
Virus *Attack*

el mejor lugar para defenderte de los virus

Anuario



2002

(Edición de Muestra – Sólo incluye el mes de Diciembre)

<http://www.virusattack.com.ar>

Introducción

Desde el 19 de Junio de 1999, **Virus Attack!** ha crecido mucho, convirtiéndose en una de las principales fuentes de información sobre virus y seguridad informática en habla hispana. Nuestro sitio contiene noticias de actualidad, información detallada de los virus más importantes, artículos de opinión, así como secciones enteras dedicadas a los Hoaxes, Scams, además de un listado de parches al día para las aplicaciones más utilizadas de internet.

Nuestro objetivo ha sido siempre brindar la mejor información para que ésta pueda ser usada como herramienta de defensa contra las amenazas que un usuario puede encontrar al navegar por internet o utilizar un ordenador. Para complementar esta idea, **Virus Attack!** ofrece asistencia gratuita en línea a sus usuarios, y otros servicios adicionales como un Ránking de virus más reportados que sirve para conocer cuales son los que actualmente se reproducen y pueden ocasionar verdaderos problemas.



Contamos también con un boletín semanal de noticias que se distribuye entre 8,000 usuarios de habla hispana de todo el mundo con el que mantenemos actualizados a nuestros usuarios, y también ofrecemos servicios gratuitos para webmasters que les

permiten incluir nuestras noticias y alertas en sus sitios de forma sencilla y automática.

También se pueden encontrar en **Virus Attack!**, documentos técnicos sobre temas específicos relacionados a la seguridad informática, entrevistas a personalidades de referencia en el ambiente que nos convoca, un listado de preguntas más frecuentes que cubre las dudas más comunes de los usuarios de internet, y una base de datos de virus con más de 500 descripciones de los más importantes.

Pero nuestra actividad no sólo se limita al sitio de internet, sino que nuestro equipo también lleva adelante desde el 2001 una columna dedicada a la seguridad informática en **Radio FM Internet** (www.radiofminternet.com), y colabora con diversos sitios y emprendimientos, como **Kriptópolis**, el **Centro de Alerta Temprana** del Ministerio de Ciencia y Tecnología español y **DiarioRed.com**, entre otros.

En el 2002, nuestro esfuerzo y trabajo fueron premiados con una invitación a participar en el **SIMO TCI** de Madrid, la feria de informática más importante de España, donde ofrecimos una charla sobre Estrategias de Seguridad en Internet y tuvimos la oportunidad de hacer más conocido nuestro emprendimiento.

Hoy, a través de este Anuario 2002 de Noticias les presentamos lo más importante de lo sucedido el pasado año en el ámbito de los virus y la seguridad informática, con la seriedad y objetividad que buscamos transmitir en nuestro trabajo.

Éste anuario es una fuente de consulta accesible obligada para cualquier persona o profesional relacionado con la informática en forma directa. Esperamos que en él encuentre lo que estaba buscando y que satisfaga completamente sus necesidades de información sobre virus y seguridad informática.

Índice

El gusano W32/Yaha.K hace de las suyas (31/12/2002)	4
Disponible exploit para vulnerabilidades en SSHv2 (30/12/2002)	5
W32/Klez.h, el virus más reportado del año (28/12/2002)	6
El Spam se encuentra con más obstáculos (26/12/2002)	6
La Firma Digital ya es legal en Argentina (24/12/2002)	8
Creador de virus se declara culpable (22/12/2002)	9
Importante falla en Winamp (21/12/2002)	10
Problemas en Windows XP con archivos de audio (19/12/2002)	11
Lioten, un gusano en acción (17/12/2002)	12
Varios parches de seguridad para productos Microsoft (15/12/2002)	12
Primera herramienta anti-spyware para Macs (13/12/2002)	13
Datafull.com acusado de robo de contenidos (11/12/2002)	14
SegundaMano.com infectado por gusano (10/12/2002)	16
El autor de DeCSS va a juicio (07/12/2002)	17
Falla en Windows XP que atenta contra la privacidad (04/12/2002)	18
Código fuente de PGP es liberado (03/12/2002)	19
Skin de Kazaa puede borrar todos sus archivos (01/12/2002)	19

El gusano W32/Yaha.K hace de las suyas (31/12/2002)

Principalmente en Europa y Estados Unidos se están detectando numerosos casos de mensajes infectados por esta versión del Yaha, descubierta el pasado 21 de Diciembre.

A principios de este año fue descubierto un gusano, denominado Yaha, capaz de propagarse por correo electrónico, el cual fue reportado en diversas partes del mundo, y alcanzó cierta notoriedad, aunque no niveles epidémicos. Durante el resto del año que se acaba, se descubrieron varias versiones de este gusano, llegando a la última de ellas, denominada W32/Yaha.K (o M, por algunos antivirus).

Esta última versión, algo más avanzada que su antepasado original, mantiene su capacidad de reproducción masiva a través del correo electrónico, agregándole la posibilidad de que el contenido y los adjuntos al mensaje en el que viaja sean aleatorios, y la funcionalidad de evitar que varias aplicaciones antivirus y firewalls (cortafuegos) puedan ejecutarse correctamente.

Además de esto, el gusano modifica el sistema de manera que pueda iniciarse con cada arranque de Windows, y modifica la página de inicio del Internet Explorer, para que apunte a algunas de las 10 posibles direcciones de sitios de internet que contiene en su código.

El día de ayer, las principales casas antivirus comenzaron a recibir reportes del gusano, por lo que modificaron su gravedad de Baja a Media. Aunque parece ser que la mayor cantidad de mensajes infectados provienen del medioeste europeo, y afectan a países de habla inglesa, ya se han detectado numerosos casos en Estados Unidos y Europa en general.

El World Tracking Center, una herramienta estadística que se nutre de los datos recogidos por los productos antivirus de Trend Micro Inc., entre ellos su antivirus online HouseCall, ubica al Yaha.K en el 5to. lugar, con 1784 casos, al momento de la edición de este artículo. De estos, el 53 % (947 casos) corresponden a Europa.

Por su parte, Message Labs, un servicio británico de revisión antivirus de correo electrónico lo tiene segundo en su ranking de virus más detectados del día, con 7377 casos en las últimas 24 horas. Vale aclarar que el servicio de Message Labs revisa antivirus corporativos, y que los casos normalmente pueden verse incrementados si una empresa de gran parque informático se ve afectada por un virus.

En España, el Centro de Alerta Temprana, a través de sus estadísticas recogidas desde diversas universidades y entidades públicas, también ubica a este gusano en segunda posición en las últimas 24 horas, con 142 casos. El hecho de que los mensajes que utiliza el gusano para reproducirse por correo electrónico estén en inglés parece atentar contra su posibilidad de alcanzar gran cantidad de infecciones en ese país.

En Virus Attack! hemos recibido algunos reportes del gusano, pero no al punto de considerarlo, por el momento, una epidemia como el Klez.h o el reciente BugBear. De todas formas, aunque el gusano no realiza acciones dañinas más allá de terminar la ejecución de antivirus y firewalls, se recomienda a todos los usuarios que lean la descripción del W32/Yaha.K para conocer los mensajes en que puede ser recibido, actualicen su antivirus, y eviten abrir archivos adjuntos a mensajes no solicitados.

