



VIRUS WHITER.F

INTRODUZIONE

Riconosciuto per la prima volta l' 11 Maggio 2005 da Panda Software, **WHITER,F** è un troyano che, facendo riferimento a la pirateria di software e musica, cancella tutti gli archivi dell' hard disk. Secondo l'ultimo informe di Panda Software (17/05/05) la pericolosità riscontrata è media, il danno molto alto e la propagazione minima.

CHE E'?

Whiter,f è un troyano, cioè si tratta di un programma che arriva al nostro computer in forma camuffata, presentandosi come qualcosa di inoffensivo. Quando si manda in esecuzione il troyano si installa e realizza determinate azioni che possono compromettere il normale funzionamento del computer o la riservatezza dei dati dell'utente. Il suo nome tecnico è *Trj/Whiter.F*. Fa in modo che il computer smetta di funzionare, rimpiazza tutti i files dell'hard disk con files di testo e posteriormente li elimina.

A QUALE CATEGORIA DI VIRUS APPARTIENE ?

Per il momento non sono uscite varianti e appartiene direttamente a la famiglia dei troyani. Esiste però una relazione con un altro virus: *Nopir*. L'obiettivo di quest'ultimo era infatti la eliminazione degli archivi di files MP3 e COM (propri della pirateria musicale) mentre che Whiter,F, pur eliminando tutti i tipi di files, lascia un messaggio che fa riferimento allo stesso tema.

COME LAVORA ?

Questa nuova variante di malware, come quasi tutti i troyani, non possiede capacità di propagazione propria. I mezzi di diffusione vanno dai tradizionali supporti fisici (CD-ROM, dischetti), a i messaggi di posta elettronica –quelli che contengono allegati-, programmi di scambio di files P2P, canali di IRC o trasferimenti di files FTP.

Una volta entrato nel computer, il troyano genera una cartella chiamata WXP nella directory principale dell'utente. Detta cartella contiene la frase in inglese "You did a piracy, you deserve it" ("Hai commesso un atto di pirateria, te lo meriti"), frase simile a quella utilizzata del creatore del virus *Nopir*.

Questo malware prima sostituisce tutti i files dell'hard disk con il file di testo prima menzionato, e di seguito li elimina completamente, in modo che il computer infettato smette di funzionare e per questo lo si considera estremamente dannoso. Inoltre questo provoca che se l'utente prova a recuperare le sue informazioni tramite uno dei software di recupero dati esistenti, l'unico che otterrà saranno files di testo del tipo menzionato.

Whiter, F è difficile da riconoscere a prima vista in quanto che non mostra nè messaggi nè avvisi della propria presenza. Per disgrazia gli unici sintomi visibili che testimoniano la presenza del troyano in un computer infettato è che quest'ultimo non riesce più a realizzare il processo di avvio o tiene notevoli problemi nel funzionare correttamente.

COME ELIMINARLO?

Come già detto questo virus non è facile da riconoscere. Al momento la unica maniera di eliminarlo è tenere un antivirus aggiornato che, dopo aver riconosciuto il virus, permetta di eliminarlo con una delle differenti opzioni che presenta.



MINIMIZZARE I DANNI DI UN VIRUS:

1. Se il suo computer è collegato ad una rete, lo isoli il prima possibile in maniera che l'infezione non si propaghi.
2. Sospenda l'accesso ad Internet del computer infetto.
3. Se possiede un software antivirus, contatti il suo fornitore e segua le indicazioni per la sua disinfestazione.
4. Aggiorni il suo antivirus e installi le opzioni di sicurezza del suo Sistema Operativo
5. Analizzi il resto dei processori connessi alla rete per controllare che non siano stati infettati.
6. Se il virus contiene un troyano che permette l'accesso esterno di hackers al suo computer, cambi tutte le passwords.
7. Se possiede copie di sicurezza o backup recenti, si assicuri che non siano stati infettati prima di recuperare i suoi dati.
8. Analizzi i buchi del suo sistema di sicurezza e tenti di eliminare gli errori che hanno permesso la infezione.

ULTERIORI INFORMAZIONI SUL VIRUS:

- Alerta Antivirus (<http://alerta-antivirus.red.es/>)
- Panda Software (<http://www.pandasoftware.es/>)
- Trend Micro (<http://es.trendmicro-europe.com/>)
- Enciclopedia Virus (Ontinent) (<http://www.enciclopediavirus.com>)
- McAfee (<http://es.mcafee.com>)
- Symantec (<http://www.symantec.com/region/es/>)
- VS Antivirus (<http://www.vsantivirus.com>)
- Kaspersky (viruslist.com) (<http://www.viruslist.com/eng/index.html>)
- Bit Defender (<http://www.bitdefender-es.com/>)
- Sophos (<http://esp.sophos.com>)
- Hacksoft (<http://www.hacksoft.com.pe>)
- PerAntivirus (<http://www.perantivirus.com/>)

GLOSSARIO:

- **Directory principale:** E' la cartella o directory principale (più importante) di un hard disk.
- **FTP (File Transfer Protocol):** E' un meccanismo che permette il trasferimento di cartelle attraverso una connessione TCP/IP (questo tipo di connessione è quella utilizzato in Internet)
- **IRC (Chat IRC):** E' normalmente conosciuto come chat. Si tratta di conversazioni scritte con una o più persone attraverso Internet e che in più permettono il trasferimento di files.
- **Malware:** E' il risultato di due parole anglosassoni : *MALicious softWARE*. Si riferisce a qualsiasi programma, documento o messaggio, suscettibile di causare danni all'utente di sistemi informatici.