Ho un virus. Adesso che faccio?

di Stefano Toria

Negli scorsi numeri si è visto come un virus può raggiungere un sistema, e quali possono essere i sintomi della presenza del virus. Con un minimo di cultura tecnica e di attenzione al proprio sistema, ciascun utente può imparare a distinguere le attività normali da quelle anomale, e tra queste in particolare identificare quelle sospette. In questo articolo sono contenute alcune indicazioni di come comportarsi nel caso in cui sia stata accertata, o semplicemente sospettata, la presenza di un virus nel proprio personal computer

Il danno è già successo

In questo caso c'è ben poco da fare. Se l'utente si accorge del virus nel momento in cui questo entra nella propria fase distruttiva, ad esempio avviando la formattazione a basso livello del disco fisso, non c'è più nulla da fare per bloccare il virus; l'unica speranza è che l'utente avesse eseguito recentemente una copia dei dati contenuti nei propri dischi: questa è una misura di sicurezza sulla cui indispensabilità non si insisterà mai abbastanza. ***È fondamentale eseguire frequentemente le copie di sicurezza, e conservarle accuratamente documentate con la data e ora di esecuzione.*** Il possesso di una serie di dischetti di backup, aggiornati di recente, è l'unico modo per uscire indenni dall'attacco distruttivo di un virus. Al più si dovrà rifare il lavoro degli ultimi giorni o delle ultime ore; ma non andrà mai perduto tutto il lavoro accumulato in mesi o anni.

A questa raccomandazione è indispensabile aggiungerne un'altra: ***conservare sempre intatti i dischi originali del sistema operativo e di tutti i programmi che si utilizzano.*** L'installazione di tutto il software dovrebbe essere effettuata con i dischetti protetti contro la scrittura; al termine dell'installazione sui dischi di lavoro o sul disco fisso, i dischetti originali vanno riposti per non essere mai più toccati, se non in caso di necessità. Non c'è niente di peggio del lavorare quotidianamente sui dischi originali, per poi ritrovarseli infettati o peggio distrutti da un virus, e non poter ricorrere a nessuna copia per riprendere il proprio lavoro.

I programmi acquistati dovranno essere installati, e i dischetti originali riposti. I programmi prelevati da BBS o gruppi di utenza dovranno essere trasferiti al sicuro su dischetti che verranno riposti anch'essi; soltanto dopo aver effettuato queste copie si potrà procedere alla scompattazione e all'installazione.

L'argomento della protezione contro i virus sarà ripreso, e trattato più diffusamente, nel prossimo numero.

Se il virus ha avuto già modo di colpire il proprio obiettivo, l'unica possibilità di cui l'utente dispone è di ripristinare ciò che è andato distrutto. La procedura più sicura prevede i seguenti passi (e presuppone che l'utente abbia seguito fedelmente le raccomandazioni accennate):

— eseguire una formattazione a basso livello del disco fisso, ridefinire le partizioni, avviare il DOS e formattare ciascuna partizione, quindi installare nuovamente il DOS sulla partizione attiva;
— in alternativa, chi non possiede disco fisso formatterà il dischetto di avvio del sistema e tanti dischetti quanti occorrono per le applicazioni che utilizza correntemente;
— effettuare nuovamente, a partire dai dischetti originali, l'installazione di tutti i pacchetti applicativi precedentemente contenuti nei propri dischi;
— effettuare un restore, dai dischi di backup, dei soli dati. Questo è un punto essenziale: *nessun programma dovrà mai essere ripreso dai dischi di backup*, in quanto potrebbe essere anch'esso infetto e riportare l'infezione sul sistema.

Possono costituire un problema quei programmi che prevedono una procedura di installazione con controllo del numero di installazioni, o in qualsiasi modo una protezione delle copie installate. Questo è un problema che sarà affrontato anch'esso nel prossimo numero, in quanto più specificamente inerente alla

protezione contro i virus piuttosto che al recupero dalle conseguenze di un'infezione; in ogni caso non si dovrà mai cedere alla tentazione di effettuare il restore dai dischetti di backup anche delle applicazioni protette, in quanto non si può essere certi che non fosse infetta anche l'applicazione che si va a ripristinare dal backup.

