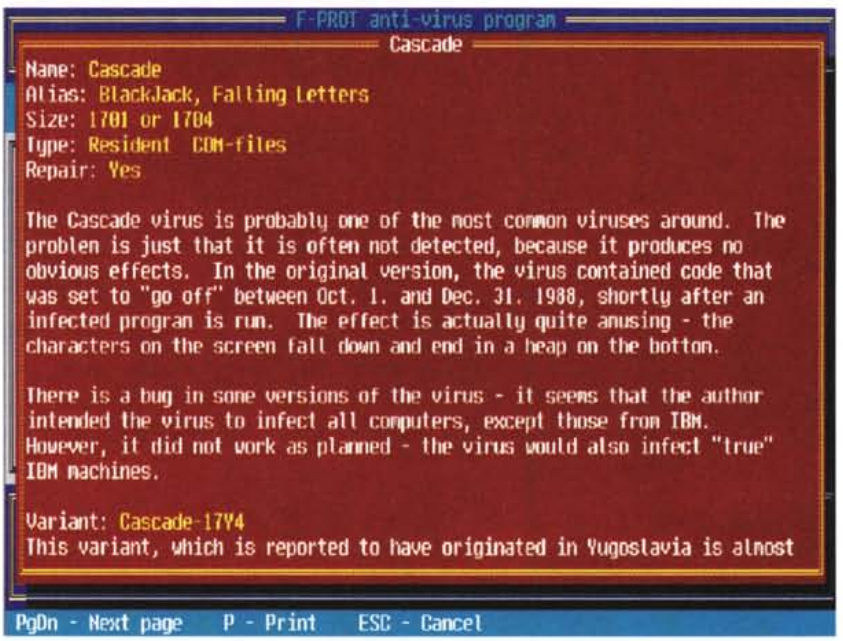
Come nasce un virus

Dopo aver esaminato le diverse tipologie di virus, in questa seconda parte del «corso» sui virus cercheremo di spiegare le ragioni del problema, che apparentemente è nato dal nulla

di Stefano Toria



Come si fabbrica un virus

No, non abbiamo alcuna intenzione di passare dall'altra parte dell'immaginaria linea del fronte e metterci a dare consigli a chi voglia andare a incrementare le schiere, già fin troppo nutrite, degli autori di virus. In questi paragrafi cercheremo di delineare quali sono gli strumenti che ha a sua disposizione chi vuole scrivere un programma autoreplicante.

Chi venga a contatto per qualsiasi motivo con il problema virus incontra presto le «varianti». Il concetto è anch'esso preso a prestito dalla biologia, come lo stesso concetto di virus d'altronde. Ma se le varianti dei virus biologici nascono dal naturale processo di mutazione genetica, le cui leggi sono spiegate solo in parte e dipendono in buona percentuale dal caso, per i virus che minacciano i nostri computer le varianti sono sempre opera di qualcuno che, non sapendo o non volendo scrivere un virus nuovo, si limita a prenderne uno esistente e a modificarlo.

Non è affatto difficile, e tutto ciò che occorre è uno strumento facilissimo da reperire, potente e semplice da usare, ossia il DEBUG che viene distribuito con tutte le copie delle diverse versioni di DOS. Servendosi del DEBUG chiunque abbia una conoscenza anche rudimentale della programmazione in Assembler può esaminare un virus e modificarlo.

I casi più frequenti di modifiche all'immagine binaria di un virus consistono nell'alterazione dei suoi effetti. Sappiamo che affinché un programma possa definirsi «virus» è sufficiente che sia capace di replicarsi ogni volta che viene eseguito; non sono pochi i virus esistenti che si limitano a replicarsi, ma è assai frequente che un virus abbia degli effetti collaterali, che in alcuni casi sono divenuti celebri: dai caratteri in discesa libera del Cascade, alla pallina del PingPong, alla finestrella del Jerusalem, fino alle decine – o meglio, centinaia – di virus che in un modo o nell'altro distruggono i dati contenuti nel disco fisso.

