MALWARE

Programas Maliciosos

Las nuevas amenazas que se presentan día a día en la red, su clasificación y manera de actuar.

Enrique Flecha – Matrícula 49116

22/09/2008

Contenido

INTRODUCCIÓN

El objetivo del presente trabajo de investigación es arrojar un poco de luz sobre el extenso tema del Malware. Hoy en día ya no se habla sencillamente de virus, ni de gusanos, la jerga utilizada para este tipo de programas nocivos que infectan continuamente nuestras computadoras ha cambiado de tal manera que se podría decir que existe una amplia fauna y flora de estos códigos nocivos.

Además la perspectiva del ataque se ha ampliado, los autores de programas maliciosos hace mucho han dejado de tener como única finalidad hacer que el ordenador víctima deje de funcionar. Hoy día se tienen diferentes ámbitos de ataque, como veremos cada caso se aprovecha de alguna vulnerabilidad para obtener algún tipo de beneficio a costa de los usuarios cuyas máquinas han sido infectadas o como alternativa hacerse con algunos datos valiosos del mismo.

Otro aspecto a tener en cuenta es que la expansión de Internet como fuente de negocios y transacciones económicas a nivel mundial ha moldeado enormemente las intenciones de dichos programas maliciosos, a tal punto de que la mayoría de los mismos tienen como finalidad última sacar algún provecho monetario, ya sea directa o indirectamente.

DEFINICIÓN DEL TÉRMINO MALWARE

Inicialmente es importante establecer cuál es el alcance del término Malware. Qué actividades incluye, qué tipos de códigos se pueden etiquetar como Malware. La mejor manera de hacerlo es citando varias fuentes, de entidades y organizaciones que trabajan en el campo de la protección y seguridad en internet, así como de otras fuentes conocidas de información, para así tener una idea bastante acabada del término.

Según *www.viruslist.com*, una página perteneciente a *Kaspersky Labs* que se encarga de recabar información sobre actividades nocivas en la red, tenemos la siguiente definición:

"Los programas maliciosos pueden dividirse en los siguientes grupos: gusanos, virus, caballos de Troya o troyanos, utilidades para hackers y otros tipos de programas maliciosos. Todos ellos han sido diseñados para causar daños al equipo infectado o a otros equipos conectados a redes."

Según *Wikipedia*, tenemos que Malware es:

"Malware (del inglés **mal**icious soft**ware**, también llamado **badware**, **software malicioso** o **software malintencionado**) es un software que tiene como objetivo infiltrarse en o dañar un ordenador sin el conocimiento de su dueño y con finalidades muy diversas ya que en esta categoría encontramos desde un troyano hasta un spyware."

"Esta expresión es un término general muy utilizado por profesionales de la computación para definir una variedad de software o programas de códigos hostiles e intrusivos."

De www.kaspersky.com, la página oficial del programa antivirus *Kaspersky Antivirus,* tenemos la siguiente definición:

"Malware, abreviatura para el software malicioso, es un término genérico que se refiere a cualquier programa de software creado deliberadamente para llevar a cabo una no autorizada y, a menudo, perjudicial acción. Se trata de una simple combinación de dos palabras creada para permitir a la gente a hablar de todos los virus y otras formas de software malicioso de manera general.

"Virus, *backdoors*, *keyloggers*, *password stealers*, virus macro de Word y Excel, los virus de sector de arranque, los virus de script (batch, windows shell, java, etc.), troyanos, *crimeware*, software espía y *adware* no son sino unos pocos ejemplos de lo que se considera los programas maliciosos."

La CME (Common Malware Enumeration), una organización que tiene como finalidad identificar a los nuevos malware que aparecen en la red, establece que:

"Malware es cualquier código o programa como ser virus, gusanos, etc, con el potencial de dañar un sistema computacional o una red".

De todas estas definiciones se puede concluir que Malware es un término de amplio espectro, que abarca a todos los programas creados con el fin de realizar comandos no autorizados e intrusivos en una computadora o sistema computacional. Sus consecuencias pueden ser variadas, yendo de prácticamente imperceptibles a catastróficamente perjudiciales, pero en general, el simple hecho de cometer una intrusión y realizar actividades no establecidas y permitidas por el usuario, define el programa como Malware.