Se l'infezione viene scoperta per tempo

In questo caso ci sono molte cose che l'utente può fare per tutelarsi dal disastro. La prima, immediata azione da eseguire in ogni caso — e questo vale anche per l'eventualità che il danno sia già accaduto — consiste nello spegnere immediatamente l'elaboratore, senza indugiare a salvare un eventuale lavoro in corso di modifica, e riaccenderlo soltanto dopo aver inserito nel drive A: il dischetto originale del sistema operativo, protetto contro la scrittura. (Naturalmente anche qui si suppone che l'utente abbia seguito scrupolosamente le raccomandazioni date più sopra).

Si dovrà quindi procedere a salvare i dati, e soltanto i dati, di tutte le applicazioni correntemente in uso. L'utente dovrà effettuare un backup simile a quello che si presume egli faccia regolarmente, ma limitato ai soli dati.

Al termine di questo backup, dovrà procedere come descritto sopra per il caso in cui il virus abbia già avviato l'azione dannosa: ossia dovrà ripartire da una formattazione a basso livello di tutto il disco fisso, quindi dovrà ridefinire le partizioni, installare il DOS etc.

Si potrà obiettare che la procedura è eccessivamente onerosa e lunga. Non è così. Il rischio costituito da un virus non deve mai essere sottovalutato. Si rammenta che la presenza di un virus in un sistema equivale alla presenza di un intruso, di un estraneo che nella migliore delle ipotesi non ha nessuna plausibile giustificazione per trovarsi dove si trova; ma potrebbe essersi introdotto nel sistema in compagnia di altri, più malintenzionati intrusi, o potrebbe essere egli stesso progettato per distruggere.

Gli utenti più smaliziati potrebbero essere tentati di disinfettare i programmi infetti utilizzando uno dei programmi antivirus attualmente in circolazione. Anche questa è un'operazione da non effettuare mai, in nessun caso. Sono stati riportati numerosi casi in cui dei file EXE sono stati infettati da varianti del ceppo Jerusalem, disinfettati utilizzando un apposito programma, per poi risultare più lunghi o più brevi rispetto all'originale prima dell'infezione; sovente tali programmi dopo il trattamento non funzionano più. Lo stesso accade con altri ceppi virali; pertanto, la disinfezione di un sistema a mezzo di un programma di disinfezione è in ogni caso da sconsigliare.

Tutt'al più un utente esperto, rilevando con certezza che il virus da cui è stato colpito ha infettato solo ed esclusivamente una specifica applicazione, potrà limitare l'opera di disinfezione alla

Fuori l'autore

Tra le attività in cui è impegnata la comunità internazionale dei ricercatori antivirus, riveste una certa importanza il tentativo di individuare l'identità degli autori dei virus. L'importanza deriva da due circostanze: innanzitutto dal fatto che in alcuni Paesi la creazione e/o la diffusione di programmi nocivi è divenuta un reato dopo l'introduzione di misure di legge contro i crimini informatici, la cui mancanza in Italia è da considerare una grave lacuna; inoltre, identificando gli autori dei virus, i ricercatori sperano di spingerli a collaborare — se si tratta di persone ragionevoli — per debellare le versioni «hackerate» delle loro creazioni, trasformate ad opera di vandali sconosciuti per aggiungere o aggravare gli effetti nocivi.

Come abbiamo annunciato nello scorso numero, una di queste investigazioni è andata in porto grazie alle capacità... sherlockiane di uno tra i più conosciuti ricercatori antivirus, l'islandese Fridrik Skulason.

L'indagine è partita da un'analisi approfondita del virus noto come «Den Zuk». Si riteneva erroneamente (e vedremo perché) che questa frase fosse in lingua olandese, in cui significa «la ricerca». Ricerca di cosa? Di altri virus, ovviamente, dato che una delle attività principali del virus Den Zuk consiste proprio nella ricerca dei ceppi Brain e Ohio; se uno di questi virus viene identificato, Den Zuk lo rimuove e lo sostituisce con una copia di se stesso.

Il nome del virus proviene dall'immagine che lo stesso virus fa rapidamente apparire e scomparire sul video quando vengono premuti Ctrl-Alt-Del. Lo strano simbolo alla destra della lettera «K» era ritenuto un marchio di qualche sconosciuta ditta o gruppo.