La cosa più semplice che possa fare chi voglia provare il discutibile brivido della clandestinità e ritenga di consegnarsi alla celebrità generando un virus consiste appunto nel modificare gli effetti di un virus di cui sia venuto in possesso. Gli esperti oramai hanno seri problemi nel classificare l'ennesima variante di Cascade o Jerusalem, per i quali siamo arrivati ad alcune centinaia di variazioni esistenti. Poiché si tratta di virus diffusissimi, è facile venirne in possesso; oramai tutti sanno come decodificare e ricodificare il Cascade, nel caso del Jerusalem non c'è nemmeno questo problema, e quindi ecco che quasi ogni mese tocca registrare un nuovo figlio di queste già sovraffollate famiglie.

Modificare un virus negli effetti collaterali, abbiamo detto, è molto semplice. In particolare è semplicissimo avviare la procedura di formattazione a basso livello del disco fisso, richiede poche istruzioni e per modificare un virus esistente affinché alla sua attivazione formatti il disco anziché fare ciò che aveva previsto originariamente il suo autore servono soltanto pochi minuti. È comprensibile quindi come siano notevolmente più diffuse le varianti ai virus esistenti rispetto ai virus di nuova generazione.

In alcuni casi peraltro è dimostrabile come un determinato virus tragga origine da un altro ma non per via di una semplice modifica ai suoi effetti o a qualche altra parte trascurabile del codice, quanto piuttosto per effetto di un'opera più approfondita. In alcuni casi

il virus originario è stato disassemblato, modificato nella forma simbolica (cioè in Assembler) e poi nuovamente compilato. In altri casi le modifiche possono essere state effettuate direttamente sull'immagine binaria, ma l'autore della correzione non si è limitato a piccoli ritocchi al codice.

Un esempio è dato proprio dal Cascade. La versione originale, lunga 1701 byte, contiene le istruzioni per effettuare un controllo sul BIOS del computer che sta eseguendo il programma, allo scopo di verificare se si tratta di un PC prodotto dalla IBM o di un'altra macchina. Nelle intenzioni dell'autore i PC IBM avrebbero dovuto essere risparmiati dall'infezione, che avrebbe dovuto per contro verificarsi nel caso di altre macchine. Ma in realtà per via di un errore il controllo non funziona, e quindi i PC IBM si infettano esattamente come tutti gli altri.

Esiste una versione modificata, lunga 1704 byte per via dell'aggiunta di una istruzione, nella quale l'errore che impedisce il funzionamento del controllo descritto poc'anzi è stato eliminato. O meglio: qualcuno ne ha tentato l'eliminazione, ma senza riuscirvi, e quindi il Cascade.1704 è perfettamente in grado di infettare le macchine IBM esattamente come il Cascade.1701. Ma non è questo che ci interessa, quanto l'idea che qualcuno abbia potuto fare una correzione a un errore in un virus, proprio come un produttore di software fa circolare una nuova release del proprio prodotto dopo averne eliminati gli errori rilevati dagli utenti.

Non è possibile tuttavia stabilire se la modifica sia stata effettuata dallo stesso autore del virus servendosi dei simboli originali, ovvero da qualcun altro che abbia agito sull'immagine binaria del virus.

In molti casi accade che qualcuno, intenzionato a scrivere un virus, cerchi di semplificare il proprio lavoro attingendo al lavoro altrui.

Normalmente un'azione di questo genere sarebbe da considerarsi molto scorretta e probabilmente anche passibile di sanzione penale, ma è evidente che i sonni di chi scrive un virus sono ben poco turbati da considerazioni di questo genere.

Pertanto chi studia un virus come ad es. il Michelangelo vi troverà notevoli somiglianze con lo Stoned, perché presumibilmente il suo autore ha preso alcune parti di quest'ultimo virus e se ne è servito per creare il proprio capolavoro; lo stesso avviene per l'Invisible Man, derivato dal Flip, e così per i virus della famiglia Vienna, etc..

In queste circostanze peraltro si preferisce parlare di nuovi virus, piuttosto che di varianti. Infine vi è il caso di chi scrive un virus partendo da zero, e pertanto crea un «prodotto» (se così lo si può definire) del tutto originale.

