

Ma gli antivirus servono a qualcosa?

di Paolo Attivissimo

Di fronte al dilagare di worm e virus, è forse il caso di riconsiderare uno dei dogmi della sicurezza informatica: l'antivirus, che si sta rivelando più un danno che una valida difesa. Urgono soluzioni alternative



C'era una volta Internet. Quella cosa bella, mitica e irraggiungibile che se l'avevi eri un essere superiore, membro di una élite di interconnessi che scambiavano gratuitamente e-mail intercontinentali mentre gli altri infelici scialacquavano fortune in fax e telefonate.

Poi sono arrivati i virus: uno, due, dieci, mille. E Internet è diventata la latrina del terzo millennio. La mia casella di e-mail, come la vostra, è un ricettacolo repellente di réclame di allungapiselli, proposte d'affari di dittatori africani in disgrazia, e soprattutto virus, virus, virus. Distillare la posta veramente utile in questo marasma è oggi una necessità nauseante, come recuperare un Rolex caduto in un orinatoio pubblico. Adesso, quando dico che lavoro con Internet, i giurassici rimasti fedeli al fax mi guardano come se fossi un addetto dell'agenzia spurghi e sogghignano, compiaciuti della loro scelta retró.

Gran parte della colpa è da attribuire a chi ha avuto la geniale trovata di scrivere programmi di posta che eseguono automaticamente qualsiasi porcheria allegata a un e-mail. In confronto, stare a bocca spalancata sotto una piccionaia è una scelta da Einstein.

I più giovani magari non se lo ricordano, ma prima dell'avvento di Outlook e soci era necessario che un utente aprisse *intenzionalmente* un allegato per farsi infettare. Lo faceva una volta e poi, se non era proprio un imbecille, imparava a caro prezzo la lezione. Ora, grazie al progresso tecnologico, i virus vengono eseguiti automaticamente, e l'utente non può far nulla per impedirlo. Dirgli di non aprire gli allegati, come si faceva un tempo, non serve più a nulla: lo fa automaticamente il computer. E' questo automatismo la causa fondamentale del dilagare violento di ogni più banale attacco virale.

Di solito a questo punto il saccente di turno alza la manina e fa notare che le cose andrebbero molto meglio se tutti usassero l'antivirus e lo tenessero aggiornato, le epidemie virali non esisterebbero. Si offende qualcuno se dico che questa è una panzana colossale?

Il giro del mondo in quindici minuti

La ragione è piuttosto semplice. Gli antivirus agiscono sempre troppo tardi per natura. Prima che possano bloccare un nuovo virus, è necessario che quel virus sia *già in circolazione* e arrivi tra le mani degli esperti, che lo esaminano e preparano di corsa un aggiornamento antivirale su misura. Poi è necessario attendere che gli utenti scarichino e installino l'aggiornamento. Solo allora si è protetti.

Questo meccanismo intrinsecamente passivo significa che anche nella migliore delle ipotesi, ossia con esperti delle società antivirali in servizio giorno e notte e con utenti diligentissimi che scaricano gli aggiornamenti ogni giorno più volte al giorno, passano comunque diverse ore fra l'inizio dell'epidemia e la disponibilità dell'aggiornamento che riconosce la nuova minaccia virale.

E a quel punto il danno è ormai fatto. Grazie anche al crescente numero di utenti permanentemente connessi, i virus più recenti si diffondono in tutto il mondo a velocità enorme, come documentato in modo impressionante da una [recente ricerca](#) su Code Red e Nimda.

Ultimamente basta infatti *qualche decina di minuti* perché vi siano migliaia di macchine infette, che a loro volta disseminano il virus tramite le loro connessioni veloci. Li chiamano addirittura i *Warhol worm*, dalla famosa frase di Andy Warhol che prevedeva un futuro in cui ognuno avrebbe avuto il proprio quarto d'ora di fama (o, in questo caso, di infamia).

In sostanza, è ormai tecnicamente possibile sviluppare un virus in grado di infettare Internet fino alla paralisi in meno di un'ora. Quelli che abbiamo subito sinora, sia ben chiaro, sono attacchi dilettanteschi: lo conferma l'analisi dei codici virali di Blaster, Sobig e compagnia bella, che pure hanno causato sfracelli. In queste condizioni, un antivirus è utile tanto quanto mettersi il casco dopo essere caduti dalla moto.

