L'assalto di Odisseo

Programmi aggressori significa, nella maggioranza dei casi, virus. Ma i rischi non vengono soltanto dai virus: questo mese parliamo di un tipo di programmi aggressori che si sta diffondendo in maniera preoccupante

di Stefano Toria

Parlando di programmi aggressori è opportuno distinguere tra diverse modalità di aggressione. I virus, che risultano i più comuni, attaccano un sistema replicandosi all'insaputa dell'utente, il quale si trova «invaso» senza sapere da dove è provenuto il programma responsabile dell'invasione.

Molti virus si limitano a replicarsi; alcuni virus portano con sé un «carico», che può essere banale come una musichetta o una scritta sul video oppure dannoso come la distruzione totale delle informazioni contenute nel disco fisso.

Il pubblico ritiene che qualsiasi programma subdolamente distruttivo sia un virus; questa idea nasce da una confusione che i mezzi di informazione non hanno contribuito a dissipare correttamente ma in realtà nelle definizioni correntemente utilizzate un virus è semplicemente un programma che si replica servendosi di un altro programma come mezzo di trasporto.

Il virus può contenere altre forme di programmi aggressori, e in particolare bombe logiche e cavalli di Troia. È di questi ultimi che parleremo stavolta, descrivendone il comportamento; l'occasione ci viene da una particolare recrudescenza di questo fenomeno, normalmente sopito e latente.

Dall'Iliade ai «Dirty Tricks»

L'uso del nome «cavallo di Troia» è piuttosto calzante. Rammentiamo il mito: la guerra dei principi greci contro Troia durava da dieci anni, la città sotto assedio non mostrava intenzione di capitolare, quando uno dei principi greci ebbe l'idea che permise a un gruppo di soldati di introdursi all'interno della città. Odisseo fece costruire un cavallo di legno, esternamente adornato come un dono di pace ma internamente cavo e fatto in modo da poter contenere dei soldati armati. Egli stesso si introdusse nel cavallo, che fu lasciato di fronte alle porte di Troia; quindi l'esercito greco abbandonò il campo durante la notte e sparì dalla vista.

Al mattino i Troiani trovarono l'assedio tolto, e il dono di pace. Portarono quest'ultimo nella città e fecero festa; ma durante la notte Odisseo e i suoi uomini uscirono fuori dal cavallo e aprirono le porte della città consentendo all'esercito greco di entrare. Così Troia fu distrutta e la bella Elena, rapita dal troiano Paride, fu riconquistata. (Nella realtà la guerra di Troia fu un affare molto meno romantico e assai più sporco, al quale non erano estranei i traffici commerciali greci verso l'Anatolia passando per lo stretto dei Dardanelli).

Abbiamo riportato la favola di Omero per confrontarla punto per punto con il comportamento di quei programmi aggressori che prendono il nome dal cavallo di legno. All'apparenza si tratta di qualcosa di positivo; programmi per la gestione della directory, programmi di contabilità, programmi di comunicazione o di compressione. Il vostro shareware preferito potrebbe essere modificato, o riscritto, in modo da comportarsi come un cavallo di Troia.

Com'è fatto

All'interno del programma, celato e invisibile a un primo esame, c'è qualcosa di inatteso. L'utente non lo sa e esegue ugualmente il programma: e mentre egli sta osservando e valutando il comportamento della parte apparente del programma medesimo, entra in gioco la parte nascosta.

Scritte sul video, distruzioni di dati, blocco del computer: qualsiasi azione dannosa può essere compiuta dal «contenuto illecito» del programma-cavallo di Troia. E a differenza dei virus, che si attaccano a un programma eseguibile all'insaputa dell'utente e in questo modo riescono a essere eseguiti, i cavalli di Troia vengono eseguiti volontariamente dall'utente stesso, ovviamente inconsapevole dell'esistenza di un «clandestino a bordo». Se i Troiani avessero saputo che nel cavallo c'era Odisseo con i suoi uomini lo avrebbero bruciato all'istante, altro che portarlo dentro la città.

La differenza, evidente, rispetto a un virus sta nel fatto che un cavallo di Troia non è in grado di replicarsi autonomamente e quindi non può, e al tempo stesso non ha bisogno, di mimetizzarsi per attendere il momento propizio per distruggere.

È sensato aspettarsi da un virus che attenda un evento preciso (es. il 6 marzo oppure il 400° avvio del sistema operativo) per attivarsi. Nel frattempo il virus avrà intercettato il funzionamento del sistema operativo, e si servirà di questo ritardo per riprodursi il più possibile. Non ha senso per contro che un cavallo di Troia attenda una condizione, perché non è dotato di funzioni autonome di replicazione; a meno che l'ignoto autore non voglia appigliarsi alla esigua probabilità che chi riceve un programma poi lo faccia a sua volta circolare, ma è più un'ipotesi teorica (e anche piuttosto stiracchiata) che una reale probabilità.

Quindi il cavallo di Troia colpisce immediatamente. L'utente avvia il programma per esaminarne il funzionamento, e l'effetto indesiderato prende subito l'avvio: in genere si tratta della cancellazione o distruzione di dati.

La difesa

A differenza dei virus i cavalli di Troia sono assai difficili da identificare. È facile che lo stesso programma «perisca» assieme ai dati distrutti, e quindi è meno frequente che i ricercatori ne vengano in possesso. Teoricamente un cavallo di Troia potrebbe essere identificato da una stringa caratteristica allo stesso modo in cui si identifica un virus, con

assai meno problemi perché ad esempio non è possibile il polimorfismo. Alcuni programmi antivirus, uno fra i tanti F-PROT, identificano correttamente un certo numero di cavalli di Troia.

