CIBERNOTICIAS

SCP

MALWARE

Cyberoam

Avira

CRYPTOPHONE

NEXXT SOLUTIONS

open source

CONTENIDO

CREDITOS:

Revista virtual de seguridad informática, recopilación de los mejores artículos de la prensa internacional.

Recopilación y edición:

Consuelo de la Torre

c.delatorre@scprogress.com (+593 979003123)

Marco de la Torre

m.delatorre@scprogress.com (+593 998053611)

Revisado por:

Arturo de la Torre

adltorre@scprogress.com (+593 999025294)

Síguenos en:

www.scprogress.com Facebook Twitter

Malware

En los últimos años, la tecnología ha avanzado vertiginosamente, los equipos informáticos, así como, el software para obtener mayores ventajas y facilidad en las tareas, se desarrollan con mayor rapidez. Al considerar la información, como el bien más valioso de las empresas y las personas, se crean mayores seguridades para protegerla, pero en la misma intensidad, se generan programas para poder sustraerla, a través de diferentes medios, ya sea sólo con el ánimo de experimentar el alcance de los programas, o para la realización de actos ilícitos.

A estos programas se los conoce comúnmente como virus, creados por hackers o crackers, pero en los últimos años, se los ha denominado malware, seguidamente realizamos una explicación más clara sobre el término.

Malware proviene de los términos en inglés “Malicious software”, que en español quiere decir código malicioso, engloba a todo tipo de programas cuyo objetivo principal es arruinar un sistema informático, o causar un mal funcionamiento en el mismo. En este grupo se encuentran términos como: Virus, Troyanos (Trojans), Gusanos (Worm), Keyloggers, Botnets, Ransomwares, Spyware, Adware, Hijackers, Keyloggers, FakeAVs, Rootkits, Bootkits, Rogues, etc.

Las motivaciones de los creadores de malware son principalmente razones económicas:

- Anuncios o redirección a sitios web con publicidad que les reportan ingresos.
- Obtención fraudulenta de datos financieros (datos de tarjeta de crédito etc.).
- Controlar el computador y usarlo como esclavo o zombi para atacar otros sistemas ("Denial of Service" o DoS).
- Fraude haciendo clic en anuncios (de Google u otros anunciantes).

Las principales vías de infección de los malware son:

- Por medio de redes para compartir software.
- Adjuntos en correos no solicitados (Spam), o al abrir correos electrónicos de remitentes desconocidos sin antes analizarlos con un software antivirus.
- Cuando navegas en internet sin actualizaciones instaladas en tu sistema operativo y tus aplicaciones, como por ejemplo tu navegador Web.
- Cuando abres archivos de extraña apariencia sin antes analizarlos con un antivirus.
- Sitios webs fraudulentos cuando se visitan o bajándose un fichero de ellas.
- Incluido en otro programa (típicamente uno gratuito o como regalo) que ha sido descargado de Internet.
- Dispositivos USB/CDs/DVDs infectados.
- A través de archivos bajados con una utilidad "peer-to-peer" (P2P).
- En un fichero enviado por mensajería instantánea o chat.

Los peligros que conllevan las diversas clases de malware son muchos, principalmente: pérdida económica; espionaje de su actividad y pérdida de privacidad; degradación del rendimiento de la computadora; y el uso de su computador para atacar a otros.

Algunos de los síntomas que tu equipo puede presentar cuando es afectado por algún malware, pueden ser:

- Ejecución de procesos desconocidos en tu sistema.
- El uso del computador va más lento.
- Interrupción de la conexión a Internet en ciertos momentos.
- Aparición de ventanas de mensajes emergentes o anuncios "pop-ups".
- Mensajes o errores inesperados.
- El computador se queda sin memoria o sin espacio en disco.
- El computador se apaga sólo de forma inesperada. No arranca de forma normal o produce mensajes extraños.
- Se producen cambios inexplicables en ficheros, como que desaparecen o cambian de nombre.

- El computador tiene comportamientos erráticos o inesperados.
- Hay procesos corriendo (en Windows se ven en el "Gestor de Tareas") que son sospechosos (son nuevos, no se sabe cuál es su función, etc.).
- Cambios en el navegador como: Página de inicio del navegador distinta; nuevo enlace "favorito"; nueva barra de herramientas.

Sin embargo, estos síntomas pueden variar dependiendo del tipo de malware que infecte a tu equipo.

¿Cómo protegernos del Malware?

Existen algunas buenas prácticas de seguridad que puedes llevar a cabo para evitar ser infectado por algún código malicioso y proteger nuestros equipos ante la posible infección de algún tipo de malware, a continuación detallamos algunas:

- Instalar y mantener actualizado un software antivirus.
- Hoy en día un antivirus no es suficiente para mantenerte protegido, por lo que debes también instalar y actualizar un software antispyware.
- Habilitar un firewall o cortafuegos en tu equipo
- Instalar en los sistemas operativos todas las actualizaciones de seguridad.
- Mantenerse medianamente informados sobre las nuevas amenazas
- No abra ficheros incluidos en mensajes de correo de personas desconocidas o incluso si conoce el remitente no lo abra si le parece sospechoso (hay virus que utilizan la libreta de direcciones de correo para propagarse).
- Use contraseñas fuertes.
- Tenga cuidado con archivos obtenidos por P2P o no use P2P.
- Mantenga su navegador y los "plugins" que usa actualizados (puede usar por ejemplo la utilidad en https://browsercheck.qualys.com para comprobarlo).
- Familiarícese con la lista de programas que su computador procesa normalmente (en Windows se ve en el "Gestor de Tareas") y cuando tenga sospechas de malware, revise la lista para comprobar si hay procesos nuevos corriendo. Puede buscar en internet por el nombre del programa sospechoso.
- Esté a la defensiva y use el sentido común.