Más información

Trend Micro - World Tracking Center
<http://wtc.trendmicro.com/wtc/>

Message Labs - VirusEye
<http://www.messagelabs.com/viruseye/>

Alerta Antivirus - Estadísticas de España
http://www.alerta-antivirus.es/virus/estad_espa.html

Virus Attack! - Descripción del W32/Yaha.K

<http://virusattack.virusattack.com.ar/base/VerVirus.php3?idvirus=599>

Virus Attack! - Descripción del W32/Yaha

<http://virusattack.virusattack.com.ar/base/VerVirus.php3?idvirus=410>

Disponible exploit para vulnerabilidades en SSHv2 (30/12/2002)

En una importante lista de discusión sobre seguridad fue distribuida una forma de aprovechar agujeros de seguridad descubiertos recientemente en el protocolo Secure SHell v2.

SSH es un protocolo que permite canales de comunicación segura entre un cliente y un servidor, proveyendo encriptación, autenticación en el servidor y protección de integridad, a través del método de intercambio de claves criptográficas, entre otras cosas. Es uno de los protocolos más utilizados para intercambio seguro de información entre equipos y para login remoto seguro de usuarios en un servidor.

El 16 de Diciembre pasado, la empresa Rapid7, en conjunto con el CERT (Computer Emergency Response Team), anunciaron la existencia de fallas en diversas implementaciones del protocolo SSHv2, tanto en clientes como servidores, que podrían llevar a la ejecución de código arbitrario en los equipos vulnerables.

El alcance de las vulnerabilidades permitió catalogarlas como críticas ya que es posible explotarlas en forma remota, y causar una denegación de servicios o ejecución de código con los privilegios del entorno en el que el servicio SSH se encuentra corriendo en el servidor.

Rapid7 creó una herramienta, SSHredder, que permite la evaluación de un equipo ejecutando un servicio SSH, con diversos paquetes de prueba, los cuales permiten saber si el mismo es vulnerable o no. Esta aplicación fue la utilizada para encontrar estas fallas, las cuales se encuentran en el proceso de intercambio de claves.

Las implementaciones vulnerables son la v2, aunque no se descarta que la v1, y la implementación para Mac, MacSSH, también lo sea. OpenSSH, la implementación de código libre de SSH no parece ser vulnerable, aunque aplicaciones de empresas como Cysco, F-Secure, Hewlett-Packard y SSH Communications Security, si lo son.

Según la advertencia publicada por CERT, la implementación de SSH Communications Security es la más afectada debido a que puede ser aprovechada de forma bastante simple para ganar acceso al servidor vulnerable.

No todos los fabricantes han liberado parches aún, por lo que el hecho que un exploit para aprovechar estas fallas haya sido liberado en la lista BugTraq, empeora el tema. Se recomienda que aquellos con implementaciones de SSH aún no corregidas, restrinjan el acceso al servicio a equipos en los que confían y no permiten conexiones de equipos externos.

Más información

Rapid7 - R7-0009 Advisory

<http://www.rapid7.com/advisories/R7-0009.txt>

Rapid7 - Rapid7 Announces SSH Vulnerabilities, Releases Free SSHredder Test Suite

<http://www.rapid7.com/News/pr021216-ssh.html>

CERT - Advisory CA-2002-36

<http://www.cert.org/advisories/CA-2002-36.html>

eWeek.com - Exploit Code Posted for SSH Flaws

<http://www.eweek.com/article2/0,3959,801913,00.asp>

W32/Klez.h, el virus más reportado del año (28/12/2002)

Tras su aparición, a mediados del mes Abril, esta variante del gusano Klez se convirtió en el virus más infeccioso del 2002, estando aún hoy en todos los rankings.

Desde todo punto de vista, el W32/Klez.h fue el virus del 2002. Fue uno de los pocos en introducir algún concepto novedoso, y con poco más de 8 meses de vida, alcanzó los mayores índices de infección del año, por encima de otros virus del 2001, activos aún, que no pudieron alcanzarlo.

Pero no sólo él tuvo un año demoledor. Su "hijo", el virus W32/Elkern, también fue uno de los virus más prolíficos del año. Este virus era liberado por el Klez.h en todos los sistemas que éste infectaba, y era tan destructivo como su "padre".

Antes de pasar a meros datos estadísticos, analicemos su comportamiento. El W32/Klez.h, como todo miembro de la familia de gusanos Klez, es capaz de reproducirse por correo electrónico. Para ello, envía distintos mensajes, con archivos ejecutables adjuntos, e intenta aprovechar una vulnerabilidad del Internet Explorer para ejecutarse cuando el mensaje en el que viaja es abierto o previsualizado.

Una vez instalado en un sistema, el W32/Klez.h, liberaba un virus llamado W32/Elkern, capaz de infectar archivos ejecutables. Además, borraba algunos archivos esenciales para ciertos antivirus y herramientas de seguridad, pero lo más importantes, en ciertas fechas, ambos virus, tanto el Klez como el Elkern, intentaban eliminar toda la información del disco duro del equipo infectado.

Su aparición en Abril del 2002 fue avasalladora. En ese mes, el 77.8 % de los virus detectados por la empresa Sophos Inc., un desarrollador británico de antivirus, famoso por su Top Ten mensual de los 10 virus más reportados, correspondieron al W32/Klez.H (W32/Klez-G para ellos). O sea, tres de cuatro casos detectados por dicha empresa se trataban de este gusano.

Hoy en día, el W32/Klez.H se convirtió en el virus más detectado por la empresa MessageLabs., una compañía dedicada a la revisión de mensajes de correo electrónico. Su sistema VirusEye marca 4,778,710 mensajes infectados por este gusano, 3 millones y medio más de los contabilizados por el segundo en su ranking.

Por su parte, en las estadísticas del Centro de Alerta Temprana español, se puede observar que el 48.9 % de los virus reportados a dicha entidad también correspondieron al W32/Klez.h. Estos datos se alimentan de sistemas antivirus instalados en universidades y entidades públicas de España. Uno de cada dos mensajes infectados enviados a dichos organismos contenían el Klez.

En sus 8 meses y medio de vida, el W32/Klez.h se convirtió, por lejos, en el virus más reportado del 2002 y todavía hoy se mantiene como uno de los más reportados de la actualidad. Si en 2/3 partes del año logró tal nivel de infecciones, ¿qué le deparará el 2003? ¿seguirá haciendo de las suyas en el nuevo año?

Más información

Sophos Inc - Top ten viruses reported to Sophos in April 2002
<http://www.sophos.com/virusinfo/topten/200204.html>

Alerta-antivirus.es – Los virus más extendidos en España
http://www.alerta-antivirus.es/virus/estad_espa.html

MessageLabs – VirusEye – All-time virus
<http://www.messagelabs.com/viruseye/default.asp?by=all>

El Spam se encuentra con más obstáculos (26/12/2002)

En una lucha que no parece tener fin, spammers y antispammers ponen a prueba sus mejores armas para lograr sus objetivos: inundar la red con sus mensajes y evitar que eso suceda, respectivamente.

