Conficker en números

Autor: Sebastián Bortnik, Analista de Seguridad de ESET para Latinoamérica
Fecha: 4 de noviembre de 2009

ESET, LLC 610 West Ash Street, Suite 1900
phone: (619) 876 – 5400, fax: (619) 437 – 7045
sales@eset.com, www.eset.com

1

Dicen que una imagen vale más que mil palabras, pero... ¿cuánto más vale un número?

Los números han acompañado a la humanidad desde los principios de la historia. Integran un sistema de comunicación que supera, incluso, barreras idiomáticas.

En el presente texto será relatada la historia del gusano Conficker desde una perspectiva numérica.

A **1 año de su aparición como amenaza**, el mismo se ha caracterizado por importantes tasas de propagación e infección, gran cantidad de variantes y características novedosas en su desarrollo y altamente peligrosas. Los números que dejó Conficker, luego de **12 meses de actividad**, son suficientes para graficar qué significará este gusano en la historia del malware y cuánto es posible aprender de él.

En las siguientes páginas se narrará una historia. Las palabras contarán lo que muestran los números, si es que éstos no hablan por sí solos.

08-067

El **23 de octubre de 2008**, Microsoft publicó su **boletín de seguridad MS08-067**. Apartándose de la política habitual de la compañía, cuyas actualizaciones el segundo martes de cada mes, el parche apareció **10 días** después de la fecha correspondiente.. La operativa de Microsoft indica que solo serán publicadas actualizaciones fuera del ciclo habitual "*ocasionalmente*" [1], lo cual confirma a priori la gravedad de una vulnerabilidad que "*no puede esperar hasta el próximo mes*".

La vulnerabilidad en el servicio del servidor de **Microsoft MS08-067** fue clasificada como *crítica* para la mayoría de los sistemas operativos que afectaba [2] (Windows 2000, Windows XP y Windows 2003) e *importante* para el resto (Windows Vista y Windows Server 2008). En resumen, en un sistema vulnerable es posible ejecutar código remoto "*si un usuario recibe una solicitud RPC especialmente diseñada*".

Aquel día de octubre, Microsoft puso a disposición de sus usuarios el parche para remediar una grave vulnerabilidad (también brindó *workarounds* provisionales) y recomendó a sus clientes que "*apliquen la actualización inmediatamente*". La historia de Conficker había comenzado.

250

En el boletín de seguridad de Microsoft se alertaba sobre la posibilidad de que la vulnerabilidad sea aprovechada por un *exploit* utilizado a través de un gusano[1] [2].

Tal como fuera anunciado, el mismo día de la aparición del parche, aparece *Win32/Gimmiv*, el primer código malicioso que explotaba la vulnerabilidad **MS08-067**. El gusano estaba diseñado principalmente para robar información, tal como nombres de usuario y contraseñas de MSN Messenger, Outlook Express e Internet Explorer, así como también *cookies* almacenadas en el sistema [3]. A pesar de su rápida aparición, Gimmiv se propagó principalmente en Asia y no obtuvo altos índices de infección ni perduró en el tiempo.

A mediados de noviembre del mismo año, menos de **1 mes** después de la publicación de la vulnerabilidad, llega la primera variante del gusano Conficker, detectada por ESET NOD32 como *Win32/Conficker.A*. En pocas semanas, el gusano demostró que sus desarrolladores habían trabajado muy bien pensando en el éxito del mismo y en sus índices de infección. Las altas tasas de propagación del gusano Conficker (que serán presentadas a lo largo del texto), se hicieron notorias antes de fin de año.

Con el gusano *in-the-wild*[2], los investigadores de seguridad analizaron el malware e inmediatamente descubrieron que se trataba de un código malicioso programado por profesionales, con rutinas de propagación y actualización que no se habían visto con anterioridad.