Disassemblando il virus si trova, in chiaro, il seguente testo, che peraltro non viene mai scritto sul video:

Welcome to the
C l u b
–The HackerS–
Hackin'
All The Time

The HackerS

Il virus infetta il boot sector, sia su dischi fissi che su dischetti. Il contenuto originario del boot sector viene spostato nella traccia 40 del settore 0, non utilizzato sui dischi da 5 1/4" da 360 Kb, ma utilizzabile sui dischi da 3 1/2" o sui dischi da 5 1/4", 1,2Mb. Inoltre l'etichetta di volume, che viene modificata dal virus Brain in «(c) Brain», viene ulteriormente cambiata dal Den Zuk che la trasforma in Y.C.1.E.R.P. una sigla che non aveva fornito nessuna indicazione in un primo tempo, ma che risulta condurre direttamente all'identità dell'autore del virus: ora si vedrà in che modo.

Si è anche visto come un'altra attività del Den Zuk consista nella rimozione del virus Ohio, che era ritenuto — correttamente — una versione precedente dello stesso Den Zuk. L'analisi comparata dei due virus mostra parecchie analogie, tra cui un testo in chiaro leggermente diverso:

V I R U S
b y
The Hackers
Y C 1 E R P
D E N Z U K O
Bandung 40254
Indonesia

(C) 1988, The Hackers Team....

Ecco quindi svelato il mistero: il nome corretto è «Den Zuko». Si trattava ora di scoprire chi si nascondesse dietro questo pseudonimo.

Qualsiasi radioamatore riconosce la sigla YC1ERP come un possibile nominativo radioamatoriale. Con una semplice ricerca sull'International Callbook Skulason scoprì che tale nominativo esiste, e risulta assegnato a un radioamatore residente a Bandung, Indonesia. Il gioco era fatto.

A questo punto Skulason decise di scrivere a questo radioamatore per chiedergli se in qualche modo egli fosse connesso con lo sviluppo di questo virus; la risposta (che non pubblicheremo per intero per ragioni di spazio) fu cortese, completa ed esauriente.

Il nome completo del radioamatore-autore del virus è Denny Yanuar Ramdhani, detto dagli amici «Denny Zuko» (da «Danny Zuko», che è il nome del personaggio interpretato da John Travolta nel film «Grease»), o per brevità Den Zuko. Studente universitario di informatica, svolge attività di programmatore freelance.

Ammette di aver sviluppato i virus Ohio (che lui chiama «Hackers») e Den Zuko nel marzo 1988, nel corso di una serie di esperimenti sui sistemi operativi su personal computer, sui linguaggi di basso livello, e sulla rapidità di diffusione dei virus; l'inclusione del suo alias nel virus era un modo di «salutare» i suoi amici ogni volta che veniva premuto Ctrl-Alt-Del. In aggiunta a ciò, Ramdhani fornisce altre informazioni tecniche sulle proprie creazioni. Da quanto scrive sembra che anche in Indonesia ferva l'attività di sviluppo di virus.

Non risulta siano state prese particolari misure contro Ramdhani.

cancellazione totale dell'applicazione infetta e alla successiva reinstallazione a partire dai dischi originali. È un procedimento più rapido, ma non garantisce la certezza totale dell'eradicazione del virus dal sistema. Infatti il virus potrebbe aver comunque infettato altri programmi eseguibili, contenuti in diverse directory. E in ogni caso è raccomandabile eseguire la procedura di disinfezione radicale, descritta nel prossimo paragrafo.

Disinfezione degli altri ambienti

Le procedure descritte qui sopra consentono all'utente di ottenere nuovamente un ambiente di lavoro libero da virus.

Ma non è sufficiente disinfettare l'ambiente di lavoro, come ben sanno alcune vittime di virus che hanno visto rispuntare le infezioni a distanza di giorni, mesi e talvolta anche anni.

L'ambiente da cui un virus si fa ospitare, come si è visto, è costituito da un programma eseguibile. Come per qualsiasi altro tipo di file, il supporto per i programmi eseguibili è costituito dai dischetti o dai dischi fissi. La facilità con cui possono essere fatti circolare questi supporti, specialmente i dischetti, e per conseguenza i file in essi contenuti motiva in parte la grande diffusione che ha avuto l'informatica personale nello scorso decennio.