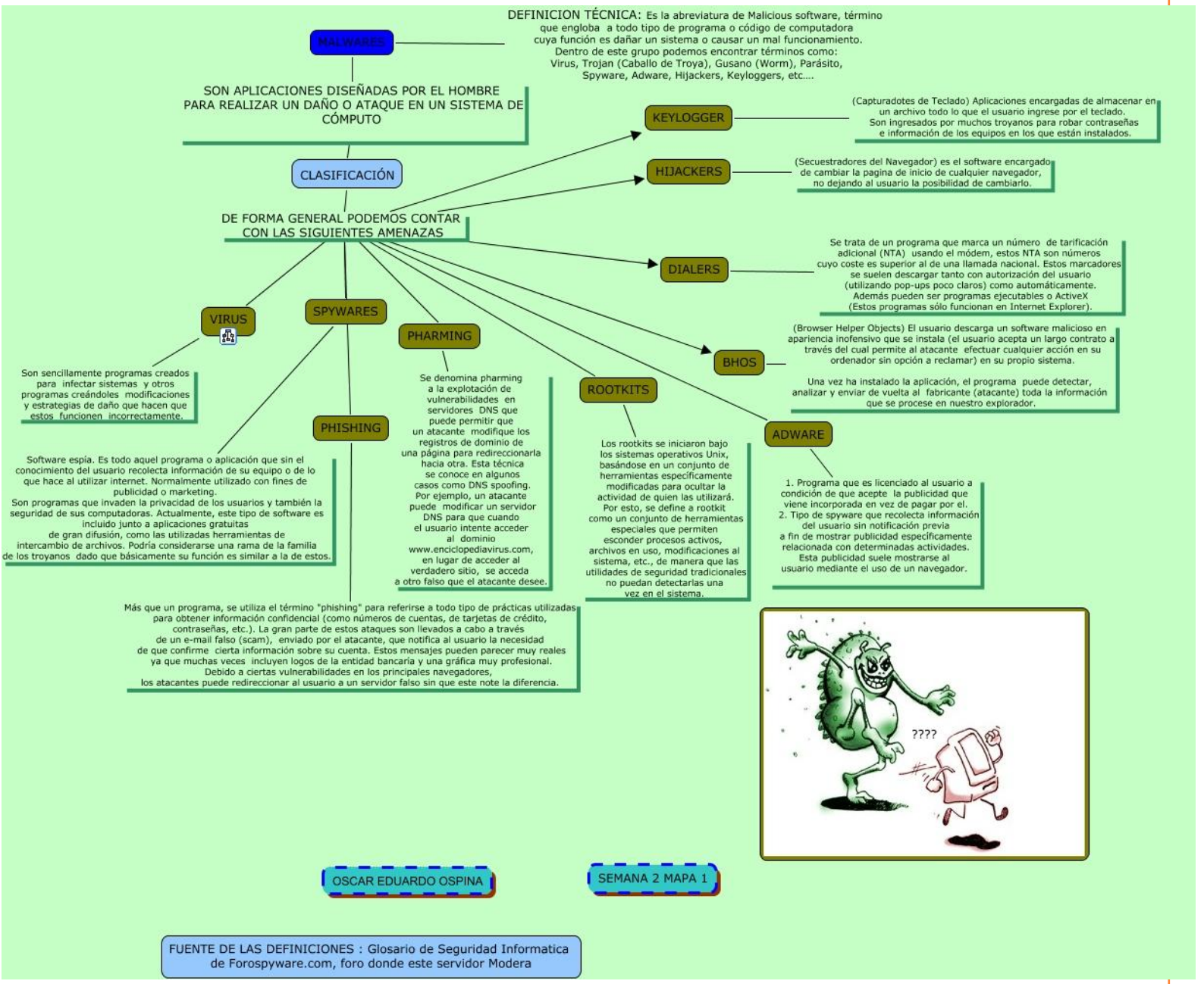
CLASIFICACIÓN DEL MALWARE

Es importante decir que la clasificación del Malware es una tarea extensa y existen categorías que aún no han sido definidas formalmente, debido a que hoy en día las actividades delictivas son tan variantes que muy a menudo incursionan en acciones que se podrían etiquetar como típicas en más de una categoría de Malware.

- ✓ Gusanos de red
- ✓ Virus Clásicos
- ✓ Caballos de Troya, troyanos
- ✓ Adware
- ✓ Spyware
- ✓ Pharming (método de estafa, no será tratado)
- ✓ Phisings (método de estafa, no será tratado)
- ✓ Keyloggers
- ✓ Exploit
- ✓ Cryptovirus, Ransomware o Secuestradores
- ✓ Pornware
- ✓ Rootkit
- ✓ Scumware
- ✓ Ladilla Virtual

Entre las nuevas clasificaciones de Malware encontramos categorías como *Crimeware* y *Grayware*, términos que serán definidos posteriormente.

