# Calendari, date e scadenze

*Nel mese di giugno si attiveranno alcuni virus piuttosto diffusi, tra cui il Pretoria. Ma noi riteniamo che non sia il caso di compilare un vero e proprio calendario di virus, e segnalare agli utenti ogni mese quali sono i virus da tenere d'occhio. Lo abbiamo fatto in casi particolari ma crediamo che sia controproducente generalizzare la pratica. Vediamo brevemente per quali ragioni*

**di Stefano Toria**

Secondo la definizione corrente un virus è un programma in grado di interferire con il percorso del codice eseguibile, replicandosi senza intervento diretto da parte dell'uomo. In realtà la categoria «virus» comprende quasi sempre, nell'idea del medio utente di personal computer, qualche elemento distruttivo. Sin dal primo caso di virus riscontrato allo stato libero, dai tempi cioè del Brain, i virus hanno spesso lasciato dietro di sé qualche modifica, qualche alterazione ai danni dell'utente che, del tutto involontariamente, li ospita.

L'effetto di un virus può essere banale (cambio di etichetta del disco, caratteri che cadono, musichette o sirene di ambulanze), improvviso e devastante (distruzione del contenuto di uno o più dischi), oppure subdolo e strisciante (ad ogni esecuzione viene variato qualche carattere) ma l'utente si è abituato all'idea che molti virus portano con sé un cavallo di Troia.

Le cose però non sono così semplici. Se l'effetto si manifestasse subito allora l'utente se ne accorgerebbe e prenderebbe provvedimenti. In questo modo il virus non riuscirebbe a diffondersi, mentre ciò che gli autori dei virus desiderano è proprio che le loro creature si diffondano il più possibile. Ecco quindi che ai cavalli di Troia si uniscono le bombe logiche, che spesso sono «a orologeria», predisposte cioè per attivarsi in una specifica data.

Questo aspetto, presente in una percentuale rilevante ma non nella maggioranza dei virus conosciuti, è stato tra i primi a rivelarsi all'attenzione del grande pubblico, quando nel 1989 la stampa di informazione costruì quella enorme e immotivata montatura sul fatto che un virus, attivandosi il successivo venerdì 13 ottobre, avrebbe «messo in ginocchio» le decine di milioni di personal computer installate nel mondo.

Sappiamo che non accadde niente di tutto ciò ma molti, anche tra gli esperti, si convinsero che i virus più temibili sono quelli che si attivano in una certa data. Il fatto si ripetè tre anni dopo con il «Michelangelo», e successivamente anche con l'«855» che noi stessi provvedemmo a segnalare in quanto rilevammo che si trattava di un virus assai diffuso in Italia.

Non sorprende quindi il fatto che molte persone ritengano che sia utile compilare, e mantenere aggiornato, una sorta di «calendario» dei virus, scritto in modo da sapere, giorno per giorno, quali sono i virus da cui guardarsi. L'idea ha allettato anche alcuni produttori di software, tra i quali una notissima e quotata azienda britannica, la S&S del Dr. Alan Solomon.

Il ragionamento è semplice e lineare: le difese contro i virus, più sono e meglio è. L'utente già sa cosa deve fare (tenere aggiornato il proprio antivirus e usarlo regolarmente, anzi usarne più di uno) e cosa non deve fare (usare dischetti di provenienza non garantita, accendere il PC con un dischetto inserito, etc.); se gli viene fornito un ulteriore strumento che gli consenta, giorno per giorno, di stare all'erta contro una breve lista di virus gli si rende un servizio in più.

## È inutile

In realtà il ragionamento è sbagliato e tenere d'occhio le date è perfettamente inutile. Il motivo è semplice: qualsiasi calendario di virus non può contenere altro che un elenco di date di attivazione di virus ben noti ai ricercatori, quanto meno al ricercatore che ha compilato il calendario.

Ma i virus noti ai ricercatori vengono anche sistematicamente e inesorabilmente rilevati dai programmi di scansione, quanto meno da quelli seri e ben progettati (ci sono ancora dei programmi di scansione dal nome altisonante che si rifiutano di riconoscere il Mutation Engine, e questo *a due anni di distanza dalla sua prima comparsa*).

A cosa serve allora tenere il calendario dei virus? Assolutamente a niente; se l'utente utilizza i suoi programmi di scansione regolarmente e in modo corretto saranno loro a fare il lavoro al suo posto, e saranno loro a segnalargli gli eventuali virus dai quali dovesse risultare, nonostante le precauzioni, contagiato.

## È dannoso

Per un'altra serie di motivi, che cercheremo ora di rendere chiari ai nostri lettori, tenere il conto delle date dei virus può essere controproducente e comportare una riduzione anziché un aumento della sicurezza generale del sistema informativo.

Come abbiamo visto più sopra un certo numero di virus sceglie di attendere una determinata data per fare ciò che i loro ignoti autori hanno previsto. Lo scopo di questa attesa è tentare di rimanere nascosti il più possibile; ma come ormai ben sappiamo un virus attivo su un elaboratore, quand'anche rimanga nascosto e non determini effetti visibili, ha tuttavia il controllo dell'elaboratore e nel periodo di latenza farà di tutto per diffondersi.

