

# Gli aggiornamenti degli antivirus

**(i tutorial di Alessandro de Simone)**

Copyright Alessandro de Simone 2007 ([www.alessandrodesimone.net](http://www.alessandrodesimone.net)) - È vietato trascrivere, copiare, stampare, tradurre, riprodurre o divulgare il presente documento, anche parzialmente, senza l'autorizzazione scritta dell'autore. I siti Internet, le case editrici e le pubblicazioni di settore che intendano utilizzare questo documento possono contattare l'autore ([www.alessandrodesimone.net](http://www.alessandrodesimone.net)) per gli accordi del caso.

Copyright Alessandro de Simone 2007 ([www.alessandrodesimone.net](http://www.alessandrodesimone.net)) - No transcribing, no copyng, no reproducing, no translating, no printing, no publishing this document - even if partially - without author's written authorization. Websites and publishing house who wish to employ this document must write the author ([www.alessandrodesimone.net](http://www.alessandrodesimone.net)).

## Premessa

Le note che seguono possono essere utili agli utilizzatori dei servizi di posta elettronica e web in generale, qualunque sia il sistema che posseggono (Win / Mac / Linux eccetera). Si vuole qui affrontare la problematica generale che riguarda la diffusione dei virus, focalizzando l'attenzione su alcuni aspetti che fin troppo spesso vengono sottovalutati, con le conseguenze che è facile immaginare.

## Come ti creo un virus

Nonostante sia scontato, è bene precisare in che modo vengono creati i virus. Non sempre i loro autori sono esperti informatici. E' ormai risaputo che un qualunque ragazzino - generalmente incosciente e privo di una cultura di base - può creare un virus grazie a sciagurati siti Internet che mettono a disposizione di chiunque veri e propri tool per la creazione, la distribuzione e la diffusione di virus.

Di certo non descriverò né i tool di sviluppo, né tanto meno i siti web da cui scaricarli. In queste pagine cercherò di puntualizzare la procedura di diffusione di un virus con l'unico scopo di favorire una responsabile cultura della prevenzione.

## Come ti diffondo un virus

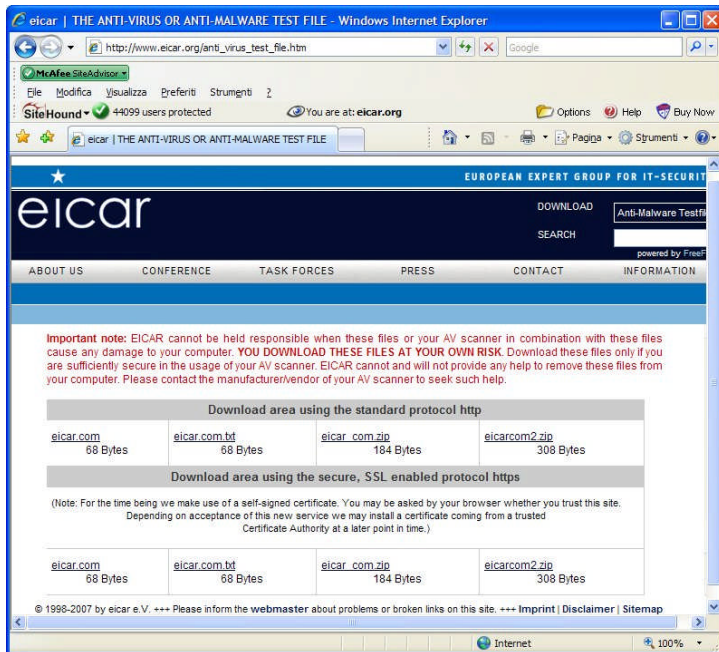
Una volta creato, il virus (ma anche il trojan e il malware in generale) è costituito da un unico file (suffisso .EXE) oppure un gruppo di file (.EXE .DLL .SYS eccetera). In ogni caso il suo effetto inizia con l'apertura di un file iniziale - di solito un .EXE - secondo modalità diverse: doppio clic sull'icona di un allegato, apertura di uno ZIP file, allocazione di una DLL e di un SYS nella cartella di apertura automatica dei programmi (che agiranno alla successiva accensione del PC) e così via.

L'effetto che ne deriva è ovviamente devastante sia per il PC infettato, sia per i PC ai quali il virus spesso si connette, all'insaputa dell'utente, con allegati a messaggi e-mail.

Da quanto detto risulta che il singolo file-virus iniziale genera una pluralità di file che si nascondono abilmente allocandosi nelle cartelle del PC infettato oppure aggiungendosi in coda a file precedentemente "sani", come programmi ma anche documenti di vario tipo.

