Virus in scatola

di Stefano Toria
(MC0170 su MC-link)

Abbiamo ripetuto più volte che nessun programma è da considerare sicuro al 100% dall'infezione da virus: nemmeno quelli acquistati in scatola sigillata. Negli Stati Uniti è già accaduto diverse volte di riscontrare la presenza di virus in programmi di questo genere. Nella maggior parte dei casi si è potuto verificare che l'infezione era dovuta al comportamento non esattamente corretto del rivenditore, che aveva «prestato» il programma a un amico o a un cliente importante, il quale lo aveva installato o comunque utilizzato, infettandolo a propria insaputa, e l'aveva quindi restituito al rivenditore il quale aveva provveduto a risigillare la scatola nel cellophan termosaldato (la macchina per fare questa operazione costa relativamente poco).
Ma almeno in un caso le cose non sono andate così. Chi ci segue rammenterà anche il caso di Aldus Freehand: il virus riuscì a passare i controlli fatti prima ancora della distribuzione del software. Al rischio-virus, già consistente, si è aggiunta una nuova componente: la possibilità che i programmi si contaminino, per così dire, «alla fonte». Vediamo cosa hanno fatto i produttori di software per ridurre al minimo questo rischio

Software di massa e rischio virus

Molti lettori, se non tutti, si saranno sottoposti almeno una volta nella propria vita a una vaccinazione, ad esempio antitetanica. Il vaccino consiste in una dose di siero (una delle componenti del sangue) contenente un certo quantitativo dell'agente patogeno, cioè della causa della malattia dalla quale il vaccino deve difendere.

Le case farmaceutiche normalmente impiegano la massima cura perché il siero sia immune da qualsiasi tipo di contaminazione.

Facciamo per un attimo una ipotesi da fantascienza catastrofica: e cioè che un lotto di vaccino, consistente in migliaia di dosi, si contamini (per errore, per caso o per un preciso atto criminale) con il virus dell'epatite. È facile immaginare il disastro che ne conseguirebbe: migliaia di persone, prima sane, all'improvviso si ammalerebbero di epatite, apparentemente senza alcun motivo.

Questo scenario corrisponde più o meno a quanto accadrebbe, seppure con effetti meno drammatici, nel caso in cui un programma «di grido» dovesse uscire dalla fabbrica ed essere messo in vendita infetto da un virus. Abbiamo ripetuto più volte che qualsiasi programma può infettarsi; quindi perché non dovrebbe accadere — ad esempio — alla nuova versione, appena pubblicata, di Paradox? O di Lotus 1-2-3? O di WordPerfect, o di PageMaker o di qualsiasi altro programma di questo genere.

Sappiamo che un fatto di questo genere si è già verificato. In quel caso soltanto la serietà e la tempestiva reazione del produttore del programma colpito riuscì a scongiurare una diffusione di massa del virus.

Ma è possibile che un simile fatto si ripeta?

Abbiamo interpellato alcuni tra i principali produttori di software standard, presso i loro uffici nel nostro Paese. Ecco il quadro risultante della situazione attuale.

BORLAND

La Borland Italia ha sede a Milano, in un ufficio che ospita sia le strutture amministrative e commerciali sia quelle tecniche e di supporto alla clientela. Le funzioni di assistenza vengono svolte in sede, mentre la riproduzione e confezione dei prodotti viene affidata in service ad altra azienda.

Nella sede sono presenti oltre trenta personal computer di marche diverse, collegati in rete con un server che contiene dati amministrativi e anagrafici.

I master con i file eseguibili provengono direttamente dalla casa madre, e sono corredati da un codice di controllo per ciascun eseguibile. All'arrivo i dischetti vengono controllati su uno dei PC del servizio tecnico; il codice di controllo di ciascun file viene ricalcolato e confrontato con l'originale, e in caso di discrepanza il processo di distribuzione si blocca in attesa di una verifica.

La procedura di controllo viene ripe-

tuta diverse volte nel corso della distribuzione; i master vengono nuovamente controllati prima di uscire per andare al centro di riproduzione, e quindi presso lo stesso centro sia all'arrivo che a campione all'uscita della riproduzione. In ogni fase il controllo consiste nel ricalcolo dei codici e nel confronto con l'originale. Ogni eventuale discrepanza dà luogo all'interruzione del processo di riproduzione. Il centro di servizi provvede anche al confezionamento del software unitamente alla documentazione (manuali, etc.); i prodotti vengono quindi inscatolati, termosaldati nella plastica trasparente e quindi inviati ai distributori e rivenditori.