Peraltro non tutti i virus scelgono di aspettare un giorno prestabilito per attivarsi; ve ne sono molti che non fanno alcun controllo sulle date ma per contro attendono altri eventi, ad esempio che il sistema venga avviato un determinato numero di volte, ovvero che rimanga acceso per un certo numero di ore e così via. Altri virus si attivano una volta su quattro, oppure una volta su sedici e così via.

Insomma, se ci si limita ad osservare ciò che può accadere alla data di oggi perché così è stato espressamente previsto dagli autori di virus si rischia di tralasciare quello che può accadere oggi per qualsiasi altra ragione, come ad esempio perché oggi è trascorso esattamente un mese dal giorno in cui il nostro sistema è stato infettato oppure perché oggi stiamo avviando il sistema per la quattrocentesima volta dall'infezione.

Ma c'è dell'altro. La data di sistema è tutt'altro che una certezza assoluta, e invece su di essa l'utente fa normalmente un certo affidamento; e con la sola eccezione di quèi pochi che ancora si servono del vecchio e glorioso XT e dei suoi compatibili, privi di un orologio ad alimentazione continua, tutti gli utenti di PC sanno che all'avvio la macchina già «sa» che giorno è oggi e che ore sono.

Non è buona norma fare affidamento su tale data. Fintanto che il PC funziona correttamente e viene mantenuto acceso, la data e l'ora sono attendibili; ma quando il PC viene spento la corretta conservazione di data e ora dipendono da un circuito CMOS alimentato da una piccola pila, solitamente al litio. Non è infrequente trovare

dei PC che sbagliano, anche grossolanamente, la data e l'ora e debbono essere «rimessi» ad ogni avvio, come vecchi orologi a cucù.

Quasi sempre un virus che prende il controllo di un PC trova modo di inserirsi nel procedimento di avvio del sistema; quindi un sistema infetto eseguirà con tutta probabilità il virus prima ancora di aver presentato il solito prompt C:\> all'utente. Prima cioè che l'utente abbia avuto modo di verificare se data e ora sono corrette. Ciò accade sicuramente con i virus da boot sector, che vengono eseguiti prima del caricamento del sistema operativo, e può accadere molto facilmente anche nel caso di virus parassiti qualora abbiano infettato degli eseguibili che vengono caricati nel procedimento di avvio, dall'interno dell'AUTOEXEC.BAT (solitamente interpreti di tastiera come KEYB.COM o programmi di servizio come DOSKEY.COM o simili).

Quindi si può ipotizzare una scenetta come la seguente: l'utente si è infettato con il Michelangelo ma non lo sa; il 13 maggio va in ufficio, la mattina, e accende il computer; sempre a sua insaputa durante la notte il circuito dell'orologio ha avuto un problema di funzionamento e all'accensione il computer «crede» che siano le 14:07 del 6 marzo 1991; indovinate un po' cosa succede al disco fisso del nostro ignaro utente, che prima di accendere il computer si era anche premurato di leggere il calendario dei virus per vedere se rischiava qualcosa? Se lo sarebbe mai potuto aspettare che proprio oggi, 13 maggio, tutti i suoi dati sarebbero stati vittima di un Michelangelo che — come tutti sanno — si sarebbe dovuto attivare, caso mai, più di due mesi fa?

## *Togliamo di mezzo questo virus*

È passato qualche tempo da quando abbiamo spiegato nei dettagli come ci si libera da un'infezione senza strascichi, i nostri lettori più recenti potranno forse trarre giovamento da una illustrazione dettagliata di come ci si comporta in presenza di una infezione vera o presunta; e anche chi ci segue da tempo potrebbe avere bisogno, proprio ora, di qualche indicazione su come trattare un problema di virus.

(Potremmo anche dire che, dopo quasi tre anni che stiamo parlando di virus e di come evitarli, se qualcuno che ci segue da tempo è riuscito comunque a infettarsi è proprio bravo, e forse è andato a cercarsela).

La prima cosa che ciascun utente di PC dovrebbe procurarsi, cinque minuti dopo aver installato il proprio computer, è l'«oggetto magico». Questo toccasana taumaturgico, che è in grado di risolvere qualsiasi problema di virus, è semplicemente un *dischetto di sistema pulito e protetto*, ottenuto tassativamente dall'originale. Cosa? Non avete l'originale del sistema operativo? Bene, questa è la buona occasione di andarvene a procurare una copia. Visto che ci siamo, vogliamo ricordare che il sistema operativo, proprio come qualsiasi altro software, deve essere rifiutato se viene presentato all'utente privo dei sigilli. Cioè se la plastica esterna termorestringente e/o il sigillo interno che chiude la busta dei dischetti presentano segni di manomissione. Solo acquistando un pacchetto software sigillato si può essere ragionevolmente sicuri di non rischiare, o quanto meno di avere tra le mani una copia del software identica a quella che è uscita dai magazzini del produttore. Può sempre accadere, e in realtà è accaduto, che si infetti l'originale prima di essere distribuito; ma allora in questo caso possedendo una copia originale del software si potrà facilmente rintracciare la fonte dell'infezione.

