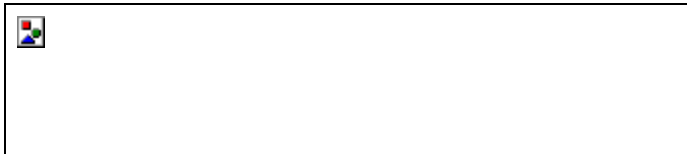

The Canaudit Perspective

(© Canaudit, Inc. 2003 - translated with permission by SAFE Consulting Group, www.safecg.com)

Puntos de especial interés:

- [Virus Informáticos – similares en naturaleza a los virus orgánicos](#)
- [Gusano Blaster o Lovsan](#)
- [Gusano Sobig F](#)
- [Protegiendo los sistemas de Virus y Worms](#)



Virus y Gusanos, La mejor defensa es la toma de conciencia

por Chad Parks – Manager, Technical Audits & Security Services – Canaudit, Inc.

Los virus y gusanos han colmado la paciencia de la industria informática durante años, con millardos de dólares de costo en pérdidas de datos, tiempo y uso del sistema. La amenaza que presentan los virus y gusanos informáticos es más que solo el hecho de no tener acceso a Internet y está más allá del temor creado por las firmas de software antivirus para incrementar sus ventas. La amenaza de virus y gusanos es real y puede afectar su propio bolsillo tanto en el trabajo como en su casa. No existen fronteras que detengan la amenaza de virus y gusanos, y no hay límites al daño y caos que pueden producir – desde el consumo de los recursos del sistema y las reinicializaciones hasta software dañado o datos irrecuperables. Es por este motivo que es responsabilidad de cada usuario de informática comprender la naturaleza fundamental de los virus y gusanos, el daño que pueden producir, y las medidas que pueden tomarse para reducir la exposición al riesgo.

Este artículo presenta a vuelo de pájaro, varios de los más recientes virus que han bombardeado nuestros sistemas de información. También trata sobre la naturaleza de los virus y gusanos y los controles sencillos que pueden implantarse para mitigar el riesgo. Este artículo tiene como propósito refrescar lo que muchos de ustedes ya saben, e intentar lograr que aquellos que no han tomado las precauciones necesarias hasta ahora, lo hagan en adelante. Está seguro que al momento que haya leído este artículo habrá nuevos gusanos y virus golpeando a su puerta. Los gusanos y virus que trataremos en este artículo ya tienen firmas identificadas desarrolladas por la mayoría de los más populares paquetes de antivirus. Una vez que un virus es detectado, la empresa de software antivirus crea una firma de manera que el virus pueda ser rápidamente aislado, en general en pocas horas. Esto demuestra la velocidad relámpago en una de las facetas de la guerra de la información. Cuando hablamos de virus y gusanos informáticos, estamos discutiendo sobre ellos en términos de horas o minutos, no días o semanas.

Los virus informáticos son similares en su naturaleza a los virus orgánicos. Infectan un servidor, y luego utilizan los recursos de este servidor para replicarse e infectar otros servidores. Los virus se fijan generalmente a programas vulnerables, toman control del objetivo y lo utilizan para acceder al sistema operativo para borrar archivos en forma arbitraria o archivos críticos del sistema y luego diseminarse a otros servidores. Los virus informáticos intentan propagarse a otros servidores a menudo como adjuntos de correos electrónicos tomando control de los servidores o del software de correo. Utilizando esta técnica el virus intentará enviar una copia de sí mismo a todas las direcciones de correo que pueda encontrar luego de escanear todas las direcciones de correo de la máquina infectada.

Los gusanos son análogos a los virus informáticos y a menudo se utilizan como medio de transporte de virus. La diferencia principal entre estas dos herramientas de destrucción es que los gusanos no requieren acceder a programas para replicarse a sí mismos. Los gusanos aprovechan las ventajas que les brindan los directorios de carpetas compartidas, las máquinas interconectadas y los servicios de red vulnerables. Los virus informáticos requieren por lo general que un usuario los active abriendo un archivo o haciendo clic sobre el ejecutable. Los Gusanos generalmente no requieren actividad alguna del usuario para infectar a otros servidores y se pueden replicar a sí mismos explotando las vulnerabilidades de recursos compartidos en redes abiertas o de servicios vulnerables en sistemas operativos.