Los criminales en internet tienen una gran inventiva y siempre están desarrollando nuevas formas de timos. Por este motivo es importante estar a la defensiva siempre y usar principios generales sólidos, como no hacer una compra en Internet como reacción a un mensaje de una página web o un email.

Si ha sido infectado o sospecha que ha sido infectado por un virus de cualquier tipo:

- Si tiene más de un computador desconecte la unidad infectada de la red para evitar posibles propagaciones del malware.
- Cierre la aplicación de email (Outlook o Thunderbird por ejemplo).
- Realice un escaneo con un anti-virus, usando un antivirus online o si el computador está desconectado de Internet, con un CD.

Si usa Internet para acceder a cuentas bancarias u otros sitios web a los que transmite información secreta considere usar un computador dedicado de forma exclusiva para esta actividad. Dicho computador no debe usar otro software que el mínimo para usar el navegador y no se debe usar para correo electrónico o para acceder a otros sitios de Internet. Tenga en cuenta que con un software de virtualización como VMware o VirtualBox puede crear una "máquina virtual" o sistema aislado dentro de otro sistema operativo para uso exclusivo en la navegación a sitios web críticos (bancos), de forma que no tiene que usar el hardware de una PC física.

FUENTE: https://www.infospyware.com/articulos/que-son-los-malwares/.
http://www.seguridad.unam.mx/usuario-casero/eduteca/main.dsc?id=193
http://seguridadinformati.ca/articulos/malware.html

Cooperativa de Ahorro y Crédito "General Rumiñahui"

Promoviendo el desarrollo y bienestar de sus socios militares y civiles desde 1993.

- **Créditos sin garante hasta 3.000 dólares.**
- **Otorgamos créditos para consumo, emprendedores y microempresarios.**
- **Las tasas de interés más bajas del mercado.**
- **Inversiones a plazo fijo.**
- **Pagos de créditos y ahorros, a través de ventanillas o con autorización de débitos bancarios del Banco Pichincha, General Rumiñahui e ISSFA.**

Suites en Tonsupa – Esmeraldas por mantener las cuentas activas, pagos puntuales e inversiones.

Calle Manuel Cabeza de Vaca N53-240 y Av. Los Pinos a 30 mts. Del Cuartel Rumiñahui.
Teléfonos: 2411-731 / 2406-117 / 0984977204
www.cooprumi.fin.ec

Malware que afecta a los equipos iPhone y Mac

La creencia de que no existen programas informáticos malignos para los sistemas de Apple es un "mito", afirman los expertos.

Desde hace años circula la creencia de que no existen virus informáticos para los sistemas operativos de Apple. Hoy los expertos quieren desmitificar con cifras esta leyenda. Desde 2012 hasta ahora se ha cuadruplicado el número de estos programas malignos: se ha pasado de 500, hace cuatro años, a 2.200 en 2015, según los datos recabados por una empresa de seguridad. Estos virus afectan tanto a la versión móvil de iOS como a los ordenadores Mac OS. "El mito de que no hay virus para Mac es historia. Sólo en 2015 han detectado el doble de malware para estos sistemas que el detectado en 2014".

"No hay nada en los equipos Apple que les haga inmunes a virus y gusanos diseñados para infectarlos", sentenciaba el profesor de Criptología y Seguridad Informática de la UPM Jorge Dávila. De hecho, en 1981 los Apple II fueron los primeros ordenadores en sufrir un virus de impacto, el Elk cloner. Entonces, ¿de dónde viene la fama?

Los sistemas de Apple son cada vez más interesantes para los desarrolladores de virus porque los utiliza mucha gente

Se debe a la baja cuota de mercado que tenía Apple hace unos años, que provocó que los piratas informáticos no se centraran en crear virus para este sistema. "Las ventas de PC sobrepasaron a las de Apple rápidamente, así que los programadores de virus se centraron en esa plataforma", detalló a este periódico David Sancho, investigador antimalware.

Pero ahora, eso ya ha cambiado. "Al ser una tecnología que utiliza cada vez más gente, los sistemas de Apple son cada vez más interesantes para los desarrolladores de malware. A cuanta más gente puedan atacar, más rentable les resulta el tiempo que invierten en crear los virus". Entre todos los programas, se ha hecho una selección de los que se consideran más modernos y peligrosos.

