Oscar Raúl Ortega Pacheco

Desde la aparición de las primeras computadoras han existido fallas en los sistemas, las cuales ocurren en ocasiones de modo inesperado pero también pueden ocurrir intencionalmente y es en este punto donde surgen los programas de código malicioso o *malware*, que son programas con la tarea fundamental de ocasionar algún daño en el equipo de cómputo o en la información para finalmente obtener algún beneficio para su creador o distribuidor.

El primer programa de código malicioso, *Darwin*, surgió como un juego informático que consistía en crear una serie de programas que competían por la memoria de la computadora, siendo ganador aquel programa que capturara la mayor cantidad de memoria y lograra eliminar a sus competidores. Esta característica de competir por los recursos del equipo (memoria, almacenamiento, etcétera) se convirtió en un elemento básico del *malware*, pues en los primeros programas de código malicioso era posible identificar cuando nuestro equipo era infectado ya que su rendimiento o capacidad de almacenamiento disminuía drásticamente, pero hoy en día los creadores de *malware* han desarrollado técnicas capaces de ocultar sus actividades maliciosas para prevenir que el usuario se percate de su existencia y así puedan garantizar su estancia en el equipo infectado (Roberts, 2008). Esto se debe a que su propósito ha cambiado pues inicialmente los desarrolladores de *malware* buscaban demostrar sus conocimientos y en muchas ocasiones trabajaban para alcanzar algún reconocimiento de la comunidad, bastaba con lograr que su programa fuera identificado por algún *software* antivirus. En nuestros tiempos, desarrollar códigos maliciosos responde a una motivación que va más allá del reconocimiento personal, pues a través de la creación de estas herramientas es posible obtener algún beneficio derivado del robo de información o abuso de los recursos del equipo comprometido (Ortega, 2008), lo que ha permitido la formación de organizaciones dedicadas a desarrollar y distribuir *malware*. Esta nueva manera de pensar, de reconocimiento a negocio, ha traído consigo una gran variedad de códigos maliciosos que podemos clasificar de la siguiente manera (Jiménez, 2007):

- **Virus**: “Programas informáticos o secuencias de comandos que intentan propagarse sin el consentimiento y conocimiento del usuario” (Fuentes, 2006) y que realizan alguna acción maliciosa. Entre sus principales características podemos identificar las siguientes:
  - Se presentan como archivos ejecutables, o han adherido su código malicioso a imágenes, hojas de cálculo o documentos.
  - No pueden reproducirse por sí mismos, es decir para infectar otras computadoras es necesario que el usuario intervenga.
  - Llevan a cabo una actividad maliciosa.

- **Caballo de troya (troyano):** "Programa de computadora que aparenta tener una función útil, pero que contiene código posiblemente malicioso para evadir mecanismos de seguridad, a veces explotando accesos legítimos en un sistema." (UNAM-CERT, *s.a.*)
- **Gusanos:** "Son programas que buscan propagarse lo más rápido posible tratando de infectar el mayor número posible de equipos, lo que en ocasiones tiene como consecuencia el colapso de las comunicaciones en la red." (López, 2006)
- ***Bot*:** "Programa o *script* que realiza funciones que de otra manera habría que hacer manualmente. También se refiere a una computadora que ha sido comprometida y que ejecuta las instrucciones que el intruso ordena." (UNAM-CERT, *s.a.*)
- ***Spyware*:** "También conocido como programa espía y comúnmente se refiere a aplicaciones que recopilan información sobre una persona u organización, las cuales se instalan y se ejecutan sin el conocimiento del usuario." (Jiménez, 2005)
- ***Adware*:** Son programas que se instalan en el equipo con o sin intervención del usuario, su objetivo principal es descargar publicidad la computadora infectada.
- ***Dialers*:** Programas que utilizan el *modem* para realizar llamadas a servicios telefónicos con alto costo.
- **Puertas traseras:** Son programas que tienen por objetivo hacer alguna modificación que permita a un tercero tener acceso total al equipo, a la red y/o a la información.

Cabe señalar que los desarrolladores de *malware* mezclan las diversas clasificaciones por lo que no es difícil encontrar programas maliciosos que se comportan como gusanos pero que tienen características de virus o *bots*. Hasta el momento hemos mencionado que estos programas realizan alguna actividad maliciosa en el equipo infectado, pero ¿qué tipo de actividad maliciosa? Entre las acciones más representativas del *malware* encontramos las siguientes:

- **Robo de información.** Entre la información que puede buscar un intruso a través de un código maliciosos encontramos: información relacionada con juegos, datos personales, información de inicio de sesión (usuarios y contraseñas) y también información relacionada con la actividad que realizamos en nuestra computadora, incluyendo hábitos de navegación y programas.
- **Envío de correo no deseado (*spam*).** Algunos programas maliciosos utilizan nuestra computadora e Internet para enviar correos publicitarios o con contenido malicioso a múltiples usuarios en Internet.
- **Control remoto.** Esta acción permite a un usuario malicioso tomar control de nuestro equipo, esto le permitiría utilizar nuestros recursos para almacenar más *malware* o para instalar programas o eliminar datos; aunque también podría utilizarse el equipo para llevar a cabo ataques a otros equipos de Internet.
- **Ataques de ingeniería social.** Existe una nueva tendencia de fabricar *malware* que tiene por objetivo intimidar, espantar o

molestar a los usuarios para que compren ciertos productos (Roberts, 2008). Por ejemplo, existe código malicioso que se hace pasar por un antivirus y alerta a los usuarios de que el equipo está supuestamente infectado y que la única manera de eliminar la infección es adquiriendo un *software* promocionado por el *malware* (Garnham, 2009).