Uno de los más recientes y ampliamente conocidos gusanos que irrumpió en los computadores alrededor del mundo es el conocido como Gusano **Blaster o Lovsan**. Probablemente usted ya haya oído de este gusano y su organización ha logrado colocar el parche para protegerse de esta vulnerabilidad. Solo mencione el Gusano Blaster a cualquiera de los amigos de TI (Tecnologías de Información), y si ve que miran al piso y sacuden sus cabezas con desagrado seguramente habrán tenido que padecer este virus de una forma u otra. El sitio web del Equipo de Respuesta a Emergencias Informáticas (Computer Emergency Response Team – CERT) , reportó que el gusano Blaster aprovechó una vulnerabilidad reciente descubierta en los sistemas operativos Windows, específicamente en Windows NT 4.0, Windows 2000, Windows XP y Windows Server 2003. Esta vulnerabilidad existe con la implantación en Windows de Llamadas a procedimientos remotos DCOM (DCOM Remote Procedure Call -RPC-). La ejecución de esta vulnerabilidad permite el acceso a la línea de comandos en forma remota con privilegios de administrador. El gusano Blaster busca en forma activa direcciones de Internet/red para encontrar servidores vulnerables e infectarlos.

Cuando logra encontrar un servidor vulnerable a esta debilidad del RPC, intenta copiar un archivo llamado msblast.exe o teekids.exe o penis32.exe en el servidor vulnerable. Una vez copiado el archivo, el servidor ahora infectado establece una conexión con otros servidores objetivos para ejecutar el código del msblast.exe. El servidor infectado comienza luego a buscar en forma activa otros servidores para infectar y lanzar un ataque distribuido de denegación de servicios contra el sitio web de actualizaciones de Microsoft.

Si por algún motivo su organización no ha instalado todavía el parche, usted se encuentra en la próxima curva del camino del gusano y debe hacerlo inmediatamente. El remedio para un servidor infectado con el Blaster puede ser complicado cuando debe aplicarse a nivel corporativo. Si bien este gusano no aparenta ser malicioso en el sentido de borrar archivos en el sistema infectado, ocupa una cantidad significativa de recursos. Cuantos más ordenadores se hayan infectado en una red, mayor cantidad de recursos serán consumidos por el gusano, llegando posiblemente al punto de una denegación de servicios a nivel de la red. El CERT recomienda primero y principal, instalar los parches provistos por Microsoft. Luego han surgido diversas mutaciones del gusano Blaster por lo que la instalación del primer parche provisto por Microsoft no es suficiente. Estos parches deben aplicarse a todos los ordenadores que cuenten con sistemas operativos vulnerables se encuentren o no infectados. El CERT también recomienda filtrar el acceso desde Internet a partir del uso de Cortafuegos (Firewalls) o filtrado de paquetes a los puertos TCP 135, 139, 445, 593 y 4444 así como a los puertos UDP 69, 135, 139 y 445. El CERT recomienda la utilización del filtro de paquetes incluido en el llamado ICF (Internet Connection Firewall) de Microsoft e inhabilitar el servicio DCOM antes de reconectar la red para descargar este parche. Este proceso puede demandar mucho tiempo para una estación de trabajo; considere todas las ramificaciones de ordenadores Windows en una red corporativa infectada, sin mencionar las diferentes variedades de mutaciones del gusano Blaster que existen.

Para información más detallada sobre este gusano visite el sitio del CERT en <http://www.cert.org/advisories/CA-2003-20.html> .

Otro desagradable gusano recientemente reportado por el CERT se llama **Sobig.F** y es un ejemplo de un gusano que se propaga utilizando el correo electrónico como medio de transporte. El Sobig.F por definición es una combinación de un virus y un gusano, ya que requiere que un usuario abra el adjunto de un correo para poder ejecutarse y luego replicarse automáticamente a través de los sistemas operativos Windows. En algunos casos, el programa de correo puede abrir el virus automáticamente si está configurado para hacerlo. En cualquier caso el Sobig.F infecta a los ordenadores a través de un adjunto a los correos con una extensión .pif (CERT).

Los correos infectados tienen temas/asuntos (subject) conteniendo uno de los siguientes de acuerdo al sitio Web del

CERT:

- Re: Thank You!
- Thank You!
- Your details
- Re: Details
- Re: Re: My details
- Re: Approved
- Re: Your application
- Re: Wicked screensaver
- Re: That movie

Los archivos infectados adjuntos a los correos tienen los siguientes nombres:

- your_document.pif
- document_all.pif
- thank_you.pif
- your_details.pif
- details.pif
- document_9446.pif
- application.pif
- wicked_scr.scr
- movie0045.pif

El gusano Sobig.F tiene que ser invocado por el usuario haciendo clic sobre el adjunto de un correo o por la aplicación de correo que abre el adjunto en forma automática. El gusano luego se instala en el ordenador y busca en los archivos todas las direcciones de correo. Específicamente observa los archivos con extensiones .htm, .html, .dbx, .hlp, .mht, .txt, y .wab. El gusano luego se envía a sí mismo a todas las direcciones de correo utilizando el motor SMTP (Simple Mail Transfer Protocol) de la máquina infectada.