1. **WireLurker.-** Este virus, detectado en noviembre de 2014, se originó en China y fue considerado como la "mayor amenaza registrada para productos de Apple". Se trataba de un malware que podía desde robar direcciones de contacto o mensajes de texto hasta tomar el control completo de los dispositivos. Se integraba en el sistema a través de lo que parecían apps normales que se podían descargar en la página oficial del Apple Store y se propagaba a otros aparatos como iPhone, iPod o iPad vía USB, al conectarlo al ordenador infectado. "Lo más curioso y peligroso de WireLurker es que no requiere de un jailbreak en iOS para poder infectarlo".
2. **KeRanger.-** Creado y detectado en marzo de este año, el KeRanger es uno de los tipos de programas maliciosos más peligrosos: un ransomware, un secuestro de los dispositivos. Se propagaba a través de Transmission, un popular cliente de BitTorrent (para descargar archivos). Una vez está instalado en tu aparato, los creadores del "virus" toman el control, te cortan el acceso a todo tipo de datos y piden un rescate —monetario, normalmente, en bitcoins (monedas virtuales)— por ellos. Es una nueva modalidad que ya se ha usado para secuestras grandes servidores de universidades y hospitales de Estados Unidos.
3. **Codgost.-** Este troyano, se descubrió en 2015, pero se actualizó de nuevo este año. Está diseñado para robar información de tu Mac. "Como la mayoría del malware para Mac OS X suele llegar a los dispositivos por medio de descargas que no son oficiales".

   CoinThief 2014 es un troyano diseñado para robar bitcoins de los dispositivos Mac OSX infectados

4. **CoinThief 2014.-** Este troyano fue descubierto hace más de dos años y estaba diseñado para robar bitcoins de los dispositivos Mac OSX infectados. Se presentaba como una aplicación con la que enviar y recibir pago de este tipo de monedas virtuales y una vez instalada robaba las credenciales. No se conoce la media que puede robar a cada usuario, pero empresas como SecureMac explicaron que alguno de los usuarios perdió hasta 12.000 dólares.
5. **Yontoo.-** Se trata de una extensión que se instala en tu navegador para inyectar publicidad maliciosa. Parece una aplicación inofensiva para descargar vídeos de forma rápida desde YouTube, pero al instalarse en tu equipo, controla los navegadores web, muestra publicidad engañosa e inyecta anuncios de forma continua a sitios comprometidos.
6. **iWorm 2014.-** Este malware fue descubierto a finales de 2014 y se calcula que ha infectado al menos a 17.000 direcciones IP en todo el mundo. La forma en la que se instala en el Mac no está clara, pero sí se sabe que crea una "puerta trasera" que une el Mac a una red zombie, que les da a los atacantes acceso a tus datos (desde contraseñas de email o redes sociales hasta cuentas corrientes) y, en ocasiones, les permite controlar el ordenador de forma remota.

   El "antivirus" gratuito "Mac Defender" es, en realidad, es un virus capaz de obtener la información de la tarjeta de crédito

7. **MacVX.-** Más que un virus, MacVX es un complemento para navegadores que permite ver vídeos con mayor calidad y a mayor velocidad. Sin embargo, está catalogado como Programa Potencialmente no Deseado (PUP) ya que inunda tu navegador de anuncios. Y aunque no es nuevo —se tiene constancia de sus implicaciones desde 2014— "afecta a casi todos los navegadores y la mayoría de la publicidad que ofrece es falsa o maliciosa", aseguran desde la empresa de seguridad informática.
8. **Janicab**.- Es un malware que afecta a la plataforma de vídeo online más grande del mundo, YouTube. Su principal función es robar información mediante la realización de pantallazos o grabación del audio de lo que el usuario está viendo o escuchando. Fue descubierto por una compañía de seguridad, F-Secure, porque dejaba comentarios en varios vídeos con direcciones IP cifradas de donde se encontraban los servidores de control.
9. **Mac Defender.-** "Se trata de una de las estafas para usuarios de Mac más antiguas y aun así, sigue siendo una amenaza al día de hoy. El funcionamiento es simple: desde sitios web legítimos se redirige a los usuarios a sitios web falsos donde se les informa de que su ordenador está infectado con un virus. Al usuario se le ofrece un "antivirus" gratuito llamado "Mac Defender" para solucionar el problema que, en realidad, es un virus capaz de obtener la información de la tarjeta de crédito. Los nombres más comunes de este software malicioso son "MacDefender", "MacProtector" y "MacSecurity".

Cómo saber si tu Mac tiene un virus

"Si ves que tu Mac, tus dispositivos móviles o weareables de Apple comienzan a funcionar de forma excesivamente lenta, o si observas un consumo elevado de la CPU, de la memoria, del disco o de la red, deberías sospechar que tu dispositivo podría haber sido infectado".

Además de la protección de un antivirus, consejo recomendado por todos los expertos en ciberseguridad. También se recomienda no descargar nada que no provenga de webs oficiales y, sobre todo, evitar los jailbreaks, los procesos que suprimen limitaciones de Apple para poder instalar aplicaciones no permitidas.

FUENTE: http://tecnologia.elpais.com/tecnologia/2016/10/20/actualidad/1476957274_848801.html

Los diez virus informáticos más peligrosos de la historia

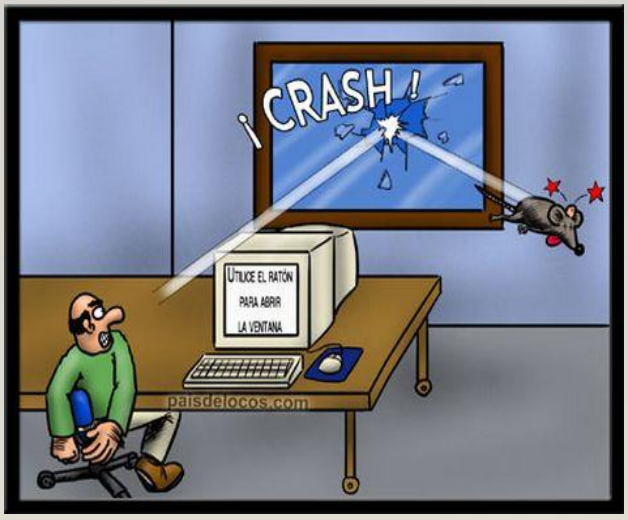
En los últimos años estamos viendo un cambio hacia ataques mucho más especializados y anónimos, con hackers que ya no buscan tanto la notoriedad como el simple enriquecimiento y organizaciones especializadas en el fraude electrónico. Por ello, resulta fundamental establecer una política empresarial de seguridad clara y contar con el apoyo de la mejor solución de seguridad posible. Aquí una selección de los virus que causaron más daño:

