Dal virus dos al virus "donna"

Roberto Turchetti

Un virus informatico è simile ad un virus biologico: si tratta di un piccolo programma contenente una sequenza di istruzioni di cui alcune deputate alla duplicazione dell'intero programma. Dopo l'iniziale fase "riproduttiva", una sorta di incubazione, i virus informatici cominciano a svolgere attività di varia natura: distruttive e/o di semplice ostruzionismo, comunque molto fastidiose.

I virus informatici, come quelli biologici, sono pericolosi per la tendenza che hanno a dare inizio a vere e proprie epidemie, soprattutto se un personal computer infettato fa parte di una rete locale (Intranet) o estesa (Internet). La diffusione avviene trasferendo file infetti da un computer ad un altro e, cosa ancor più grave, il loro effetto non sempre è immediatamente manifesto.

Mentre i virus della prima generazione attaccavano soltanto i file eseguibili (che nel sistema operativo DOS erano riconoscibili per l'estensione .COM o .EXE), i virus attuali riescono ad inquinare molti altri tipi di file; sono anche in grado di cambiare le istruzioni del BIOS caricate in RAM, di diffondersi attraverso gli stessi supporti fisici contenuti nel PC e di danneggiare fisicamente persino l'*hard disk*.

I virus informatici della prima generazione si diffondevano autoreplicandosi per mezzo degli stessi programmi che venivano inquinati. Tipicamente le funzioni da essi svolte erano due:

- dapprima copiavano se stessi in programmi non infettati;
- in seguito, dopo un prestabilito numero di esecuzioni, eseguivano le loro istruzioni specifiche che consistevano nella visualizzazione di messaggi, nella cancellazione o nella alterazione di file, fino alla cancellazione del contenuto dell'intero *hard disk*, nella peggiore delle ipotesi.

In questi virus, la sequenza di istruzioni che si attaccava al programma sano era sempre la stessa. I programmi antivirus riuscirono inizialmente a contrastare tale genere di infezione definendo al loro interno delle "librerie" contenenti le stringhe di riconoscimento per le diverse tipologie di virus.

Tali stringhe venivano poi aggiornate periodicamente con nuove sequenze di istruzioni caratteristiche dei nuovi virus che via via venivano scoperti. In questo modo gli antivirus potevano neutralizzare l'infezione, ma era necessario il loro continuo aggiornamento allo scopo di ampliare sempre più il contenuto delle librerie.

Un sostanziale passo "in avanti", si fa per dire, nello sviluppo dei virus fu rappresentato dai cosiddetti Virus TSR (Terminate and Stay Resident). Si trattava di virus che, una volta eseguiti insieme ad un programma infetto, rimanevano residen-

ti nella memoria labile (memoria RAM) del computer e infettavano in maniera non ripetitiva altri programmi nel momento in cui qualcuno tra questi rispondeva a determinate caratteristiche. La contromossa delle case produttrici di antivirus fu di dotare tali programmi della capacità di "marcare" (vaccinare) i programmi sani, in modo da poter riconoscere immediatamente un'eventuale variazione a loro carico.

Una nuova generazione di virus si manifestò con attacchi alla cosiddetta "Boot Area" del disco, cioè del primo settore dell'*hard disk* o del *floppy disk*, che è quella parte del disco deputata al mantenimento delle conoscenze riguardanti l'organizzazione logica del contenuto del disco stesso. I nuovi antivirus dovettero quindi provvedere a controllare la presenza di virus anche in queste aree critiche dei dischi.

Tutto il sistema di riconoscimento dei virus a mezzo di stringhe è venuto poi meno con la recente comparsa dei cosiddetti Virus Multipartiti o Mutanti, la cui peculiarità risiede nel fatto di poter cambiare fino a milioni di volte il loro codice eseguibile, cioè la sequenza di istruzioni contenuta nei virus stessi. In alcuni casi cambiano le istruzioni, ma il comportamento rimane lo stesso; in altri cambiano anche le azioni che il virus compie. A tale famiglia di virus possono essere inoltre assimilati i cosiddetti Virus Extra Traccia, i quali collocano una parte del loro codice sulle tracce dei dischi che loro stessi creano. In tutti questi casi, ovviamente, il riconoscimento per stringhe specifiche perde gran parte del suo significato.