Ma nella pratica è difficile servirsi di tale identificazione. Si può fare qualche affidamento sulle tecniche di analisi euristica di programmi come TBSCAN o lo stesso F-PROT, seppure non efficaci al 100%.

L'unico vero modo per difendersi dai cavalli di Troia è di non usare software di provenienza non certificata. A differenza dei virus, che possono infettare un programma commerciale all'insaputa di chi lo maneggia, i cavalli di Troia debbono essere appositamente scritti. È piuttosto inverosimile che 123.EXE, WIN.COM o TELIX.EXE, prelevati dai rispettivi dischi originali, siano cavalli di Troia; per contro è possibile che ciascuno di quei file si infetti con un virus laddove i file vengono eseguiti su un computer infetto senza aver protetto i dischetti dalla scrittura.

Un programma di provenienza anonima, scritto da una persona che non si conosce, può benissimo risultare cavallo di Troia. Se proprio lo si vuole usare si faccia prima una prova su un computer che non contiene dati irrinunciabili. Se non si può fare a meno di provarlo sul proprio computer almeno si faccia una copia di sicurezza dei dati insostituibili, o meglio ancora si approfitti dell'occasione per fare una copia totale del sistema. Meglio perdere mezz'ora tra copia e eventuale ripristino una volta successo il danno piuttosto che perdere tutto il proprio lavoro se il danno si verifica senza che ci siano copie recenti a disposizione.

Cavalli italiani

Abbiamo colto l'occasione per parlare di cavalli di Troia da un fatto piuttosto inquietante: si starebbero diffondendo in Italia programmi scritti apparentemente dalla stessa persona, i quali distruggono senza troppi scrupoli tutto il contenuto del disco C: sul computer su cui vengono eseguiti.

Non possiamo né intendiamo dare maggiori informazioni su questi programmi, per due ragioni. La prima è che sarebbe inutile fornire nomi di file che sono facilissimi da modificare per «riciclare» i programmi incriminati. La seconda, ben più importante, è che non abbiamo nessuna intenzione di dare pubblicità all'ignoto autore o agli ignoti autori. È accertato che una delle motivazioni che spingono un programmatore a scrivere un virus o un cavallo di Troia è la speranza di «consegnare alla posterità» il proprio operato. Possiamo immaginare questi ragazzotti maniaci del byte che si raccontano le rispettive prodezze: «Pensa, sull'ultima edizione di VSUM Patricia Hoffman ha inserito anche il mio virus! Ne parla per una intera schermata!». «Ma che vuoi che sia», replica l'amico «del mio virus ne parla addirittura per due schermate!».

Persone di questo calibro non meritano ulteriore attenzione. Il messaggio da ricordare comunque è chiaro: attenzione ai programmi di provenienza non certificata, soprattutto a quelli prelevati da BBS o da collezioni di shareware.

E con questo non abbiamo alcuna intenzione di gettare discredito sulle BBS amatoriali. Conosciamo personalmente e frequentiamo un certo numero di questi sistemi e non abbiamo alcuna riserva nel riconoscere la serietà e la professionalità con cui la maggior parte di essi sono gestiti, anche se si tratta quasi sempre di attività hobbistiche. Non pensiamo tanto alla mala fede quanto all'imprevisto; e qualche «sysop», che magari non abbia il tempo di sperimentare personalmente tutti i programmi che riceve, potrebbe diventare l'inconsapevole diffusore di un programma-killer. MC

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

Falso allarme

Secondo «Il Sole-24 Ore» di giovedì 24 giugno sarebbe in arrivo anche in Italia il Tremor, un «supervirus» che «in pochi giorni si è diffuso in tutta la Germania». «Allo stato - prosegue l'articolo apparso in prima pagina sul quotidiano economico - non è possibile rimuoverlo senza cancellare i file colpiti».

Considerata l'autorevolezza del giornale, alieno in genere da toni allarmistici o sensazionali, è comprensibile l'apprensione suscitata da una notizia del genere nei lettori, tanto più che della «scoperta» si farebbero garanti ricercatori universitari, consulenti governativi, operatori del settore.

In realtà eravamo già da tempo a conoscenza di questo virus, uno fra i tanti che ogni mese compaiono e vengono recapitati in un modo o nell'altro anche nei nostri uffici.

Entrando nel dettaglio, non è esatto affermare, come fa l'articolo de «Il Sole», che il virus sarebbe impossibile da rimuovere senza cancellare i file colpiti: sono almeno tre i programmi in grado di disinfettare correttamente i file infetti, tra cui l'ottimo TBCLEAN disponibile come shareware.

Ma il motivo per cui questo virus attirò la nostra attenzione a suo tempo era un altro: si trattava del primo virus riconosciuto in grado di attaccare direttamente il nuovo antivirus incluso nella versione 6 dell'MS-DOS. È questa la vera caratteristica di spicco di questo virus, piuttosto che la sua variabilità o la modalità con cui si è verificata la diffusione.

Ci auguriamo che in un modo o nell'altro anche i lettori del «Sole-24 Ore» vengano presto tranquillizzati su questa ennesima «tigre di carta» del sottobosco informatico.

Da quel giornale, e dai suoi collaboratori che ben conosciamo e stimiamo, ci aspettiamo, anche in questo campo, un'accuratezza nell'informazione e un senso di responsabilità che non facciano loro torto.

S.T.