Tutte queste fasi prevedono dei rigorosi controlli a campione. Alcune delle scatole già confezionate e pronte alla vendita vengono riaperte per un ulteriore ricalcolo dei codici di controllo; una eventuale differenza provocherebbe il blocco dell'intera partita di prodotti, e l'avvio di una serie di verifiche ed eventualmente la ripetizione della riproduzione dal master.

Ma il punto più delicato dell'intera struttura consiste nel centro di assistenza. Questo è il luogo a cui sono destinati i dischetti che per qualsiasi motivo tornano indietro dalla vendita: può trattarsi di dischi difettosi in quanto il supporto magnetico era in qualche modo deteriorato, oppure di dischi utilizzati in modo incorretto dall'acquirente. Per prima cosa ogni dischetto che rientra all'assistenza viene controllato con il prodotto VIRUSCAN della McAfee Associates.

Soltanto in seguito a questa verifica il dischetto viene trattato dai tecnici dell'assistenza. Accade frequentemente infatti che i prodotti che tornano all'origine siano infetti: questo è un sintomo del fatto che sono pochi gli utenti di personal computer che rispettano quella che dovrebbe essere la prima norma di sicurezza, e cioè non scrivere mai per nessun motivo sui dischetti originali di qualsiasi prodotto software regolarmente acquistato. Per ridurre comunque al minimo i rischi dell'infezione e della trasmissione di un virus, la Borland Italia ha adottato due ulteriori misure di sicurezza: tutti i computer installati nell'ufficio sono stati corredati della versione più recente di VIRUSCAN, mediante il quale sono stati calcolati i codici di controllo di tutti i file eseguibili installati, in modo da poter rapidamente verificare se per qualsiasi motivo vi siano state modifiche sospette agli eseguibili; inoltre, al personale che in qualche modo ha a che fare con la distribuzione dei prodotti è stata fornita una specifica formazione sulla natura e gli effetti dei virus e sulle modalità di protezione dall'infezione.

Non ce n'era bisogno, grazie

Nel numero 108, lo scorso giugno, abbiamo pubblicato due mappe con la situazione comparativa, a nove mesi di distanza, della distribuzione dei virus per origine. Nel settembre 1990 un solo virus risultava provenire dall'Italia; a maggio 1991 erano diventati otto. Adesso a fine novembre siamo a ben ventitré virus riportati dalla lista di Patricia Hoffman.

Qualcuno si deve essere dato molto da fare in questi ultimi tempi, considerato oltretutto il fatto che una buona parte di questi nuovi virus sembrano essere stati scritti dalla stessa persona o gruppo di persone.

Peraltro sembrerebbe che molti di questi nuovi virus siano stati scritti per esperimento. Infatti ciò che è pervenuto al gruppo di ricerca che li ha analizzati non è un programma normalmente infettato dal virus, ma l'originario programma di lancio, cioè quel programma che l'autore di un virus scrive al fine di realizzare per la prima volta l'infezione di un programma-veicolo.

Ancora una volta vogliamo attirare l'attenzione dei lettori sui rischi che si corrono giocando imprudentemente con i virus. Si ha notizia sempre più spesso di persone che «collezionano» o «studiano» virus. È un'attività rischiosa, che va lasciata a chi è effettivamente in grado di occuparsi di questi programmi. Si è verificato poi che questi «studi» consistono per lo più semplicemente nell'analizzare i programmi sospetti a mezzo di un programma di scansione.

Per non parlare poi di chi sviluppa o modifica un virus. Ci è stato recapitato in redazione il lavoro di un lettore che ha scritto un virus finalizzato alla diffusione di un messaggio dai contenuti positivi. Comprendiamo e apprezziamo le buone intenzioni dell'autore, ma abbiamo dovuto scoraggiarlo — e con lui chiunque altro intendesse dedicarsi a un'attività del genere — da quella che è un'attività pericolosissima. Un virus benigno può essere modificato in pochi istanti da chiunque abbia sufficienti conoscenze, e divenire distruttivo. Inoltre in alcuni Paesi (ad esempio in Gran Bretagna) lo sviluppo di programmi virali è vietato dalla legge, e i trasgressori rischiano pene detentive piuttosto severe. Un cittadino di un altro Paese, conosciuto in Gran Bretagna come sviluppatore di virus, verrebbe identificato alla frontiera e respinto.

Lotus

L'intervista con la Lotus ha costituito una piacevole sorpresa. Sapevamo già che la casa di 1-2-3 da tempo aveva manifestato interesse per il problema dei virus: nello scorso mese di ottobre una autorevole pubblicazione specializzata in virus riportava un articolo di un ricercatore della Lotus in cui veniva descritto il sistema di classificazione e denominazione dei virus adottato da quella casa.