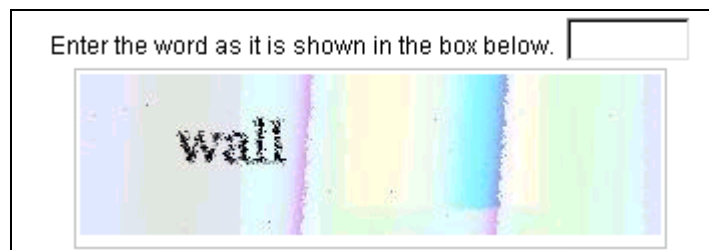
Spam es todo aquel mensaje no solicitado que llega a nuestra casilla de correo electrónico y que normalmente tiene fines publicitarios o de marketing. Detrás de él existen miles de personas que viven gracias al envío de esos mensajes publicitarios, o recolectando las direcciones de correo electrónico que pasaran a ser parte de las bases de datos que usan luego los spammers.

Existen varias herramientas antispam que buscan filtrar mensajes no solicitados en el propio servidor de correo electrónico o integrándose con nuestro cliente de correo, ya sea el Outlook, Netscape o algún otro. También existen las famosas Black Lists donde se listan direcciones de dominios catalogados como spammers para que nosotros podamos comprobar si un correo que nos ha llegado es o no spam.

Pero, los spammers no sólo envían spam, sino que crean cientos de cuentas de correo electrónico ficticias en proveedores gratuitos como Yahoo! o Hotmail para desde ellas enviar sus mensajes sin necesidad de utilizar sus propias cuentas y que éstas sean luego agregadas a las Black Lists.

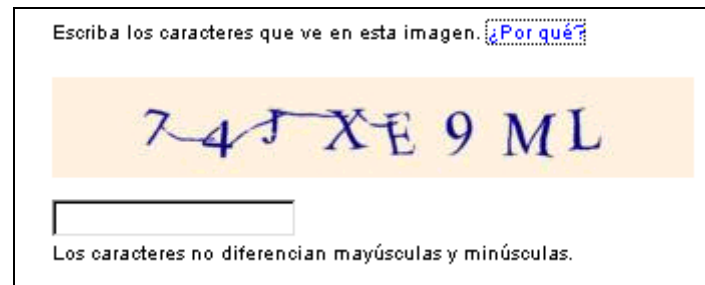
Para esa tarea, y para recolectar las direcciones de correo electrónico adonde enviaran el spam, los spammers utilizan programas capaces de dar de alta nuevas cuentas de correo electrónico en forma automática, llamados Web Bots (o Web Robots). Su tarea es sencilla: se conectan al servidor web de algún proveedor gratuito de correo electrónico, llenan el formulario de registración y obtienen una nueva cuenta desde dónde enviar spam.

A fin de evitar estas altas automáticas, Yahoo! implementó hace ya un año un sistema llamado Gimpy, desarrollado por la Universidad Carnegie Mellon, dentro del Captcha Project. Dicho sistema incluye dentro de la registración una imagen creada dinámicamente, la cual contiene una palabra tomada de un diccionario de 850 posibilidades, sobre la cual se agregan líneas de colores y manchas. Incluso un chico de 5 años puede leer la palabra allí escrita y completar el proceso de registración, pero a un Web Bot, por más inteligente que sea, no le será fácil.



(Ejemplo de Gimpy en Yahoo!)

Por su parte, Hotmail, el servicio de correo electrónico gratuito de Microsoft, implementó hace poco tiempo un sistema similar, el cual muestra una imagen con letras y números aleatorios, con el mismo fin: evitar que un programa inteligente pueda interpretarlos y así obstaculizar el proceso de creación de cuentas automático que utilizan los spammers.



(Ejemplo de Captcha en Hotmail)

Esta tecnología, está basada en el test de Turing, utilizado para distinguir a las personas de programas de computadoras inteligentes, y lleva el nombre de Captcha, que es la abreviatura de "completely automated public Turing tests to tell computers and humans apart" (Pruebas de Turing completamente automáticas y públicas para diferenciar humanos y computadoras).

De todas formas, aunque estos captchas significan un nuevo reto para los spammers, no son infalibles, y pueden ser escritos programas que hagan cientos de pruebas aleatorias por segundo para intentar quebrar por fuerza bruta estos obstáculos.

Por ejemplo, en la Universidad de California, en Berkeley, investigadores han podido crear programas inteligentes capaces de interpretar las imágenes dinámicamente generadas por Gimpy, y en muchos casos, pasar así su validación.

Lo cierto es que, en una batalla en la que los spammers siempre parecen llevar las de ganar, los captchas significan un avance en las técnicas antispam y, al menos, dificultan su tarea de llenar nuestras casillas con su correo basura.

Más información

CBSNews.com - Attack Of The Killer Web Robots
<http://www.cbsnews.com/stories/2002/12/26/tech/main534348.shtml>

La Firma Digital ya es legal en Argentina (24/12/2002)

Finalmente, la ley promulgada en Diciembre del 2001, ha sido reglamentada mediante un decreto presidencial que lleva la firma del propio presidente Eduardo Duhalde.

Como muchos saben, la firma digital es una forma de aplicar cierta autenticación a un documento o archivo de computadora, mediante algún algoritmo matemático que permita que sólo uno mismo pueda firmar de cierta manera sus documentos, y otras personas puedan verificar que esa firma es válida.

Los algoritmos más utilizados para la creación de pares de claves utilizados en la firma digital de documentos son el RSA y Diffie-Hellman, y existen protocolos seguros como S/MIME que utilizan el concepto de certificados para realizar una función similar.

Muchos países ya han comenzado a reconocer la firma digital como medio de autenticar documentos de computadora, y a permitir que la misma sea utilizada en el intercambio de información que hasta hace poco tiempo requería de la firma real de una persona encargada, como contratos, documentos legales, etc.

Argentina ya había sancionado en Noviembre de este año la Ley de Firma Digital (Ley 25506), la cual había sido promulgada por el congreso en Diciembre del año anterior, y fue reglamentada finalmente el pasado 20 de Diciembre mediante el decreto presidencial 2628/2002, y ya publicado en el Boletín Oficial.

Esta ley reglamenta la validez de los documentos y transacciones que se realicen a través de medios electrónicos y digitales, y es la primera de su tipo en Sudamérica. Además de considerarse un factor que ayudará notablemente al correo electrónico, el Gobierno estimó que "otorga un decisivo impulso para la despapelización del Estado, contribuyendo a mejorar su gestión, facilitar el acceso a la información y posibilitar la realización de trámites por Internet en forma segura".

Toda la administración y control de la Ley de Firma Digital será encargada a un Ente Administrador de próxima creación, el cual dependerá directamente de la Jefatura de Gabinete de Ministros, y tendrá la misión de regular los intercambios de información firmados electrónicamente y de validar la creación de certificados digitales.

La sanción de esta ley ayudará seguramente a la seguridad de las transacciones electrónicas permitiendo a los argentinos contar con una infraestructura que asegure una parte de su actividad online, privada y personal.

Más información

Portal de Abogados - Ley de Firma Digital

<http://www.portaldeabogados.com.ar/derechoinformatico/firmadigargentina.htm>

Yahoo! Noticias - La Firma Digital ya es ley: ahora será el tiempo de implementarla

<http://ar.news.yahoo.com/021221/3/3flv.html>

Creador de virus se declara culpable (22/12/2002)

Simon Vallor, un galés de 22 años, se pronunció responsable del desarrollo del gusano Gokar, que según los fiscales del caso infectó, al menos, 27,000 ordenadores en 42 países.

