

ENTRADAS RECIENTES

Win32/Conficker.X :
W32/Conficker.worm :
Downadup/Conficker :
Conficker.A : Conficker.B :
Problema y Solución :Clean

Malas noticias económicas en
Japón

Estudiantes del MIT
construyen aplicaciones
móviles en 13 semanas

Científicos extraen imágenes
directamente desde el cerebro
de una persona

Confirmaron existencia de un
agujero negro en el centro de la
Vía Láctea

Videos Virales - ¿Dónde diablos
está Matt? (2008)

Videos de Youtube - Noize MC
За Замкнutoй Дверью

Google Chile Zeitgeist 2008

José Luis Nazar Teleton 2008 :
Otro gran aporte : Mil Millones

Leonardo Farkas Teleton
2008 : El más grande aporte :
Mil Millones

Buscador de Contenidos
Duplicados

ENERGIA NUCLEAR :
Reflexiones

Posicionamiento en
buscadores

Seguridad en Internet -
Seguridad en redes

Test Velocidad Internet -
Banda Ancha - ADSL

GOOGLE TALK

Chat with Edreams
Busy

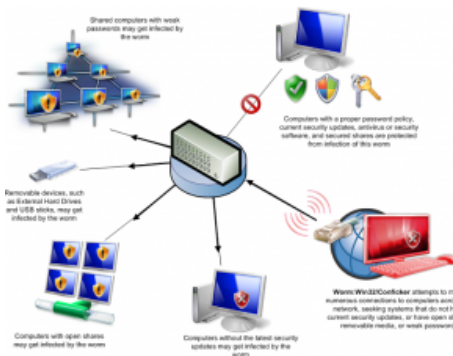
POSICIONAMIENTO - SEO



Win32/Conficker.X : W32/Conficker.worm : Downadup/Conficker : Conficker.A : Conficker.B : Problema y Solución :Clean

14 de Enero 2009

ACTUALIZACION: Nuevas Variantes del **W32/Conficker.worm** han salido, ahora está la de **Conficker.B** que aprovecha las debilidades de las passwords y se intercambia a través de medios removibles.



EL día 13 de Enero de 2009 Microsoft actualizó el Malicious Software Removal Tool (MSRT), con lo cual se puede por fin limpiar el conficker.

Para el Microsoft Windows **Malicious Software Removal Tool** en un entorno empresarial ver: <http://support.microsoft.com/kb/891716>

Según **F-Secure** al 13 de Enero de 2009 hay casi 2.5 millones de computadores infectados con el **Conficker** worm, también conocido como **Downadup**, pero al ver la cifra del 14 de Enero del 2009, un día solamente más, ahora hay **3.5 millones** de computadores infectados. Como el gusano tiene la capacidad de bajar nuevas versiones de si mismo, se esperó que la propagación siga en aumento.

Hay 3 versiones de este gusano, el **Conficker.A** que explota la vulnerabilidad del **RPC** en **windows**, y el **Conficker.B** y **.C** que también hacen lo mismo, más la capacidad de romper contraseñas administrativas débiles a través del uso de un diccionario de claves. Por eso se aconseja a los administradores parchar el sistema, y a la vez usar contraseñas fuertes.

F-Secure recomienda a los **administradores de sistemas** que bloqueen los siguientes sitios usados por este **gusano**, los sitios van cambiando, así que ver la actualización en: <http://www.f-secure.com/weblog/archives/00001574.html>

F-Secure también tiene una herramienta para la desinfección, la puedes bajar aquí: [F-Secure Clean Downadup/Conficker](#)



Shelfari: Book reviews on your book blog
Share a [book review](#) on Shelfari, where this [reader](#) meets fellow readers.

ETIQUETAS

aaron wall abogados Adobe
buscadores chile google comandos
yum crisis economica
edreams factores claves fair
use fcc Firefox Flash Flash Killer

gigabytes **Google**
importancia
posicionamiento
buscadores Leonardo
Farkas Linux Live Search API
Isot Microsoft Microsoft
Silverlight PageRank
posicionamiento chile
posicionamiento
en buscadores
posicionamiento
google
posicionamiento
paginas web
posicionamiento
web propiedad intelectual
revision de sitios robots.txt
seobook **seo chile** Silk Road
sockets Teleton Titosky uso justo
video wifi WIFI con esteroides
wireless youtube yum

VIDEOS VIRALES

Source: Viral Video Chart

Luego de autoejecutarse, el gusano Conficker.A corrige la misma vulnerabilidad que acaba de explotar, descargando el parche desde el sitio de Microsoft.