1. Virus CHI o Chernobyl: Apareció en 1998 y puso en el punto de mira a los sistemas equipados con Windows 95, 98 y Me. Se estima que infectó a un total de 60 millones de equipos, provocando unas pérdidas totales que rondaban los 1.000 millones de dólares, debido especialmente al valor de la información que destruía. Una vez dentro del equipo infectado CHI eliminaba la información del equipo, pero también podía llegar a suprimir la BIOS, de forma que hacía imposible el arranque.
2. I Love You: Uno de los más conocidos, llegó allá por el año 2000, disfrazado de correo electrónico con tintes de romanticismo. En un tiempo donde los usuarios eran mucho más ingenuos y los filtros anti-spam claramente mejorables consiguió infectar a más de 50 millones de equipos con gran rapidez. El virus del amor generó 5.500 millones de dólares en pérdidas, afectando a entidades tan importantes como el Pentágono o el Parlamento Británico, además de a numerosas empresas españolas.
3. SQL Slammer: Este gusano no se instalaba en el disco duro de los equipos, sino en la memoria RAM. Así, desaparecía con un simple reinicio pero eso fue suficiente para infectar a medio mundo en solo 15 minutos. SQL Slammer afecto a compañías aéreas, cajeros automáticos y dejó sin internet a Corea del Sur y Portugal, provocando una situación de serio riesgo para millones de personas.
4. Melissa.- En marzo de 1999, el virus Melissa pudo infectar a más de 100 mil ordenadores en tan solo 3 días. Este virus prometía las contraseñas de decenas de sitios web pornográficos de pago, sin embargo, poco después, sorprendía a los usuarios.
5. Conficker: Este fue el último gran virus que afectó a los sistemas informáticos del mundo. En el 2008 este virus se hizo popular ya que era muy difícil de eliminar. Conficker desactivaba las actualizaciones de Windows y de los antivirus instalados, impedía el acceso a páginas web y eliminaba los puntos de restauración del sistema.
6. Cryptolocker: Este troyano infecta equipos y encripta el disco duro. Además, despliega un cronómetro que amenaza con borrar todos los archivos si el contador llega a cero, para lo que pide un pago económico mediante formas de dinero cibernético para liberarlo.
7. Sasser: Este virus se volvió popular durante el 2004. Del mismo modo que el Blaster, se aprovechaba de una vulnerabilidad de Windows para propagarse. Sasser se hizo muy popular porque infectó los sistemas informáticos de hospitales, universidades, bancos, compañías aéreas, agencias de noticias, etc.
8. Brain: fue un virus para MS-DOS que infectó varios sistemas en 1986. Con Brain empezaron los sofisticados virus informáticos, este atacaba el sector de arranque de los discos e intentaba ocultar su presencia.
9. Core War: En 1959, los ingenieros de AT&T crearon un juego llamado Core War. Este consistía en reproducirse y ocupar la memoria del oponente. Si bien en ese momento los sistemas no alcanzaban ni siquiera un MB de RAM, este puede ser considerado como el precursor de los virus informáticos.
10. Morris: Este pequeño gusano que robaba la memoria RAM de los ordenadores infectó hasta algunos ordenadores de la NASA. Su creador, Robert Morris Jr., hijo de uno de los creadores de Core Wars, tuvo que pasar 3 años en libertad condicional por ello.

FUENTES: http://www.diariosur.es/tecnologia/internet/201602/19/cinco-virus-raros-internet-20160219211433.html
http://www.sololistas.net/10-virus-informaticos-que-causaron-panico-en-el-mundo.html
http://virusinformaticosyobi.blogspot.com/2016_03_01_archive.html
http://www.muycomputerpro.com/2015/03/18/cinco-virus-mas-peligrosos-historia
http://seguridad.foroes.org/t10859-los-10-virus-informaticos-mas-peligrosos

Humor


¡¿SE PUEDE SABER QUÉ ES ESTÁ CARTA EN EL BOLSILLO DE TU AMERICANA DIRIGIDA A «CUCURUCHITO MÍO»?!
EM...
¡SPAM!
ESO, SPAM


¡CRASH!
UTILICE EL RATÓN PARA ABRIR LA VENTANA
paisdelocos.com


¿Sabes que le dijo una impresora a la otra?
mmmm...
nooo...
ESTA COPIA ES TUYA O ES IMPRESION MIA.....JEJEJE
JAJAJA..... BUENISIMO.....