Per contrastare tali tipi di virus sono stati creati degli antivirus che effettuano ricerche euristiche o che effettuano un controllo *runtime*.

La ricerca euristica si basa sul seguente assunto: ogni virus, quando entra in funzione, usa delle specifiche sequenze di istruzioni per nascondersi, assumere il controllo del PC, modificare i programmi eseguibili, ecc.

Avendo a disposizione una libreria delle funzioni impiegate dai vari virus si può pensare di intercettare anche virus sconosciuti purché per attivarsi utilizzino tali funzioni.

Il problema che si pone in questo caso è che i virus possono impiegare delle *routine* di funzionamento perfettamente legali, utilizzate pure dai normali programmi. Di conseguenza, il rischio che si potrebbe correre è quello di creare antivirus "troppo sensibili", che riconoscano come virus persino dei programmi perfettamente normali, o, al contrario, degli antivirus "troppo poco sensibili", che consentano ad alcuni virus di agire indisturbati.

Una ulteriore e fondamentale questione è relativa al fatto che, nel conflitto, chi per primo, fra virus ed antivirus, riesce a prendere il controllo del PC, ha ovviamente le maggiori possibilità di risultare vincitore.

Un problema analogo si pone con i cosiddetti sistemi di rilevamento *runtime* (trappole intelligenti) che agiscono con diverse modalità ma che, in definitiva, hanno anch'essi efficacia solo qualora prendano il controllo del PC prima dei virus.

Ad aggravare la situazione sono comparsi due altri tipi di virus:
– Virus dell'*input/output*;
– Virus delle *directory*.

In questi casi il livello di azione dei virus è estremamente sofisticato in quanto essi riescono ad assumere il controllo del PC indipendentemente dal sistema operativo impiegato intervenendo a livello del BIOS.

Da non molto tempo sono infine comparse delle nuove specie di virus, i cosiddetti "Virus delle Macro", che infettano file documento generati per esempio con Microsoft Word o Microsoft Excel.

Bisogna prestare particolare attenzione a questi virus in quanto essi si possono facilmente trasmettere mediante lo scambio di file di tipo "documento" (ad esempio, mediante la posta elettronica), anche fra sistemi operativi diversi (MacOS, DOS/Windows o anche Unix).

Tali virus si pongono in memoria quando viene caricato il documento infetto che li contiene e, allorché vengono compiute determinate operazioni, come il salvataggio automatico, la ricerca o sostituzione di parti di testo, essi prendono il controllo del programma in questione, in barba ad eventuali antivirus che non possono o non devono interferire con le normali attività del programma. Così, può capitare che, al momento del salvataggio finale, sparisca dal disco fisso un'intera *directory* per effetto di un ordine di cancellazione (perfettamente lecito dal punto di vista funzionale) impartito dal virus stesso.

Ovviamente il documento infetto trasmetterà l'infezione a qualunque altro documento dello stesso tipo aperto durante la medesima sessione di lavoro e questo, a sua volta, se aperto in un altro PC, trasmetterà a sua volta l'infezione ad altri documenti presenti in un altro PC. La presenza di un virus delle macro solitamente si manifesta con una molteplicità di problemi, tra i quali i più diffusi sono: l'impossibilità di salvare il documento in un formato diverso da .txt, la cancellazione di icone, l'occupazione eccessiva di memoria fino al blocco totale del sistema.

Tutte le considerazioni fatte fin qui e la continua evoluzione dei virus consente di affermare che attualmente non esiste un antivirus migliore degli altri. Quelli in circolazione, in media, mancano il bersaglio nei confronti del 10-12% dei virus presenti in quel momento. Nemmeno dotandosi di 5-6 antivirus, è possibile risolvere il problema della prevenzione o della disinfestazione.