En Diciembre del año pasado, fue descubierto uno de los tantos gusanos que aparecieron en los últimos tiempos, el cual fue denominado W32/Gokar (o Worm/Gokar, entre otros nombres similares). El gusano, que se reproducía por correo electrónico e IRC, y si infectaba un servidor web, modificaba sus páginas para que los visitantes del mismo bajarán, sin darse cuenta, una copia de sí mismo.

Además de causar molestias, y de existir la posibilidad de que sobrecargara algún servidor de correo, el gusano no contenía rutinas dañinas que pudieran afectar el buen funcionamiento de los ordenadores que infectaba. Su única funcionalidad grave era la posibilidad de hacer que algunos antivirus dejaran de funcionar correctamente.

Dado que el gusano logró reproducirse mundialmente, trepando alto en los rankings de virus en sus primeros meses de vida, el FBI comenzó a buscar al autor del Gokar, y con la ayuda de ciertas pistas recopiladas en internet, en Febrero del 2002, Scotland Yard y la policía de Gales del Norte, detuvieron a Simon Vallor, un galés, de 21 años entonces, autor de otros dos gusanos: W32/Redesi y W32/Admirer.

Vallor, Disc Jockey (DJ) y diseñador de sitios de internet, desarrolló los gusanos, pero de acuerdo a sus dichos, no los distribuyó más que a otros autores de virus y a las compañías antivirus. Ahora enfrenta una posible condena de hasta 5 años de prisión, bajo el Computer Crime Act de 1990, un acta del gobierno del Reino Unido que legisla fraudes y crímenes informáticos.

El pasado 20 de Diciembre, Simon Vallor se declaró culpable de haber creado los 3 gusanos, y ahora espera que el juez determine la sentencia que debe cumplir, según nos comunicó en un contacto que mantuvimos con él esta tarde a través del correo electrónico.

Graham Cluley, Consultor Senior de la empresa antivirus británica Sophos, realizó algunas declaraciones acerca de Vallor y su perfil. "El sitio web de Vallor muestra que encaja muy bien en el perfil de un típico creador de virus – es joven, interesado en la tecnología y preocupado por la desnudez femenina", afirmó en un comunicado de prensa publicado por su empresa ante el conocimiento de las declaraciones del galés sobre su culpabilidad.

Simon Vallor, quien además de los cargos por la creación de los virus también había sido acusado de poseer pornografía infantil, acusación que luego fue retirada, respondió de forma bastante agresiva a los dichos de Cluley, invitándolo a que visite realmente su sitio, devilwithin.com, o trate de conocerlo personalmente, antes de hablar libremente en la prensa como si realmente lo conociera.

Desde Virus Attack! lo consultamos por alguna opinión adicional a la publicada en su sitio, pero nos contestó que prefiere guardar silencio hasta que la sentencia final sea anunciada. Su ánimo no era el mejor, y espera que el castigo no sea demasiado duro.

Si es sentenciado, se sumará a la lista de personas como Christopher Pile (conocido como Black Baron, el primer convicto por crímenes informáticos en Inglaterra), David L. Smith (creador del Melissa) y Jan de Wit (autor del gusano Kournikova).

Más información

Sophos - Welsh virus writer pleads guilty to infecting 27,000 PCs
<http://www.sophos.com/virusinfo/articles/vallor2.html>

Virus Attack! – Descripción del W32/Gokar
<http://virusattack.virusattack.com.ar/base/VerVirus.php?idvirus=363>

Virus Attack! – Descripción del W32/Redesi
<http://virusattack.virusattack.com.ar/base/VerVirus.php?idvirus=339>

Virus Attack! – Descripción del W32/Admirer
<http://virusattack.virusattack.com.ar/base/VerVirus.php?idvirus=407>

Importante falla en Winamp (21/12/2002)

Foundstone Research Labs. descubrió que las dos últimas versiones de este reproductor multimedia contienen agujeros de seguridad que podrían traer problemas a sus usuarios.

Winamp es uno de los reproductores de archivos de audio más utilizado, siendo la opción obvia para escuchar los famosos archivos MP3. Como muchos otros reproductores es capaz de interpretar las etiquetas ID3v2, utilizadas para agregar información acerca de los archivos multimedia, como el nombre del tema, autor, y demás.

Tony Bettini, del laboratorio de investigación de la empresa Foundstone, descubrió sendas fallas en la interpretación de dichas etiquetas, en las dos últimas versiones del reproductor: la clásica (2.81) y la recientemente liberada 3.0. Ambas versiones tienen buffers no chequeados correctamente en el procesamiento de ciertas etiquetas ID3v2, que pueden llevar a un desbordamiento y posterior ejecución de código arbitrario.

Específicamente en la versión 2.81, la falla se produce si el Winamp intenta abrir un archivo MP3 con una etiqueta ID3v2 de Artista demasiado larga, lo cual produciría que el programa falle, y permita la ejecución de código arbitrario con los privilegios del usuario del sistema.

En cambio, en la versión 3.0, el agujero de seguridad no se encuentra directamente en el Winamp, sino en su Biblioteca de Media (Media Library), la cual posee dos buffers no chequeados, en las funciones que procesan las etiquetas de Artista y Album de cualquier archivo que esté en la biblioteca. De la misma manera que la vulnerabilidad en la otra versión, cargar un archivo MP3 en la biblioteca puede producir la falla de la aplicación y la posterior ejecución de código arbitrario.

Es posible entonces que una persona cree un archivo MP3 con las etiquetas ID3v2 suficientemente largas para que cuando el usuario lo ejecute, o agregue en la Biblioteca de Media, la aplicación no funcione correctamente, y la seguridad del equipo sea comprometida.

Nullsoft, la empresa que creó el Winamp, ya ha puesto a disposición de los usuarios versiones corregidas de su aplicación, tanto para la 2.81 como la 3.0, y las mismas pueden ser descargadas desde su sitio oficial www.winamp.com.

Al Winamp Team, encargado del desarrollo del reproductor, no parece haberle caído muy bien el descubrimiento de estas fallas, debido a que una nota de prensa donde se advierte de ellas, comentan "Alguna gente parece tener demasiado tiempo en sus manos", en alusión a quienes descubrieron los agujeros de seguridad antes mencionados.

De todas formas, recomiendan que todos aquellos que hayan bajado el Winamp antes del 17 de Diciembre, vuelvan a descargarlo para tener las últimas versiones de la aplicación, las cuales no son susceptibles a estas fallas, y permitirán que los usuarios puedan seguir reproduciendo e intercambiando archivos MP3 en forma segura.

Más información

Foundstone.com - Research Labs Advisory - FS2002-10

<http://www.foundstone.com/knowledge/randd-advisories-display.html?id=338>

Winamp.com - Descarga de la versión 3.0

<http://www.winamp.com/download/>

Winamp.com - Descarga de la versión 2.81

<http://classic.winamp.com/download/>

Virus Attack! - Parches para Winamp

<http://virusattack.virusattack.com.ar/parches/VerParche.php3?aplicacion=28>

Problemas en Windows XP con archivos de audio (19/12/2002)

Se anunció una grave falla en el sistema operativo de Microsoft, asociada a los archivos MP3 y WMA, entre otros, que puede llevar a la ejecución de código arbitrario en un equipo vulnerable.

