

CERTuy

Guía rápida sobre el worm Conficker (a.k.a. Downadup)

Tabla de Contenidos

Introducción.....	3
¿Cómo se propaga?.....	3
¿Que síntomas pueden existir?	4
¿Cómo estoy seguro de que estoy infectado?.....	4
¿Cómo prevenir la infección?.....	5
¿Qué pasos ejecuto para limpiar una máquina?.....	5
Clausula de exención de responsabilidades.....	6
Referencias	6

Introducción

Conficker, también conocido como Downup Devian, Downandup y Kido, es un worm que apareció en octubre de 2008, ataca el sistema operativo Microsoft Windows. El gusano explota una vulnerabilidad en el servicio Windows Server usado por Windows 2000/XP/Vista/Server 2003/Server 2008 y la beta de Windows 7.

El virus se propaga a sí mismo principalmente a través de una vulnerabilidad del desbordamiento de bufer del servicio Server de Windows. Usa una solicitud RPC especialmente desarrollada para ejecutar su código en el computador objetivo.

Para una mejor descripción se recomienda leer el siguiente documento del Honeynet Project:

<http://honeynet.org/files/KYE-Conficker.pdf>

¿Cómo se propaga?

1. Intenta infectar otras computadoras en la red explotando la vulnerabilidad [MS08-067](#) en los sistemas operativos de MS.
2. Intenta copiarse a sí mismo en el directorio compartido para administración ADMIN\$ de la máquina a la que está atacando. Este directorio es el de Windows por defecto. Para intentar lograrlo lo hace con la cuenta del usuario que se encuentra logueado a la máquina infectada, en caso de no lograrlo, tiene una lista de usuarios y contraseñas con las cuales comienza a realizar intentos de logueo. Cuando lo logra y tiene permiso para escribir en el ADMIN\$, se copia a sí mismo.
3. Se copia a sí mismo a dispositivos removibles como discos USB agregando un archivo de extensión INF cuando se accede al dispositivo, esto hace que al correr el Autoplay, la primera opción que se muestra para ejecutar sea una que el worm agrega, la cuál al ser ejecutada, hace que el worm se ejecute.

Se agrega como servicio y agrega una clave en la registry para ejecutarse cada vez que levanta el equipo, termina varios servicios e intenta terminar cualquier programa/servicio de antivirus o similar que se encuentre instalado en el equipo (tiene una lista); adicionalmente bloquea el acceso a los sitios de Windows Update y de los fabricantes de AV, impidiendo de esta forma que se pueda actualizar los parches de seguridad y la lista de los AV. Instala un servicio con nombre aleatorio y una dll con

nombre randomico en un directorio, oculta y con una ACL muy restringida, lo cual hace que sea bastante compleja su detección y remoción.

¿Que sintomas pueden existir?

Aquí se encuentra una lista (no exhaustiva) de los síntomas que se pueden percibir al tener una infección por el Conficker:

- No se puede actualizar Windows mediante Windows Update.
- No se puede actualizar el AV automáticamente o acceder a la página del fabricante.
- Archivos .INF no conocidos en la raíz de los discos duros, discos USB ó en la Papelera de Reciclaje.
- En ambientes con usuarios de MS-AD con política de bloqueo de cuentas al n intentos: bloqueo de las cuentas de usuarios.
- Ciertos servicios (Automatic Updates, BITS, Windows Defender, Error Reporting Services están deshabilitados.
- Se puede ver cierta lentitud en los Domain Controllers de MS-AD
- Escaneos del puerto 445/TCP.
- Actividad anormal a nivel de lookup en el DNS.
- Accesos a shared administrativos no están habilitados.

¿Cómo estoy seguro de que estoy infectado?

- Acceder a http://www.confickerworkinggroup.org/infection_test/cfeyechart.html ó a http://four.cs.uni-bonn.de/fileadmin/user_upload/werner/cfdetector/
- Existen varias herramientas que permiten detectarlo en la red (scripts en Phyton) y otras para limpiar la memoria, firmas para Snort, etc. en: <http://iv.cs.uni-bonn.de/wg/cs/applications/containing-conficker/>
- Herramienta de Mc Afee <http://www.mcafee.com/us/enterprise/confickertest.html> (para red).

Las de acceso online son prácticas para pocos casos, para casos de redes muy complejas o grandes se recomiendan los scripts o la de Mc Afee.

¿Cómo prevenir la infección?

- Aplicar los parches correspondientes para la [MS-08-067](#).
- Deshabilitar [compartir archivos e impresoras](#).
- [Utilizar passwords complejas](#).
- [Deshabilitar el autorun en las máquinas](#).

¿Qué pasos ejecuto para limpiar una máquina?

- Desconectar los PCs infectados de la red y comenzar en cada uno de ellos un proceso de limpieza que se describe a continuación.
- [Deshabilitar la opción de System Restore de Windows XP](#) para evitar que el Conficker permanezca oculto en esos archivos.
- Rebootear el PC en modo [“A Prueba de Fallos sin conexión a la red”](#).
- Ingresar al PC con un usuario local con privilegios de administrador.
- Instalar como mínimo el parche de [MS08-067](#).
- Ejecutar alguna de las herramientas de remoción del Conficker:

<http://www.confickerworkinggroup.org/wiki/pmwiki.php?n=ANY.RepairTools>

http://www.symantec.com/security_response/writeup.jsp?docid=2009-011316-0247-99 (Symantec)

<http://www.sophos.com/support/knowledgebase/article/54457.html>

(Sophos - para una máquina y para la red).

http://vil.nai.com/vil/conficker_stinger/S.T.I.N.G.E.R.exe (Mc Afee)

<http://www.pandasecurity.com/homeusers/security-info/about-malware/encyclopedia/overview.aspx?lst=sol&idvirus=204292> (Panda)

<http://iv.cs.uni-bonn.de/wg/cs/applications/containing-conficker/>

<http://support.microsoft.com/kb/890830> (Microsoft)

NOTA: algunas pueden requerir botear multiples veces e inclusive correrlas más de una vez para realizar la desinfección correctamente.

- Instalar un antivirus con la lista de actualización al día de la fecha y configurarlo correctamente.
- Conectar el PC a la red
- Ingresar a los sitios web de chequeos online.

Clausula de exención de responsabilidades

Este documento es una guía de referencia, no siendo obligatorio para el lector ejecutar dichos pasos al pié de la letra. No nos hacemos responsables de daños ocasionados por la implementación de las recomendaciones descritas.

Referencias

- www.microsoft.com
- www.sophos.com
- www.symantec.com
- www.pandasecurity.com
- www.mcafee.com
- www.confickerworkinggroup.org
- iv.cs.uni-bonn.de
- www.honeynet.org
- www.wikipedia.com