## Come ti blocco un virus

Va da sé che un programma antivirus può agire meglio se intercetta il file-virus originario *prima* che questo abbia il tempo di attivarsi e scatenare l'infezione. In linea di massima un antivirus può intervenire anche *dopo* che l'infezione si è scatenata, individuando e rimuovendo i file dannosi e ripristinando quelli infetti. E' tuttavia fuor di dubbio che il lavoro di un antivirus viene agevolato se si agisce non appena il file potenzialmente dannoso viene individuato, per essere subito annichilito.



Ogni file-virus ha una struttura tale che, opportunamente analizzata, fornisce chiare indicazioni sulla sua nocività. Si tratta della ben nota "firma", cioè una successione di byte che – per nostra fortuna – viene correttamente interpretata dall'antivirus, a patto che questo agisca in background. Inutile dire che, in particolari circostanze, una determinata successione di byte posti all'interno di un file del tutto innocuo può essere erroneamente interpretata come virus, facendo scattare il meccanismo di difesa dell'antivirus. Nella figura qui a sinistra è raffigurata la schermata del sito...

[http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm)

...che mette a disposizione degli interessati alcuni file, del tutto innocui, che però riescono a trarre in inganno gli antivirus. Simulando il *download* di uno qualunque di essi, infatti, l'antivirus visualizza una finestra di pericolo e chiede all'utente in che modo comportarsi (vedi figura qui a destra). Tralasciando il fatto che occorre una certa prudenza nel gestire questi file (si noti l'avvertimento, in rosso, nel sito web citato) spetta all'utente stabilire se l'avvertimento dell'antivirus è un cosiddetto "falso positivo" oppure no. In ogni caso, è proprio questa, cioè la fase iniziale, in cui l'antivirus esplica tutta la sua potenza: se l'utente impedisce al file di entrare nel proprio PC, il 99,99% del lavoro è già fatto; rifiutandosi di scaricare il file si raggiunge il 100% di sicurezza.



## Come ti aggiorno l'antivirus

Riassumendo, il problema principale da risolvere consiste nel possedere un programma antivirus che sia in grado di riconoscere la pericolosità di un file che sta per agire (o semplicemente entrare) nel nostro computer. Un antivirus, ovviamente, agisce in base a

un elenco di virus di cui conosce le firme. Va da sé che se alla collezione di firme manca proprio quella relativa al file-virus che stiamo scaricando in questo momento, beh, il file entra nel computer, pronto a compiere i danni per cui è stato progettato.

Ed ecco l'uovo di Colombo: tutte le volte che ci colleghiamo al web – e prima di iniziare una qualunque attività (web surfing, download di posta elettronica, chat e altro) – basterà avere l'accortezza di scaricare l'ultimo aggiornamento, se disponibile, dal sito del produttore del nostro antivirus. E già qui c'è da evidenziare una condotta scandalosamente “leggera”, per non dire incosciente e autolesionista: moltissimi utenti ritengono che sia sufficiente scaricare gli aggiornamenti una volta alla settimana, se non una volta al mese; altrettanti utenti ritengono – chissà perché – che il loro antivirus sia automaticamente impostato per scaricare automaticamente gli aggiornamenti ogni volta che il PC si connette al web. E non si sognano nemmeno di verificare se tale affermazione è vera, né tanto meno controllano se realmente funziona! Personalmente mi è capitato di intervenire su PC il cui aggiornamento era rimasto fermo a più di due mesi prima. In altri PC, poi, l'impostazione automatica risultava del tutto disabilitata. ***Ribadisco ancora una volta che sono ormai disponibili aggiornamenti con frequenza quotidiana. In alcune giornate mi è capitato di scaricare fino a quattro aggiornamenti, spesso definiti “vitali” dal programma antivirus!***

## Come ti aggiro l'aggiornamento

L'antivirus del nostro PC è impostato per effettuare un download degli aggiornamenti ogni volta che ci colleghiamo al web. Per sicurezza, inoltre, effettuiamo manualmente il collegamento al sito del produttore, ma un rassicurante messaggio “*Non sono disponibili aggiornamenti*” ci assicura che la procedura è attiva e funziona benissimo.

**Possiamo quindi scaricare ciò che vogliamo, sicuri che l'antivirus intercetterà eventuali file pericolosi?** Ovviamente la risposta è negativa e vedremo subito il perché.

Per capire come funziona un aggiornamento è necessario risalire a monte, cioè dal momento in cui un virus viene creato. Seguitemi nel ragionamento:

**Lunedì:** l'imbecille di turno crea un virus, lo allega a una mail e la manda, magari in CC, a un elevato numero di indirizzi, sperando che il virus si diffonda quanto più rapidamente è possibile.

