

Desinfección sencilla de Malware

Autor: Adrian Abras

Edición y Corrección: Lic. Cristian Borghello, MVP - CISSP

Fecha Publicación: 05 de marzo de 2010

Publicado en [Segu-Info](http://www.segu-info.com.ar)

Malware

¿Qué es Malware?

El término malware (una abreviatura de la frase, software malicioso) como un sustantivo colectivo para referirse a los virus, gusanos y caballos de Troya. La gran cantidad y variedad de códigos malintencionados existentes, hace que sea difícil dar una definición perfecta de cada categoría de malware. Para discusiones generales de antivirus, las siguientes definiciones simples de malware se aplican:

Trojan Horse (trojano): un programa que parece ser útil o inofensivo, pero que contiene código oculto diseñado para explotar o dañar el sistema en el que se ejecuta. Los troyanos se envían normalmente a los usuarios a través de mensajes de correo electrónico, mensajería, redes P2P, redes sociales, etc.

Worm: un gusano propaga por sí mismo código malicioso que puede automáticamente distribuirse de un equipo a otro a través de conexiones de red. Un gusano puede realizar acciones dañinas, tales como consumir los recursos de la red y causar un ataque de denegación de servicio.

Virus: un virus utiliza el código escrito con la intención expresa de auto-replicarse. Un virus intenta esparcirse de computadora a computadora adjuntándose o inyectándose en un programa host. Este puede dañar hardware (en muy raras ocasiones), software o datos. Cuando el host es ejecutado, el código del virus también es ejecutado, infectando a otros hosts.

Objetivos

El malware intenta atacar un host, hay un número de componentes específicos que este necesita antes de que el ataque sea satisfactorio. Los siguientes son algunos ejemplos de que puede requerir el malware para atacar.

- **Dispositivos:** algunos malware específicamente apuntan a un tipo de dispositivo, como PCs, Macintosh o *smartphone*, etc.
- **Sistemas Operativos:** el Malware puede requerir un sistema operativo particular para ser efectivos.
- **Aplicaciones:** puede requerir que una aplicación particular este instalada en la computadora victima antes de que este ejecute su payload.

Transporte

Si el malware es un virus, este intentara abordar un objeto transportador para infectarlo. El número y tipo de transportadores pueden variar ampliamente, está es una lista de los más comunes:

- **Ejecutables:** .com, .pif, .scr, .sys, .dll, .ovl, .ocx
- **Scripts:** .vbs, .js, .wsh, .pl.
- **Macros:** embebidos en macros de herramientas de ofimática, etc.
- **Sector de Booteo**

Control de la infección y Recuperación

Dado que los ataques de malware han crecido en complejidad, no existe un solo proceso para removerlo del sistema. Cada tipo de ataque tiene su propio remedio. Sin embargo, esto no disminuye el valor de la definición de un proceso de identificación, y la recuperación ante un ataque. Los pasos serían:

- Confirmar la infección
- Respuesta ante el incidente
- Análisis del Malware
- Recuperación del sistema

Confirmar la infección

La habilidad de determinar si el sistema fue infectado, nos da la posibilidad de disminuir el riesgo de infección.

Hay muchas formas diferentes de malfuncionamiento que pueden ser malinterpretados como comportamientos de malware, este debe ser determinado por el soporte técnico, y a partir de allí tomar la acción necesaria.

Si durante el comportamiento sospechoso, el antivirus no reporta ningún virus, también es importante el uso de programas como malware-bytes, y de [SpyBot Search and Destroy](#), que permitan buscar otros malware.

También es importante el escaneo del disco rígido desde otro equipo, removiendo el disco infectado del equipo e instalando en otro equipo destinado para esa función, preferentemente con un antivirus diferente al usado por el equipo infectado.

Otra posibilidad es el uso de CD booteables desde el cual es posible arrancar el sistema y escanear el disco sospechado de estar infectado.

Respuestas ante el incidente

En caso de estar infectado, lo primero que debe hacer es aislar el equipo del resto, luego:

Crear una imagen del sistema dañado, para hacer las siguientes tareas, así podemos analizar el tipo de infección y el comportamiento.

Si la imagen se realiza y es ejecutada en una maquina virtual, considerar que algunos malware detectan que están siendo ejecutados en entornos virtuales y no ejecutan su payload, para que no puedan ser analizados.

Procesos Activos y Servicios

Una vez aislado el equipo, hay que determinar el comportamiento que tiene el malware, para ello se encuentran una serie de herramientas muy útiles:

- [SysInternals](#)
- Antivirus
- [Malwarebytes](#)
- [Microsoft Removal Tool](#)
- Otras

Ver la siguiente información:

- PID, CPU Usage, CPU Time, Memory Usage, Peak Usage, I/O reads, I/O Writes
- Ver cuáles son los procesos que consumen los recursos y el programa asociado al mismo
- Se puede obtener también un listado de los procesos con
`tasklist /v > tasklist.txt`
- Revisar cualquier instancia que se esté ejecutando de conexiones de red (ftp, smtp, web, telnet)
- Si no está seguro de un proceso, buscar en [Process Library](#) para obtener información del mismo.
- Ver todos los procesos, en ejecución y detener los sospechosos.
- Averiguar el Path del programa que está ejecutando el proceso para luego proceder a su eliminación

Revisión de las carpetas de inicio

Es importante revisar todas las carpetas de inicio y configuraciones para evitar que el malware se encuentre alojado allí, intentando ejecutarse al próximo reinicio.