D'altro canto si è visto come l'attività di molti virus abbia inizio con un periodo di latenza, durante il quale la presenza del virus passa del tutto inosservata e questi si limita a riprodursi. Questa è la fase in cui l'utente ha la massima possibilità di diffondere il virus, specialmente se egli fa ampio uso di programmi su dischetti.

Alcuni virus — ad es. lo Stoned — non richiedono nemmeno che vengano eseguiti programmi dai dischetti che usano come veicolo per l'infezione: è sufficiente introdurre un dischetto e accedervi, perché esso venga infettato. Se poi il dischetto infetto viene lasciato chiuso in un drive, per disattenzione, all'atto dell'avvio di un diverso sistema, quest'ultimo si infetta.

È molto probabile pertanto che l'utente il cui computer è stato vittima di un'infezione sia in possesso di un certo numero di dischetti anch'essi infetti. Tali dischetti dovranno essere verificati uno ad uno; questa può essere la procedura più gravosa e costosa di tutta l'attività di disinfezione, ma una corretta disinfezione totale assicura contro il rischio di infezioni recidive a distanza di tempo.

È consigliabile spendere qualche tempo per effettuare un'operazione radicale quando il problema è ancora ben presente nella mente di tutti coloro che ne sono stati colpiti, piuttosto che non rimandare a un secondo tempo un'operazione noiosa e apparentemente improduttiva con il rischio di trascurarla e

I virus nel mondo

Nello scorso settembre (MC 99, pp. 60-61) mostravamo un'analisi dei virus per zona geografica di provenienza. A nove mesi di distanza la situazione si è modificata con una rapidità preoccupante.

I ceppi conosciuti quando fu scritto il precedente articolo (luglio 1990) erano circa 110, attualmente (maggio 1991) sono più del doppio, dato che se ne contano oltre 260. Molti di questi ceppi poi danno luogo a diverse varianti, che portano il numero totale di virus a poco meno di 500.

L'imprecisione è d'obbligo quando si tratta di numeri di virus, dato che non esiste una tassonomia ufficiale e non vi è nemmeno un coordinamento tra gli sforzi dei ricercatori, che agiscono separatamente e indipendentemente, con il risultato che talvolta i loro risultati non coincidono.

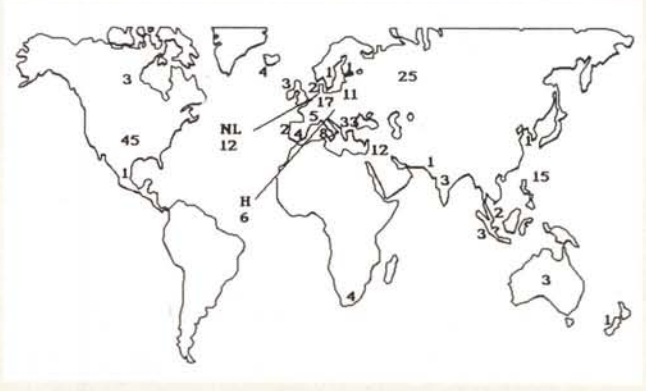
Rispetto alla situazione di nove mesi fa, il primo dato che balza all'occhio è la preoccupante espansione dell'attività di sviluppo virale nei paesi dell'est europeo. A settembre si contavano otto virus bulgari, tre polacchi e uno sovietico; oggi la situazione è di 33 virus bulgari, 11 polacchi, 25 sovietici e sei ungheresi. Si potrebbe tentare un'analisi in chiave socio-politica di questo fenomeno, ma ce ne asterremo lasciando eventualmente il compito ad altri, più qualificati commentatori.

Anche nell'Europa occidentale i vandali informatici non sono rimasti inattivi: sei nuovi virus in Germania, quattro nei Paesi Bassi, sette in Italia, due in Svizzera e tre in Austria (questi ultimi due dati non compaiono sulla cartina per ragioni di spazio). In alcuni paesi i numeri sono diminuiti, per via del fatto che le indagini sull'origine dei virus hanno fornito risultati più precisi: ad esempio, in Spagna i virus sono scesi da 5 a 4 in quanto uno dei virus di presunta origine spagnola si è rivelato di provenienza portoghese.