El nuevo gusano se propagaba, al igual que Gimmiv, a través de la vulnerabilidad en el protocolo RPC ya mencionada. La principal característica innovadora que destacó a Conficker fue su mecanismo de actualización a través de la generación de nombres de dominio pseudo-aleatorios. Cuando un sistema está infectado con Conficker activo, el gusano entra en un bucle infinito por medio del cual se generan por día **250 nombres de dominio de forma pseudo-aleatoria** (tomando como valor de referencia la fecha y hora del sistema). Durante el bucle, el malware contacta a cada uno de los **250 dominios** generados en búsqueda de un archivo binario en el **puerto 80** de los servidores correspondientes. Si se encuentra allí un archivo ejecutable, el mismo es descargado y puesto en funcionamiento en el sistema infectado.

Esta característica permite que cualquier persona que conozca el algoritmo de generación de dominios pueda descargar y poner en ejecución un archivo malicioso en todos los sistemas infectados con Conficker.

---

[1] Las palabras en inglés utilizadas para tal fin fueron "*wormable exploit*"

[2] Un malware se encuentra in-the-wild cuando figura en la wild-list. Más información: http://www.wildlist.org/

Asimismo, esta característica dificulta limitar el control del sistema por parte de los atacantes. Mientras el sistema esté infectado, contactará diariamente 250 dominios distintos desde donde el atacante puede controlar el sistema.

El **29 de diciembre** se hizo pública la primera variante de Conficker. A partir de esta, conocida como Conficker.B (y detectada por ESET NOD32 como *Win32/Conficker.AA)*, el gusano no solo podía propagarse a través de equipos en red con la vulnerabilidad de RPC, sino también a través de dispositivos USB y carpetas compartidas que tuviesen contraseñas débiles por medio de ataques de diccionario con una base de datos de **248 posibles contraseñas** (casi 250) para acceder a recursos en otros sistemas [5].

Conficker.B también incorporó rutinas para evitar su desinfección, cerrando procesos de los más reconocidos fabricantes antivirus (utilizando un diccionario de **52 palabras** a buscar en los procesos y su información) y bloqueando el acceso a sitios web en cuyos nombres hubiese cadenas específicas (un diccionario también de **52 palabras** entre las que se incluyen, por ejemplo, "windowsupdate", "eset" y "nod32").

Con la aparición de esta variante, los equipos que ya hubieran instalado el parche de seguridad de Microsoft **MS08-067** también podrían infectarse a través de los nuevos mecanismos de propagación; un detalle importante en el secreto del éxito de Conficker como gusano.

Las redes infectadas con Conficker sufrían, entre otros inconvenientes, tráfico elevado en las redes internas, saturación de servicios, denegaciones de servicio asociadas al tráfico de red, utilización de direcciones IP de la compañía y fuga de información.

En enero, el Laboratorio de ESET Latinoamérica indicaba que "*Conficker llegó para quedarse un tiempo*" [6], y no estaba equivocado. Las tasas de infección de Conficker seguían creciendo. Y todavía había tiempo para más.

USD 250.000

El **12 de febrero de 2009**, cuando Conficker ya era una epidemia infectando millones de sistemas, Microsoft anunció a través de un comunicado de prensa [7] la creación de una **recompensa de 250.000 dólares** a cambio de "*información que resulte en el arresto de los responsables de la creación y propagación de Conficker en Internet*".

El hecho de que Microsoft pusiera una recompensa (que finalizando el año **2009** aún no ha sido cobrada por nadie dado que los responsables aún no han sido encontrados) corrobora la gravedad de Conficker como amenaza. Microsoft había tomado acciones similares, por ejemplo, ante epidemias como la del gusano Slammer en el año **2003** [8].

En el mismo comunicado, la empresa anunció el trabajo conjunto con otras organizaciones, entre las que se destacaban el ISC (Internet Storm Center), Verisign y particularmente ICANN, para bloquear los dominios utilizados por Conficker. Greg Rattray, Jefe de Seguridad en Internet para ICANN, declaró en aquel entonces: "*La mejor manera de enfrentar amenazas como Conficker es con el trabajo conjunto de las comunidades de seguridad y nombres de dominio*".

