM, RIVOLGETEVI AGLI SPECIALISTI

WIN • DOS ONE CD-ROM

OLTRE 500 MB DI FREESOFTWARE E SHAREWARE NUOVISSIMO SELEZIONATO DALLE MIGLIORI BBS MONDIALI PER GLI UTILIZZATORI DI MS-DOS E WINDOWS: QUASI 20.000 FILES CON CENTINAIA DI UTILITIES, FONTS, GIOCHI, SUONI, ANIMAZIONI...

L. 175.000 + IVA 12 %

VHS FILM GUIDA ON DISK

IL LIBRO PIU' FAMOSO TRA GLI APPASSIONATI DI VIDEO ORA SI FOGLIA AL COMPUTER: "VHS FILM GUIDA ON DISK" E' LA BANCA DATI PER IL VOSTRO PC. AGGIORNATO A SETTEMBRE 1992: OLTRE 16.000 TITOLI A PORTATA DI MOUSE. DISPONIBILE SU DISCHETTI PER WINDOWS O IN VERSIONE CD-ROM (CON LE COPERTINE DELLE VIDEOCASSETTE) PER WINDOWS O MACINTOSH. AGGIORNAMENTI TRIMESTRALI

IN OFFERTA DI LANCIO L. 175.000 + IVA 12 %

IMAGINARIO/PC CD-ROM

OLTRE 500 IMMAGINI INEDITE A COLORI IN FORMATO EPS PRONTE PER ILLUSTRARE BROCHURES FLYER CATALOGHI LIBRI GIORNALI RIVISTE E... UNA BANCA DATI ECCEZIONALE PER DTP, GRAFICI E ILLUSTRATORI. RICHIEDE WINDOWS 3.X

L. 249.000 + IVA 12 %

SEVENPLUS MAC CD-ROM

SHAREWARE E FREESOFTWARE PER MACINTOSH - RICHIEDE SYSTEM 7

L. 159.000 + IVA 12 %

MACDEMOS CD-ROM

OLTRE 350 DIMOSTRATIVI PER MACINTOSH - RICHIEDE SYSTEM 7

L. 159.000 + IVA 12 %

IMAGINARIO MAC CD-ROM

VERSIONE PER MACINTOSH - RICHIEDE 4 MB RAM, SYSTEM 7

L. 249.000 + IVA 12 %

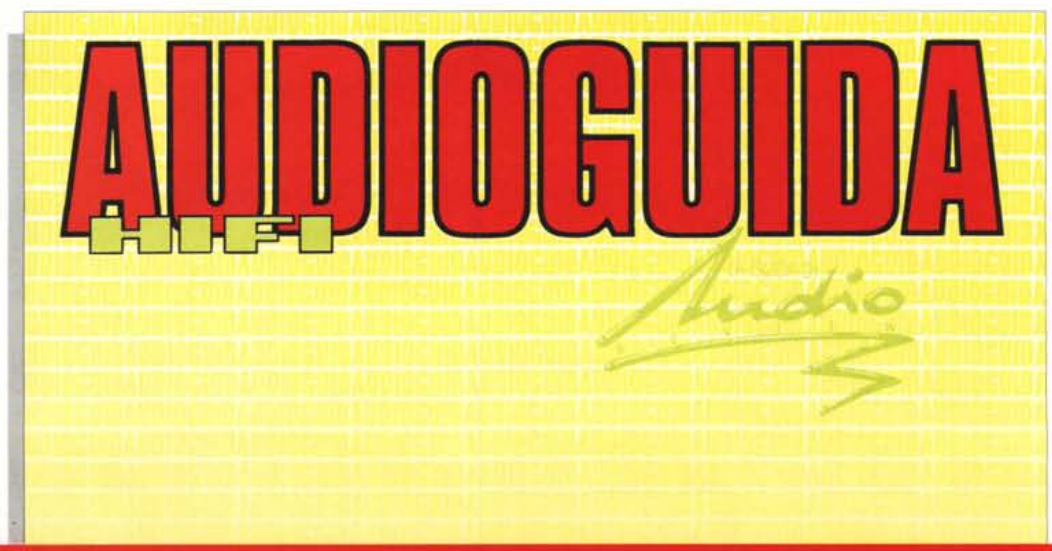
IN OMAGGIO A RICHIESTA CD-ROM MAGAZINE

MGE COMMUNICATIONS

ORDINI TELEFONICI: 06 / 3243289 - FAX 06 / 3243088 - VIA COLA DI RIENZO 163 - 00192 ROMA

Più di settecento pagine, novemilacinquecento prodotti hi-fi con relativi prezzi (che sono aggiornati mese per mese su AUDIOREVIEW), seimilacinquecento foto, cinquanta pagine di articoli monografici che svelano tutto ciò che è necessario sapere prima di scegliere ogni singola parte del vostro impianto hi-fi. Tutto questo è AUDIOGUIDA HI-FI: l'alta fedeltà al gran completo. Ideale per ascoltare bene, indispensabile per acquistare meglio.

Indispensabile volume d'ascolto.



technimedia
Pagina dopo pagina, le nostre passioni.

©RcpAssociati

AUDIOGUIDA HI-FI '92/'93. Una sonora lezione.