I limiti degli antivirus

C'è da aspettarsi delle uscite dal mercato degli antivirus, scrivevamo un anno e mezzo fa. C'è da aspettarsene ancora molte altre da oggi, ora che il ritmo di crescita del numero di virus si è stabilizzato intorno al centinaio al mese e che molti programmi di scansione sembrano lì lì per scoppiare. Ma esaminiamo brevemente come è fatto un antivirus.

Nella sua forma originaria un antivirus non era altro se non un programma di ricerca e confronto di stringhe. Da una parte il motore, dall'altra le stringhe, ad ogni nuovo virus scoperto bastava aggiungere la relativa stringa, in quei bei tempi in cui non esistevano né polimorfismo né stealth, tempi andati per sempre che non torneranno più.

Man mano che cresceva il campionario di virus cresceva anche il database delle stringhe. Poi sono comparsi i primi virus codificati, poi quelli polimorfi come il 1260 e suoi successori, e i produttori di antivirus per rimanere sul mercato si sono dovuti adattare: non più un database di firme ma un insieme di «regole», atte a stabilire se il dato file contiene o meno il determinato virus.

Poi a complicare le cose ci si è messo Dark Avenger con il suo MtE, prontamente seguito da vari epigoni, e le «regole» sono divenute via via più complesse.

I limiti dei programmi antivirus consistono oggi in due ordini di problemi: la complessità delle regole identificative necessarie a scoprire parecchi virus, e la impressionante massa di virus nuovi che arrivano ogni giorno. Per poter mantenere i propri livelli di efficacia gli antivirus debbono riuscire a vincere questa lotta impari, che si combatte su due fronti scombinati, su uno dei quali vi è di volta in volta un solo combattente, isolato e ben in luce, e sull'altro i combattenti sono centinaia, sconosciuti e nell'ombra. E ciascuno di essi può colpire duro, come dimostra lo scenario descritto appresso.

Immaginiamo che un'azienda, per esempio una banca, abbia speso alcune decine di milioni per acquistare un numero adeguato di licenze per l'antivirus XYZ. Installazione e formazione del personale aumentano il costo totale dell'antivirus, andando a sommarsi al prezzo di acquisto delle licenze. Gli aggiornamenti vengono ricevuti regolarmente e immediatamente fatti circolare tra gli utenti, che li installano subito. Gli stessi utenti provvedono a un uso ottimale dell'antivirus.

Una situazione idilliaca, quale non riuscirei a sognare nemmeno se mio figlio, di un mese e mezzo, mi lasciasse dormire di notte.

L'idillio viene rotto da un virus, sviluppato dagli amici del figlio di un funzionario che viaggia tra ufficio e casa con un portatile, agganciato normalmente alla rete locale dell'ufficio.

Il virus trova la strada aperta per passare dal portatile al server, dal server a tutte le macchine installate. Poiché si tratta di un virus nuovo, l'antivirus non segnala nulla. Cinque giorni dopo il virus si attiva, distruggendo abbastanza informazioni sui dischi fissi di tutti i PC colpiti da rendere inutilizzabile ciò che resta.

I responsabili della banca se la prenderanno ovviamente con il povero antivirus XYZ, colpevole di non aver segnalato il problema per tempo. E ovviamente provvederanno ad acquistarne uno diverso.

Non sempre le storie finiscono così ma si tratta comunque di uno scenario assai verosimile, reso ancora più verosimile da un fatto, che probabilmente a molti sarà sfuggito: che l'Italia è oggi ai primi posti nel mondo per lo spiacevole primato dello sviluppo di nuovi virus. Non più la Bulgaria, dove le acque si sono calmate ormai da quasi due anni, non più gli Stati Uniti ma proprio il nostro paese è divenuto un centro di produzione di programmi aggressori.

Per questa ragione quella che prima sembrava un'ipotesi astratta, cioè di essere colpiti da un virus sconosciuto agli antivirus, è divenuta un rischio concreto, con il quale è urgente confrontarsi.

Le soluzioni sono molteplici, e variano dal semplice affidarsi ad almeno due antivirus (difficilmente coincideranno le date di aggiornamento dei due prodotti, e uno sarà sempre più recente dell'altro) alla scelta oculata di strumenti alternativi rispetto ai programmi di scansione.