Tener en cuenta que la mayoría de los datos a buscar van a estar oculto. (dir /a)

Ver la siguiente información:

c:\Documents And Settings\All users\Start Menu

c:\Documents And Settings\"usuario"\Start Menu (donde usuario detalla el nombre del mismo)

c:\Documents And Settings\"usuario" (muchos tipos de malware, se ocultan debajo de esta)

Revisión de los temporales del usuario, y luego vaciamiento (disco local, IE, firefox, etc)

Revisar el scheduler mediante

```
at > c:\jobs.txt
```

Análisis del registro

Tenga en cuenta que cualquier manipulación que se haga sobre el registro puede dañar el funcionamiento del equipo, bien sea este por error humano, o por el payload que pueda ejecutar el malware.

Ver la siguiente información:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\KnownDLLs

HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\KnownDLLs

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\RunOnce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\RunOnceEx

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows

("run=" line)

HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\RunOnce

HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\RunOnceEx

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows ("run=" value)

HKEY_CLASSES_ROOT\CLSID{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32, controla la carga de IE.

También se puede usar la herramienta System Configuration Utility, disponible en:

http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/msconfig_usage.msp?mfr=true

Revisar malware y archivos corruptos

Una forma de saber que archivos fueron modificados en el sistema es realizar una búsqueda, de los archivos modificados, con la herramienta de búsqueda de Windows.

- Si ejecuta herramientas como malwarebytes, este le informa de los archivos de malware, y no se debe tomar ninguna acción, sino averiguar para cada uno de ellos como trabajan, así se encuentran los archivos asociados, y las modificaciones al Registry.
- Antes que nada, vaciar todos los temporales del sistema (C:, IE, firefox, archivos temporales, etc), para evitar que se alojen en esos lugares.
- Obtener un listado de todos los archivos que se encuentran en el sistema, y guardarlo en un archivo de texto para su análisis:

```
dir /s /-c /o:-d /t:c /q > filelist.txt
```

- Uno de los archivos que mas usan los malware es el archivo svchost.exe que está en %WINDIR%\system32.
- También el malware se aloja en RECYCLER, el cual debe ser vaciado.
- NO usar puntos de restauración, dado que también es un punto donde se almacena el malware.
- Prestar atención a los archivos que fueron renombrados, principalmente que se le cambio la extensión, ejemplo .exe por .ex_.
- Algunos malware afectan el archivo *hosts* (en %WINDIR%\system32\drivers/etc), renombrando el original y agregando allí su código de redirección de DNS.
- Una de las características avanzadas del File System NTFS es File Streaming, y esto hace que el malware se oculte detrás de un archivo valido.(ej: archivo.txt, pero realmente es archivo.txt:malware.exe)
- Revisar en %WINDIR%\win.ini, %WINDIR%\system.ini, %WINDIR%\autoexec.nt, %WINDIR%\config.nt
- Ver la secuencia de carga de Windows y los procesos, y eliminar servicios que no sean necesarios o sospechosos.(usar SysInternals)

Importante: Una vez detectados los archivos de malware, buscar en internet para entender como es su payload, y si genera otros archivos, para buscarlos y eliminarlos.

Revisar usuarios y grupos

Algunos malware intentan elevar privilegios de usuarios existentes, revisar las configuraciones de los mismos, para ver si hubo modificaciones, revisando:

- Nombres de usuarios extraños
- Derechos de usuarios inválidos
- Grupos que contiene miembros inválidos
- usuario recientemente creados
- Revisar que usuarios pertenecen al grupo Administradores
- Revisar también las carpetas compartidas, y los permisos de cada usuario.
- Ver Well-known security identifiers in Windows operating systems, en: <http://support.microsoft.com/?kbid=243330>

Conexiones de Red

Es básico en todo entorno de computación que la red este funcionando correctamente, hay bastantes malware que atacan a los servicios de red, generando una denegación de servicios en la red, e infectando a otros equipos también.

Es importante revisar:

- Que puertos tiene abierto el firewall

- Que programas están transmitiendo/recibiendo.
- Analizar las conexiones de red (netstat, tcpview)
`netstat -ano >c:\red.txt`
- Revisar la configuración de red, (ip, dns, wins)
- Revisar el archivo *hosts* ya mencionado

Revisión de Logs

Es posible usar el sistema de manejo de eventos de MS, para revisar los logs, y analizar el comportamiento del malware. Los archivos están almacenados en *C:\Winnt\System32\Config* y se llaman *AppEvent.evt*, *SecEvent.evt*, y *SysEvent.evt*.

- Buscar por cambios al momento de la infección
- Comparar las horas de los eventos, con las fechas de modificación de los archivos
- Buscar cuentas que hayan creado o cambiado la clave erróneamente, a la hora de la infección

Recuperación del sistema

Una vez que haya eliminado el malware, y obtenido toda la información del malware, se debe pasar a reparar los archivos de Windows o aplicativos necesarios.

Para ello:

- Reparar con programas como [Tuneup](#) (pago) el registry para que elimine las claves dañadas que quedan de la eliminación de los archivos infectados.
- Si determinamos que el sistema está limpio, instalar el SP último para la versión de Windows, para que repare los archivos dañados.
- Instalar la última versión de IE8, Firefox, etc.
- Revisar los programas aplicativos que no estén dañados, y reponerlos en caso de que sea necesario
- Usar [MSBA](#), para que revise que patches hacen falta al sistema operativo.

Hay que tener en cuenta que los ataques de los gusanos más sofisticados tienen diferentes payloads, variando a medida que están siendo eliminados, y esto puede hacer que el sistema sea inutilizado.