In questa occasione peraltro abbiamo appreso da una gentile funzionaria della Lotus Italia che tutte le versioni correnti di 1-2-3 (le versioni Dos, la versione per Windows e quella per il Macintosh) incorporano un controllo di integrità pensato appositamente per l'identificazione precoce di una eventuale infezione da virus.

In altre parole, all'atto del caricamento di 1-2-3 si attiva un modulo detto IVCHECK, mediante il quale è lo stesso programma ad autoanalizzarsi, alla ricerca delle tracce di un'infezione da virus. Se queste tracce vengono riscontrate allora viene emessa una adeguata segnalazione all'utente, il quale deciderà cosa fare: se interrompere l'esecuzione, distruggere il programma, etc.

Questa è una prassi che ci piacerebbe vedere imitata da altri produttori di software, sebbene la sola adozione di una tutela software non possa costituire un mezzo di protezione sufficiente a tutelare l'utente da tutti i rischi. Abbiamo infatti già messo in guardia i lettori contro questo rischio: non basta un antivirus, occorrono misure congiunte consistenti in copie di backup regolari e controlli di integrità fisica dei file eseguibili.

La persona che abbiamo contattato in Lotus ci ha fatto anche una interessante anticipazione: la casa si starebbe predisponendo ad entrare nel mercato del software antivirus con uno specifico prodotto. Ma su questo argomento non abbiamo potuto avere ulteriori informa-

zioni, dato anche il fatto che il progetto è ancora in fase di definizione.

Microsoft®

Alcune società tra quelle da noi contattate non producono software nel nostro Paese, ma lo ricevono già confezionato e pronto per la distribuzione. Una di queste è la Microsoft. Tutto il software prodotto dall'azienda di Bill Gates, e destinato al mercato italiano, proviene dall'Irlanda. I programmi vengono compilati, riprodotti, controllati e confezionati direttamente negli impianti irlandesi, per essere poi distribuiti sui singoli mercati nazionali.

Tutto il controllo di qualità viene effettuato quindi all'estero, e pertanto negli uffici italiani non è stata predisposta alcuna specifica misura di prevenzione contro il rischio di infezione dei prodotti da distribuire.

Peraltro non risulta si sia mai verificato che un prodotto sia rientrato dopo la vendita perché difettoso e si sia riscontrato che il difetto consistesse nella presenza di un virus.

NOVELL

Abbiamo incluso la Novell tra le aziende contattate non soltanto perché si tratta indubbiamente di uno tra i principali produttori di software, ma anche perché le reti locali presentano alcune particolarità rispetto ai virus.

Innanzitutto è evidente la differenza tra un personal computer, sul quale può operare al più una sola persona per volta, e un server di rete locale, che può essere acceduto simultaneamente da decine o centinaia di persone. Qualsiasi software di rete locale — Novell NetWare tra questi — dedica una buona parte delle proprie risorse alla gestione della sicurezza, in modo da impedire che i programmi e in genere i file residenti sul server vengano toccati da chi non è autorizzato a farlo.

Eppure, nonostante il NetWare sia riconosciuto come uno tra i migliori sistemi sotto questo punto di vista, sembrerebbe che un particolare virus sia riuscito a penetrarne le difese. Si tratta di una variante del ceppo Jerusalem, e il fatto è parzialmente confermato da un rapporto pubblicato dalla stessa Novell a seguito di un esperimento effettuato negli impianti della società a Paramus, New Jersey, il 12 luglio 1990. Nel rapporto, a firma del vicepresidente della Novell Richard King, non si parla tuttavia di aggiramento delle difese ma di propagazione in assenza di difese. In ogni caso la presenza di una rete locale rende indispensabili maggiori controlli, come testimonia anche l'esistenza di una versione specifica per rete locale dei principali prodotti software antivirus tra cui VIRUSCAN, che prevede un apposito NETSCAN per il controllo dei server

Il virus nella CMOS

Si riaffaccia ogni tanto lo spauracchio di un ipotetico virus contenuto nella memoria CMOS.

La CMOS (dall'inglese Complimentary Metal Oxide Semiconductor) è una memoria di dimensioni piuttosto ridotte e dal consumo di energia trascurabile, che si trova ormai su tutti i personal computer, e che viene utilizzata per conservare le informazioni necessarie al BIOS per configurare la macchina con le relative periferiche: in particolare i dischi. Nella CMOS si trovano anche alcune altre informazioni, tra cui data e ora, l'eventuale password e poco più.