In alcuni casi (piuttosto estremi per la verità) può essere utile assicurarsi la collaborazione di un esperto programmatore in Assembler, che renda superfluo il ricorso ai programmi di scansione.

In ogni caso è fondamentale attribuire il giusto ruolo ai programmi di scansione, che non sono portatori di Verità Rivelate ma semplici strumenti, e come qualsiasi altro strumento vanno usati con il criterio e la supervisione di qualcuno che sappia come servirsene.

Stefano Toria

```
C:\UTY\VIRUS\F-PROT>debug f-prot.exe
-u
1757:0000 FC            CLD
1757:0001 06            PUSH    ES
1757:0002 1E            PUSH    DS
1757:0003 0E            PUSH    CS
1757:0004 8CC8          MOV     AX,CS
1757:0006 01063501      ADD     [0135],AX
1757:000A BAC31A        MOV     DX,1AC3
1757:000D 03C2          ADD     AX,DX
1757:000F 8BD8          MOV     BX,AX
1757:0011 055515        ADD     AX,1555
1757:0014 8EDB          MOV     DS,BX
1757:0016 8EC0          MOV     ES,AX
1757:0018 33F6          XOR     SI,SI
1757:001A 33FF          XOR     DI,DI
1757:001C B90800        MOV     CX,0008
1757:001F F3            REPZ
1757:0020 A5            MOVSW
-_
```

Un esempio di uso di DEBUG.

A supporto degli autori

Scrivere un virus non è alla portata di tutti. Occorre saper programmare in Assembler, e saper programmare bene; serve una discreta conoscenza delle funzioni del sistema operativo, e una considerevole quantità di documentazione. È indispensabile un assemblatore, un programma di debug e parecchio tempo a disposizione.

Occorre anche una certa predisposizione caratteriale, ma di questo parleremo tra breve.

Non tutti posseggono tutto il materiale elencato. La dotazione più frequente, a giudicare dai risultati, consiste... nella predisposizione caratteriale, che unitamente a DEBUG ha consentito la creazione di una buona parte dei virus esistenti.

In particolare difettano le capacità di programmazione. Scrivere due righe in Basic è alla portata di molti. Scrivere del buon codice in Assembler non lo è affatto, e la maggior parte dei virus che gli esperti si vedono recapitare hanno l'effetto di farli piangere dalla noia. Incompetenza, sciatteria, ignoranza sono le qualità che regnano sovrane tra i programmatori di virus.

Per ovviare a questo stato di cose vi è stato chi ha provveduto a mettere a disposizione degli aspiranti autori di virus dei veri e propri strumenti di CASE, di sviluppo di software assistito dallo stesso computer. VCS, Mutation Engine, VCL, PS-MPC, TPE, G^2 sono sigle note da tempo a chi studia i virus. Si tratta di strumenti che, in un modo o nell'altro, semplificano il lavoro di chi voglia scrivere un virus. In alcuni casi si tratta di funzioni di libreria da richiamare e includere in un virus sviluppato in proprio, in altri casi di ambienti di sviluppo con gradevoli interfacce-utente, che producono come risultato programmi pronti per essere compilati.

Ma chi sono questi autori?

La curiosità è legittima, ma nella maggior parte dei casi è destinata a rimanere insoddisfatta perché non vi è alcun modo di identificare l'autore di un virus, che può essere uno qualsiasi degli oltre cento milioni di utenti di personal computer compatibili in tutto il mondo.

Tuttavia le informazioni ottenute analizzando i virus, e i dati disponibili sui pochi virus di cui si conosca l'autore, permettono di identificare alcune categorie di personaggi che hanno tratti caratteriali diversi e motivazioni differenti:

– *hacker*, ossia i più esperti, spesso grandi appassionati di informatica, dotati di notevoli capacità e di una profonda cultura tecnica; una volta il termine hacker indicava il «superesperto», oggi piuttosto il «pirata», quello che penetra sistemi informatici senza essere autorizzato, che rimuove gli schemi di protezione dai programmi commerciali, che – appunto – scrive virus e cavalli di Troia;