La empresa Foundstone, dedicada a la seguridad informática, descubrió tiempo atrás una vulnerabilidad en Windows XP, a través de la cual es posible ejecutar código arbitrario aprovechando la funcionalidad que brinda este sistema operativo de leer los atributos de ciertos archivos de audio, como los conocidos MP3 o WMA (Windows Media Audio).

La falla se encuentra específicamente en un buffer no chequeado en un método nativo del Windows Shell de XP, la interface de usuario del sistema, el cual puede ser sobrescrito para lograr un desbordamiento y posterior compromiso del sistema y ejecución de código arbitrario.

Según la advertencia publicada en el sitio de Foundstone por Tony Bettini, integrante del laboratorio de investigación de la empresa, esta falla puede ser aprovechada en forma local, o a través de un sitio de internet o mensaje de correo electrónico en formato HTML.

Si un usuario visualiza un directorio con el Explorador de Windows, y en éste se almacena un archivo especialmente manipulado para aprovechar la falla o si visita un sitio de internet que contenga en sus páginas el código necesario para hacerlo, la seguridad de su sistema podrá ser comprometida, y quien haya creado el archivo podrá haberle incluido funciones para realizar todo tipo de acción en el equipo vulnerable.

Todas las versiones de Windows XP, incluida la de 64-bits, son vulnerables a este agujero de seguridad, y por ello, Microsoft ya ha liberado un boletín de seguridad que incluye un parche que corrige la falla, además de brindar información detallada al respecto.

Es importante aclarar que los reproductores de archivos MP3 y WMA, como el Winamp o el Windows Media Player, no son vulnerables, sino que el problema es parte del propio Windows.

El boletín de seguridad MS02-072 califica la falla como crítica y urge a los usuarios a que apliquen la solución lo antes posible para evitar problemas relacionados con esta vulnerabilidad, ya que una persona maliciosa podría llegar a escribir un virus o gusano, entre otras cosas, que aproveche el problema de seguridad y causar graves problemas a los usuarios que no hayan instalado el parche.

Más información

Virus Attack! - Parches para Windows XP

<http://virusattack.virusattack.com.ar/parches/VerParche.php3?aplicacion=20>

Foundstone.com - Research Labs Advisory FS2002-11

<http://www.foundstone.com/knowledge/randd-advisories-display.html?id=339>

Lioten, un gusano en acción (17/12/2002)

Ante el incremento de escaneos al puerto UDP 445, asociado al protocolo SMB de Microsoft, se descubrió un nuevo gusano que intenta reproducirse a través de internet.

Como ya hemos comentado con anterioridad, SMB (Server Message Block) es un protocolo utilizado por Windows para compartir archivos, sobre el cual ya se han descubierto varias vulnerabilidades, y utiliza el puerto 445 para entablar sus comunicaciones.

myNetWatchman.com, un sitio dedicado al monitoreo contiguo del tráfico de internet, detectó hace pocos días, más precisamente el 14 de Diciembre, un incremento en los escaneos al puerto utilizado por el SMB, y después de realizar un análisis de esta actividad fuera de lo normal, comprobó que se trataba de un nuevo gusano.

Denominado W32/Lioten, o IraqOil, este nuevo gusano aprovecha la existencia de equipos NT/2000/XP con la posibilidad de iniciar sesiones nulas en ellos (con usuario y contraseñas nulas) para recuperar el listado de usuarios del sistema e intentar un pequeño ataque de fuerza bruta para loguearse y copiarse en ellos.

Para reproducirse, realiza escaneos de equipos vulnerables, y si detecta un servidor con el recurso IPC\$ compartido, intenta obtener un listado de los usuarios del mismo, y prueba contra ellos varias contraseñas simples, que parecen estar dándole resultado, dado que desde su descubrimiento, myNetWatchman ha detectado casi 12,000 hosts infectados.

También el Internet Storm Center, una iniciativa similar a myNetWatchman, pero solventada por The SANS Institute, un organismo estadounidense con apoyo gubernamental, ha registrado el aumento en los escaneos al puerto 445, producto de la actividad del nuevo gusano. Los registros en su base de datos pasaron de 193 fuentes el 14 de este mes, a 10457 en el día de hoy.

Las compañías antivirus ya se han hecho eco de la aparición del Lioten, y han incorporado mecanismos de detección y eliminación del gusano a sus productos. En Virus Attack! hemos realizado una descripción completa del mismo que puede ser consultada para más información sobre sus funcionalidades.

El incremento de equipos afectados por el gusano hace que las posibilidades de que el gusano se reproduzca también se incrementen, dado que así tendrá un mayor poder de escaneo que si los hosts afectados fueran pocos.

De todas formas, no hay que alarmarse dado que el gusano no realiza ninguna acción dañina, y es muy simple evitar que infecte su servidor. Deshabilitando las sesiones nulas, y utilizando contraseñas fuertes, el gusano no tendrá posibilidades de reproducirse. Si su servidor se encuentra detrás de un firewall que bloquee el uso de SMB, tampoco podrá verse afectado por el Lioten.

Más información

myNetWatchman - Alert: IraqWorm

<http://www.mynetwatchman.com/kb/security/articles/iraqworm/index.htm>

Internet Storm Center - Estadísticas del puerto 445

http://isc.incidents.org/port_details.html?port=445

BrownEdu - Disabling Null Sessions

<http://www.brown.edu/Facilities/CIS/CIRT/help/netbiosnull.html>

Virus Attack! - Descripción del W32/Lioten

<http://virusattack.virusattack.com.ar/base/VerVirus.php3?idvirus=591>

Varios parches de seguridad para productos Microsoft (15/12/2002)

Se han liberado una serie de actualizaciones que incluyen correcciones para la Máquina Virtual Java y el protocolo SMB de Windows 2000/XP, entre otros.

En las últimas dos semanas Microsoft publicó 5 nuevos boletines de seguridad con actualizaciones para el Internet Explorer, el Microsoft Outlook e importantes componentes de las versiones más utilizadas de su sistema operativo Windows, habiéndose encontrado fallas en su JVM (Java Virtual Machine), en su protocolo nativo Server Message Block (SMB) y en sus rutinas de comunicación entre procesos mediante mensajes.

La primera de las actualizaciones mencionadas, publicada el pasado 4 de Diciembre, contiene una corrección para una falla existente en la versión 2002 de Microsoft Outlook, el cliente de correo electrónico y organizador personal del paquete de aplicaciones Office.

Específicamente, la falla se encuentra en el procesador de encabezados del Outlook 2002, el cual puede ser sobrecargado si se crea un mensaje con cierta malformación, lo que llevaría a un ataque de denegación de servicios.

En cuanto al Internet Explorer, Microsoft liberó un parche acumulativo en la misma fecha, el cual contiene correcciones para fallas consideradas como críticas después de un importante debate entre los encargados de seguridad de la empresa de Bill Gates y varios expertos en seguridad informática como Thor Larholm.

El principal de los agujeros de seguridad que la actualización acumulativa corrige permitiría, mediante la explotación de un problema con el manejo de los objetos cacheados, la ejecución de comandos en un equipo vulnerable si el usuario accede a un sitio o mensaje de correo electrónico en formato HTML.

Una semana después, el 11 de Diciembre, Microsoft publicó un boletín que comentaba, y contenía soluciones, para 8 problemas de seguridad en la Máquina Virtual Java de Microsoft. La más grave de estas fallas podría permitir a un usuario tomar control de un equipo vulnerable en forma remota.