A VER, ALUMNOS, ENCIENDAN EL ORDENADOR
CLIC CLIC CLIC CLIC CLIC CLIC
ENCIENDAN LA PDA
CLIC CLIC CLIC CLIC CLIC CLIC
ENCIENDAN EL CEREBRO
LA NATURALEZA NOS DIO CIEN MIL MILLONES DE NEURONAS. A TODAS LUCES, UN DESPILFARRO
VAYA, POR DIOS. VOLVIÓ A FALLAR LA LÍNEA

Actualidad

EE. UU. Acusa a Rusia de dirigir hackeo para interferir en sus elecciones

EE. UU. Acusó oficialmente a Rusia de los recientes ataques cibernéticos contra personas e instituciones estadounidenses, incluido el Comité Nacional Demócrata (DNC), para interferir en las elecciones del 8 de noviembre.

El Departamento de Seguridad Interior de Estados Unidos y el director de inteligencia nacional afirmaron hoy (07.10.2016)en un comunicado conjunto estar seguros de que Rusia está detrás de los ataques a sistemas informáticos de instituciones y organización políticas.

Los e-mails del Comité Demócrata Nacional filtrados en julio expusieron una fuerte oposición al precandidato demócrata Bernie Sanders, lo que llevó a la renuncia de la líder de la formación, Debbie Wasserman Schultz.

Intención de interferir con el proceso electoral

El Departamento de Seguridad Interior dijo que las revelaciones a través de páginas web, incluyendo Wikileaks, "son congruentes con los métodos y motivaciones de los esfuerzos dirigidos por Rusia" e interferencias similares de Moscú con la política en otras partes. "Estos robos y revelaciones tienen la intención de interferir con el proceso de elecciones de Estados Unidos", subrayó el Gobierno norteamericano.

Según EE. UU., "tal actividad no es nueva para Moscú. Los rusos han utilizado tácticas y técnicas similares en Europa y Eurasia, por ejemplo, para influir allí en la opinión pública". "Creemos que, teniendo en cuenta el alcance y la sensibilidad de estos esfuerzos, sólo los más altos funcionarios de Rusia podrían haber autorizado estas actividades", subraya el comunicado.

Por su parte, el presidente ruso, Vladímir Putin, ha negado en el pasado cualquier relación con los ataques. "No sé absolutamente nada sobre eso. Rusia nunca ha hecho algo así a nivel estatal", alegó Putin el pasado mes en una entrevista con *Bloomberg*.

FEW (dpa, EFE)

FUENTE: http://www.dw.com/es/ee-uu-acusa-a-rusia-de-dirigir-hackeo-para-interferir-en-sus-elecciones/a-35994360#nomobile.

6 consejos para los fanáticos de las redes sociales y la mensajería instantánea

El reino de Internet ha cambiado mucho en los últimos años. Antes, navegar significaba usar motores de búsqueda hasta llegar a contenidos específicos, o leer artículos en tus sitios de noticias favoritos. Hoy, las redes sociales, los videos y la mensajería instantánea son centrales para la experiencia online de un usuario, especialmente en la generación más joven.

Pero la comodidad de interactuar con amigos y conocidos tiene su precio. Una nueva serie de riesgos ha aparecido y a pesar de que las redes sociales están haciendo un esfuerzo importante, con frecuencia es la negligencia de los usuarios la que lleva a que se comprometa su seguridad.

Dado que octubre es el mes de la ciberseguridad en Europa y ESET lo apoya publicando contenidos para profundizar la concientización de los usuarios, es hora de listar algunos consejos que te ayudarán a protegerte en estos populares servicios.

1. Actualiza todo tu software y mantén tus dispositivos seguros.- Tu sistema operativo y aplicaciones, así como todo tu software (especialmente los navegadores) deben estar al día. Además, para mantener a los villanos lejos de ti, usa una solución de seguridad completa y confiable tanto en tu computadora como en tus dispositivos móviles.

2. Usa contraseñas fuertes.- Esta práctica no solo aplica para las redes sociales, sino también para el reino cibernético en general. Recuerda que tus contraseñas deben ser fuertes, robustas y únicas, de modo que no se repitan en distintos servicios; combina mayúsculas, minúsculas, números y caracteres especiales, y ten en cuenta que no es necesario preocuparte por tener que memorizarlas todas, ya que puedes usar un gestor de contraseñas para evitar que te fatiguen los asuntos de seguridad.

3. Revisa la configuración de tus cuentas.- Tu prioridad principal al crear un nuevo perfil es revisar las opciones de seguridad y privacidad que ofrezca el servicio y configurarlas correctamente. Asegúrate de que tus publicaciones solo sean visibles para tus amigos cercanos o para el grupo que tenías en mente, y no para cualquiera. Si añades detalles a tu perfil, como datos personales, escóndelos de extraños y posibles estafadores para que no los puedan extraer; podrían tratar de usarlos para adivinar tus contraseñas o robar tu identidad.

Si no sabes por dónde empezar, tenemos más consejos para revisar los ajustes de tus redes sociales. Y recuerda que las compañías los cambian en forma periódica, por lo que es importante que les prestes atención cada tanto.

4. Piensa dos veces antes de publicar.- Aun cuando mantengas la mayor privacidad posible en tus ajustes, capturas de pantalla de tu perfil, publicaciones o mensajes podrían terminar diseminadas por la Web si alguien en quien confías tiene malas intenciones y se lo propone. Por lo tanto, piensa siempre antes de publicar un texto, foto, opinión, mensaje personal o video. Una vez online, será difícil retirarlo por completo.