Conficker seguía afectando a los usuarios de computadoras, y las más reconocidas empresas y organizaciones del mercado debían aunar fuerzas para combatirlo. A pesar de los esfuerzos por bloquear los nombres de dominios a los que se conectarían los equipos infectados, el gusano seguiría infectando sistemas y continuarían apareciendo nuevas variantes en los meses siguientes.

01/04/2009

El **4 de marzo de 2009** apareció otra variante de Conficker que lo ubicaría nuevamente en boca de todos los medios de comunicación dedicados a la tecnología. A pesar de que dicha variante no representaba mayores riesgos que las versiones anteriores del gusano [9], contaba con una característica de gran noticiabilidad e impacto mediático: una bomba de tiempo.

La variante reconocida como Conficker.C (identificada proactivamente por ESET NOD32 como *Win32/Conficker.X*) se mantendría inactiva en los sistemas infectados hasta el **1º de abril de 2009**. En esa fecha, comenzaría a buscar actualizaciones a través del método de generación de dominios pseudo-aleatorios con una salvedad: esta nueva variante generaría **50.000 direcciones URL** a consultar diariamente (en contraposición con las **250** de las primeras versiones). Esta decisión de los creadores de Conficker se corresponde claramente con la intención de la comunidad de la seguridad de trabajar en el bloqueo de nombres de dominio (ver sección anterior). Ahora **deberían controlar 50 mil dominios diarios en lugar de 250**.

El **1º de abril** Conficker.C comenzó el nuevo ciclo de búsqueda de actualizaciones. El **8 de abril, 7 días** más tarde, los equipos infectados con esta variante descargaron una nueva versión del gusano, la última conocida a la fecha, detectada proactivamente por la heurística de ESET NOD32 y luego establecida bajo la firma *Win32/Conficker.AQ* [10]. La misma incorporaba como único mecanismo posible de actualización el

empleo de una red *peer-to-peer* como comunicación de la *botnet* de todos los equipos infectados con esta variante. Esto indica que la motivación y el objetivo principal de los desarrolladores del gusano era la creación de una red de equipos zombies.

Como se puede observar, las diferentes variantes de Conficker demuestran el trabajo profesional de sus creadores, incorporando nuevos mecanismos de propagación e infección con el transcurrir de los meses. Las tasas de infección, que serán presentadas a continuación, avalan este razonamiento.

12 x 11 x 03

En **febrero de 2009**, el Laboratorio de ESET Latinoamérica comparaba las tasas de infección de Conficker indicadas en la presente tabla [11]:

Fecha	Detección (Mundiales)	Detección (América Latina)
24 de enero de 2009	5,08 %	8,07 %
18 de febrero de 2009	3,52 %	8,86 %

Tabla 1: Tasas de infección mundiales de Conficker

Según los datos presentados, se concluía que los valores se mantenían estables "*a pesar de que han pasado **20 días***" [11] entre una fecha y otra. En pleno crecimiento de la epidemia Conficker, mientras se alertaba en innumerables sitios sobre la importancia de actualizar los sistemas operativos, utilizar software antivirus y configurar los sistemas para evitar la propagación del gusano, casi **3 meses** después de la aparición del gusano, los usuarios continuaban desprotegidos y la propagación continuaba su curso. Los índices de detección de Conficker se mantenían estables a pesar de que las medidas de seguridad para la protección ya existían. ¿Cuántos días más necesitarían los usuarios para protegerse de esta amenaza? ¿30 días más? ¿2 meses?