Seguidamente se presenta un gráfico que ilustra las categorías más comunes del malware.



A continuación, se dará una descripción de los tipos de programas maliciosos no tan comunes, como Ransomware, Pornware, Rootkit, Scumware, Ladillas virtuales, etc. Los programas maliciosos muy comunes como los gusanos, virus clásicos, troyanos, keyloggers, exploits, podrán ser brevemente tratados con el objetivo de dar a entender mejor algún otro programa malicioso relacionado con los mismos, pero la intención es no mencionar de ser posible, malware muy conocidos, con el objetivo de mantener el trabajo centrado únicamente en malware reciente.

Adware

Contracción de ***Ad****vertisement* y *soft****ware***. Este también está considerado como un programa malicioso común, por lo tanto, se dará solamente una breve descripción del mismo.

Este software muestra o baja anuncios publicitarios que aparecen inesperadamente en el equipo, pudiendo hacerlo simultáneamente cuando se está utilizando la conexión a una página Web o después de que se ha instalado en la memoria de la computadora.

Los desarrolladores usan el adware como recurso para lograr ingresos económicos de sus programas, que usualmente son gratuitos. A veces los usuarios pueden pagar para que desaparezca la publicidad de las aplicaciones adware.

Algunas aplicaciones adware populares son: TopMoxie, 180 Solutions, 180SearchAssistant, Zango, Bonzi Buddy, ClipGenie, Comet Cursor, Cydoor, Daemon Tools, ErrorSafe, Gator Hotbar, PornDigger!, Smiley Central, WeatherBug, WhenU, WinFixer.

Spyware

Es un software espía. Cualquier aplicación informática que recolecta información valiosa de la computadora desde donde está operando. Es un tipo de malware que por lo general se introduce y opera en las PCs sin que el usuario lo advierta. Este es uno de los programas maliciosos más comunes hoy en día.

También hay espías que entran en las computadoras cuando el usuario acepta las condiciones de uso de un programa al instalarlo, por lo general ese texto es obviado en la instalación.

Además de verse vulnerada la privacidad de los usuarios, los spywares pueden producir pérdidas económicas pues pueden recolectar números de tarjetas de crédito y claves de accesos. También pueden producir gran deterioro en el funcionamiento de la computadora tales como bajo rendimiento, errores constantes e inestabilidad general.

Keylogger

Un keylogger es un malware del tipo daemon. Son programas espías para espiar y robar información, monitorear el sistema, registrando las

pulsaciones del teclado, para robar las claves, tanto de páginas financieras y correos electrónicos como cualquier información introducida por teclado, en el equipo utilizado para saber lo que la víctima ha realizado como conversaciones que la misma tuvo, saber donde ha entrado, qué ha ejecutado, qué ha movido, etc. Los keyloggers forman parte de muchos malware más elaborados, por ese motivo los definimos aquí.

Rootkit

El Rootkit es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers que consiguen acceder ilícitamente a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos.

Hay rootkits para una amplia variedad de sistemas operativos, como Linux, Solaris o Microsoft Windows. Por ejemplo, el rootkit puede esconder una aplicación que lance una consola cada vez que el atacante se conecte al sistema a través de un determinado puerto. Los rootkits del kernel o núcleo pueden contener funcionalidades similares.

Un backdoor puede permitir también que los procesos lanzados por un usuario sin privilegios de administrador ejecuten algunas funcionalidades reservadas únicamente al superusuario. Todo tipo de herramientas útiles para obtener información de forma ilícita pueden ser ocultadas mediante rootkits.

Estos programas tratan de encubrir a otros procesos que están llevando a cabo acciones maliciosas en el sistema. Por ejemplo, si en el sistema hay una puerta trasera para llevar a cabo tareas de espionaje, el rootkit ocultará los puertos abiertos que delaten la comunicación; o si hay un sistema para enviar spam, ocultará la actividad del sistema de correo.

Los rootkits, al estar diseñados para pasar desapercibidos, no pueden ser detectados. Si un usuario intenta analizar el sistema para ver qué procesos están ejecutándose, el rootkit mostrará información falsa, mostrando todos los procesos excepto él mismo y los que está ocultando.