Estos problemas ocasionados por los códigos maliciosos pueden ser mitigados si como usuarios de los sistemas establecemos mecanismos para prevenir o erradicar una infección. Para ello es indispensable que identifiquemos si nuestro equipo ha sido infectado; anteriormente hemos mencionado que los desarrolladores de *malware* han mejorado sus técnicas para prevenir que los usuarios localicen su presencia, a pesar de ello aún existen características que nos permiten identificar si nuestra computadora está infectada:

- **Disminución del rendimiento del equipo:** Cuando un código malicioso se ejecuta utiliza recursos de memoria y procesamiento por lo que podemos identificar la presencia de *malware* si nuestro equipo se vuelve más "lento" sin razón aparente.
- **Problemas en la red:** Debido a que algunos códigos maliciosos hacen uso de la conexión a red, podemos detectar su presencia si se presentan fallas en la red (no es posible conectarse a sitios, no se pueden compartir archivos, etcétera) o simplemente si nuestras transferencias tardan más de lo esperado.
- **Aparición inesperada de publicidad.**
- **Pérdida inesperada de información.**
- **Aparición de nuevos archivos no creados por el usuario:** Algunos códigos maliciosos crean archivos en el sistema por lo que la disminución repentina de espacio en disco, así como la aparición de archivos en el sistema que no hayan sido creados por el usuario puede ser un síntoma de infección.
- **Desactivación del antivirus y otro *software* de seguridad:** Algunas variantes de códigos maliciosos son capaces de desactivar la protección antivirus y del *software* de seguridad de nuestro equipo como *firewall*, *antispyware*, etcétera.

Una vez identificada la infección por *malware* en nuestro equipo es necesario:

- **Realizar un escaneo con un antivirus y *antispyware* actualizados:** Un antivirus y un *antispyware* actualizados podrían localizar la infección y erradicarla por completo del equipo. El escaneo se puede realizar mediante el antivirus instalado en el equipo o utilizando el servicio de un antivirus en línea.
- **Utilizar programas de eliminación automática:** Podemos encontrar en Internet herramientas automatizadas que permiten eliminar códigos maliciosos, la desventaja es que solamente eliminan una variedad o un código malicioso muy específico.
- **Eliminar manualmente:** Si investigamos acerca del código malicioso que afecta al sistema encontramos cuáles son las acciones que realiza y cómo se eliminaría manualmente, sin embargo estos procedimientos se recomiendan solamente a usuarios experimentados.

- **Reinstalar el sistema operativo:** Este método sólo debe ser utilizado cuando no es posible eliminar al *malware* por ninguna de las recomendaciones anteriores, sin olvidar que se debe respaldar la información antes de llevar a cabo ésta acción.

Sin embargo no es suficiente tomar acciones reactivas ante una infección por *malware*, pues actuar solamente cuando el *malware* ha tenido algún efecto podría traer consigo un daño a las computadoras o a la información que pudiera ser irreversible, por lo que es necesario que también establezcamos acciones preventivas que nos ayuden a disminuir las probabilidades de que códigos maliciosos nos afecten:

- **"Instalar y actualizar un *software* antivirus.** Un *software* antivirus no evita la infección por parte de un virus de Internet, pero si ayuda a la detección de éste tipo de código malicioso. Es necesario instalar, administrar y actualizar un *software* antivirus de forma correcta, pero no debe ser el único *software* de seguridad en el equipo" (Fuentes, 2006).
- "**No abrir archivos adjuntos contenidos en correos electrónicos de procedencia extraña**. Una gran diversidad de virus en el Internet se propagan a través del correo electrónico, adjuntando a estos un archivo infectado con lo cual se puedan seguir propagando" (Fuentes, 2006), por lo que sólo deben de ser abiertos aquellos documentos adjuntos que provengan de una fuente confiable y siempre que haya sido analizado por un antivirus antes de abrirlo.
- **Analizar los archivos con un antivirus antes de abrirlos.** Es recomendable solicitar al antivirus que lleve a cabo un análisis antes de que abramos un archivo, en especial debemos realizar esta acción cuando son archivos que abrimos por primera vez y/o que provienen de otro equipo.
- **Analizar medios extraíbles como:** disquetes, memorias usb, cd's, etcétera. Cuando insertamos medios extraíbles en otros equipos pueden contagiarse de algún tipo de código malicioso, por lo que antes de abrir el dispositivo y los archivos que contiene debemos analizarlo con un antivirus en búsqueda de *malware*.
- "Actualizar el sistema constantemente. Algunos virus pueden tomar ventaja de algunas vulnerabilidades no actualizadas en el sistema, por lo que es indispensable instalar las actualizaciones de seguridad más recientes. Esto permitirá estar protegido contra posibles ataques de distintos virus que traten de tomar ventaja de una vulnerabilidad no actualizada." (Fuentes, 2006)