Todas las versiones de la VM (Virtual Machine) menores o iguales a la 5.0.3805 son vulnerables a estas 8 fallas, que afectan varias partes de este componente, como la JDBC API, el manejo de objetos COM, la validación de dominios, y otras funcionalidades más.

También se publicaron dos boletines más, los cuales solucionan fallas en las versiones corporativas de Windows, como NT, Windows 2000 y XP. El primero de estos agujeros de seguridad, que sólo afecta a las versiones 2000 y XP, permite, mediante la explotación de un problema en el manejo de las firmas de los paquetes del protocolo SMB (nativo de Microsoft), la modificación de las políticas de grupo de un equipo (o varios) conectados a un servidor de dominio vulnerable.

Y, para concluir, la última vulnerabilidad reportada, que afecta a Windows NT, 2000 y XP, se encuentra en el manejo del mensaje WM_TIMER, un aviso que le permite a un proceso conocer si un control del tipo timer ha expirado o no. La falla, corregida en el último boletín de Microsoft, permite que un usuario pueda elevar sus privilegios dentro de un equipo afectado por el problema.

Todos estos parches, incluidos en los boletines del MS02-067 al MS02-071, se encuentran ya disponibles en Windows Update, y se recomienda a los usuarios que los instalen a la brevedad posible.

Más información

Microsoft.com - Windows Update
<http://www.windowsupdate.com>

Virus Attack! - Parches
<http://virusattack.virusattack.com.ar/parches/>

Primera herramienta anti-spyware para Macs (13/12/2002)

SecureMac.com, un sitio dedicado a la seguridad informática para ordenadores Macintosh, ha creado una herramienta que permite detectar y eliminar spyware.

Los ordenadores Macintosh, o Macs, de Apple Inc., han sido durante varios años los únicos competidores, en lo que a estaciones de trabajo se refiere, de las IBM PCs que hoy lideran el mercado de las computadoras personales.

Obviamente, de la misma manera que existen aplicaciones, han comenzado a aparecer cada vez más troyanos, keyloggers y spyware para la plataforma Macintosh, junto a la creciente aparición de software gratuito con versiones para Macintosh, como reproductores multimedia o programas de intercambio de archivos.

Por ello, SecureMac.com, uno de los más importantes sitios sobre seguridad informática para esta plataforma, ha creado un programa shareware llamado MacScan que permite revisar una Mac por la existencia de malware como los antes mencionados, y aislarlos o removerlos.

Además, ha creado una base de datos con información de los más conocidos troyanos, backdoors, keyloggers y spyware para esta plataforma, que puede ser consultada por los usuarios del programa cuando el mismo detecta algún malware.

MacScan también escanea el ordenador por la presencia de cualquier tipo de herramienta de administración remota, sea comercial, shareware o freeware, y avisa al usuario de su existencia, para que si la han instalado sin su conocimiento, pueda proceder a eliminarla del sistema.



Tiene una interface de uso bastante simple y sencilla, basada en el formato de web, que hace fácil el uso de la herramienta hasta para el usuario más inexperto. El programa está disponible para las versiones Mac OS Classic o Mac OS X del sistema operativo para Macintosh.

Más información

SecureMac – MacScan Macintosh Security Scanner

<http://macscan.securemac.com/>

SecureMac – MacScan Press Release

<http://macscan.securemac.com/press-release-12-13-2002.html>

Datafull.com acusado de robo de contenidos (11/12/2002)

Poco tiempo atrás, un importante sitio de shareware, WebAttack.com, acusó al conocido portal argentino de robarles sus descripciones y análisis de programas.

WebAttack.com es un conocido sitio estadounidense con revisiones de programas freeware y shareware de todo tipo, y cuya base de datos tiene más de 5000 aplicaciones, separadas en 280 categorías, revisadas y listas para bajar por cualquier usuario de internet, con más de 5 años en línea. Es un sitio independiente, que gracias al esforzado trabajo de sus fundadores y colaboradores ha llegado a ser un referente.

Por su parte, datafull.com es un portal con contenidos orientados a informática, internet y entretenimientos, idea de Hernán Arrojo, ex dueño del proveedor de servicios de internet SION. El sitio también es del conocido conductor y productor televisivo Mario Pergolini, quien muchas veces brinda su imagen para promocionarlo. Tiene un staff permanente de más de 15 personas y miles de usuarios lo visitan diariamente, siendo uno de los portales argentinos más conocidos.

Una de las secciones principales del sitio argentino se llama "Descargando" y contiene revisiones y direcciones de descarga de interesantes y novedosos programas gratuitos o shareware que muchas veces Hernán Arrojo comenta en el programa de radio Cual Es, que Pergolini conduce por la radio Rock & Pop.

Poco tiempo atrás el WebAttack.com lanzó dadafull.com, un sitio donde denuncia que el sitio argentino copia diariamente las revisiones de software que hacen, palabra por palabra e incluyendo imágenes, y las publican en la sección "Descargando" como si fueran de generación propia de datafull.com, sin autorización ni acuerdo previo con los autores originales de las mismas.

Según la gente del sitio estadounidense, en un comunicado algo irónico y bastante revelador, ellos se han comunicado una y otra vez con los responsables de datafull.com para que cesen de copiar contenidos de WebAttack.com y publicarlos como propios, pero nunca han recibido respuesta.

Pese a las advertencias, datafull.com sigue publicando día a día (según las fuentes de WebAttack, todos los días a las 5.00 PM) las revisiones del sitio estadounidense, cosa que en Virus Attack! pudimos comprobar hoy mismo al comparar la revisión del programa de portada de "Descargando", llamado Audio Record Wizard 3.00, donde se puede ver que el comentario del sitio argentino está, literalmente, traducido del original publicado en WebAttack.com.

En internet, se cuentan por cientos los casos en los que un sitio acusa a otro de "robarle" contenidos, pero nunca un caso había involucrado a un portal de tanto renombre como datafull.com. Es normal que aquellos dedicados a la generación de contenidos se basen en informaciones recopiladas por otros sitios pero la copia de información, palabra por palabra, es una grave violación a los derechos del autor original.

Y, como para confirmar un poco más que no se trata de una simple casualidad, la gente de WebAttack publicó en su sitio las versiones originales y las copias, y allí se puede comprobar como algunas de ellas (Photolightning 1.0 o Free Easy PDF 2.0) tienen incluso las mismas imágenes de muestra en ambos sitios, mostrando además que no son casos aislados.

Pero, eso no es todo.... entre una de las imágenes que la gente de WebAttack.com presenta como prueba, la que se incluye junto a la revisión del programa NotePadXP, se puede leer en ella la leyenda "tested by WebAttack.com", puesta allí por los propios autores para corroborar el hecho y que fue copiada y publicada en el sitio argentino Datafull.com, junto a la revisión traducida ¡Increíble!

¿Hace falta decir más? Tan sólo que Pergolini, uno de los dueños de Datafull.com, suele quejarse públicamente cuando alguna de sus ideas es copiada por otra productora televisiva. ¿Ladrón que roba a otro ladrón tiene cien años de perdón?