Tra i virus, particolari attrattive destano oggigiorno quelli con suadenti nomi di donna o frasi gentili: non che siano meno pericolosi degli altri, ma certamente, almeno nel nome, dànno la sensazione di poter causare minori danni al nostro sistema.

Molti di questi si diffondono con la posta elettronica, come Melissa, W32/Bride, I love you.

W32/Bride, ad esempio, si diffonde via posta elettronica e viene eseguito automaticamente da alcuni sistemi operativi, come Microsoft Windows. La sua fase di incubazione iniziale consiste nel creare un file EML sul *desktop*, installando anche il virus Funlove sul sistema operativo. Il nuovo impulso all'attivazione del virus giunge via *e-mail* in un messaggio senza soggetto, ma con un allegato, solo apparentemente innocuo, di nome README.EXE.

A questo punto Bride si attiva: effettua la copia di se stesso e muta il proprio nome in EXPLORER.EXE, collocandosi sul *desktop* del computer.

In questo modo saremo infettati, per giunta da un virus che si presenta con la medesima icona di Internet Explorer. Se il file "explorer.exe" viene eseguito da un PC infetto, Bride cerca di stabilire delle connessioni verso i siti Internet Hotmail.com e Sex.com. Un ulteriore effetto secondario è quindi l'installazione sul *desktop* dell'utente del file HELP.EML con l'icona tipica di Microsoft Windows.

Ultimamente, si stanno presentando anche degli pseudo-virus informatici che colpiscono gli utenti in modo ingannevole, invitandoli per *e-mail* a fare clic su un *link* che consente di aprire una cartolina illustrata inviata da un'anonima "ammiratrice".

Facendo leva su una legittima curiosità, non appena si effettua il clic sul *link*, per visualizzare la cartolina in arrivo all'utente viene richiesto di scaricare un programma .exe e di attivarlo. Quel software consente di scollegarsi da Internet e telefonare ad un numero a pagamento con il quale è vero che è possibile visualizzare la cartolina, ma, nello stesso tempo, vengono addebitati al malcapitato ben 10 euro più IVA!

Del resto, quando questa cartolina viene spedita, in maniera ovviamente anonima, il mittente può indicare per la medesima spedizione numerosi indirizzi *e-mail*, i cui titolari non possono sottrarsi preventivamente alla ricezione dei messaggi. Si tratta dunque di un *tool* che potrebbe moltiplicare le *e-mail* non richieste in arrivo nelle caselle degli utenti potenzialmente all'infinito.

Tra l'altro, la situazione è aggravata dal fatto che l'utente che riceve una simile cartolina non può evitare di riceverne altre in futuro e non c'è antivirus che tenga. Un meccanismo che si presta, dunque, a numerosi possibili abusi da parte di terzi.

L'iniziativa "commerciale" dietro questa operazione appare in sé legittima, ma il costo elevato per visualizzare una cartolina, pari appunto a 10 euro più IVA, deve indurre gli utenti a leggere sempre attentamente le condizioni di servizio di questo genere di offerte. In tal caso le condizioni vanno cercate all'interno del programma per la connessione a pagamento. Solo così si viene a sapere del costo delle telefonate.

Quindi occorre fare attenzione ad *e-mail* inviate da sconosciute con nomi allettanti: Elisa, Cinzia, Emanuela e via dicendo. Un esempio? Eccolo:

Ti ho inviato una cartolina digitale! Clicca qui e segui le istruzioni per visualizzarla!
CODICE CARTOLINA: 4888-2297-1517

Questo messaggio automatico ti è stato inviato perché qualcuno ti ha mandato una E-cartolina da (*omissis*). Ti raccomandiamo di prendere visione delle condizioni del servizio riportate all'interno del sito. Potrai rispondere alla persona che ti ha scritto o mandare a chiunque altro vuoi una *e-card* scelta nella nostra ampia collezione!