Iván Mauricio Alvarado Limones
Julio César García Vizcaíno

Hace algunos años era imposible pensar en la existencia de códigos maliciosos para dispositivos móviles (teléfonos celulares, PDA's, memorias USB, etcétera). Sin embargo, códigos como *Cabir, Comwar* o *Skuller.gen,* nos ponen en alerta, pues los códigos maliciosos en dispositivos móviles son un problema que debemos enfrentar para prevenir que estos sistemas accedan, modifiquen o alteren la información o el funcionamiento de nuestros dispositivos.

Su surgimiento ha sido gracias al rápido avance en la tecnología móvil ya que precisamente, la capacidad y el método de almacenamiento de datos, la sincronización con la computadora de la oficina o de la casa, la integración del correo electrónico y el desarrollo de aplicaciones empresariales y personales que nos permiten guardar datos y realizar operaciones que normalmente realizaríamos con una PC y si bien este tipo de ataques se ha considerado como "nuevo", la realidad es que son técnicas que se han manejado en el mundo de las computadoras personales desde sus inicios, pues los códigos en dispositivos móviles, al igual que en las computadoras, son códigos capaces de ocasionar algún daño en el sistema o en la información.

Entre las diferentes versiones o variantes de estos códigos existen comportamientos muy similares ya que aprovechan vulnerabilidades que permiten robar información personal, replicarse hacia sus contactos de la agenda para continuar la infección, establecer contacto remoto con alguna entidad externa para que ésta controle por completo el dispositivo siendo capaz de descargar imágenes, realizar llamadas y conectarse a Internet sin autorización del propietario del dispositivo. Pero estos no son los únicos ataques existentes en los dispositivos móviles, pues debido a las actividades que llevamos a cabo podemos encontrar ataques de *smishing* que son ataques que buscan obtener información confidencial de los usuarios a través de mensajes SMS. Y aunque son muchas las vulnerabilidades explotadas y los códigos maliciosos desarrollados para dispositivos móviles, la principal vulnerabilidad no está en los sistemas, si no en la desinformación y la falta de cultura de seguridad informática existente entre los usuarios de tecnología móvil, pues los distribuidores de códigos maliciosos utilizan técnicas de ingeniería social para convencer al usuario de ejecutar su código malicioso.

De manera que para mejorar la seguridad en los dispositivos móviles podemos llevar a cabo algunas actividades como las siguientes:

- Mantener desactivada las tecnologías de comunicación inalámbrica como *Bluetooth* e Infrarrojo mientras no se esté utilizando, pues muchos códigos maliciosos aprovechan este medio para propagarse.

- No aceptar transferencias de archivos, ni descargas de fuentes no confiables, así como también, evitar el acceso a sitios Web desconocidos.

- Utilizar una contraseña de inicio del equipo y otra diferente para el acceso a los datos o información importante.

- Actualizar constantemente el sistema operativo y las aplicaciones del dispositivo.

- Si se maneja información confidencial en estos dispositivos, se recomienda cifrarla para evitar su lectura en caso de extravío o robo del dispositivo.

- Efectuar un respaldo periódico de información.

- En las empresas podrían implementarse políticas de seguridad que definan el uso adecuado de los dispositivos móviles, al tiempo que definan mecanismos de control de acceso a los recursos compartidos mediante móviles.

Es importante mencionar que en el mercado existen otros métodos de protección como la adquisición de *software* de seguridad para dispositivos móviles que provean de protección a la información ante eventos de robo. Sabemos que no existe seguridad al 100%, pero es posible disminuir los riesgos a los que nos enfrentamos si como usuarios realizamos un uso adecuado y consciente de la tecnología, conociendo los peligros existentes y lo más importante adoptando medidas para protegernos.

Rubén Aquino Luna

En los meses recientes y particularmente en los primeros meses de 2009 casi todos hemos escuchado hablar sobre el gusano *Conficker* a través de los medios de comunicación. Es probable también que muchas veces no quede totalmente claro por qué este gusano parece tan importante y por qué es distinto a otros. En este artículo se describe qué es C*onficker*, su evolución y su impacto en redes de México.

El origen

El 20 de noviembre de 2008 se comenzó a propagar un gusano que aprovechaba la vulnerabilidad en el servicio de servidor de sistemas Windows documentada en el boletín de seguridad Microsoft MS08-067 que fue liberado de manera extraordinaria el 23 de octubre de 2008.