Más información

dadafull.com - Comunicado original de WebAttack.com sobre los reiterados incidentes
<http://www.dadafull.com>

WebAttack.com

<http://www.webattack.com>

Datafull.com - Sección Descargando

<http://www.datafull.com/descargando/index.php>

WebAttack.com - Audio Record Wizard 1.0

<http://www.webattack.com/newapp.php?id=104786>

Datafull.com - Audio Record Wizard 1.0

<http://www.datafull.com/descargando/index.php?id=4380&sys=1&view=prog>

SegundaMano.com infectado por gusano (10/12/2002)

El equipo de Virus Attack! pudo comprobar que durante la tarde-noche del Domingo 8 de Diciembre, el sitio argentino SegundaMano.com se encontraba infectado por el gusano CodeRed.

El sitio Segunda Mano, de Trader Classified Media, se dedica a la recepción y publicación de avisos clasificados de todo tipo, abarcando un amplio espectro de rubros que cubren desde instrumentos musicales hasta viviendas y automóviles, entre otras cosas.

Gracias al aviso de un colaborador de Virus Attack!, pudimos comprobar que, al menos, entre las 16 y 22 horas del Domingo 8 de Diciembre, el sitio www.segundamano.com estuvo infectado por el gusano CodeRed, debido a que algunas de sus páginas mostraban su aviso característico, invitando al visitante a www.worm.com.

El CodeRed es un gusano que, descubierto en Julio del 2001, infectó cerca de 30,000 servidores en sus primeros días de vida, atacando una vulnerabilidad en el Index Server de Microsoft, un servicio incluido al Internet Information Server, el servidor web de la empresa, y que puede ser utilizado sobre Windows NT, 2000 y XP.

Desde entonces, el gusano sigue rondando por internet pese a que desde el 18 de Junio del 2001 existe un parche para solucionar el agujero de seguridad que aprovecha para infectar servidores.

El gusano no causa daños en los equipos que infecta, salvo que puede llegar a consumir el 100 % del procesador, e intentar un ataque de denegación de servicios (DoS) contra el sitio de la Casa Blanca de los Estados Unidos de América.

Utilizando la herramienta Retina Code Red, de eEye Digital Security, el equipo de Virus Attack! pudo comprobar que el sitio, pese a que sus páginas habían sido restablecidas, aún era vulnerable al problema en el Index Server y puede ser reinfectado por el gusano si los administradores del servidor no toman las medidas necesarias y aplican los parches que corrigen el agujero de seguridad.

Inmediatamente se pusieron en contacto con los responsables técnicos de SegundaMano.com, y de la empresa Net Express, cuyos DNS (servidores de nombre de dominio) son utilizados para manejar el dominio infectado, a fin de informarles del incidente y de la necesidad de actualizar su servidor para evitar futuros problemas, pero no recibieron respuesta alguna.

Dos días después, el servidor sigue vulnerable al agujero de seguridad que aprovecha el gusano Code Red, y el alerta enviado por Virus Attack! a las distintas direcciones de contacto de SegundaMano.com no fue tenido en cuenta.

Es importante notar que si el servidor está infectado por dicho gusano no es directamente peligroso para los usuarios que accedan a él, pero lo que sí puede ser causante de males para los visitantes de SegundaMano.com es que aún sigue siendo vulnerable al problema en el Index Server de Microsoft.

Es por ello que recomendamos a los usuarios del sitio tener cuidado si lo utilizan frecuentemente, recordando actualizar antes su navegador y su antivirus para evitar problemas que puedan ser ocasionados en caso que el mismo sea nuevamente infectado por algún gusano y/o sus contenidos manipulados por un usuario malicioso.

Más información

SegundaMano.com - Quienes Somos

<http://www.segundamano.com/ar/about-us.asp>

Virus Attack! - Imagen de la página de SegundaMano.com infectada

<http://virusattack.virusattack.com.ar/noticias/especiales/segundamano.php>

EEye Digital Security - CodeRed Scanner

<http://www.eeye.com/html/Research/Tools/codered.html>

Microsoft.com - Windows Update (para actualizar su PC)

<http://www.windowsupdate.com>

Microsoft.com - Boletín de Seguridad MS01-033

<http://www.microsoft.com/technet/security/bulletin/MS01-033.asp>

Virus Attack! - Código rojo para los servidores Microsoft

<http://virusattack.virusattack.com.ar/noticias/VerNoticia.php?idnotas=76>

El autor de DeCSS va a juicio (07/12/2002)

El creador del software para hackear los DVD-Rom y convertirlos en archivos gráficos de computadora irá a juicio en Noruega.

DeCSS es una herramienta para Windows que permite obtener contenido desde un DVD-Rom, en formato CSS (Content Scrambling System), y convertirlo en un formato gráfico legible para cualquier computadora, como el MPEG-2.

Jon Lech Johansen, un noruego de 18 años, y otros dos programadores anónimos, un ruso y un holandés, escribieron el programa hace poco más de 2 años. DeCSS, según las autoridades y las compañías productoras de películas, viola los derechos de autor de los DVD, y por ello se han levantado cargos contra los autores.

Aunque ya ha habido varios juicios en los Estados Unidos sin conclusión, el caso en Noruega es muy importante para evaluar la importancia que le darán a las leyes de piratería y hacking de computadoras de ese país, y ha recibido por ello gran atención de la prensa.

Los defensores de Johansen argumentan que el muchacho, de entonces 15 años, no infringió ninguna ley al escribir el programa; del otro lado, las empresas defienden sus derechos sobre las películas, y llevan las de ganar para la opinión pública.

La queja que inició el juicio fue enviada por la Motion Picture Association of America, y se basa en que el programa DeCSS permite que la propiedad de los productores de películas pueda manejarse a su antojo por terceros, copiarse, distribuirse e incluso venderse sin su consentimiento.

Johansen, quien puede llegar a ser sentenciado a 2 años de prisión, dijo en su defensa, que escribió el programa para poder ver las películas en su equipo con sistema operativo Linux, el cual carecía del software necesario para visualizar DVD-Roms.

Dado que el programa comenzó a ser distribuido, y muchas personas alrededor del mundo comenzaron a utilizarlo para crackear películas DVD, se iniciaron varias acciones legales contra los autores del DeCSS, sin ninguna sentencia firme hasta ahora. Ahora, Johansen, el héroe de muchos, enfrenta un nuevo juicio, y posiblemente, éste lo lleve a la cárcel.

Más información

OpenLaw DVD/DeCSS Forum - FAQ List

<http://eon.law.harvard.edu/openlaw/DVD/dvd-discuss-faq.html>

Vninet - DVD Hacker hero goes on trial

<http://www.vninet.com/News/1137440>

Falla en Windows XP que atenta contra la privacidad (04/12/2002)

¿Hasta que punto puede considerarse un riesgo a la seguridad esta falla de Windows XP?.

Recientemente ha sido publicado un exploit que afecta a Windows XP, incluso en la versión SP1.

Este exploit permite que aquellos usuarios que han sido degradados de usuarios administrativos a usuarios normales, puedan aún acceder al administrador de tareas.

Windows XP utiliza una nueva opción llamada "Fast User Switching" (FUS) (Cambio rápido de usuario), que permite a múltiples usuarios acceder en forma local a la misma computadora (aunque un solo usuario a la vez pueda trabajar con la interface gráfica). Esta opción es una variante de los servicios de Terminal Service, que permiten que varios usuarios se conecten de forma interactiva a un equipo y que se muestren los escritorios y aplicaciones de equipos remotos.