La respuesta puede ser resumida por medio de las estadísticas mundiales de detección de Conficker por el sistema ThreatSense.Net de ESET [12][3]:

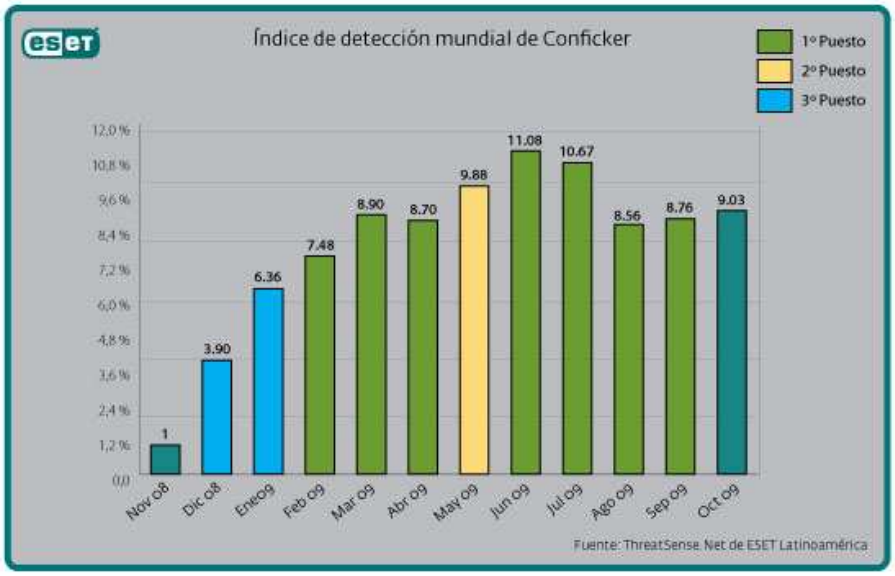

Imagen 1: Detección de gusano Conficker

Estos valores confirman que las tasas de infección de Conficker continuaron estables durante los **12 meses** de historia que posee el gusano. Durante un año, el gusano ha mantenido un índice de detección mundial que permite afirmar que continúa presente en **1 de cada 10** equipos donde fue detectada la presencia del malware.

En los reportes mensuales de amenazas realizados por ESET, el gusano Conficker ha sido el malware de mayor índice de detección en **7 de los 11 meses**[4] **que lleva el año**, ubicándose en el **primer lugar del ranking**. Asimismo, a partir de su primer mes completo de aparición, se ha ubicado siempre dentro del **TOP 3 de amenazas** en el resto de los informes.

[3] Los valores correspondientes a octubre de 2009 corresponden a las detecciones realizadas hasta el 20 de ese mes, fecha de cierre de redacción del presente artículo.

[4] No se considera octubre de 2009 en este dato por no haberse realizado el informe final a la fecha de redacción del presente artículo.

Al **15 de octubre de 2009**, según el Conficker Working Group [13] son más de **6.000.000 de direcciones IP** públicas las infectadas por el gusano Conficker. Además, en cada una de ellas puede haber muchos equipos infectados.

Las tasas de infección del gusano Conficker no sólo han sido altas, ocupando los primeros lugares del ranking, sino que han sabido mantenerse en el tiempo. La combinación de ambas características es otro motivo para considerar a Conficker como la amenaza más importante del año 2009 y darle un lugar relevante en la historia de los códigos maliciosos.

USD 9.100.000.000

Si se analiza Conficker desde una perspectiva numérica, resta determinar cuál fue el impacto económico de la epidemia. En abril de 2009, el Instituto de Ciber Seguridad realizó un estudio al respecto [14], estimando que las pérdidas causadas por el gusano podrían alcanzar los **9100 mil millones de dólares**. El mismo informe analiza que, aún considerando un número bajo de equipos comprometidos (**200.000** sistemas infectados), para cada uno de ellos los costos en pérdida de tiempo, recursos y esfuerzos utilizados para la remediación alcanzarían los **200 millones de dólares**.

Estos valores analizan el conjunto en su totalidad aunque gran parte de las infecciones de Conficker se relacionan con redes corporativas u organizaciones cuyos valores de pérdidas pueden ser aún superiores.