El nuevo gusano, sin embargo, no fue el primer "artefacto" conocido que aprovechaba la vulnerabilidad en el servicio de servidor y que permitía la ejecución de código de manera remota a través del envío de paquetes RPC diseñados especialmente al puerto 445/TCP de la máquina víctima. Desde septiembre de 2008 se distribuía un *toolkit*, que permitía explotar un nuevo hueco de seguridad en un componente de los sistemas Windows (llamado (RPC-DCOM), a un costo de 37 USD.

Los primeros intentos por vulnerar de forma masiva PCs a través del nuevo hueco de seguridad fueron relativamente infructuosos. Hasta el 23 de octubre de 2008 en que comenzó la propagación del gusano *Conficker*, o *Downadup* como también se le conoce. La primera versión, conocida como *Conficker.A*, se propaga masivamente a través de la explotación de la vulnerabilidad documentada en el boletín MS08-067, buscando equipos vulnerables en la red.

Evolución

Conficker no es un gusano que únicamente busca propagarse e infectar otros equipos. Además del comportamiento de auto-propagación propia de un gusano, una vez que ha infectado un equipo, *Conficker* busca descargar archivos maliciosos adicionales o actualizaciones desde un conjunto de dominios que genera diariamente de manera aleatoria.

Este comportamiento permite conformar una *botnet* controlada de forma descentralizada con las instrucciones enviadas a los *bots* a través de la descarga de archivos desde los sitios web direccionados a través de dominios aleatorios.

Cada día, cada instancia de *Conficker* genera una nueva lista de dominios a los cuales buscará conectarse. Esta característica de operación se aprovechó también como elemento de mitigación, ya que a partir del análisis del binario, se descubrió el algoritmo de generación de los nombre de dominios y los responsables de los *Top Level Domains*

(como NIC-MX en México) pudieron actuar de manera conjunta para registrar los nombres de dominio que usaría *Conficker* y redirigir el tráfico hacia *sinkholes*, que son instrumentos de mitigación y monitoreo. Los *sinkholes* han permitido "engañar" al gusano que busca actualizarse y, en lugar de conectarse a un sitio de actualización, se conecta a un equipo controlado en el que no se responde a sus peticiones de descarga de archivos y sólo se registran sus datos para identificar el equipo infectado.

Existen diversas variantes de *Conficker* que han ido surgiendo y cambiando desde la primera versión de *Conficker.A*. Desde noviembre de 2008 se han observado al menos 3 variantes de esta amenaza, de las cuales las versiones A y B han sido las de mayor impacto desde su aparición y hasta la actualidad. La variante B de *Conficker* agregó métodos de propagación que resultaron muy eficientes. Además de buscar la vulnerabilidad en el servicio de servidor de Windows, *Conficker.B* se propaga a través de recursos compartidos en red a través de NetBIOS. Busca recursos compartidos sin restricciones y si es necesario, realiza ataques de fuerza bruta para buscar vulnerar los objetivos. Además, implementa la propagación a través de dispositivos de almacenamiento USB, copiándose en el *autorun.inf* en los dispositivos removibles, lo que hace que el binario se ejecute cada vez que el dispositivo USB se conecta a un equipo.

Durante su evolución, *Conficker* también ha tenido vulnerabilidades significativas. *Conficker.B* implementó el uso del algoritmo *hash* MD6 para ofuscar la información que se transmitía entre las PCs infectadas y los sitios de control. El 15 de enero de 2009 el MIT publica una vulnerabilidad en MD6 y al mismo tiempo libera el parche. Esta vulnerabilidad "expone" la información transmitida entre sitios de control y *bots*. La ofuscación en los datos se implantó en *Conficker* para evitar que bandas rivales tomaran control de la *botnet*. La versión C de *Conficker* incluye el parche de la vulnerabilidad pero además incluye el intercambio de información a través de protocolos P2P entre *bots*, lo cual descentraliza totalmente el control de la *botnet* y complica su detección y monitoreo.

El siguiente gráfico muestra una línea de tiempo con la información más importante sobre la evolución de *Conficker*.

Gráfica 1
Evolución de Conficker

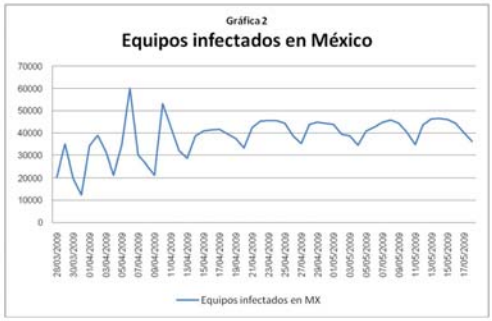
El impacto inicial y el potencial malicioso de *Conficker* hizo que muchas de las principales organizaciones relacionadas con la seguridad informática en el mundo canalizaran los esfuerzos de mitigación de esta amenaza a través de la creación del *Conficker Working Group*, desde donde han surgido muchas de las acciones de mitigación globales.