Una volta ottenuto l'originale si procederà ad avviare il PC dall'originale, spegnendo la macchina, introducendo il dischetto e quindi riaccendendo. È importante evitare di usare Ctrl-Alt-Del perché alcuni virus riescono a intercettare questa sequenza di tasti e fanno credere all'utente di aver fatto un reset mentre non è così. Si procederà quindi a costruire un dischetto di sistema copiando l'originale (*protetto dalla scrittura*) su un dischetto vergine e togliendo tutti i file che non servono, generalmente tutti tranne il COMMAND.COM (stiamo spiegando la procedura per un PC IBM o compatibile; il mese prossimo vedremo come si fa su un Macintosh). Potrà essere utile trasferire su questo dischetto anche i file FDISK.EXE e SYS.COM, per motivi che vedremo tra poco.

Il passo successivo consiste nel trasferire sul dischetto di sistema i programmi antivirus, evidentemente non prelevandoli dal disco fisso ma dai dischetti originali dai quali sono stati a suo tempo prelevati. È importante che i programmi antivirus siano mantenuti aggiornati alla più recente versione disponibile; avere un antivirus dell'anno scorso equivale a non avere alcun antivirus.

A questo punto, con l'oggetto magico pronto e disponibile (e protetto), si spegnerà nuovamente il computer, lo si riaccenderà e si manderanno in esecuzione i programmi antivirus, al fine di rilevare se e quali programmi presenti sul disco fisso siano infetti:

— se risulterà infetto il master boot record sarà sufficiente, al termine dell'esecuzione dell'antivirus, dare il comando FDISK /MBR (una funzione non documentata del DOS nelle versioni dalla 5 in su) per ricostruire un master boot record esente da infezioni; tipici esempi di questo tipo di virus sono lo Stoned e il Michelangelo;

— se risulterà infetto il partition boot record o DOS boot record basterà dare il comando SYS C: per ricostruire il programma di avvio del DOS; tipici esempi di questi virus sono il Form e il Ping-Pong;

— se risulteranno infetti uno o più file eseguibili li si dovrà rimuovere e sostituire con delle copie originali, eventualmente reinstallando i pacchetti infetti o prelevandole da un precedente backup (a proposito: quando avete fatto l'ultimo backup serio del vostro sistema?);

— se non dovesse risultare nulla di infetto si eviterà comunque di fregarsi le mani e abbassare la guardia; c'è sempre la possibilità di essersi infettati con un virus ancora sconosciuto agli autori degli antivirus. Si prenderanno quindi le precauzioni opportune.

La prima cosa da farsi dopo aver accertato la presenza di un virus, o anche dopo aver fatto un controllo con esito negativo, è una copia ragionata di tutto il sistema. Ciascun utente dovrebbe avere un buon programma di copia di sicurezza, e specialmente coloro che si servono del computer per il proprio lavoro, e quindi tengono sul PC informazioni che hanno un valore, dovrebbero essere opportunamente attrezzati per le copie. Normalmente le copie si faranno su dei dischetti; non è un'idea sbagliata procurarsi un dispositivo a nastro («streamer») che consente di accelerare le procedure di copia, svincolando l'utente dal compito noioso di cambiare i dischetti.

Si procederà quindi a trasferire tutti i dati, possibilmente suddivisi per applicazione (i dati dei fogli elettronici; i testi; le immagini; etc.), sul supporto esterno. Si provvederà quindi a rimuovere l'infezione, reinstallando ciò che occorre, e per verificare che tutto si sia risolto si passerà nuovamente l'antivirus, sempre avviando il sistema dal dischetto pulito e protetto.

Se il controllo risulta negativo si eseguirà la stessa procedura su tutti i dischetti di cui l'utente dispone. Questo controllo, necessario in ogni caso, è indispensabile nei casi di infezione da virus di boot sector. Le probabilità sono tutte in favore del fatto che il virus sia arrivato tramite un dischetto di dati, lasciato accidentalmente nel drive durante l'avvio del PC.

Ma anche il controllo di tutti i dischetti di per sé non è sufficiente. Ci sarà senz'altro qualche dischetto che s'è nascosto in fondo a un cassetto o sotto una pila di carte, per risbucare fuori a distanza di qualche mese quando ormai l'allarme è cessato. Questo è l'unico caso in cui un programma antivirus residente risulta effettivamente indispensabile. L'utente dovrà installare un antivirus residente che servirà a scongiurare il rischio di una nuova infezione proveniente da qualche dischetto dimenticato. Ovviamente in caso di aggiornamento dell'antivirus principale non si dovrà tralasciare l'aggiornamento anche del residente. MC

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