

HISTORIA DE CONFICKER (DOWNADUP)

**Introducción al gusano Conficker y su
evolución**

ÍNDICE

1.	INTRODUCCIÓN A CONFICKER	3
2.	PRINCIPIOS: DOWNADUP.A	5
3.	LA EVOLUCIÓN: DOWNADUP. B Y DOWNADUP.B++	6
4.	CONFICKER.C	7
5.	LA ÚLTIMA VERSIÓN: CONFICKER.E	8
6.	PREGUNTAS FRECUENTES RELATIVAS A CONFICKER	9
6.1.	¿Qué significa que Conficker.C se activa el 1 de abril?	9
6.2.	Cuáles son las principales características de cada versión	10
6.3.	¿Qué es el Conficker Working Group?	10
6.4.	¿Para qué se conecta Conficker a Internet?	11
6.5.	¿Quién ha creado Conficker?	11
6.6.	¿Cómo puedo saber si estoy infectado?	11
6.7.	Mi ordenador está infectado con Conficker ¿Cómo puedo eliminarlo de mi equipo?	12

1. INTRODUCCIÓN A CONFICKER

A finales de noviembre de 2008 surgió un nuevo malware que fue llamado por las casas antivirus como Conficker, Downadup o también Kido.

Este gusano, en lo que viene a ser una practica creciente, fue diseñado con el objetivo de que el atacante pudiera tomar el control de las maquinas infectadas, formando parte de lo que se conoce como [red zombie o botnet](#).

Dos de las características más destacables del gusano son que:

- Para infectar los sistemas aprovechaba la vulnerabilidad [CVE-2008-4250](#)¹, que permitía ejecutar remotamente código en el sistema. Destacar que mientras que el gusano apareció en noviembre, la vulnerabilidad ya había sido previamente solucionada por Microsoft en octubre, en su [parche MS08-067](#)².
- Para conectarse con el creador del malware y recibir nuevas instrucciones, accedía a determinadas direcciones de Internet. Diariamente se conectaba a 250 direcciones de Internet, lo que hacía prácticamente inviable su bloqueo.

Posteriores versiones del gusano, además de dificultar su detección y desinfección, también añadían nuevos mecanismos de propagación, utilizados anteriormente en otras familias de gusanos:

- A través de carpetas compartidas en red protegidas con contraseñas débiles.
- Mediante la compartición de dispositivos extraíbles, por ejemplo, lápices USB.

Debido a que el principal mecanismo de propagación era a través de una vulnerabilidad que ya estaba resuelta, la mayoría de organismos de seguridad no lo consideraron una amenaza seria. Estas previsiones resultaron ser erróneas, y a mediados de enero se estimaba que había casi 9 millones de ordenadores infectados³ con este gusano, o con alguna de sus versiones.

Sin embargo, se podían haber evitado estas infecciones siguiendo unas [buenas prácticas](#)⁴:

¹ http://www.inteco.es/vulnDetail/Seguridad/INTECOCERT/Actualidad/Actualidad_Vulnerabilidades/detalle_vulnerabilidad/CVE-2008-4250

² <http://www.microsoft.com/spain/technet/security/Bulletin/MS08-067.msp>

³ <http://www.f-secure.com/weblog/archives/00001584.html>

⁴ http://www.inteco.es/Seguridad/INTECOCERT/Formacion/Buenas_Practicas/Ciudadanos_Consejos_de_Seguridad/

- Tener todo el software del ordenador debidamente actualizado. Para facilitar esta tarea se recomienda [activar las actualizaciones automáticas](#).
- A parte de tener instalado un antivirus (y actualizarlo frecuentemente), también tener instalado un cortafuegos configurado para que no permita el tráfico de información de aplicaciones que no se conocen ni tenga abiertos puertos que no se utilizan.
- Utilizar contraseñas robustas en las carpetas compartidas en red.
- No tener activada por defecto la opción de autoarranque para los dispositivos extraíbles⁵.

Por último, comentar que aunque hasta abril el gusano había permanecido relativamente “dormido”, según fuentes especializadas⁶, actualmente la red zombie esta siendo explotada para el envío de correo basura –spam- y la venta de [falsas soluciones de seguridad](#).

A continuación se indican brevemente la evolución de la familia Conficker, con las y principales características de cada una de las diferentes versiones de este código malicioso.

⁵ Debido a esta característica del virus, Microsoft ha incorporado una mejora de la gestión del Autorun por parte de su próximo sistema operativo, Windows 7.