– *studenti universitari*, spesso hacker, hanno accesso a grandi risorse informatiche e hanno mediamente molto tempo a disposizione; in molti casi vengono incoraggiati dagli stessi docenti a sperimentare, esplorare, tentare nuove vie;

– *computer club*, associazioni di appassionati o di utenti interessati alla cooperazione e allo scambio di esperienze; sono quasi sempre ambienti in cui regnano onestà e correttezza, ma in alcuni casi sono sorti con finalità dichiaratamente clandestine;

– non ci sono prove specifiche, ma si sospetta che alcuni virus siano stati scritti appositamente per colpire in situazioni particolari, per esempio da parte di *dipendenti insoddisfatti*.

Dopo che il virus è stato scritto

Così come non esiste una procedura standard per produrre un programma «buono», non vi è una serie di fasi codificate che l'autore di un virus segue per diffondere la propria creatura.

La diffusione del virus segue grosso modo due strade distinte a seconda che si tratti di un virus di boot sector o di un parassita; i virus multipartiti evidentemente le seguono entrambe.

Nel caso di un virus di boot sector l'autore può scegliere la strada di far circolare direttamente i dischetti infetti, oppure di servirsi di un programma intermedio che agisca da vero e proprio «untore», inserendo il virus nel boot sector del computer sul quale viene eseguito.

Per i virus parassiti i problemi sono minori perché far circolare un programma senza farsi notare risulta più facile: basta depositarlo in un BBS dopo essersi collegati in forma anonima, ed è in questo modo che prendono l'avvio la maggior parte dei nuovi virus parassiti o multipartiti.

Successivamente la circolazione del virus può essere favorita da diversi fattori: innanzitutto dal fatto che esistono, come abbiamo già detto, oltre cento milioni di computer compatibili in tutto il mondo; inoltre possono essere le stesse caratteristiche del virus a rendere più o meno agevole la sua circolazione. Infine il virus può andare soggetto a un vero e proprio «colpo di fortuna», capace di accelerarne la circolazione. È il caso del «Form», un virus come tanti altri ma che è riuscito a balzare in testa alle statistiche di diffusione proprio grazie a uno di questi «colpi di fortuna». È accaduto infatti che un noto produttore di supporti magnetici abbia distribuito una grande partita di dischetti preformattati per PC IBM, che erano stati inavvertitamente contagiati da questo virus. MC

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

PORT·ABLE *sound* PLUS™

QUALITÁ AUDIO CD SENZA ALCUN COMPROMESSO. ORA É POSSIBILE ANCHE SUL VOSTRO PORTATILE.

Ravvivate le vostre presentazioni, rendete più efficaci i vostri training e, perchè no, aggiungete un pó di pepe ai vostri giochi. Dovunque e sempre. Ora c´è PORT•ABLE Sound Plus, la prima vera periferica esterna portatile capace di qualità musicale CD a 16 bit stereo. Non vi serve essere un ingegnere e neppure usare un cacciavite. Collegatelo alla porta parallela per la vostra stampante del vostro PC IBM compatibile sia esso un portatile, un notebook o un desktop.

Ecco qualcosa di differente! Musica per le vostre orecchie: PORT•ABLE Sound Plus è dotato di tutto ciò di cui avete bisogno compreso un altoparlante hi-fi con microfono incorporato. Ospita ingressi CD e Registratore ed un´uscita per una coppia di altoparlanti attivi e non è tutto! Una porta parallela passante vi permette di non dover rinunciare alla vostra stampante. Credeteci non vi serve altro!

OMAGGIO!!!
SOFTWARE AGGIUNTIVI

DSP Registratore per Windows (utility su standard OLE). WinReader per Windows, una utility di sintesi vocale molto semplice. Applicazioni di sintesi vocali per DOSTalk e DosReader by DSP. Multimedia Show & Tell per ragazzi (opzionale).

- Compatibile Sound Blaster
- Qualità CD Audio a 16 bit
- Tecnologia Avanzata DSP

Distribuito da: Datamatic S.p.a. Via Agordat, 34 - Milano - Tel. 02/ 2871131 - Fax 02/ 2619243