L'antivirus non solo è sostanzialmente inutile contro un'epidemia: offre un senso di sicurezza del tutto fasullo, che è notoriamente più pericoloso della consapevolezza di essere in pericolo. Se l'antivirus ci dice che un allegato è pulito, è probabile che cederemo alla tentazione di aprirlo, anche se è di provenienza dubbia. Non abbiamo modo di sapere se l'allegato alberga in realtà un virus troppo recente per essere riconosciuto persino dall'antivirus fresco di aggiornamento.

L'esempio classico è il recentissimo [Swen/Gibe](#). Ha cominciato a inondarmi la casella di posta diverse ore prima che le società antivirali producessero l'aggiornamento che lo riconosce. Durante quelle ore, l'esame con l'antivirus aggiornato indicava che l'allegato di Swen era in regola. Mi ha salvato dall'infezione soltanto la mia diffidenza verso gli allegati in generale, perché il messaggio era davvero ben confezionato e faceva leva sull'ansia generata dagli attacchi precedenti. Molti altri utenti non sono stati così accorti.

I danni degli antivirus

L'antivirus, insomma, ci lascia in braghe di tela proprio quando più ne abbiamo bisogno. Il massimo che può fare è confermarci, a distanza di qualche ora, che un allegato sospetto è davvero infetto. Ma se già sospettavamo, la conferma è quasi superflua. Se non sospettavamo, ormai abbiamo aperto l'allegato e ci siamo infettati. Bell'aiuto.

L'unica vera utilità di un antivirus è la verifica di quei pochi file che dobbiamo aprire perché ce li ha mandati intenzionalmente qualcuno che conosciamo (un cliente, per esempio) ma che potrebbe essere infetto a sua insaputa. Verificare un allegato proveniente senza preavviso da uno sconosciuto è invece del tutto superfluo, perché l'allegato è quasi sicuramente un virus e va cancellato senza indugi.

L'antivirus ha oltretutto un costo tangibile. Non solo occorre quasi sempre acquistarlo o perlomeno pagare un canone per i suoi aggiornamenti (anche se esistono validi antivirus gratuiti), ma lo scaricamento necessariamente frequente degli aggiornamenti comporta un dispendio di tempo e un consumo di banda che, specialmente per gli utenti collegati via modem in dial-up, si traduce spesso in un aggravio notevole di spesa. E' anche per questo che molti utenti non scaricano regolarmente gli aggiornamenti: costano e sono una scocciatura.

Oltretutto, neppure usare il miglior antivirus e sistemi operativi alternativi a Windows ci mette al riparo dall'altro spreco di banda: quello dovuto al bombardamento dei virus *ricevuti*. L'antivirus, se installato sul nostro computer, agisce *dopo* che abbiamo scaricato l'immondizia infetta. Quindi anche gli utenti Mac e Linux, notoriamente immuni a quasi tutti i virus in circolazione, ne subiscono comunque il peso, perché si trovano la casella di posta intasata da virus dedicati agli utenti Windows e da quei pestiferi messaggi *"attento, mi hai mandato un virus"* generati dagli antivirus troppo cretini per capire che da anni la maggior parte dei virus falsifica il mittente del messaggio infetto. Non si salva nessuno, insomma.

E' insomma evidente che l'approccio dell'antivirus è fondamentalmente sbagliato e insufficiente. Ci vuole un altro sistema. Un sistema preferibilmente semplice, oltre che efficace, e che non sia a carico dell'utente, altrimenti sarebbe condannato in partenza al fallimento, vista l'ingenuità diffusa dei tanti che si affacciano oggi a Internet.

Tutti banditi

Una soluzione ci sarebbe: bandire gli allegati e l'interpretazione dei linguaggi nei programmi di posta, punto e basta. Suvvia, non ridete.

Praticamente tutti i virus si diffondono sotto forma di allegati (Blaster è una rara eccezione). Se la posta non può trasportare allegati, il virus non può diffondersi. Se l'e-mail contiene soltanto testo e il programma di posta non ne esegue in alcun modo il contenuto (niente interpretazione di HTML e simili), l'utente è immune a ogni infezione via e-mail. Il canale primario di proliferazione virale viene sbarrato completamente.