⁶ <http://www.viruslist.com/en/weblog?weblogid=208187654>

2. PRINCIPIOS: DOWNADUP.A

El 23 de Noviembre de 2008 surgió un nuevo *malware* que fue llamado por las casas antivirus Downadup, Conficker o también Kido y que sus características principales son:

Se propaga explotando la vulnerabilidad [CVE-2008-4250](#)⁷ que ya había sido parcheada por Microsoft en su boletín: [MS08-067](#)⁸.

Se conecta a determinadas direcciones de Internet, la forma que utiliza para saber a qué dirección se tiene que conectar es consultando en alguna página de Internet – preferiblemente un buscador - la fecha actual y en función de la fecha, calcula cuál es la URL a la que tiene que acceder en ese momento. El número de páginas diarias a las que podía acceder el gusano ascendía a 250.

- **Muestra publicidad de varias herramientas falsas de seguridad**, para engañar al usuario de que su equipo está infectado y es necesario desinfectarlo. Estas herramientas son falsas y la única infección que hay en el ordenador es la producida por el gusano, que no se elimina comprando el producto que ellos ofrecen.

⁷ http://www.inteco.es/vulnDetail/Seguridad/INTECOCERT/Actualidad/Actualidad_Vulnerabilidades/detalle_vulnerabilidad/CVE-2008-4250

⁸ <http://www.microsoft.com/spain/technet/security/Bulletin/MS08-067.msp>

3. LA EVOLUCIÓN: DOWNADUP. B Y DOWNADUP.B++

A finales de Diciembre se detectó una nueva versión de este gusano, la versión B, con las siguientes características:

Utilizaba los siguientes mecanismos de propagación:

- Explotando la vulnerabilidad CVE-2008-4250, igual que la primera versión de Conficker.
- **Dejando copias de sí mismo en las carpetas compartidas de Microsoft** que estuviesen protegidas por contraseñas débiles –esto hizo que gran cantidad de ordenadores de una misma empresa se quedasen infectados rápidamente-.
- **Dejando copias de sí mismo en dispositivos extraíbles** con un fichero de autoarranque para que, cuando se conectase el dispositivo en un ordenador, se ejecutase automáticamente y el nuevo equipo quedase infectado.
- **Aunque un ordenador tuviese instalado el parche de Microsoft, se podía quedar infectado de alguna de las otras dos formas añadidas.**
- Bloqueaba algunas medidas de seguridad, por ejemplo, impedía el acceso a Internet de programas antivirus para que no pudiesen actualizar sus firmas de virus y que así les resultase más difícil eliminar el gusano y detectar nuevas versiones de malware.

Pesé a que el principal método de propagación era utilizando una vulnerabilidad que ya había sido solucionada por Microsoft, gran cantidad de ordenadores resultaron infectados por este virus

4. CONFICKER.C

A principios de Marzo surgió la versión C de este gusano –[Downadup.C](#)⁹–, que tiene las siguientes características:

Contiene un listado de direcciones de Internet a las que acceder, pero en vez de ser 250, como en versiones anteriores, al día genera **50.000**^{10 11}, lo que hace prácticamente inviable bloquear todas ellas. Aunque realmente sólo utilizará 500 de las 50.000 direcciones¹² creadas y, **el acceso a Internet sólo está implementado para que funcione a partir del 1 de abril.**

Esto tiene el inconveniente de que algunas de las direcciones a las que puede acceder el gusano, son legítimas y existen en la actualidad, por lo que si un administrador Web decide bloquear el acceso a todos los sitios de Internet que va a acceder el programa malicioso, impedirá el acceso a algunas páginas legítimas¹³.

- Su código está muy ofuscado, lo que hace muy difícil analizarlo¹⁴.
- Es más “agresivo” que sus versiones anteriores, detiene la ejecución de varios programas e impide el acceso a determinadas direcciones de Internet de páginas de seguridad. De este modo, ni los programas antivirus pueden actualizar sus firmas, ni un usuario puede acceder a estas direcciones para consultar información de seguridad o descargarse alguna herramienta que permita la desinfección de este virus. También detiene la ejecución de varios procesos¹⁵ y elimina la opción de volver a un punto de restauración anterior y todos los puntos de restauración que hubiese creados en el sistema¹⁶.