El 23 de noviembre, Microsoft solucionó una vulnerabilidad crítica presente en RPC bajo Windows, sin esperar el próximo parche mensual, programado para el segundo martes de diciembre. La compañía tuvo buenas razones para acelerar la publicación del parche debido a que se ha detectado un gusano que aprovecha precisamente tal vulnerabilidad, incluso estando ya solucionada. El riesgo radica en que numerosos usuarios no han instalado la actualización, por lo que sus sistemas siguen siendo vulnerables.

El gusano **Conficker.A** ya ha infectado una red corporativa en Estados Unidos, y también se han detectado incidencias en Europa, Asia y Sudamérica.

El gusano en cuestión **ejecuta un servicio similar a un servidor web en la computadora infectada**, usándolo para descargar e instalar nuevo código maligno.

Una curiosidad es que, luego de instalarse, el gusano descarga la actualización de Microsoft que corrige el agujero de seguridad que el mismo gusano acaba de explotar. Claro está, no actúa movido por la generosidad, sino más bien por un intento de dejar fuera a otros gusanos de RPC.

Protegerse contra el gusano es relativamente fácil. Aparte de la instalación del parche de Microsoft es imprescindible tener activada constantemente un cortafuego.

En su sitio **Malware Protection Center**, Microsoft presentará una descripción detallada del gusano del procedimiento para proteger el sistema.

Este es un gusano residente en memoria, reportado el 24 de Noviembre del 2008 que se propaga explotando la vulnerabilidad del Servicio de Servidor RPC, que permite la ejecución de códigos arbitrarios en forma remota. Infecta a Windows 95/98/Me/NT/2000/XP/Vista y Server 2003, está desarrollado en Assembler con una extensión de 62,976 bytes y comprimido con rutinas propias.

- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250>
- <http://www.securityfocus.com/archive/1/archive/1/497816/100/0/threaded>

Una vez ingresado al sistema se copia a la siguiente ruta:

%System%\[nombre_aleatorio].dll

Para ejecutarse la próxima vez que se re-inicie el sistema crea la llave de registro:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\netsvcs\Parameters]
"ServiceDll" = "[Ruta_al_gusano]"
```

System% es la variable C:\Windows\System para Windows 95/98/Me, C:\Winnt\System32 para Windows NT/2000 y C:\Windows\System32 para Windows XP y Windows Server 2003.

Al siguiente inicio del equipo, el gusano borra cualquier punto de Restauración creado por el usuario y genera el siguiente servicio:

Nombre: netsvcs

Ruta de imagen: %SystemRoot%\system32\svchost.exe -k netsvcs

Luego revisa redes externas buscando explotar la vulnerabilidad del Servicio de Servidor RPC (MS08-067) y se conecta a los siguientes URLs para obtener la dirección IP del sistema infectado:

<http://www.getmyip.org>
<http://getmyip.co.uk>
<http://checkip.dyndns.org>

a continuación se conecta a la siguiente dirección web y descarga un malware, el cual ejecuta:

[http://trafficconverter.biz/4vir/antispyware/\[Removido\]](http://trafficconverter.biz/4vir/antispyware/[Removido])

El gusano crea un servidor HTTP en el puerto TCP 80 u 8080 y envía esa dirección a sistemas remotos.

Si logra explotar la vulnerabilidad RPC, la computadora remota se conectará a ese URL y descargará una copia del gusano. De tal modo que cada sistema vulnerable podrá propagar el gusano por sí mismo.

Seguidamente el gusano se conecta a un ruteador UPnP (plug & play), abre el puerto TCP 80 (HTTP) y ubica la red registrada como puerta de entrada a Internet (Gateway), permitiendo que intrusos puedan ingresar al equipo infectado desde redes externas.

El gusano intenta descargar un archivo de datos desde el siguiente URL:

[http://www.maxmind.com/download/geoip/database/Geo\[Censurado\]](http://www.maxmind.com/download/geoip/database/Geo[Censurado])

Para obtener la fecha del día vigente, el gusano se conecta a las siguientes direcciones web:

- <http://www.w3.org>
- <http://www.ask.com>
- <http://www.msn.com>
- <http://www.yahoo.com>
- <http://www.google.com>
- <http://www.baidu.com>

La información es usada para generar una lista de dominios, a los cuales se conecta el gusano para descargar archivos adicionales.

Los Nombres que se le conoce son:

Antivirus	Version	Last Update	Result
AhnLab-V3	-	-	-
AntiVir	-	-	Worm/Agent.NB
Authentium	-	-	-
Avast	-	-	Win32:Trojan-gen {Other}
AVG	-	-	-
BitDefender	-	-	-
CAT-QuickHeal	-	-	-
ClamAV	-	-	-
Comodo	-	-	Worm.Win32.Agent.~BM
DrWeb	-	-	-
eSafe	-	-	Suspicious File
eTrust-Vet	-	-	-
Ewido	-	-	-
F-Prot	-	-	-

F-Secure	-	-	Worm.Win32.Agent.nb
Fortinet	-	-	W32/Conficker!worm
GData	-	-	Win32:Trojan-gen {Other}
Ikarus	-	-	Worm.Win32.Agent
K7AntiVirus	-	-	-
Kaspersky	-	-	Worm.Win32.Agent.nb
McAfee	-	-	W32/Conficker.worm
McAfee+Artemis	-	-	Generic!Artemis
Microsoft	-	-	Worm:Win32/Conficker.A
NOD32	-	-	a variant of Win32/Conficker.X
Norman	-	-	-
Panda	-	-	W32/Conficker.A.worm
PCTools	-	-	Worm.Agent!sd6
Prevx1	-	-	-
Rising	-	-	-
SecureWeb-Gateway	-	-	Worm.Agent.NB
Sophos	-	-	Mal/Conficker-A
Sunbelt	-	-	-
Symantec	-	-	W32.Downadup
TheHacker	-	-	W32/Agent.nb
TrendMicro	-	-	WORM_DOWNAD.A
VBA32	-	-	Worm.Win32.Agent.nb
ViRobot	-	-	-
VirusBuster	-	-	-

Solución

Si utilizas Trend Online Scanner para la desinfección, este lo encontrará con el nombre: WORM_DOWNAD.A.

Los pasos son se encuentran en la siguiente : [Trend AntiVirus](#)

Si quieres ocupar otros Antivirus ONline, los pasos son los mismos:

- 1.- Si ocupas windows XP, deshabilita el Punto de restauración.
- 2.- Reinicia a modo a prueba de fallos con red(o modo seguro con red)
- 3.- Escanea por los bichos, y procede a eliminarlos:

- Symantec Security Check | [proceed](#)
- TrendMicro Housecall | [proceed](#)
- Ewido Networks | [proceed](#)

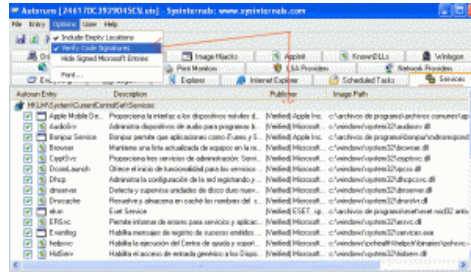
- Panda ActiveScan | [proceed](#)
- BitDefender | [proceed](#)
- F-Secure | [proceed](#)

4.- Reinicia, pero esta vez normalmente.

5.- Has otro scan para verificar

Otra Forma:

La otra es bajarse el: [Autoruns for Windows](#) , aquí si lo corremos vamos a la pestaña servicios, clickeamos también en el menu Options, por Verify Code Signatures, y si vemos bien ahora veremos :



Y si aquí vemos un .DLL que no este verificado, ahí disparamos las alarmas, vemos como se llama el proceso por ejemplo:

TytskyMalAware y vemos la ruta: C:\WINDOWS\system32
 \mardadozo.dll

Aquí podemos eliminar el servicio y el archivo que usa, y después revisar el registro como se decía anteriormente.

Saludos y Feliz Año Nuevo

{ 0 comments... [add one now](#) }

Leave a Comment

Name

E-mail

Website

You can use these HTML tags and attributes: <abbr title="">
 <acronym title=""> <blockquote cite=""> <cite> <code> <del datetime="">
 <i> <q cite=""> <strike>

Submit