5. Sé escéptico.- Una regla general: "Si algo suena demasiado bueno para ser cierto, probablemente lo sea". Así que si alguien te ofrece un nuevo auto, computadora o Smartphone a cambio de información sensible como fecha o lugar de nacimiento, documento o teléfono, es probable que sea una trampa. Recuerda que los engaños en la Web pueden presentarse en múltiples formas y se valen de la vieja y conocida Ingeniería Social para pescar víctimas.

Mantén tus datos sensibles en privado y, antes de proporcionarlos en algún sitio o participar de sorteos y concursos, verifica su autenticidad.

6. Evita a los extraños.- ¿Acabas de recibir un mensaje instantáneo de alguien atractivo? ¿Lo conoces o has visto a esa persona? Si no, ten cuidado. El ciberespacio puede proporcionarles anonimato y "camuflaje" a los actores maliciosos, lo que les permite manipular a sus víctimas para que ejecuten acciones que normalmente no aceptarían. Para mantenerte protegido, limita la cantidad de personas que pueden contactarte y, si es posible, interactúa solo con quienes realmente conoces.

FUENTE: http://www.welivesecurity.com/la-es/2016/10/12/consejos-fanaticos-de-las-redes-sociales/

Análisis de las tecnologías utilizadas para combatir a la Cyberdelincuencia

Por Arturo de la Torre
Departamento de Ciencias de la Computación, Escuela Politécnica del Ejército, Sangolquí, Ecuador

1. INTRODUCCIÓN

Según datos del Ministerio del Interior Ruso, la Cyberdelincuencia ha generado en un solo año más de 100 mil millones de dólares, como resultado de actividades que van desde el cifrado de los datos de usuarios en computadoras y la exigencia de pagos a cambio de la solución del problema, el secuestro completo de redes corporativas en las cuales no es posible trabajar hasta que se pague a los malhechores, y por supuesto la piratería de software, películas y música.

Figura 1. Pirámide de los actores en materia de seguridad informática

Las variadas formas de acceder a los equipos de los usuarios por parte de los delincuentes ha cambiado drásticamente en los últimos años, los ya celebres gusanos de red como el código rojo, nimda, msblast y otros parecen ser cosas del pasado; en especial una vez que los principales sistemas operativos poseen sus propios cortafuegos (firewalls) y los usuarios de estos sistemas operativos los han activado y aprendido a utilizarlos. Los desarrolladores de sistemas operativos han tomado conciencia que ideas como la aplicabilidad de los usuarios Invitados (anónimos) y el uso compartido simple de archivos, aparentemente facilitan el trabajo de los usuarios, pero a corto plazo comprometen la seguridad del sistema. Las herramientas informáticas como antimalware y firewalls personales no pueden solos resolver la complejidad de amenazas y vulnerabilidades existentes, más bien los sistemas requieren de soluciones a nivel de una continua mejora y actualización del software, por lo que están en constante desarrollo eliminando las fallas básicas de seguridad.

En la actualidad los cyberdelincuentes usan técnicas muy innovadoras para infectar las máquinas de los usuarios, como por ejemplo distribuyen malware a través de imágenes adjuntas a los correos electrónicos, o intervienen las comunicaciones peer-to-peer de los usuarios, entiéndase enviar programas maliciosos a través del Messenger, sistemas de voz sobre IP, y por supuesto también al descargar la información requerida desde sitios web o ftp públicos que previamente fueron víctimas de ataques de estos modernos bandoleros.

El objetivo principal de este artículo, es dotar a los aficionados y expertos de las TI, de un conjunto básico de conceptos técnicos que les permitan evaluar los productos de software para seguridad informática. Considerando que un buen producto cumple con dos criterios, el del rendimiento que no debe afectar a la productividad y el de proactividad y retrospectiva que debe permitir detectar nuevos tipos de amenazas en base a su posible comportamiento; lo que se conoce con el nombre de heurística y proactividad y mas no en base al análisis de los datos que ya causaron y la determinación de patrones de comportamiento.

2. DESARROLLO

Consideramos que el sistema operativo está instalado en un equipo que responde a sus más elementales necesidades en cuanto a procesador, memoria, disco duro y otros. Es importante indicar que en muchos casos los problemas que se presentan en los computadores no son resultado de malware , sino más bien de la falta de un adecuado y oportuno mantenimiento de los equipos, también es consecuencia de un desbalance entre los programas instalados y el hardware en el cual se ha instalado.

2.1 Características para analizar la relación entre rendimiento del software y la productividad de los usuarios.

Analizar esta relación es fundamental para tener una valoración adecuada del software a instalarse, ya que el costo real de un producto no es solo su valor comercial, sino también el costo de hacer una correcta instalación más el costo de mantenimiento y el costo de operación, a lo cual se denomina gastos ocultos en la explotación de los sistemas. En el mercado existen muchos productos de precios muy bajos, sin embargo el costo de mantener funcionando correctamente a los mismos es muy alto, si valoramos las varias horas a la semana de trabajo calificado, en consideración que los usuarios tienen problemas con los equipos y no pueden trabajar, lo que además obliga a que los técnicos de soporte continuamente los entiendan y no alcancen a cumplir su trabajo. Como es fácil entender el producto tiene un precio bajo, pero el precio en gastos ocultos que la Corporación paga por este concepto es de varias veces este valor, por lo que su precio real supera al valor inicial de productos con un precio más alto pero que representan menores gastos ocultos a las personas o Instituciones.