Questa strategia tanto draconiana quanto apparentemente banale è in realtà assai flessibile: si può implementare in molti modi e a molti livelli secondo le esigenze. Il primo livello è quello personale: si stabilisce la norma che tutti gli allegati ricevuti, di qualunque tipo e chiunque ne sia il mittente, vengono cancellati senza pietà, automaticamente o manualmente. E' necessario essere così drastici perché un virus può essere annidato in *qualsiasi* tipo di file, compresi i documenti e i filmati, o spacciarsi per un'immagine o un file di testo apparentemente innocuo.

Questa è una regola che chiunque può decidere di mettere in pratica sin da subito. Naturalmente il programma di posta usato non deve essere così stupido da eseguire automaticamente gli allegati o i codici contenuti in un e-mail, ma non è difficile: da qualche tempo persino Outlook Express è [configurabile](#) in questo modo.

Il secondo livello è quello della rete aziendale: tutti gli allegati, di ogni sorta e senza eccezioni, vengono purgati a livello del gateway verso Internet. Gli utenti non hanno bisogno di fare assolutamente nulla per difendersi.

Meglio ancora sarebbe adottare questa strategia al terzo livello, quello del provider: immaginate di avere un account di posta che cestina automaticamente ogni e qualsiasi allegato *quando è ancora sul server*, un po' come già si fa per lo spam. Quante copie di Swen ricevereste? Nessuna. Non so voi, ma io pagherei volentieri per un servizio del genere. Provider, pensateci.

Idem dicasi per gli altri virus e per le immagini porno che accompagnano molto spam. Non avreste neppure l'onere di scaricare tutti i messaggi infetti, e aggiornare l'antivirus diventerebbe quasi superfluo. Forse è questo il motivo per cui non si è ancora adottata questa soluzione: nocerebbe ai produttori di antivirus. Eh già, perché più virus ci sono, più antivirus si vendono. Poco importa se non funzionano granché: danno sicurezza, come la coperta di Linus (quell'altro, non Torvalds).

Avanti, verso il passato

Bandire gli allegati non significa rendere impossibile lo scambio di file: significa semplicemente rendere impossibile lo scambio *automatico* che i virus sfruttano per diffondersi. I file si possono comunque scambiare tramite i mille altri modi sicuri e ben collaudati che Internet offre da sempre: ftp, scp, Web, giusto per citarne qualcuno, e persino [Bittorrent](#), che si sta rivelando così prezioso per la distribuzione legale di Linux e del software libero in generale. Fra l'altro, l'alt agli allegati ci sbarazzerebbe di tutte quelle odiose presentazioni PowerPoint contenenti trite parole di "saggezza cinese" o altri luoghi comuni che certi utenti non sanno trattenersi dal diffondere all'intero globo terracqueo, ma questa è un'altra storia.

Certo non è una soluzione perfetta: ci sono molti modi per aggirarla, ad esempio tramite il classico *social engineering* (tecniche psicologiche di persuasione che gabbano l'utente anziché le sue tecnologie informatiche), ma sarebbe un enorme passo avanti. O per meglio dire un passo *indietro*, dato che ci riporterebbe all'Internet dei bei tempi andati. Quella che funzionava.

Il fattore che permette a un virus moderno di commettere stragi è la modalità di diffusione: automatica e ad alta velocità. Se il virus ha bisogno di un'azione manuale per diffondersi (ad esempio deve essere scaricato da un sito, eseguendo una procedura protetta da password), la sua propagazione è drasticamente rallentata, tanto da dare il tempo ai produttori di antivirus di realizzare e distribuire l'aggiornamento apposito e soffocare i pochi focolai sul nascere. Ci sarebbe dunque lo stesso un mercato per gli antivirus, anche se meno vasto di quello attuale.

Naturalmente la tecnologia da sola non basta: bisogna anche educare gli utenti a una sana diffidenza, in modo da evitare le insidie del *social engineering*. Ma la diffidenza è un comportamento istintivo, di gran lunga più facile da instillare anche nell'utente meno esperto che l'uso di una tecnologia che per molti è estranea e astrusa oltre che carente nei risultati, come lo è attualmente quella degli antivirus. Chiunque capisce la regola "*non fidarti di nessuno*". Diamine, *X-Files* l'abbiamo visto tutti.

Una cosa è certa: così non ha più senso andare avanti. Se vi accontentate di una soluzione che debella il 99% dei virus passati, presenti e futuri, potete adottarla sin da subito, almeno a livello personale. La Rete intera ve ne sarà grata.