**Martedì mattina:** (vedi dopo)

**Martedì pomeriggio:** l'infezione, infatti, si diffonde, ma per fortuna giunge anche agli indirizzi-civetta, gestiti dal produttore di antivirus. Immediatamente i consulenti si mettono al lavoro, individuano la firma e la inseriscono subito in un file di aggiornamento. A partire da questo istante (supponiamo **ore 14:00 di martedì pomeriggio**), chi scarica l'aggiornamento può individuare – e quindi bloccare sul nascere – il pericolo di infezione / diffusione. Subito dopo, però, i consulenti studiano gli effetti del virus – magari lasciandolo agire su un computer-cavia – stabiliscono le contromosse e inseriscono la procedura di disinfezione in un altro file da scaricare. A partire da questo istante (supponiamo **ore 18:00 di martedì pomeriggio**), l'utente che non ha fatto a tempo a scaricare l'aggiornamento precedente (che si limitava a individuare il file, per impedire il suo download) ed è stato infettato, può comunque provvedere alla disinfezione.

Il problema assume quindi aspetti drammatici, nell'esempio proposto, il **martedì mattina**, quando cioè il virus si sta diffondendo, ma non è ancora giunto all'attenzione dei consulenti. Ne consegue che se martedì mattina abbiamo scaricato il file-virus, questo non può essere individuato dal nostro antivirus. Se i danni che provoca sono limitati, si può porre rimedio il martedì dopo le 18:00, quando saranno disponibili gli aggiornamenti

adeguati. Ma se le cose stanno come descritto, non possiamo fare a meno di trarre la seguente considerazione:

**Se, in questo preciso momento, un nuovo virus si sta diffondendo, nulla vieta che raggiunga il nostro PC prima di quello dei consulenti dell'antivirus. Ma ragionando in questo modo non si può mai avere la certezza assoluta che il nostro PC sia protetto.**

Purtroppo è proprio così, anche se, nel malaugurato caso di infezione, la disinfezione del PC è garantita nell'arco di una giornata: in linea di massima, per nostra fortuna, passano poche ore dal momento della creazione di un virus al momento della sua individuazione e della successiva generazione di contromosse.

Rimane tuttavia il fatto che, almeno in teoria, il nostro PC potrebbe essere uno dei primi a essere infettato da un nuovo virus. Come comportarsi in un caso come questo?

## Come ti frego il virus

Un sistema per limitare drasticamente il pericolo di un'infezione ancora sconosciuta forse c'è. Seguitemi tenendo presente l'esempio di prima:

**Martedì mattina:** scarico file (ma non li apro), scarico mail (ma non le leggo): potrebbero infatti essere infetti di un virus ancora sconosciuto.

**Mercoledì pomeriggio:** sono passate più di 24 ore ed è ragionevole presumere che siano disponibili contromosse per eventuali virus diffusi ieri. Scarico quindi gli aggiornamenti dell'antivirus e sottopongo a esame i file scaricati ieri mattina, che utilizzerò come di consueto se la scansione antivirus non visualizza pericoli di sorta. Subito dopo scarico (eventualmente) nuovi file e nuove mail e – come ieri – li deposito in una cartella sicura, senza aprirli: a loro penserò domani, dopo aver effettuato il download degli aggiornamenti.

**Giorni successivi:** insomma, il trucco è tutto qui. Basta usare file e programmi solo dopo averli sottoposti alla scansione di un antivirus il cui aggiornamento è più recente di almeno 24 / 48 ore dalla data di creazione dei file sospetti.

Pensate che sia un comportamento parzialmente paranoico? Certo, ma... conoscete un informatico realmente "normale"?

**Verifica la disponibilità di eventuali aggiornamenti di questo Tutorial, o la pubblicazione di altre documentazioni, visitando periodicamente il sito:**

[www.alessandrodesimone.net](http://www.alessandrodesimone.net)

**Altri siti con i quali collaboro:**

**easyHDR PRO 1.30** - <http://www.easyhdr.com> - Programma grafico per la gestione della modalità HDR

**FastSum:** <http://www.fastsum.com> Programma per la creazione dell'impronta digitale dei file (metodo MD5)

**TagTuner:** <http://www.tagtuner.com> Programma per la gestione dei file musicali

**Il presente Tutorial è stato modificato il giorno 28 giugno 2007  
Per ulteriori aggiornamenti consultare il sito [www.alessandrodesimone.net](http://www.alessandrodesimone.net)**