In America l'esplosione del fenomeno è ancor più marcata: il numero di virus si è triplicato in nove mesi, passando da 14 a 45.

Anche in Asia e in Oceania sembra essere diffusa l'attività di sviluppo dei virus, sebbene appaiano diverse le motivazioni di chi li sviluppa (si veda il riquadro sul virus «Den Zuko»). Due virus in Malaysia, due nuovi virus in Australia, dodici nuovi virus nella prospera e tecnologicissima Taiwan.

Riportiamo il grafico apparso sul numero 99 di MCmicrocomputer (settembre '90).



Questo grafico mostra invece la distribuzione aggiornata dei virus.

di doverne sopportare le conseguenze a distanza di mesi o anni.

Ciascun utente troverà il modo migliore per le proprie necessità e per la propria organizzazione; di seguito è descritta una delle possibili sequenze di azioni:

— acquistare uno stock di dischetti nuovi, possibilmente con il jacket di un colore particolare, unico e distintivo. Sono in vendita dischetti delle marche più rinomate e affidabili, confezionati in jacket di diversi colori (rosso, giallo, blu, verde etc.); in alternativa, potranno essere utilizzati degli ordinari dischetti neri, opportunamente contrassegnati con un'etichetta che consenta di distinguerli a colpo d'occhio. Formattare i nuovi dischetti dopo aver completato la disinfezione dell'ambiente principale (disco fisso o dischetto master);

— copiare i «vecchi» dischetti, sospetti di infezione, sui «nuovi»; la copia dovrà essere effettuata file per file, e limitatamente ai soli file di dati. Non dovranno essere trasferiti i file COM o EXE o tutti quelli che possano contenere programmi eseguibili (OVL o simili). I programmi eseguibili che risiedevano sui dischetti dovranno essere reinstallati, o prelevati da copie sicuramente non infette;

— man mano che i dischetti vecchi vengono trasferiti sui nuovi, i vecchi dovranno essere individualmente riformattati. Potranno essere riutilizzati (p. es. per sequenze di backup) soltanto dopo che la procedura di disinfezione sarà stata completata;

— durante tutta questa procedura, si dovrà curare di non eseguire nessun programma dai dischetti, e di non lasciare mai nessun dischetto nel drive quando il sistema viene acceso. Queste precauzioni sono fondamentali.

A questo punto per l'utente inizia il periodo di «vigilanza». Si è riscontrato con frequenza che una gran parte delle reinfezioni provenivano da un dischetto, dimenticato per qualche tempo sotto una pila di carte, che rispuntava all'improvviso dopo mesi o anni, quando l'infezione originaria era stata ormai dimenticata. Inserito in un drive e utilizzato, il dischetto aveva ovviamente ritrasmesso l'infezione causando nuovamente tutti i problemi già sperimentati in passato. Questo è il motivo per cui si consiglia l'acquisto di dischi di un particolare colore: in questo modo l'utente potrà accorgersi immediatamente della presenza di un disco sospetto, genericamente nero, in mezzo ai nuovi dischi tutti di un particolare colore.

Questa precauzione vale ben poco nel caso in cui un utente abbia frequenti scambi di dischi con altre persone, dato che è piuttosto poco probabile che questi utilizzino dischi dello stesso colore. In ogni caso, gli scambi frequenti costituiscono proprio uno dei comportamenti a rischio per la diffusione dei virus, e andrebbero effettuati con particolare cautela.