Otra función del Sobig.F es que en ciertos momentos predeterminados intenta contactar una de las veinte direcciones IP sobre el puerto UPP 8998. El CERT cree que esta conexión es un intento de bajar información adicional desde o hacia el servidor infectado. Sería prudente bloquear todo tráfico entrante y saliente de estas direcciones. Para más información sobre estas direcciones puede visitar el siguiente URL: http://www.cert.org/incident_notes/IN-2003-03.html

La mayoría si no todas las firmas de software antivirus desarrollaron identificación basada en firmas para el gusano Sobig.F. El CERT recomienda instalar la última actualización del software antivirus para proteger sistemas potencialmente vulnerables. El CERT también recomienda a los usuarios no descargar o ejecutar programas de organizaciones o personas que no sean confiables. A menos que el adjunto se esté esperando, no debería abrirse hasta que el que lo envía pueda verificarlo como un archivo legítimo. El CERT también dice que bloqueando el tráfico de los siguientes puertos UDP 123, 995, 996, 997, 998, 999, y 8998 reducirá también la exposición y el efecto de este gusano.

El CERT también reportó otro gusano basado en correo llamado Swen.A. El gusano Swen.A, es más que un gusano de correo. El Swen.A es similar en naturaleza a otros dos gusanos llamados GIBE.F y GIBE.B, los que tienen por objetivo atacar sistemas operativos Windows. Estos gusanos se replican a sí mismos a través de recursos de red compartidos y correo electrónico. Para activar este gusano, debe ser abierto el adjunto por un usuario o por la aplicación de correo en forma automática. Este gusano es bastante peligroso ya que intentará inhabilitar la seguridad y los procesos antivirus que se ejecutan en el ordenador infectado. Así como el Sobig.F, este gusano busca en el ordenador todas las direcciones de correo e intenta enviarse a sí mismo a las direcciones como un adjunto. El correo infectado aparenta ser una actualización de Microsoft, con la intención de que los usuarios lo abran. Así como para el gusano Sobig.F, el CERT indica que la mejor defensa para este gusano es actualizar y ejecutar el software antivirus. Además los usuarios deben saber que Microsoft nunca envía actualizaciones por correo electrónico. Como

se mencionó anteriormente, los usuarios deben ser conscientes del peligro que representan los adjuntos que no esperan o que no pueden ser verificados por el emisor.

Cuando se trata de **proteger sistemas de virus y gusanos**, deben considerarse una serie de controles sencillos. Primero es importante implantar un sólido proceso de actualización de firmas antivirus. La mayoría de las aplicaciones antivirus son capaces de verificar automáticamente las firmas actualizadas de forma programada. Los usuarios en su propia casa, también deberán ser prudentes y actualizar su software antivirus regularmente. Segundo, las organizaciones deben entrenar a sus empleados para que no abran mensajes adjuntos no esperados –como si no lo hubiese oído anteriormente!-. Lo mismo si usted tiene un ordenador en su casa, sería una buena idea que hable de esto con su familia. Finalmente, los equipos de seguridad de la organización deben consultar frecuentemente el sitio web del CERT para obtener la información más actualizada sobre antivirus, gusanos y otras vulnerabilidades. La información detallada ofrecida por el CERT es invaluable en la protección contra virus, gusanos, y caballos de Troya entre otros aspectos relacionados con la seguridad de TI. El uso de un Cortafuegos (Firewall) personal actualizado o un firewall central también ofrece un nivel de protección contra virus y gusanos. Considere estos controles como el sistema inmunológico de su ordenador. Estos son los controles básicos, también existen muchos otros pasos y controles complejos que pueden utilizarse para asegurar los sistemas de información. El objetivo de este artículo es el de refrescar lo que usted ya sabe y darle una visión de alto nivel sobre un tema técnico y complicado que afecta a las organizaciones y a los usuarios hogareños por igual. Tenga presente que cuanto mas sólido sea su sistema inmunológico, menor será la chance de que se pesque un resfriado.

Por favor envíe sus comentarios en relación a este correo a chad@canaudit.com. Espero revisarlos y responder a sus preguntas o comentarios. Si desea enviar comentarios en castellano puede hacerlo a SAFE Consulting Group en info@safecg.com

Chad Parks
Manager, Technical Audits & Security Services
© Canaudit, Inc. 2003

Si usted considera interesante este artículo por favor reenvíelo a sus colegas o asociados profesionales. Por cualquier comentario por favor envíe un mail a publicaciones@safecg.com

Importante: Las opiniones expresadas representan los puntos de vista del autor de las mismas.-