O si se intenta ver un listado de los ficheros de un sistema, el rootkit hará que se muestre esa información pero ocultando la existencia del propio fichero del rootkit y de los procesos que esconde.

Cuando el antivirus haga una llamada al sistema operativo para comprobar qué ficheros hay, o cuando intente averiguar qué procesos están en

ejecución, el rootkit falseará los datos y el antivirus no podrá recibir la información correcta para llevar a cabo la desinfección del sistema.

Un caso interesante y famoso de infección por Rootkits se dio cuando la discográfica Sony BMG fué demandada (11/2005) mediante una acción popular en California por los consumidores que afirmaban que sus ordenadores habían sido dañados por el software antipiratería de algunos CDs de esta compañía.

La demanda aseveraba que Sony BMG actuó mal al no revelar la verdadera naturaleza del sistema de administración de derechos digitales que usaba en sus CDs y miles de usuarios han infectado sus ordenadores sin saberlo, según los documentos del tribunal.

La denuncia, interpuesta el 1 de noviembre en el Tribunal Superior de Los Ángeles, pide a la corte que Sony BMG deje de vender CDs protegidos adicionalmente con el software antipiratería y compensaciones económicas para los consumidores californianos que los adquirieron.

Exploit

Exploit (del inglés to exploit, explotar, aprovechar) es el nombre con el que se identifica un programa informático malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad de otro programa.

El fin puede ser la destrucción o inhabilitación del sistema atacado, aunque normalmente se trata de violar las medidas de seguridad para poder acceder al mismo de forma no autorizada y emplearlo en beneficio propio o como origen de otros ataques a terceros.

Los xploits se pueden caracterizar según las categorías de vulnerabilidades utilizadas:

- Vulnerabilidades de desbordamiento de buffer
- Vulnerabilidades de condición de carrera
- Vulnerabilidades de error de formato de cadena
- Vulnerabilidades de Cross Site Scripting XSS
- Vulnerabilidades de Inyección SQL
- Vulnerabilidades de Inyección de Caracteres CRLF
- Vulnerabilidades de denegación del servicio
- Vulnerabilidades de ventanas engañosas o mistificación de ventanas Window Spoofing.

En definitiva, el exploit es generalmente utilizado como la punta de lanza para realizar una intrusión en algún sistema informático. Existen páginas donde uno puede ver y conocer distintos tipos de exploits para más de un sistema operativo, como por ejemplo: http://www.elhacker.net/exploits/

Ransomware

El término se utiliza para hacer referencia a aquellos malware que "secuestran" archivos y piden "rescate" en dinero por ellos. Por lo general estos programas malignos encriptan la información de algunos archivos considerados importantes para el usuario, y no entregan la clave para lograr desencriptarlos si el usuario no paga. Estos virus también son llamados criptovirus.

La modalidad de trabajo es la siguiente: el código malicioso infecta la computadora del usuario por los medios normalmente utilizados por cualquier malware y procede a cifrar los documentos que encuentre (generalmente de ofimática), eliminando la información original y dejando un archivo de texto con las instrucciones para recuperarlos.

En los casos mencionados el rescate ha sido el depósito de dinero en una cuenta determinada por el creador del código malicioso. Luego que el dinero es depositado, se le entrega al usuario la clave para descifrar los archivos.

Hasta ahora, y por ser los primeros especímenes "menos desarrollados", los métodos de cifrado han sido sencillos y fácilmente reversibles, lo que permite a los especialistas conocer la clave y evitar que los usuarios pierdan dinero.

Además, el modo de utilización de cuentas bancarias aún no se ha perfeccionado, lo que permite rastrearlas en forma relativamente sencilla.

Esta nueva modalidad de virus ha visto la luz en mayo de 2005 con GpCoder, y regresado con el recientemente descubierto CryZip.

Es fácil imaginarse que cuando estos métodos se perfeccionen ocurrirá lo inevitable: las técnicas de cifrado utilizadas se aproximarán al modelo de Young-Yung, utilizando Criptografía simétrica fuerte, o incluso criptografía asimétrica, lo que imposibilitará el descifrado de los archivos.

Sería bueno preguntarse: ¿hay remedio a este nuevo tipo de ataques? La respuesta es que sí, a los actuales ataques sencillos sin criptografía avanzada, pero como ya se ha dicho es inevitable que este sistema de secuestro se perfeccione y tienda a la Criptovirología y Kleptografía.