MC

Nel prossimo numero

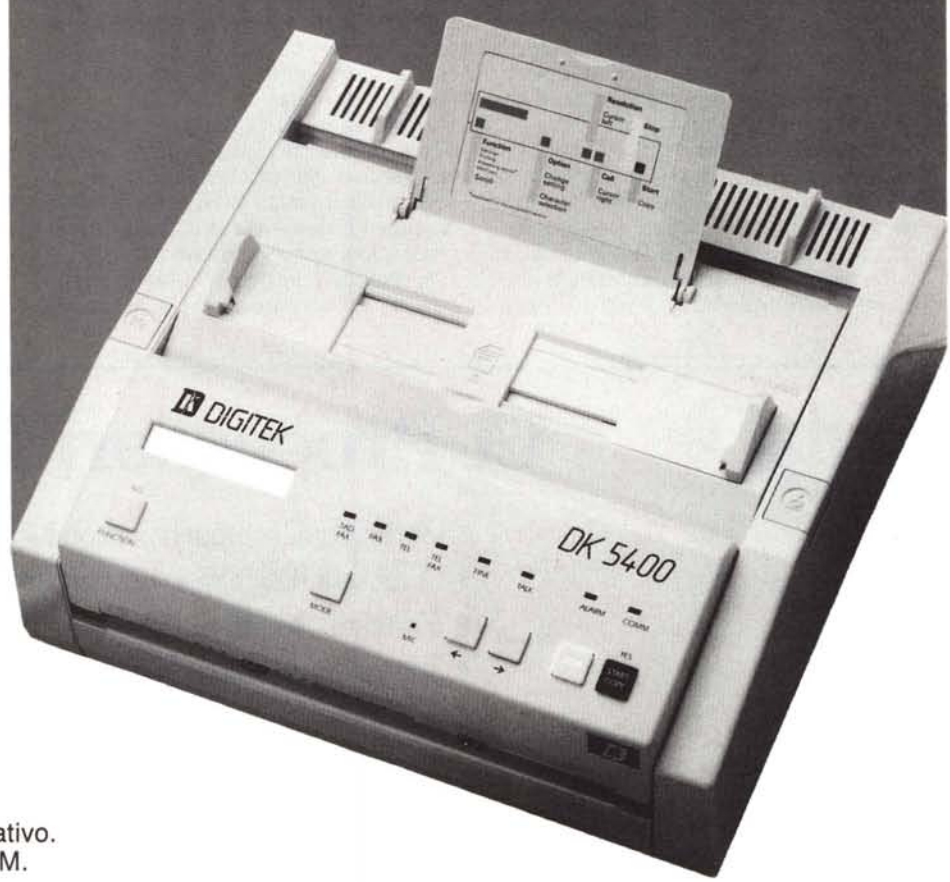
Gli argomenti che verranno affrontati nel numero di luglio/agosto riguardano i diversi aspetti del problema della protezione contro i virus.

L. 1.165.000
Versione Base
IVA ESCLUSA

DIGITEK

DK 5400

L'ALTERNATIVA INTELLIGENTE



Il fax intelligente che cresce secondo le Vostre esigenze, il DK 5400 è il primo terminale facsimile che mediante una serie di optional può implementare le proprie funzioni.

Funzioni del Modello Base

- Interfaccia RS 232.
- Ricezione selezionabile automatica/manuale.
- Identificativo utente.
- Commutazione automatica della comunicazione in arrivo su fax o telefono.
- Report di trasmissione, singolo e di gruppo.
- Rapporto di errore.
- Controllo risoluzione.
- 16 Tonalità di grigio.
- Funzione di copia.
- Richiesta di comunicazione.
- Autodiagnosi.
- Display LCD a 16 cifre.
- Identificazione segnali di allarme.

Gli Optional

- Telefono multifunzione.
- Interfaccia RS 232 & SoftWare operativo.
- TAD, risponditore e segreteria in RAM.

Telefono opzionale DK 7345, 14 numeri memorizzabili di cui 4 a chiamata rapida e 10 con selezione a due cifre, tastiera in gomma antisdrucciolo con tasti illuminati.

Al DK 5400 è possibile installare l'opzione SoftWare; questa Vi permetterà oltre ad una completa e sofisticata gestione della Vostra messaggistica, l'impiego del DK 5400 come Scanner e Stampante di sistema.

TAD, Telephon Answering Device, una opzione che Vi permetterà, a Vostra scelta, di utilizzare il DK 5400 come un risponditore o come una segreteria telefonica digitale. Avrete la possibilità di registrare, nella funzione risponditore, un messaggio della durata di 72 secondi. Nella funzione di segreteria potrete registrare un messaggio di 18 secondi e potrete ricevere quattro messaggi da 18 secondi cadauno. Il tutto automaticamente.

DIGITEK

Via Valli, 28 - 42011 Bagnolo in Piano (RE)
Tel. (0522) 951523 - Fax (0522) 951526 - Telex 530156 I