Si un usuario es degradado de un rol de administrador al de usuario normal (el administrador lo cambia del grupo de administradores al de usuario común), y en el momento de esa acción, la casilla "Mostrar procesos de todos los usuarios" está marcada en la sección "Procesos" del Administrador de tareas, al logearse luego éste usuario, el mismo podrá acceder a la lista de procesos usados por el usuario que estuvo antes que él, aún cuando ya no sea miembro del grupo de administradores.

Aunque no se han probado que clase de acciones maliciosas podrían ser posibles (como las de eliminar a otro usuario), si podría considerarse un riesgo para la privacidad, al revelarse información como cuáles aplicaciones se estaban ejecutando, tiempo de utilización de la computadora, etc., lo que bien podría considerarse como una forma de vigilancia.

Aunque no se ha probado, podría también ser posible utilizar alguna herramienta como "kill.exe" de Windows 2000 (para "matar" un proceso determinado). Por ejemplo, sabiendo que procesos o programas utiliza la otra persona, se le podría enviar un mensaje falso con un enlace al "kill.exe" y las instrucciones para eliminar los procesos deseados.

La solución para cambiar esta situación está en borrar al usuario afectado, y luego crearlo en el grupo correspondiente, en lugar de cambiarlo de grupo.

Sin embargo, la principal discusión es, hasta que punto esta situación es un verdadero riesgo.

Según Microsoft, la característica FUS (cambio rápido de usuario), está orientada al consumidor doméstico, y está habilitada por defecto en la versión Windows XP hogareña. En la PRO solo puede ser habilitada en forma premeditada, y en un solo grupo de trabajo.

La idea del cambio rápido de usuario es permitir a varias personas mantener sus propias configuraciones personalizadas e independientes al acceder a la misma computadora.

Cada integrante de la familia puede mantener cuentas separadas de correo electrónico, perfiles del MSN Messenger, etc. Dentro de la familia, el grado de confianza entre usuarios suele ser mayor que en otros ambientes.

Difícilmente esta falla pueda ser considerada crítica en algún momento. Aunque el tema de la falta de privacidad todavía puede ser discutido, por supuesto.

(Noticia extraída de VSAntivirus.com con el debido consentimiento y aprobación de su autor)

Código fuente de PGP es liberado (03/12/2002)

Cuando PGP Corp. fue separada de Network Associates Inc. había prometido hacer público el código fuente de su aplicación estrella, y finalmente, lo ha hecho.

PGP (Pretty Good Privacy) es una aplicación que permite el intercambio seguro de correo electrónico a través de claves de encriptación y firma digital. Fue creada por Phil Zimmerman y adquirido luego por la empresa Network Associates Inc. quien a partir de la versión 7.0 dejó de liberar su código fuente.

Ahora, con la creación de la nueva empresa PGP Corporation, y el lanzamiento de la versión 8.0 del producto, la nueva empresa, ya sin relación con NAI, ha puesto a disposición del público el código fuente de su aplicación, para que cualquier pueda chequear su contenido, y asegurarse que hace sólo lo que debe hacer.

Desde que PGP había sido adquirido por Network Associates Inc., y especialmente desde que su código dejó de ser libre, rumores sobre la posible inclusión de troyanos en la aplicación se habían hecho moneda corriente, en gran medida debido a los contratos existentes entre la compañía y el gobierno estadounidense, siempre sospechado en temas de privacidad en internet.

Pese a la venta de la compañía, aquellos rumores se mantenían, pero con el lanzamiento de la versión 8.0, y la disponibilidad del código fuente de la aplicación, ya es posible corroborar el correcto funcionamiento de PGP.

La nueva versión 8.0 ya está disponible en sus versiones Freeware, Personal y Enterprise, y en sus versiones Desktop para Windows (en todas sus versiones) y Mac OS X. Contiene gran cantidad de nuevas funcionalidades, como su integración con el Active Directory de Microsoft, y otros importantes servicios de directorios.

Respecto de la liberación del código fuente, Phil Dunkelberger, CEO de PGP Corporation, dijo "PGP es la única empresa de software de seguridad suficientemente comprometida con la integridad y seguridad de su producto para publicar su propiedad intelectual en la forma de código fuente para revisión".

Vale destacar que el código fuente de PGP 8.0 está disponible sólo para consulta, y no puede ser modificado o utilizado para basar otras aplicaciones en él como sucedía hasta la versión 6.5.8. De todas maneras, es un paso adelante en la reimplantación de una de las aplicaciones de seguridad y privacidad más utilizadas.

Más información

PGP Corp. - PGP Corporation Announces the Release of PGP 8.0 Source Code
<http://www.pgp.com/display.php?pageID=51#anch107>

PGP Corp. - PGP Corporation Announces the Release of PGP 8.0 for Windows and Macintosh
<http://www.pgp.com/display.php?pageID=51#anch105>

Skin de Kazaa puede borrar todos sus archivos (01/12/2002)

Un troyano que intenta eliminar todos los archivos del sistema donde se ejecuta está siendo distribuido como un skin para la aplicación de intercambio de archivos Kazaa.

Si hay aplicaciones realmente utilizadas hoy en día en internet son las que permiten el intercambio de archivos de música, software y películas, y entre ellos, Kazaa es uno de los de mayor difusión, con varios millones de usuarios en todo el mundo.

Dicha popularidad lo ha hecho un nuevo blanco de los troyanos y gusanos informáticos, habiendo aparecido este año varios de ellos que aprovechan sus capacidades para intentar reproducirse entre sus usuarios, simulando ser "tentadores" canciones musicales o películas recién estrenadas.

Recientemente se ha descubierto la existencia de un troyano que simula ser un skin para el Kazaa, es decir, un programa que permite cambiar su apariencia. El mismo se encuentra comprimido en un archivo .ZIP, denominado eightball2.zip, y su nombre simulado es "Magic Eightball" (mágica bola ocho).

Cuando dicho archivo es abierto y su contenido ejecutado, intenta eliminar todos los archivos en la unidad principal del usuario, causando que el sistema operativo deje de funcionar correctamente, y que toda la información almacenada allí se pierda. Para volver a utilizar su computadora correctamente, el usuario deberá reinstalar el sistema operativo que utilice.

Debido a que utiliza ciertas funcionalidades sólo disponibles en Windows XP, el troyano no podrá ejecutarse correctamente en otros ambientes Windows, y sólo podrá causar el daño antes descrito si es descargado y ejecutado en un equipo con la última versión del sistema operativo de Microsoft.

Éste no es el único programa que hace este tipo de cosas, por lo que es importante que el usuario tenga cuidado al bajar un archivo de la red Kazaa y no lo ejecute sin antes haber chequeado que se encuentra libre de virus y que tiene la extensión de lo que busca, dado que muchos archivos que simulan ser música o vídeos, suelen ser en realidad ejecutables con extensión .EXE, y presumiblemente, troyanos que pueden causar daño a su equipo.

Kazaa ha implementado un módulo antivirus para su producto, llamado Bullguard Lite, que puede ser activado desde el menú Herramientas de la aplicación, en la pestaña Tráfico, pero no cubre todas las necesidades de seguridad que un usuario necesita. Por ello, la mejor recomendación es no abrir archivos ejecutables que sean descargados desde esta aplicación. Podemos perdernos de algo interesante, pero al menos nuestra PC se mantendrá segura.