Conficker en México

En las redes de México hemos padecido y seguimos padeciendo el efecto de la propagación de *Conficker* en sus distintas versiones. A lo largo de estos meses hemos visto redes completas que en algún momento se vuelven prácticamente inoperantes debido a la actividad del gusano que, una vez habiendo infectado un equipo, se propaga rápidamente al resto de la red si en ella se encuentran equipos vulnerables o que comparten recursos sin ninguna restricción.

Desde finales de Marzo de 2008, UNAM-CERT realiza un monitoreo diario de la cantidad de equipos en redes de México que están infectados con alguna variante de *Conficker*. La evolución de la infección desde esa fecha se muestra en la gráfica 2.

De acuerdo a un censo realizado por SRI International, desde el inicio de la propagación de *Conficker* y hasta principios de marzo de este año, se había observado actividad del gusano en 151,861 direcciones IP distintas en redes de México.



El país con mayor número de infecciones era China y en Latinoamérica Brasil, Argentina, Chile y Colombia superaban a México en número de direcciones IP infectadas.

Los países que se encuentran en los primeros 18 lugares en número de infecciones, de acuerdo a este censo, se listan en la siguiente tabla.

País	Total	*Conficker.A*	*Conficker.B*
CN	2,649,674	1,265,792	1,558,286
BR	1,017,825	314,574	786,014
RU	835,970	229,497	718,883
IN	607,172	296,544	423,945
AR	569,445	458,403	240,301
TW	413,762	311,305	125,779
IT	374,513	94,210	290,102
CL	280,182	208,514	136,799
UA	274,411	35,422	255,889
MY	212,477	102,099	135,737
KR	201,107	38,340	169,911
DE	195,923	76,154	122,682
US	191,531	121,323	75,262
RO	182,790	38,497	153,666
CO	169,597	99,603	94,134
TH	165,080	39,000	135,546
ID	164,794	66,623	123,717
MX	151,861	95,694	72,287

Conclusiones

Conficker y sus diversas variantes han mostrado el potencial malicioso que puede llegar a tener en la actualidad una amenaza informática que se propaga masivamente y cómo ésta puede evolucionar rápidamente para hacerse más eficiente en su operación. Algunas de las técnicas que usa *Conficker* para propagarse no son nuevas. Aprovecha de manera eficaz, una vez más, el eslabón más débil de la seguridad informática. La propagación inicial aprovechaba una vulnerabilidad conocida para la cual ya existía un parche. Otra forma muy eficiente de propagación de este gusano es a través del intercambio de dispositivos de almacenamiento USB, lo cual permite evadir la protección perimetral con que muchas organizaciones cuentan en la actualidad. Nos recuerda, por tanto, que la protección perimetral no es suficiente para asegurar los activos informáticos de una organización.

Por otro lado, la colaboración construida entre diversas organizaciones dedicadas a proveer productos y servicios de seguridad informática funcionó de manera notable para lograr contener el impacto de *Conficker* y representa una importante lección sobre la forma en que puede mitigarse una amenaza informática global de este tipo. En la contención de la amenaza participaron fabricantes de antivirus, organizaciones dedicadas al análisis de códigos maliciosos, analistas de amenazas informáticas, proveedores de Internet, proveedores de servicio de nombres, equipos de respuesta a incidentes, etc.

Referencias

[1] http://www.confickerworkinggroup.org
[2] http://mtc.sri.com/Conficker/
[3] http://www.honeynet.org
[4] http://www.microsoft.com/latam/technet/seguridad/boletines/2008/ms08-067.mspx
[5] http://www.seguridad.unam.mx

Julio César García Vizcaíno
Oscar Raúl Ortega Pacheco

A través de los años hemos visto gran cantidad de productos orientados a proteger a nuestros equipos de cómputo y, en especial, a la información que contienen. Los productos más comunes han sido los antivirus y dado que las necesidades de protección han incrementado encontramos en el mercado productos como *antispyware*, barras *anti-phishing,* protección para correo electrónico, etcétera. Manejar estos productos por separado complica a usuarios y administradores verificar su funcionamiento y nivel de actualizaciones, lo que podría poner en riesgo a la información de la compañía o de nuestro hogar, es por ello que los diversos fabricantes de *software* de seguridad han introducido las *suites de seguridad*.

Una *suite de seguridad* "es un conjunto de aplicaciones que se ejecutan en un sistema de cómputo para proveer de protección ante agentes externos que puedan afectar la integridad, disponibilidad y confidencialidad de la información almacenada en ese equipo de cómputo […]" (García, 2009:29), es decir una *suite de seguridad* incorpora a diversos productos de protección a la información, por ejemplo, en el mercado podemos encontrar *suites* que provean protección antivirus al mismo tiempo que nos protegen de ataques en Internet o de robo de identidad. Esto nos lleva a plantear los tipos de suites de seguridad que existen en el mercado:

- **Soluciones corporativas:** son aplicaciones que proveen de protección a equipos pero que trabajan en una administración centralizada, esto significa que a través de un servidor central se puede instalar, configurar o eliminar reglas de protección. Su principal mercado son entornos empresariales.
- **Soluciones de usuario final: son** aplicaciones que proveen de protección a equipos de trabajo y sus configuraciones se pueden realizar directamente en el equipo sin la necesidad de contar con un servidor.
- Estas aplicaciones se recomiendan para hogares y con poco equipo de cómputo.