Dicevamo che si tratta di uno «spauracchio» perché un virus che eleggesse la CMOS a propria sede — qualora esistesse — sarebbe l'unico virus in grado di sopravvivere a una ripartenza a freddo, addirittura allo spegnimento del computer. Se un simile virus potesse essere scritto, sarebbe in grado di assumere il controllo del computer prima ancora che venga caricato qualsiasi sistema operativo dai dischi, quindi prima dell'adozione di eventuali misure antivirus.

Le voci su un virus localizzato nella memoria CMOS persistono tra gli utenti meno informati, grazie anche all'azione di persone più informate (e che dovrebbero saperla più lunga). È opportuno pertanto fornire qualche chiarimento in proposito.

Qualsiasi tipo di memoria può essere utilizzato per conservare qualsiasi tipo di informazione: dati, programmi, configurazioni, etc. La memoria CMOS non differisce in questo senso dalla normale RAM e pertanto potrebbe senz'altro contenere del codice eseguibile, in particolare un virus. Tuttavia questo è reso estremamente improbabile dalla concomitanza di altri fattori.

La memoria CMOS non è collegata al bus del personal computer allo stesso modo in cui è connessa la RAM. (Per i lettori che non siano a conoscenza della struttura interna di un computer, accenneremo brevemente che il bus è il principale veicolo di transito di informazioni e istruzioni eseguibili tra il microprocessore — il cuore, o meglio il «cervello» del computer — e tutto il resto della macchina, tra cui la memoria). La CMOS viene vista esclusivamente da un apposito programma in grado di accedervi, viene utilizzata soltanto per contenere dati e configurazioni e in ogni caso qualora contenesse delle istruzioni di programma queste non potrebbero essere eseguite là dove si trovano ma dovrebbero essere preventivamente trasferite nella RAM, che è l'unica deputata a contenere istruzioni eseguibili.

Il contenuto della CMOS viene riversato dal programma di controllo in una locazione precisa della RAM, e a questo fine la CMOS viene acceduta tramite due porte di input/output esattamente come avviene per tutte le periferiche: dischi, stampante, porta seriale, tastiera. E viene acceduta allo stesso modo in cui vengono accedute le altre periferiche: un byte alla volta.

Non è impossibile però che una CMOS possa essere utilizzata per contenere un virus, ma un simile virus avrebbe bisogno di un apposito programma — stavolta residente su supporti, per così dire, tradizionali come un disco — che lo prelevi, byte per byte, e lo trasporti nella RAM per eseguirlo. Non si vede per quale motivo si debba utilizzare un meccanismo così complesso quando, dal punto di vista dell'autore di un virus, è molto più semplice scrivere un programma interamente contenuto su disco.

Inoltre la necessità di un apposito programma di caricamento renderebbe tutto il virus, e in particolare quest'ultimo programma, suscettibile di essere identificato come qualsiasi altro virus. Senza considerare il fatto che questo ipotetico virus, allo stesso modo di qualsiasi altro virus, potrebbe essere identificato all'atto della replicazione.

Va poi considerata la totale mancanza di standard per quanto riguarda l'uso che viene fatto della CMOS. Ciascun costruttore si aggiusta i propri dati come meglio crede. Un virus scritto per occupare locazioni libere nella CMOS di un computer quasi certamente corromperebbe dati vitali su un computer di marca differente.

In conclusione non si ritiene di dover considerare il mito del virus della CMOS più di quanto esso effettivamente è, e cioè appunto un mito.

di rete. Anche la Novell Italia, come la Microsoft, riceve tutto il proprio software già confezionato e controllato in fabbrica.

Tutte le operazioni di riproduzione e controllo vengono effettuate in un apposito impianto in California; l'assenza di versioni di NetWare tradotte in lingue diverse rende più semplice questa concentrazione.

Il responsabile del sistema informativo interno della Novell Italia ha ritenuto opportuno installare un prodotto antivirus sui personal computer utilizzati negli uffici; peraltro non è stato possibile avere informazioni precise su quale prodotto venga utilizzato.

Tuttavia, poiché dagli uffici italiani non viene distribuito software di alcun genere (patch, driver, etc.) e l'assistenza viene effettuata direttamente dai distributori, la presenza di questo software antivirus non ha alcuna rilevanza ai fini della sicurezza dell'integrità del software acquistato dall'utente finale.

WordPerfect ITALIA

Quanto già detto per Microsoft e Novell vale anche per WordPerfect. Il software viene confezionato all'estero, a Rotterdam in Olanda e a Provo nello Utah, sottoposto localmente agli opportuni controlli di qualità tra cui un controllo antivirus, e quindi distribuito in tutto il mondo.

