

## Il virus «benigno»: un mito duro a morire

di Stefano Toria

*Continuiamo a leggere, sia su carta che su conferenze telematiche, articoli e discussioni sulla possibilità di scrivere un virus «benigno», cioè un programma che abbia le caratteristiche di autoreplicazione tipiche del virus ma che anziché portare con sé un cavallo di Troia — situazione tipica del virus «maligno» — porti anzi degli effetti positivi. Un programma di questo genere ci è persino giunto in redazione, da parte di un lettore del quale, per comprensibili ragioni, non faremo il nome. Vedremo in questo articolo per quale ragione non è mai possibile parlare di virus benigni, e perché qualsiasi virus è per definizione un aggressore da cui difendersi e il suo autore nella migliore delle ipotesi una persona poco accorta, nella peggiore un criminale*

### Una lunga lista di virus «buoni»

La prima documentazione su un virus è reperibile nel saggio «Computer Viruses, Theory and Experiments»<sup>1</sup>, di Fred Cohen. Nel suo lavoro, Cohen manifestava il suo interesse per una nuova tecnologia di software autoreplicante, la quale sembrava in grado di offrire numerosi vantaggi, pur non tralasciando di esprimere il dubbio che si potesse anche fare un uso dannoso della medesima tecnologia.

Cohen non poteva immaginare, nel 1984, che soltanto pochi anni dopo i virus sarebbero diventati quel problema con cui qualsiasi utente di personal computer deve bene o male confrontarsi, per uscirne spesso perdente. Eppure egli era animato dalle migliori intenzioni, esattamente come molti altri dopo di lui.

Uno dei primi a scrivere un virus intenzionalmente benevolo nei suoi intenti fu Denny Yanuar Ramdhani. Ne abbiamo parlato nel numero 108, nel giugno dello scorso anno: è l'autore del virus che inizialmente avevamo chiamato «DEN ZUK» e poi, più precisamente, «DEN ZUKO». Questo virus, nella sua versione originale, verifica se sul disco ospite sono presenti i virus Ohio e Brain ed eventualmente li sostituisce con una copia di se stesso. Identificato da un ricercatore islandese Ramdhani affermò di aver scritto il virus per misurare le proprie capacità come programmatore Assembler, aggiungendo una schermata grafica per «salutare» i suoi amici di Bandung in Indonesia. La tecnologia autoreplicante veniva utilizzata per la prima volta per uno scopo dichiaratamente utile anziché per danneggiare un numero imprecisato di computer.

Altrettanto animato da buoni intenti sembrerebbe essere stato Ralf Burger,

che nel 1987 pubblicò in Germania la prima edizione di un libro che successivamente apparve negli Stati Uniti con il titolo «Computer Viruses — a High Tech Disease»<sup>2</sup>. Burger incluse nel proprio libro il disassemblato di alcuni virus effettivamente funzionanti, tra cui il «Vienna», allo scopo dichiarato di favorire lo studio di questo fenomeno e lo sviluppo di misure antivirus. In realtà Burger non era l'autore dei virus che pubblicava, e si limitò a riportare informazioni che aveva prelevato altrove. Tuttavia il suo libro fece scalpore tra i ricercatori antivirus più per l'irresponsabilità con cui un simile materiale era stato fatto circolare che per il valore del suo contenuto, piuttosto scarso per la verità.

Lo stesso Burger, nel suo libro, affermava che i virus «correttamente utilizzati potrebbero portare alla creazione di una nuova generazione di sistemi operativi automodificanti». Prestando fede alle proprie parole, Burger fece circolare dei dischetti con un programma-virus dimostrativo, dal nome poco originale di VIRDEM.

Il caso forse più noto tra quelli di questo genere riguarda un sedicente «ricercatore antivirus», ben noto alla comunità degli autentici ricercatori. Il suo solo lavoro di ricerca sembrerebbe essere consistito nello sviluppo di una intera famiglia di virus, con il fine dichiarato di produrre un virus che sfugga completamente ad ogni possibilità di identificazione. A questo punto è necessario aprire una parentesi.

Abbiamo visto in alcuni degli articoli già pubblicati come uno dei metodi cor-

<sup>1</sup>7th Security Conference, DOD/NBS sett. 1984, rist. in *Computers & Security*, vol. 6 (1987), pp. 22-35.

<sup>2</sup>1989, *Abacus*, 5370 52nd St. SE, Grand Rapids, MI 49508, USA.


 DEN ZUK

rentemente utilizzati per difendersi dai virus, ancorché non sia efficace al 100%, consiste nell'utilizzo di un programma di scansione che esamina il contenuto di un disco alla ricerca di particolari sequenze esadecimali che sono state riconosciute come univocamente appartenenti a uno specifico virus. Ripetendo l'operazione su ciascun file con tutte le sequenze note si riesce (teoricamente) a identificare qualsiasi virus tra quelli conosciuti.