Durante su año de vida, Conficker logró infectar, entre otros, a equipos de la marina francesa (impidiendo la partida de aviones al no poder acceder a la base de datos) [15] y del parlamento británico [16].

∞

¿Cuándo bajarán los índices de propagación de Conficker? A casi **1 año** de la aparición del gusano la respuesta a esta pregunta resulta incierta y pensarla en fechas concretas puede llevar a una respuesta tan **infinita** como la que se muestra en el título de esta conclusión. Rodney Joffe, director del Conficker Working Group, afirmó (consumada la epidemia) que es "*prácticamente imposible remover completamente a Conficker*" [17]. Él mismo justificó su afirmación recordando que si en una red se quita el gusano de **99 de los 100** sistemas infectados, desde ese único equipo intentará propagarse nuevamente por la red.

En unos meses quizás sea posible observar cómo las tasas de propagación de Conficker van disminuyendo. Sin embargo, la solución para que la respuesta sea más alentadora, es preguntarse **qué aprendió la comunidad, de la aparición de Conficker**.

El gusano fue detectado casi **1 mes** después de haber aparecido el parche y,sin embargo, los índices de propagación se mantuvieron altos durante los casi **12 meses** de vida del código malicioso. Si una epidemia como esta no permite que los usuarios aprendan a gestionar eficientemente la seguridad, el problema hoy es Conficker pero mañana será otro malware.

Las actualizaciones de software se posicionan como una medida de seguridad imperativa, dada la muy frecuente utilización de *exploits* por parte del malware en la actualidad. En zonas como Latinoamérica, los altos índices de piratería afectan notoriamente este factor, siendo grande el número de usuarios que no tienen la costumbre de utilizar software legal con todas las actualizaciones correspondientes de seguridad instaladas.

En casos como estos, donde a pesar de existir las tecnologías de protección los equipos de los usuarios se siguen infectando, se confirma aquello que se menciona regularmente desde ESET Latinoamérica: la educación de los usuarios es un pilar importante en la seguridad de la información como complemento de las tecnologías proactivas de detección. Los usuarios educados y debidamente capacitados no sólo se expondrán con menor frecuencia a las amenazas informáticas, sino que también tomarán mejores decisiones en el uso y disposición de tecnologías de seguridad. Justamente lo que falló en el caso de Conficker.

Por ese motivo, de no capacitar a los usuarios de un modo correcto y educarlos para enfrentar de un modo consciente y responsable el complejo panorama de malware actual será "*imposible*" , utilizando las palabras de Rodney Joffe, dar solución final al problema.

Referencias

[1] http://www.microsoft.com/security/updates/bulletins/default.aspx

[2] http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx

[3] http://www.eset.com/threat-center/blog/2008/10/24/a-closer-look-at-gimmiva

[4] http://mtc.sri.com/Conficker/

[5] http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fConficker.B

[6] http://blogs.eset-la.com/laboratorio/2009/01/16/conficker-atraves-autorun/

[7] http://www.microsoft.com/Presspass/press/2009/feb09/02-12ConfickerPR.mspx

[8] http://www.eset-la.com/press/informe/cronologia_virus_informaticos.pdf

[9] http://blogs.eset-la.com/laboratorio/2009/03/28/1-abril-comienza-conficker/

[10] http://blogs.eset-la.com/laboratorio/2009/04/10/nueva-variante-funcionalidades-conficker/

[11] http://blogs.eset-la.com/laboratorio/2009/02/18/novedades-conficker/

[12] http://www.eset-la.com/threatsense.net

[13] http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking

[14] http://cybersecureinstitute.org/blog/?p=15

[15] http://www.pcworld.com/article/159224/conficker_worm_sinks_french_navy_network.html

[16] http://www.h-online.com/security/news/item/Conficker-infects-UK-parliament-740811.html

[17] http://www.smh.com.au/technology/security/internet-meltdown-threat-conficker-worm-refuses-to-turn-20090922-fzlh.html