Vi è tuttavia una particolarità. WordPerfect prevede numerosi driver per stampanti, dei quali soltanto una parte viene distribuita insieme al pacchetto software in vendita. I rimanenti vengono inviati ai clienti che ne fanno richiesta, e a questo fine vengono riprodotti localmente. Negli uffici italiani le macchine destinate alla duplicazione dei driver vengono controllate periodicamente con Norton Antivirus.

Conclusioni

Apparentemente i «grandi» sono preoccupati per il fenomeno dei virus. Giustamente preoccupati, a nostro avviso, perché il rischio di diffondere un virus è tutt'altro che remoto.

E il danno per un grande produttore di software potrebbe essere incalcolabile: sia in termini di immagine che anche in termini economici, se si dovesse verificare una vasta diffusione di un virus nocivo con la conseguente necessità di risarcire i danni subiti dai dati dei clienti.

Non ci è stato possibile ricevere, in tempo per la pubblicazione di questo articolo, informazioni dalla Aldus.

Sarebbe stato interessante conoscere nei dettagli le misure che sono state prese per evitare il ripetersi del noto fatto.

Ci ripromettiamo tuttavia di parlarne in un prossimo numero.

MC

"Killer Price And A Terrific Warranty"

PC Word - giugno 1990

Direttamente dagli USA

GARANZIE:
* 5 anni in laboratorio (mano d'opera)
* 2 anni su scheda base e parti speciali (sk. VGA Orchid, tastiera, HD Maxtor, ecc.)
* 1 anno sulle parti standard
* Soddisfatti o rimborsati entro 30 giorni dall'acquisto

PC MAGAZINE EDITORS' CHOICE

INFO WORLD TOP 100

"Excellent value"
"An impressive package"

Poly 386 - 25/Cache
* 2 MB RAM
* 80 MB Hard Disk
* Sk. graf.VGA
* Monitor Mono 640x480 VGA
* contenitore tower

Lire 2.850.000

INFO WORLD

"Compared with the top 18 manufacturers, Polywell ranked fastest and lowest priced..."

Poly 386sx - 25
* 1MB RAM
* 40MB Hard Disk
* Sk. graf.VGA
* Monitor Mono 640x480 VGA

Lire 2.050.000

PC MAGAZINE

"Shines in its attention to detail."

Poly 386 - 33/Cache
* 64K Cache
* 4MB RAM
* 120 MB Hard Disk
* Sk. graf. Orchid Pro II 1024
* Monitor colore VGA 1024x768

Lire 3.960.000

"Stands out on the video benchmark tests"

PC MAGAZINE

Poly 486 - 33
* 128K Cache
* 4MB RAM
* 200MB Hard Disk
* Sk. graf. Orchid Pro II 1024
* Monitor colore VGA 1024x768

Lire 5.830.000

Tutti i sistemi sono forniti con licenza MS-DOS e manuali d'uso FDD da 3,5" o da 5,25", porte seriale e parallela.
Altre configurazioni sono disponibili su richiesta.
I prezzi sono IVA esclusa e possono subire variazioni senza preavviso.

Nuovi Annunci e Prodotti Speciali
- 386 il sistema può ospitare le CPU 386/25/33/40, 486sx, 486/25/33/50 consentendo un aggiornamento delle prestazioni a prezzi competitivi.
- Sceda Grafica VGA Edsun (Continue Edge Graphics) rende disponibile una risoluzione fino a 2500x2500 con 700.000 colori su monitor VGA standard.
- 486 a 50 Mhz con 256 Kb di memoria cache. "TOP GUN"
- Scheda Accelleratrice per PS/2 modelli 50/60s. Aumenta la velocità della CPU a 20 Mhz con 32 Kb di memoria cache.

Tutti i marchi citati sono marchi registrati dalle rispettive case.

Per informazioni e ordini telefonici chiamateci al numero:

(011) 4373313

Linea diretta assistenza tecnica tel. (011) 489059

POLY SYSTEMS

Polywell Computers Inc.
61"C" airport Boulevard
South S.Francisco CA 94080 U.S.A.
FAX(415)583-1974

importatore e distributore esclusivo per l'Italia

M.C.E. Manutenzioni e Costruzioni Elettroniche srl
Via Capellina 12 - 10144 TORINO
FAX (011) 4730512

M.C.E. in Italia è:
- *Assistenza tecnica*
- *Reti locali*
- *Prodotti d'avanguardia*