Questo fatto è ben noto a chi sviluppa virus. Negli ultimi tempi è invalsa l'abitudine di produrre virus che in qualche modo tentano di difendersi dai programmi di scansione, mettendo in atto tecniche di crittografia del codice eseguibile del virus, con una chiave che non sia sempre la stessa in modo da ottenere in ciascuna infezione una diversa configurazione della rappresentazione su disco del codice eseguibile del virus.

Questo metodo funziona soltanto in parte; per poter essere decrittato un virus deve necessariamente iniziare con delle istruzioni «in chiaro», cioè non crittografate, che possano essere eseguite direttamente dalla CPU e che servano a decrittare il resto del virus. Ebbene, sia il mini-programma di decrittazione che il programma stesso (una volta decrittato e residente in memoria) possono essere identificati da un programma di scansione sufficientemente accorto.

Lo scopo perseguito da questo ricercatore è di realizzare un virus che sia realmente impossibile da identificare, per esplorare i limiti dei programmi di scansione. Attualmente infatti la maggior parte delle misure di difesa antivirus disponibili sul mercato consiste in programmi di scansione. Così facendo questo ricercatore ritiene di rendere un servizio alla collettività, sottoponendo gli sviluppatori di software antivirus a

una sfida continua contro le maggiori difficoltà che potrebbero teoricamente incontrare nella propria attività.

Un virus «benigno» ci è stato recapitato anche qui in redazione. Nelle note che accompagnavano il programma l'autore manifestava la sua intenzione di servirsi di un virus per diffondere messaggi dal contenuto promozionale. L'esempio che ci è stato inviato conteneva infatti un testo in favore dell'acquisto di copie originali del software.

L'ultimo in ordine di tempo a credere nella possibilità di servirsi dei virus a fin di bene è stato lo stesso Fred Cohen. Sugli ultimi numeri di alcune autorevoli pubblicazioni, tra cui ad esempio *NetWare Solutions*, Cohen bandisce un concorso per autori di virus. Il primo premio consiste nella somma di \$ 1.000, donata dalla ASP, società di cui Cohen è fondatore e presidente. L'opinione di Cohen è che sia ancora possibile fare un uso positivo della tecnologia del software autoriproduttore.

### **Ma le cose non stanno così**

Purtroppo tutte queste benevole intenzioni da parte di persone più o meno seriamente intenzionate a far del bene all'umanità non tengono conto di un fatto essenziale e fondamentale: il software autoriproduttore per definizione si riproduce senza l'intervento

dell'uomo, e così facendo circola liberamente fino a raggiungere persone che non sono animate dagli stessi intenti benefici degli originari autori, persone che spesso sono mosse da motivazioni di senso del tutto opposto.

Quello che un uomo ha fatto un altro può riprodurre, diceva Sherlock Holmes nel racconto «I pupazzi danzanti». E il virus scritto da una persona può essere agevolmente modificato da un'altra. Chiunque possieda anche dei rudimenti di linguaggio macchina è in grado di prendere un virus che nella sua versione originaria si limita a scrivere «Buon compleanno» sul video, e modificarlo perché in luogo della scritta esegua una formattazione a basso livello del disco fisso.

È nostra ferma e convinta opinione che molti dei virus attualmente noti, o meglio delle varianti, non esisterebbero se non fossero esistiti i virus originari da cui traggono origine. Peraltro la nostra opinione è confermata da una montagna di prove documentate dell'avvenuta mutazione di virus sedicenti «benigni» in virus maligni e dannosi. Non è esattamente la cosa più semplice di questo mondo scrivere un programma autoreplicante, e richiede delle capacità di programmazione che non sono alla portata di chiunque possieda un personal computer. Richiede una buona conoscenza del funzionamento

del sistema operativo e la disponibilità di parecchia documentazione, talvolta difficile da trovare. Mentre fare una piccola modifica a un programma già esistente e funzionante è molto più semplice. Abbiamo già parlato in passato di questo problema, quando abbiamo sconsigliato di mantenere «collezioni»

di virus. Eravamo, e restiamo, dell'opinione che un virus è sempre un intruso, spesso un fastidio e non di rado un pericolo, e che far circolare inavvertitamente un virus è una grave colpa. Farlo circolare deliberatamente è un crimine, anche se le leggi del nostro Stato ancora non si sono conformate a quelle

attualmente in vigore nei Paesi più avanzati sotto questo punto di vista e se nessun Tribunale italiano condannerebbe l'autore di un simile atto. Non ancora, almeno. MSS

*Stefano Toria è raggiungibile tramite Mc-link alla casella MC0170.*

## Tavola rotonda con John McAfee

Si è svolta il 15 gennaio alle 3 di notte (ora italiana) su CompuServe la prima tavola rotonda telematica con John McAfee. L'autore di SCANVIRUS e dei programmi accessori non ha bisogno di presentazioni presso chi segue questa rubrica; ricercatore antivirus da anni, fondatore e presidente della Computer Virus Industry Association (CVIA) e quotatissimo consulente per la sicurezza dei sistemi informativi, McAfee si è intrattenuto per un'ora con una trentina di utenti di CompuServe su temi vari inerenti la minaccia dei virus. Abbiamo ottenuto da CompuServe e dallo stesso McAfee l'autorizzazione di riprodurre parti della conferenza.