2.1.1 Criterios sobre el rendimiento.

Cuando analice el beneficio del software de seguridad, entiéndase: antimalware , firewalls, Sistemas Detectores de Intrusos, protectores de web u otros sistemas similares, es esencial tener un conocimiento global de su comportamiento. Uno de los principales parámetros que debemos analizar es el impacto que el producto produce en la velocidad de los procesos que se ejecutan en los equipos, en los cuales se instalara o aquellos que estén en su ámbito de influencia, y que lógicamente producen pérdida de productividad, en virtud que los usuarios pierden la paciencia al tratar de ejecutar tareas que no responden en forma eficiente.

2.1.2 El grado de satisfacción de los usuarios que utilizan un determinado producto.

Un criterio importante antes de instalar cualquier software es realizar un seguimiento del producto entre las personas que lo utilizan, muchas veces el marketing no permite que excelentes productos entren a un mercado por considerarlo muy pequeño o por que tradicionalmente se han venido utilizando herramientas de algún proveedor especifico. Sin embargo, es positivo consultar entre los usuarios de otros productos su grado de satisfacción, y considerar que si un grupo de usuarios está satisfecho de un producto también usted lo puede estar.

2.1.3 ¿Recomendaría usted un producto específico de seguridad informática a sus amigos?

En determinadas ocasiones usamos productos que son estándares institucionales, o porque simplemente ya los compraron. Sin embargo, es bueno preguntar entre los usuarios de un producto si recomendarían utilizar este producto a sus amigos, es importante considerar que en este caso influyen factores como la facilidad en la

instalación y en el uso del producto, la integración con el entorno del usuario y finalmente la experiencia y el soporte que los proveedores garanticen al cliente. En fin, debe considerar que si alguien lo aprecia seguramente no le recomendara un mal producto.

2.2 Parámetros técnicos que deben analizarse del software.

Entre los principales parámetros técnicos de un software para seguridad informática, debemos mencionar la proactividad y la retrospectividad del producto en la detección de virus y malware (Caballos de Troya, Spyware, dialers, etc), también se debe considerar la velocidad durante el escaneo de los diferentes dispositivos de almacenamiento que un determinado producto presenta y el número de falsos positivos (errores cometidos en la detección de amenazas) que el software en estudios independientes realizados a alcanzado.

2.2.1 La proactividad del software.

Esta es la capacidad del producto para determinar comportamientos anómalos de códigos, programas o paquetes que se instalen o ejecuten en los computadores; y que pueden afectar al buen funcionamiento de los equipos o la red. Se puede decir que la proactividad del software consiste en controlar situaciones a través de acciones provocadas en ambientes virtuales dentro del sistema o por el cumplimiento de reglas preestablecidas, y por tanto previene el desarrollo de amenazas en lugar de tomar acciones cuando estas ya se han cumplido.

Como es lógico entender un software moderno de seguridad informática es mejor en cuanto más eficiente es su proactividad, ya que le permite evitar la mayor cantidad de amenazas existentes y predecir casi la totalidad de nuevas amenazas. En la actualidad son pocos los paquetes de seguridad que poseen un grado avanzado de proactividad, ya que su implementación requiere de algoritmos más complejos que la simple comparación de firmas o huellas dejadas por los antivirus.

Algunas de las principales amenazas que pueden detectarse eficientemente a través de las técnicas de proactividad son:

- Los típicos virus que afectan a la memoria, al sistema de partición o archivos del sistema operativo, entiéndase virus de Windows.
- Los macro virus.
- Los scripts que poseen código pernicioso, entiéndase scripts de malware.
- Los gusanos de red y aquellos que se reproducen dentro de los directorios del sistema operativo.
- Los malware que abren puertas traseras en el sistema operativo o substraen información importante de los usuarios.
- Los Caballos de Troya que ejecutan órdenes desde sitios remotos y comprometen la seguridad del usuario.
- Otras formas de malware.

2.2.2 Las funciones de retrospectividad.

En la actualidad muchas de las empresas dedicadas al desarrollo de software de seguridad, utilizan como su principal técnica de detección la retrospectividad, que consiste en el análisis forense de los rastros que dejan distintos tipos de malware en los equipos afectados para determinar patrones de comportamiento, lógicamente hacer eficiente esta técnica requiere de un número muy grande de recursos involucrados en el análisis y clasificación de los patrones de los virus y otras formas de malware, adicionalmente requieren de una continua actualización de las bases del sistema o de los patrones de comparación de las amenazas para poder funcionar eficientemente. Esta técnica desprotege al usuario contra nuevas amenazas que a la fecha no han sido clasificadas.

La retrospectividad es el factor fundamental por el cual los productos de seguridad informática hacen lentos a los equipos, ya que esta técnica de continua comparación de patrones requiere del uso constante del procesador y la memoria, con lo cual los recursos que requiere el sistema para sus tareas cotidianas se encuentran ostensiblemente

limitados. Se puede decir que aquellos productos de seguridad informática, que utilizan la retrospectividad como su principal herramienta de detección y prevención, son los más antiguos y cuyos fabricantes no han encontrado un camino efectivo hacia la innovación del software.

En síntesis, podemos indicar que la retrospectividad consiste en comparar patrones de amenazas conocidas, clasificarlas y finalmente compararlas con otras, para en base a un análisis promiscuo determinar semejanzas de comportamiento y por tanto clasificarlas como detecciones positivas.