Prácticamente todas las suites de seguridad proveen protección contra códigos maliciosos con un buen nivel de respuesta, esto se debe a que combinan diversas técnicas de detección y erradicación, por lo que antes de considerar adquirir una debemos tomar en cuenta otras características que vayan más allá de la protección de códigos maliciosos:

- **Integración con el sistema operativo:** se debe de asegurar que la suite de seguridad pueda ejecutarse sin problemas en nuestro sistema operativo.

- **Protección proactiva al navegar en Internet:** la suite debe de ser capaz de prevenir ataques provenientes de Internet, así como también de la capacidad de detener la descarga de archivos que sean perjudiciales para el equipo de cómputo.
- **Protección para correo electrónico:** mucha de la información que se comparte con diferentes usuarios es mediante el correo electrónico, es por ello que el *software* malicioso podría utilizar este medio para infectar el equipo de cómputo. La protección que pueda proveer para el correo electrónico será mediante los diferentes protocolos: POP3, IMAP, MAPI, *Exchange*, SMTP.
- **Protección contra robo de identidad:** en la actualidad es común el robo de identidad, la solución que se adquiera debe de tener la capacidad de proteger al usuario del robo de información confidencial, esto lo se verificar si la *suite de seguridad* contiene un componente que proteja los datos que incluimos en un formulario o si tiene algún mecanismo para evitar que las claves almacenadas en el equipo sean descubiertas.
- **Protección contra pérdida de información:** la capacidad de desinfectar archivos va muy de la mano con el manejo que la *suite de seguridad* pueda realizar en el sistema de archivos. Un manejo incorrecto puede ocasionar pérdidas de datos. La *suite de seguridad* seleccionada debe de contar con mecanismos que permitan la recuperación de archivos infectados.
- **Protección de *firewall*:** la solución debe de proveer un firewall que permita bloquear el acceso al equipo de cómputo así como también de conexiones no deseadas generadas hacia y desde nuestro equipo de cómputo.
- **Protección en tiempo real:** al adquirir una suite de seguridad es necesario que mantenga protegido a nuestro equipo y en general a la información que en él está almacenado. La protección en tiempo real significa tener uno o varios procesos de la suite de seguridad que entran en acción al detectar actividad maliciosa en el equipo, por ejemplo la descarga de un archivo que contiene algún malware o la apertura de un archivo en un dispositivo de almacenamiento externo. El primer mecanismo de protección de una suite de seguridad es la protección en tiempo real.

Finalmente, al momento de adquirir una *suite de seguridad* recomendamos tener en cuenta las necesidades de nuestro hogar o nuestra empresa, así como las características adicionales que provea, sin olvidar que todos los productos instalados en nuestra computadora deben estar actualizados y en el caso particular de las *suites de seguridad* es importante observar que se actualice su base antivirus todos días y que se mantenga activa la protección en tiempo real.

Oscar Raúl Ortega Pacheco
Tania Gabriela Montero Trejo
Julio César García Vizcaíno

1. Actualiza tu sistema operativo y aplicaciones

Frases como "Está disponible la nueva versión del programa", "Hay actualizaciones listas para instalar" o "Hay actualizaciones de *software*" aparecen con cierta frecuencia en nuestros sistemas de cómputo y es que los fabricantes de los sistemas emiten actualizaciones con cierta periodicidad, pues a pesar de que los sistemas de cómputo se someten a diversas pruebas de calidad y seguridad antes de ser distribuidos al público, es posible identificar fallas en su funcionamiento. Estos errores derivan en problemas de seguridad, es decir, podrían permitir a un atacante realizar acciones maliciosas en nuestro equipo, como instalar programas; leer, modificar o eliminar nuestros datos; o utilizar nuestra computadora como un medio para hacer otros ataques en Internet. Es por ello que como usuarios de los sistemas de cómputo debemos mantener al día nuestros sistemas pues las actualizaciones que proporcionan los fabricantes solucionan las vulnerabilidades existentes, además de que algunas de ellas pueden mejorar el rendimiento de las aplicaciones o proporcionar características adicionales que faciliten nuestras actividades.