**S**i ricevono in continuazione annunci di nuovi virus, sia dai vostri programmi che da altre fonti. È necessario tenere gli occhi aperti per ciascun nuovo virus oppure possiamo aspettarci di trovare sempre gli stessi 10-20 virus nella maggior parte dei casi di effettiva infezione?

**T**ra i virus che conosciamo, quelli effettivamente circolanti sono circa il 10%. Tuttavia una certa percentuale di nuovi virus prima o poi diventerà una potenziale minac-

cia. Poiché non possiamo stabilire in anticipo quali virus circoleranno, dobbiamo tenerli d'occhio tutti.

**S**i sono mai verificati casi di ROM infette? Gli attuali metodi di identificazione dei virus sono in grado di riconoscere questi casi?

**N**on risulta si sia mai verificata un'infezione di ROM a tutt'oggi. Naturalmente è possibile che questo accada se si infetta il programma che deve essere registrato nella ROM. Se dovesse succedere, provvederemo ad aggiornare SCAN in modo da identificare la presenza di questo virus.

**Q**ual è il peggior virus in circolazione?

**Q**uesta è una domanda interessante. Abbiamo appena ricevuto un nuovo virus che si chiama «Pogue», che è crittografato con un algoritmo estremamente complesso. Serviranno delle tecniche di indagine completamente nuove per identificare le varianti di questo virus.

Ci stiamo tuttora lavorando, e ne sapremo di più tra qualche giorno.

**C**i sono in prospettiva degli accordi nell'industria del software per standardizzare le denominazioni dei virus?

**S**i è tenuta lo scorso novembre la conferenza della NCSA (National Computer Security Association, N.d.R.). Tutti i produttori di programmi antivirus presenti alla conferenza si sono accordati per utilizzare le denominazioni fornite dal VSUM di Patricia Hoffman. Confidiamo che entro la prossima estate tutti si saranno adeguati.

**Q**uali sono secondo lei le procedure più adatte a identificare e rimuovere eventuali virus in aziende di medie o grandi dimensioni?

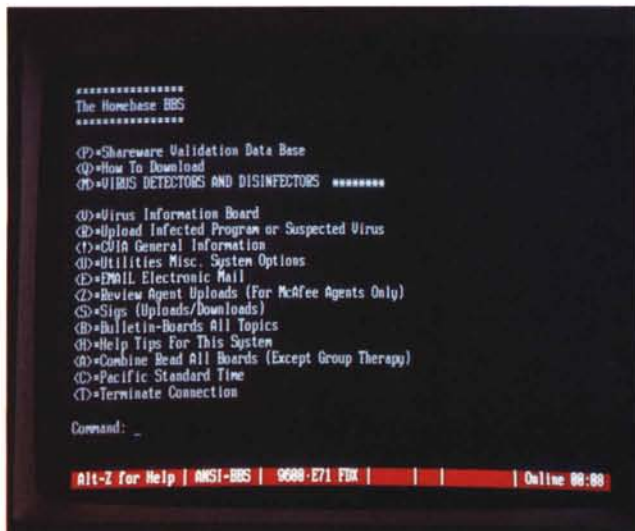
**T**utti gli utenti di PC dovrebbero essere dotati di un programma di scansione e istruiti sull'uso da farne. Dovunque le condizioni lo permettono dovrebbero essere installati programmi residenti di protezione antivirus. I programmi di rimozione tuttavia non dovrebbero essere forniti agli utenti finali. La rimozione di un virus è spesso un'operazione delicata e dovrebbe essere gestita dal personale di supporto tecnico della stessa azienda. Inoltre quando un virus colpisce la direzione dovrebbe essere informata; se vengono forniti i programmi di rimozione direttamente agli utenti, è possibile che la direzione non venga mai a conoscenza del rischio potenziale.

**S**i dice che la CVIA abbia riscontrato nel solo 1990 oltre 300.000 casi di infezione. Ci potrebbe fornire qualche informazione in più?

**N**ello scorso anno abbiamo registrato oltre 750.000 PC infettati.

**R**itiene che i programmi di scansione stiano per raggiungere il loro limite fisico?

**L'**attuale tecnologia impiegata nel software di scansione è in grado di supportare ben oltre 30.000 tipologie diverse di virus. Adottando alcune modifiche all'architettura dei programmi si possono superare i 50.000 virus (i virus noti sono sotto il migliaio, N.d.R.). Con il tasso attuale di crescita dei virus dovremmo essere pronti a fronteggiare l'attività degli sviluppatori di virus per una buona parte del 21mo secolo.



*John McAfee, uno dei massimi esponenti mondiali di virus, è fondatore e presidente della CVIA (nella foto: "The home base", il BBS della CVIA).*