⁹ http://www.inteco.es/virusDetail/Seguridad/INTECOCERT/Actualidad/Actualidad_Virus/Detalle_Virus/Downadup_C

¹⁰ <http://www.diarioti.com/gate/n.php?id=21582>

¹¹ <http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FDOWNAD%2EKK&VSect=T>

¹² <http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FDOWNAD%2EKK&VSect=T>

¹³ <http://www.sophos.com/security/blog/2009/03/3457.html>

¹⁴ <http://mtc.sri.com/Conficker/addendumC/>

¹⁵ <http://blog.s21sec.com/2009/03/confickerc-mas-peligroso-que-los.html>

¹⁶ <http://www.ca.com/us/securityadvisor/virusinfo/virus.aspx?id=77976>

5. LA ÚLTIMA VERSIÓN: CONFICKER.E

Después de la expectación surgida durante los primeros días de abril acerca de la conexión a Internet de Conficker.C, el día 7 de abril se descubrió una nueva variante de este gusano: [Downadup.E](#)¹⁷. Sus principales características son:

- **No se conecta a direcciones de Internet** como sus versiones anteriores. Lo que sí que hace es conectarse a través de P2P con otros ordenadores que también estén infectados con Conficker. De este modo, ya no es posible bloquear las direcciones de Internet a las que se va a conectar el gusano.
- **Muestra publicidad de falsos productos de seguridad informática.**
- **Tiene fecha de desactivación.** Cuando detecte que la fecha del sistema es el **3 de mayo** o posterior, se autoeliminará del ordenador, borrando todos los ficheros y entradas del registro que haya creado para su funcionamiento en el equipo.
- Explota nuevamente la vulnerabilidad de Microsoft solucionada en su [parche MS08-067](#)¹⁸, si un ordenador no tiene instalada esta actualización, puede quedarse infectado fácilmente.

¹⁷ http://www.inteco.es/virusDetail/Seguridad/INTECOCERT/Actualidad/Actualidad_Virus/Detalle_Virus/Downadup_E

¹⁸ <http://www.microsoft.com/spain/technet/security/Bulletin/MS08-067.aspx>

6. PREGUNTAS FRECUENTES RELATIVAS A CONFICKER

Las preguntas más usuales que se suelen hacer de este gusano son:

6.1. ¿Qué significa que Conficker.C se activa el 1 de abril?

El gusano Conficker se caracteriza por acceder a determinadas direcciones de Internet. La dirección a la que accede depende de la fecha y hora del sistema. Sin embargo, Conficker.C sólo intentará acceder a Internet con su listado de direcciones a partir del 1 de Abril ¹⁹²⁰, si la fecha del sistema es anterior al 1 de abril, no intentará el acceso a Internet.

El 1 de abril en varios países es el día de los inocentes, por lo que algunas empresas de seguridad han creado artículos con un doble sentido como:

[New Conficker Variant Not Fooling Around](#)²¹

Excepto el listado de direcciones a las que acceder, el resto de acciones que realiza Conficker.C están siempre habilitadas, desde el primer momento de la infección, sin importar que la fecha de la infección sea anterior al 1 de abril.

Aunque algunos medios de comunicación fueron muy catastrofistas acerca del 1 de abril y de la conexión a Internet por parte de Conficker.C, en realidad, no sucedió nada especial ese día.

¹⁹ <http://www.ca.com/us/securityadvisor/virusinfo/virus.aspx?id=77976>

²⁰ <http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FDOWNAD%2EKK&VSect=T>

²¹ <http://community.ca.com/blogs/securityadvisor/archive/2009/03/11/new-conficker-variant-not-fooling-around.aspx>

6.2. Cuáles son las principales características de cada versión

A continuación se muestra una tabla con diferentes características de cada versión:

	W32.Downadup	W32.Downadup.B	W32.Downadup.C
Propagación	<ul style="list-style-type: none"> Explotación de la ausencia MS08-67 	<ul style="list-style-type: none"> Explotación de la ausencia de MS08-67 Compartición forzada a través de P2P Medios extraíbles 	No tiene
Comandos y control (C&C)	<ul style="list-style-type: none"> HTTP 	<ul style="list-style-type: none"> HTTP Antigua P2P 	<ul style="list-style-type: none"> HTTP mejorado P2P robusta
Medidas de Autoprotección	Ninguna	<ul style="list-style-type: none"> Detiene la revisión de los DNS Detiene las actualizaciones automáticas Firmado del código HTTP y P2P 	<ul style="list-style-type: none"> Para la revisión de los DNS Impide las actualizaciones automáticas Firma el código HTTP y P2P Detiene el software de seguridad

Tabla de Symantec 1

Esta tabla se encuentra disponible en:

https://forums2.symantec.com/t5/blogs/blogarticlepage/blog-id/malicious_code/article-id/253

6.3. ¿Qué es el Conficker Working Group?