Para nosotros como usuarios existen varios mecanismos para actualizar nuestras aplicaciones, el más sencillo de ellos es solicitarle a nuestro sistema que nos avise cuando existan nuevas actualizaciones y si es posible solicitar que las instale de manera automática. La otra opción es estar al pendiente de cuál es la versión más actual del programa y si apareciera una nueva versión, ir directamente al sitio del fabricante y descargar el paquete de actualización para finalmente instalarlo. Para más información recomendamos el siguiente artículo:

- Métodos y herramientas de actualización http://www.seguridad.unam.mx/usuario-casero/secciones/herramientas.dsc

2. Utiliza una cuenta de correo alternativa

Uno de los grandes problemas que se vive a diario en el mundo de las tecnologías de información y telecomunicaciones es el correo *spam* o correo no deseado, estos mensajes electrónicos que pueden contener publicidad o *software* malicioso se han convertido en un gran reto de seguridad pues llegan a saturar servidores de correo y hasta ancho de banda de una red. A nosotros como usuarios este correo nos ocasiona gran pérdida de tiempo al momento de seleccionar los mensajes válidos de aquellos que son *spam*, además del riesgo de recibir virus, gusanos, *spyware* y otros códigos maliciosos. Debemos de tomar en cuenta que cuando acabamos de crear una cuenta de correo recibimos una cantidad muy pequeña de *spam*, sin embargo conforme pasa el tiempo esta cantidad aumenta, ello se debe al uso que damos a nuestra cuenta

de correo, pues al inscribirla en foros, listas de correo, suscripciones gratuitas, servicios en línea, etcétera incrementamos las probabilidades de recibir correo no deseado, ya sea de los sitios a los que nos hemos inscrito, o de otros pues en ocasiones algunos sitios venden la lista de suscriptores a *spammers*. Es por ello que recomendamos tener una cuenta de correo alternativa, es decir, manejar una cuenta de correo para actividades de trabajo, así como para mantener contacto con nuestros amigos y conocidos y una segunda cuenta que utilicemos cuando accedemos a servicios que nos solicitan un registro.

3. Protégete del *phishing*

El *phishing* "es un conjunto de técnicas y mecanismos empleados por los intrusos o hackers con el propósito de robar información personal de un usuario y así poder suplantar su identidad" (UNAM-CERT, *s.a.*). Normalmente la información más buscada por los intrusos está relacionada con información financiera (usuarios, claves y números de cuenta), aunque otro tipo de información como cuentas y contraseñas de correo electrónico o de acceso a algún portal o equipo dentro de una compañía también es altamente recurrida. La pregunta que surge es, ¿cómo podemos prevenir este tipo de ataques? Antes de responder a la pregunta debemos explicar cómo se lleva a cabo un ataque de *phishing*. Inicialmente un intruso crea un sitio Web con el objetivo de hacer creer a un usuario que es el sitio verdadero, posteriormente el intruso envía una serie de correos electrónicos a los usuarios tratando de persuadirlos para que ingresen al sitio y envíen los datos solicitados; una vez que el usuario ha enviado los datos, el intruso puede utilizarlos libremente. Entonces para prevenir que estos ataques tengan éxito te sugerimos lo siguiente:

- No respondas a correos que soliciten información personal.
- Instituciones serias no solicitan a los usuarios que confirmen su usuario y contraseña a través de un correo electrónico, por lo que si recibes un correo de este tipo te recomendamos no acceder al sitio mencionado en el correo.
- Algunos navegadores tienen incluido un filtro *antiphishing* así que te sugerimos lo mantengas activo pues este tipo de filtros podrían advertirte cuando accedas a un sitio falso. En caso de que el navegador no cuente con este filtro podrías obtener una barra *antiphishing* de Internet.

4. Actualización de *suite de seguridad*

Una forma de proteger a tu equipo de cómputo es mediante el uso de una *suite de seguridad* mejor conocida como antivirus, programa que te protege de amenazas como virus, gusanos, *software* espía, etcétera. Ahora bien la *suite de seguridad* requiere de la actualización de los archivos utilizados para proteger la información de tu equipo. La forma de realizar dicha protección es mediante la descarga de archivos, desde el

sitio del fabricante, mismo, que contiene información precisa para la detección de las distintas amenazas. Una incorrecta configuración y la no actualización de tu *suite de seguridad* podrían hacer vulnerable tu equipo a las distintas amenazas desconocidas por la propia suite de seguridad. La manera más sencilla de actualizar tu *suite de seguridad* consiste en verificar que tu *software* se actualice diariamente. La forma de verificar esto es, en la pestaña de configuración del producto y dentro de la sección de actualización.

5. Importancia del *Firewall*

Un *firewall* en simples palabras es un filtro que controla el intercambio de información entre redes, examinando el tráfico entrante y saliente, permitiendo o negando el acceso dependiendo de las reglas o políticas que se hayan definido. Nos brinda distintas alternativas para proteger la red, dependiendo de la configuración de esté, podemos realizar el filtrado de paquetes a partir de los distintos campos de los protocolos de comunicación, por ejemplo si utilizamos el protocolo TCP/IP podemos utilizar las direcciones IP para establecer reglas de filtrado hacia y desde nuestra red.

El controlar los datos que entran y salen de nuestra red nos permite protegernos de accesos no autorizados del exterior, proteger información sensible de la organización, optimizar los accesos y comunicación entre los diferentes elementos de la infraestructura.