2.2.3 La velocidad en el escaneo de diversos dispositivos.

Este parámetro es fundamental en el comportamiento de los sistemas de seguridad informática, en virtud que existen diferencias notables de comportamiento entre los diferentes productos. Cabe mencionar que al analizar la velocidad de escaneo de un producto es fundamental determinar qué tan confiable es su detección para las amenazas y los agentes de software maliciosos, además de la velocidad con la cual se ejecuta. Es fundamental identificar si el software de seguridad utiliza durante el escaneo emuladores de código y por tanto puede detectar códigos polimorficos que atenten contra el sistema, es decir, posee un eficiente sistema heurístico. También se debe considerar la capacidad para analizar archivos comprimidos y la capacidad del software para realizar este escaneo a través de diferentes capas de compresión.

Consecuentemente, podemos indicar que la velocidad de escaneo de un software se debe calcular como el resultado de dividir la cantidad de Mb que se pretende efectivamente analizar y limpiar de todos los agentes maliciosos, dividida por el tiempo necesario para concluir el escaneo expresado en segundos. Lógicamente para hacer este cálculo se requiere considerar que los equipos en los cuales se desarrollen las pruebas sean de iguales características de hardware y software; ya que una variación en el software existente en uno de los equipos puede producir resultados muy contradictorios.

2.2.4 Los falsos positivos.

Son estos un grupo de archivos a los cuales por sus características y comportamiento los productos de seguridad informática los pueden clasificar como código peligroso o amenazas al sistema, siendo esta evaluación errónea. Este inesperado resultado puede ser consecuencia de la aplicación de una heurística defectuosa o deficientemente implementada. Lógicamente un software que comete muchos errores en el reconocimiento de amenazas o códigos maliciosos puede funcionar en forma más rápida, ya que simplemente todo lo que desconoce lo clasifica como reconocimiento positivo de amenaza. Estos errores pueden ocasionar pérdidas irreparables de datos o la mala ejecución de programas, lo que afecta en forma drástica a la productividad de los usuarios. Por tanto es conveniente seleccionar aquel software que tenga el menor número de falsos positivos.

3. CONCLUSIONES

En los últimos años las tecnologías de seguridad informática se han desarrollado en forma muy dinámica, a consecuencia del desarrollo de las técnicas de proactividad que pretende evitar los daños que pueden ocasionar códigos maliciosos, en base al análisis preventivo de su comportamiento. Complementariamente, se ha planteado que el análisis retrospectivo, conocido como método de comparación de firmas, no es una forma efectiva de evitar los daños que causan el malware y más bien produce que los equipos se hagan muy lentos. Estos últimos programas son el resultado de tecnologías obsoletas y anticuadas que no están en capacidad de trabajar al ritmo que exigen las nuevas aplicaciones y equipos contemporáneos. Cuando se selecciona un nuevo sistema detector de intrusos, antimalware o sistema para la protección contra el despliegue de información basura, conocidos como protectores de web; considere que es importante conocer cuál de los productos utiliza la mejor heurística, es decir la tecnología más moderna; en otras palabras cual tiene los mejores resultados en términos de proactividad y el número de falsos positivos es menor. Además, antes de adquirir uno revise detalladamente los últimos resultados publicados en algunos de los sitios web independientes, donde se informa sobre las evaluaciones realizadas a diferentes productos.

4. BIBLIOGRAFIA

- www.wikipedia.org
- www.scprogress.com/noticias.html
- www.cert.org
- www.virusbtn.com
- www.av-comparatives.org

“Pienso que los virus informáticos muestran la naturaleza humana: la única forma de vida que hemos creado hasta el momento es puramente destructiva”

— Stephen Hawking —

Novedades

GANADORES DE LA ENCUESTA DE CONOCIMIENTOS SOBRE LOS PRODUCTOS Y SERVICIOS DE SCPROGRESS

Del 28 de septiembre al 9 de octubre, SCProgress realizó la encuesta de conocimientos sobre las soluciones de software y hardware de seguridad informática que ofrecemos, tuvimos una gran acogida por parte de nuestros clientes y seguidores, a quienes les damos las gracias profundamente por su preferencia, fidelidad y confianza en nuestra empresa, así como, en nuestros productos y servicios.

Los ganadores de las encuestas en esta ocasión son:

1. Para el primer lugar, el Señor Pablo Estrella, quién se lleva una Tablet Samsung Galaxy de última generación. Felicitaciones por sus amplios conocimientos.

2. La ganadora del segundo lugar, es la Srta. Amparo Navas, quién podrá disfrutar de un combo pizza, alitas BBQ y postres para cuatro personas.

Estamos complacidos por la atención y seguimiento a las promociones de SCProgress. Reiteramos nuestro agradecimiento y profundo compromiso, para continuar cumpliendo con las expectativas y requerimientos tecnológicos de nuestros clientes, manteniendo siempre la mejor tecnología y la mayor responsabilidad, así como, seguir contando con los precios más competitivos del mercado.

Responsables del evento:

Ing. Marco de la Torre
Ing. Consuelo de la Torre

Adicionalmente, nos complace indicar que en el mes de noviembre se realizará una nueva promoción, en la que el primer premio es una fantástica notebook. Los mantendremos informados a través de nuestra página web, Facebook y Twitter.

www.scprogress.com

Noviembre 2016