También conocido por Conficker Cabal, es una asociación formada por varias empresas de seguridad informática, la ICANN –organismo internacional encargado de asignar las diferentes direcciones IP y nombres de dominio a nivel mundial- y Microsoft, con el objetivo de detener las acciones realizadas por el gusano Conficker. Su principal labor es impedir que Conficker se conecte a las direcciones de Internet que tiene programadas, para ello, intentan bloquear todas estas direcciones. Han creado una página Web con sus acciones que se puede consultar en este enlace:

<http://www.confickerworkinggroup.org/>

6.4. ¿Para qué se conecta Conficker a Internet?

Los creadores de programas maliciosos que se conectan a determinados sitios de Internet, para recibir órdenes de los creadores del *malware*.

Conficker no es una excepción y se conecta a Internet para realizar dos acciones:

- Actualizar su código.
- Recibir órdenes de un atacante remoto, con las que podría realizar diferentes actividades maliciosas:
 - Capturar información personal sensible, como datos bancarios (números de tarjetas o claves de cuentas).
 - Lanzar ataques de denegación de servicio a determinadas IP o páginas Web.
 - Envío de spam, aprovechando la gran cantidad de ancho de banda disponible.
 - Instalar cualquier otro tipo de malware en el equipo.
 - Embaucar al usuario del PC infectado en la compra de falsas soluciones antivirus.

6.5. ¿Quién ha creado Conficker?

Se desconoce quién es el autor de este programa malicioso. De hecho, Microsoft ha ofrecido una sustanciosa recompensa para quien le informe del creador del gusano aunque, por el momento, no se tiene noticia de que nadie haya cobrado la recompensa.

6.6. ¿Cómo puedo saber si estoy infectado?

La forma más fiable es analizar todo su equipo con un antivirus actualizado, de todos modos si sigue sospechando que su equipo está infectado y su antivirus no le detecta la infección, puede probar a analizar su ordenador con un antivirus en línea.

Debido a que Conficker bloquea el acceso a gran cantidad de páginas de seguridad, es posible que tenga problemas para actualizar su antivirus y probar antivirus en línea, en este caso el Conficker Working Group ha creado un sencillo test de visualización de imágenes, puede acceder a él desde este enlace, en el que también se indica cómo interpretar el resultado de las imágenes vistas:

http://www.confickerworkinggroup.org/infection_test/cfeyechart.html

También puede utilizar alguna herramienta específica que le indique si su equipo está infectado o no. Algunos fabricantes antivirus han generado varias herramientas gratuitas para identificar la infección, como:

- McAfee: <http://www.mcafee.com/us/enterprise/confickertest.html>

6.7. Mi ordenador está infectado con Conficker ¿Cómo puedo eliminarlo de mi equipo?

El primer paso es intentar eliminar la infección utilizando un antivirus actualizado, de todos modos, si no logra borrar el virus, puede utilizar alguna herramienta específica para eliminarlo. Es importante que esta herramienta la obtenga de alguna fuente fiable.

Se han detectado gran cantidad de fraudes que aprovechan Conficker para ofrecer soluciones de falsos antivirus, que no sólo no eliminan la infección, sino que también solicitan dinero para “ejecutar” el falso programa y, en algunos casos, descargan más programas maliciosos en el equipo.

A continuación ofrecemos un listado de herramientas legítimas que eliminan este programa malicioso, indicando la empresa de seguridad que la ha desarrollado:

- BitDefender: <http://www.bdtools.net/>
- Trend Micro: http://www.trendmicro.com/ftp/products/pattern/spyware/fixtool/SysClean-WORM_DOWNAD.zip
- Symantec: http://www.symantec.com/security_response/writeup.jsp?docid=2009-011316-0247-99
- Kaspersky: <http://support.kaspersky.com/faq/?qid=208279973>
- ESET: <http://www.eset-la.com/support/tools.php>
- Sophos: <http://www.sophos.com/kb/54457.html>

NOTA: Estas herramientas no son antivirus completos, ni sirven como sustitutos de tener un antivirus instalado en el equipo, tan sólo son herramientas que sirven para eliminar Conficker de los ordenadores, pero no eliminan otras infecciones ni previenen de que se puedan producir.

Una vez que haya limpiado completamente su ordenador de éste y otros virus que tenga en su equipo, **actualice completamente todo su sistema operativo.** Ayudará a evitar futuras infecciones.