Contar con las ventajas que proporciona un *firewall* en nuestra red nos permite tener un mayor nivel de seguridad en la misma, sin embargo el muro protector que levantamos con un *firewall* no es infalible por lo que no podemos dejar toda la seguridad de nuestra red a este elemento. En contraste no contar con la protección de un *firewall* es equivalente a dejar la puerta de nuestra casa abierta, dejando que cualquier persona entre y tome lo que desee sin poderlo evitar.

Tener un *firewall* en nuestra red puede ahorrarnos muchos dolores de cabeza.

Bibliografía

Fuentes, Luis (2005). *Nuevas tendencias del Malware*. Enter@te [en línea] N° 41. Ciudad de México, México: Universidad Nacional Autónoma de México. Recuperado el 4 de marzo de 2009 de http://www.enterate.unam.mx/Articulos/2005/agosto/malware.htm.

Fuentes, Luis (2005). *Troyano* [en línea]. Ciudad de México, UNAM-CERT, Noviembre 2005. Recuperado el 12 de marzo de 2009 de http://www.seguridad.unam.mx/usuario-casero/secciones/troyano.dsc.

Fuentes, Luis (2006). *Análisis de Malware en el UNAM-CERT* [en línea]. En: Semana de la Seguridad Informática 2006, Instituto Politécnico Nacional. Recuperado el 4 de marzo de 2009 de http://www.malware.unam.mx/descarga_archivo.dsc?doc_id=23.

Fuentes, Luis, *et al.* (2006). *Combatiendo códigos maliciosos* [en línea]. En: Día Internacional de la Seguridad en Cómputo 2006, noviembre de 2006, UNAM-CERT. Recuperado el 4 de marzo de 2009 de http://www.malware.unam.mx/descarga_archivo.dsc?doc_id=22.

Fuentes, Luis, *et al.* (2006). *Virus* [en línea]. Ciudad de México, UNAM-CERT, Junio 2006. Recuperado el 12 de marzo de 2009 de http://www.seguridad.unam.mx/usuario-casero/secciones/virus.dsc.

Fuentes, Luis, *et al.* (2007). *Códigos maliciosos y otros ataques informáticos* [en línea]. En: XV Aniversario del centro Nuevo León de la Dirección General de Servicios de Cómputo Académico, abril de 2007, DGSCA-UNAM. Recuperado el 4 de marzo de 2009 de http://www.malware.unam.mx/descarga_archivo.dsc?doc_id=55

García, Julio (2009). *Metodología para el análisis de comportamiento de códigos maliciosos*. Tesina de licenciatura, Facultad de Ingeniería, UNAM, Ciudad de México, febrero de 2009.

Garnham, Oliver (2009). *Scam Antivirus App Spreads Malware* [en línea]. PCWorld, Febrero 2009. Recuperado el 12 de marzo de 2009 de http://www.pcworld.com/article/159974/supposed_antivirus_program_spreads_malware.html.

Jiménez, Jesús (2005). Spyware [en línea]. Ciudad de México, UNAM-CERT, Marzo 2005. Recuperado el 12 de marzo de 2009 de http://www.seguridad.unam.mx/usuario-casero/secciones/spyware.dsc.

Jiménez, Jesús (2007). *¿Qué es malware?* [en línea]. Ciudad de México, UNAM-CERT, Junio 2007. Recuperado el 4 de marzo de 2009 de http://www.seguridad.unam.mx/usuario-casero/secciones/segumalware.dsc.

López, Juan, *et al.* (2006). Gusano de internet [en línea]. Ciudad de México, UNAM-CERT, Junio 2008. Recuperado el 12 de marzo de 2009 de http://www.seguridad.unam.mx/usuario-casero/secciones/gusanos.dsc.

Ortega, Oscar; *et al*. (2008). *50 años de seguridad en cómputo*. Póster conmemorativo para el Congreso de Seguridad en Cómputo 2008, septiembre de 2008, UNAM-CERT.

Ortega, Oscar*; et al.* (2008). *Códigos Maliciosos. Evolución*. Enter@te [en línea] N° 70. Ciudad de México, México: Universidad Nacional Autónoma de México. Recuperado el 4 de marzo de 2009 de http://www.enterate.unam.mx/artic/2008/junio/art6.html.

Roberts, Raymond (2008). *Malware development life cycle* [en línea]. Virus Bulletin Conference October 2008, Microsoft Corp., Australia. Recuperado el 4 de marzo de 2009 de http://download.microsoft.com/download/9/3/b/93b3344c-15f0-4f13-b915-d8954ac1604f/Roberts-VB2008.pdf

Symantec Corp. (*s.a.*). *Cómo Atacan* [en línea]. Recuperado el 4 de marzo de 2009 de http://www.symantec.com/es/mx/norton/security_response/malware.jsp.

UNAM-CERT (*s.a.*). *Diccionario* [en línea]. Recuperado el 12 de marzo de 2009 de http://www.seguridad.unam.mx/usuario-casero/secciones/diccionario.dsc.