



VIRUS WHITER.F

INTRODUCCIÓN

Reconocido por primera vez el día 11 de Mayo de 2005 por Panda Software, **WHITER.F** es un troyano que, haciendo referencias a la piratería de software y música, borra todos los ficheros del disco duro. Según el último informe de Panda Software (17/05/05) su peligrosidad es media, el daño es muy alto y la propagación mínima.

¿QUÉ ES?

Whiter.F es un troyano, es decir, se trata de un programa que llega al ordenador de manera encubierta simulando tratarse de algo inofensivo. Cuando se ejecuta, el troyano se instala y realiza determinadas acciones que pueden afectar el buen funcionamiento del equipo o a la confidencialidad del usuario afectado. Su nombre técnico es *Trj/Whiter.F*. Hace que el ordenador deje de funcionar, ya que reemplaza todos los archivos del disco duro por un archivo de texto, y posteriormente los elimina.

Whiter.F está escrito en el lenguaje de programación Visual C++. Este troyano tiene un tamaño de 295158 Bytes, y está comprimido mediante PE-Compact.

Por el momento, el país más infectado por este virus es Japón.

¿QUÉ CLASES HAY?

Por el momento no han surgido variantes y se relaciona directamente con la familia de los troyanos. Si bien se busca una relación con un gusano aparecido unas semanas antes: *Nopir*. El objetivo de este gusano era la eliminación de los ficheros MP3 y COM del ordenador. La única relación entre ambos es que *Nopir* ataca ficheros propios de la piratería musical, mientras que *Whiter.F*, a pesar de que borra todos los ficheros del ordenador, deja un mensaje alusivo al tema de la piratería.

¿CÓMO ACTÚA?

Esta nueva variante de malware, como la práctica totalidad de los troyanos, no posee capacidad de propagación propia. Los medios de propagación van desde los tradicionales soportes físicos (CD-ROM, disquete), a los mensajes de correo electrónico –en los que se integran como adjuntos–, programas de intercambio de ficheros P2P, canales de IRC o transferencia de ficheros FTP.

Una vez instalado al ordenador, el troyano genera un fichero llamado WXP en el directorio raíz del equipo del usuario. Dicho archivo contiene la frase en inglés "You did a piracy, you deserve it" ("Cometiste un acto de piratería, te lo mereces"), lo que se asemeja a las amenazas lanzadas por el creador del gusano *Nopir*.

Tras ello, este malware sustituye todos los ficheros del disco duro por dicho archivo de texto y, a continuación, los elimina completamente, de modo que el ordenador afectado deja de funcionar, por lo que se considera a este troyano extremadamente dañino. Esto provoca además que, si el usuario pretende recuperar su información por medio de alguna de las herramientas existentes a tal efecto, sólo obtendrá ficheros con el mencionado mensaje.

Whiter.F es difícil de reconocer a simple vista, ya que no muestra mensajes ni avisos que alerten sobre su presencia. Por desgracia, los únicos síntomas visibles que delatan la presencia del troyano en un ordenador afectado es que este no pueda arrancar o tenga problemas para funcionar correctamente.



¿CÓMO ELIMINARLO?

Como ya se ha mencionado, no es un virus que sea fácil de reconocer. Por el momento, la única manera de eliminarlo es tener el antivirus actualizado y una vez que éste lo haya localizado, eliminarlo con las diferentes opciones que le ofrece su antivirus.

MINIMICE LOS DAÑOS DE UN VIRUS:

1. Si posee ordenadores conectados en red, aíse el ordenador o Pc infectado para que la infección no se propague.
2. Suspenda el acceso a Internet del ordenador infectado.
3. Si posee software antivirus, contacte con su proveedor y siga las indicaciones para su desinfección.
4. Actualice el antivirus e instale los parches de seguridad de su sistema operativo.
5. Analice el resto de equipos de la red, por si han sido infectados.
6. Si el virus contiene un Troyano que permite el acceso externo de hackers a su equipo, cambie las contraseñas.
7. Si posee copias de seguridad o backups recientes, asegúrese de que están libres de virus antes de recuperarlos.
8. Analice los fallos de su sistema de seguridad y subsane los errores que permitieron la infección.

MÁS INFORMACIÓN SOBRE 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.encyclopediavirus.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/>)

GLOSARIO:

- **Directorio raiz:** Es la carpeta o directorio principal (más importante) de un disco.
- **FTP (File Transfer Protocol):** Es un mecanismo que permite la transferencia de ficheros a través de una conexión TCP/IP (este tipo de conexión es el utilizado en Internet)
- **IRC (Chat IRC):** Es lo que se conoce vulgarmente como chat. Son conversaciones exritas con una o más personas a través d eInternet, y que además permiten la transferencia de ficheros..
- **Malware:** Es el resultado de dos palabras anglosajonas: *MAL*icious soft*WARE*. Es cualquier programa, documento o mensaje, susceptible de causar perjuicios a los usuarios de sistemas informáticos.