Cuando esto suceda la respuesta a la pregunta planteada será un rotundo no y entonces sólo tendremos dos caminos posibles: realizar copias de seguridad de nuestra información en forma periódica, y contar con una defensa preactiva para nuestros sistemas, que nos proteja en todo momento de amenazas conocidas y desconocidas.

Ejemplo de Ransomware:

Virus.Win32.Gpcode.ak

Programa nocivo que cifra los ficheros del usuario en el ordenador infectado. El gusano es una aplicación para Windows (archivo PE EXE) y tiene un tamaño de 8030 bytes.

Después de lanzarse, el virus crea en la memoria del ordenador un identificador único (mutex)_G_P_C_ para señalar su presencia en el sistema.

Después, el virus empieza a hacer un barrido de todos los disco lógicos en busca de ficheros para cifrarlos. El virus cifra todos los ficheros del usuario que tienen las siguientes extensiones:

7z	abk	abd	acad arh	arj	ace	arx asm	bz	bz2	bak
bcb	c	cc	cdb cdw	cdr	cer	cgi chm	cnt	cpp	css
csv	db	db1	db2 db3	db4	dba	dbb dbc	dbd	dbe	dbf
dbt	dbm	dbo	dbq dbx	Djvu	doc	dok dpr	dwg	dxf	ebd
eml	eni	ert	fax flb	frm	frt	frx frg	gtd	gz	gzip
gfa	gfr	gfd	h inc igs	iges	jar jad Java		jpg	jpeg	
Jfif	jpe	js	jsp hpp	htm	html	key kwm	Ldif	lst	lsp
lzh	lzw	ldr	man mdb	mht	mmf	mns mnb	mnu	mo	msb
msg	mxl	old	p12pak	pas	pdf	pem pfx	php	php3	php4
pl	prf	pgp	prx pst	pw	pwa	pwl pwm	pm3	pm4	pm5
pm6	rar	rmr	rnd rtf	Safe	sar	sig sql	tar	tbb	tbk
tdf	tgz	txt	uue vb	vcf	wab	xls xml			

Para cifrar los ficheros el virus usa un criptoalgoritmo integrado en el sistema Windows (Microsoft Enhaced Cryptographic Provider v1.0). Los

ficheros se cifran mediante el algoritmo RC4. La llave de cifrado se cifra con una llave abierta RSA de 1024 bits contenida en el cuerpo del virus.

El algoritmo RSA se basa en la división en dos llaves: la llave secreta y la llave abierta. El principio de cifrado mediante RSA dice: para cifrar datos es suficiente tener sólo la llave abierta. Pero para descifrar los datos hay que tener la llave secreta.

El virus crea una copia cifrada del fichero que lleva el nombre original del fichero y a cuya extensión se le añade _CRYPT. Ejemplo:

> WaterLilles.jpg — fichero original
>
> WaterLilles.jpg._CRYPT — fichero cifrado

Después, el fichero original se elimina.

En cada catálogo donde se hayan cifrado ficheros, el virus pone el fichero read_me.txt, que tiene el siguiente contenido:

> Tus ficheros están cifrados con el algoritmo RSA-1024 .
>
> Para descifrar tus ficheros, tendrás que comprar nuestro software.
>
> Para comprar nuestro software, escríbenos a: [censored]@yahoo.com
>
> === BEGIN ===
>
> [key]
>
> === END ===

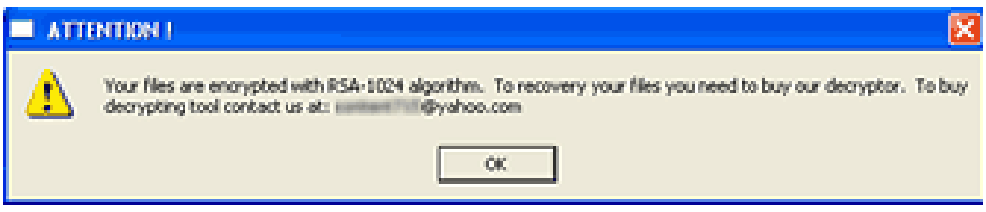
Los ficheros que se encuentran en el catálogo Program Files no se cifran. El virus tampoco cifra los siguientes ficheros:

los que tienen atributo de “sistema” y “oculto”;

los que tienen un tamaño menor a 10 bytes;

los que tienen un tamaño mayor a 734003200 bytes

Al concluir su trabajo el virus crea un fichero VBS que elimina del equipo el cuerpo del virus y muestra en la pantalla un MessageBox:



Durante su trabajo el virus no se inscribe en el registro del sistema.

Pornware

El término pornware denota a programas que están relacionados con el despliegue de contenidos pornográficos al usuario. Las clases de pornware incluyen programas Porn-Dialer, Porn-Downloader y Porn-Tools entre otros.

Los Dialers se conectan a servicios telefónicos pornográficos, este tipo de pornware está se está extinguiendo con la disminución de las conexiones via modem. Los Downloaders bajan material pornográfico a la máquina del usuario. Por último los Porn-Tools cubren todas las utilidades necesarias en buscar y bajar material pornográfico (por ejemplo, toolbars especiales para los buscadores o reproductores de video).

Es muy fácil ejecutar una aplicación Pornware porque en la mayoría de los casos el software antivirus no reconoce el programa como malicioso.

Los programas Pornware pueden ser instalados por un usuario deliberadamente con el fin de buscar y acceder a material pornográfico. En tales casos, los programas no son vistos como malicioso.

Sin embargo, estos programas también puede ser instalados en la máquina con intención maliciosa, a través de operativos o vulnerabilidades del navegador, o mediante el uso de Trojan-Downloaders o Trojan-Droppers. Esto normalmente se hace para promocionar o hacer publicidad de sitios pagos de pornografía que de otra manera no hubiesen llegado al usuario.

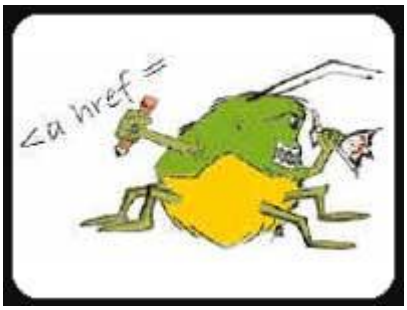
Ladillas Virtuales

Este tipo de programa maligno que, como analogía al parásito de transmisión sexual, entra en una computadora a través del sexo virtual, sitios pornográficos o cualquier aplicación relacionada. Los sitios web pornográficos suelen ser un gran caldo de cultivo para estos Malware virtuales.

En realidad, la categoría de Ladillas Virtuales, incluye a los Malware que infectan a sus víctimas en el entorno mencionado anteriormente. Por

supuesto, entre estos programas podríamos encontrar todo tipo de Malware, desde troyanos hasta pornware, ransomware, etc.

Scumware



Scumware es cualquier software que hace cambios significativos en la apariencia y funciones de las páginas Web sin permiso del Administrador (Webmaster) o propietarios. Por ejemplo, un número de productos sobreponen la publicidad de los banners con otros anuncios, a veces para los productos de la competencia. El Scumware puede agregar hyperlinks desautorizados a la sección opinión de una página Web - a veces usar de un usuario acoplamientos a los sitios posiblemente desagradables. Tales programas pueden interferir con hipervínculos (hyperlinks) existentes agregando otros destinos a los previstos. A veces, el Scumware es conocido como thiefware.

Su modo de operación consiste básicamente en desviar sin permiso el tráfico de un sitio web hacia otro. Las técnicas son múltiples, pueden ser desde cubrir los banners de los anunciantes con otros, crear hiperenlaces de manera artificial e incluso desviar direcciones web hacia otras páginas.

Existen técnicas de Scumware que podríamos denominar 'suaves', por ejemplo cubrir los banners de un sitio con otro de las mismas dimensiones, de manera que, por ejemplo, Coca Cola podría ocultar todos los anuncios de Pepsi-Cola de un determinado sitio con otro de exactamente las mismas dimensiones pero suyo. El resultado final sería que un visitante de una página vería anuncios de Pepsi-Cola cuando en realidad es Coca-Cola la empresa que está pagando a la empresa desarrolladora de la página.

Pero lamentablemente existe otro tipo de técnicas bastante más agresivas, una vez que se ha abierto la Caja de Pandora el límite está en la imaginación humana.

Existen muchos programas que incorporan software Scumware, uno de los más conodidos fue Kazaa, un software de intercambio de archivos similar a Napster y que está adquirió muchísima popularidad entre la comunidad internauta en su época.

Según las últimas estimaciones Kazaa ha sido descargado por más de 7 millones de personas, pero lo que muy pocas de ellas llegaron a saber es que simultáneamente al programa de intercambio de archivos también habían

descargado un programa tipo Scumware denominado TopText y que funcionaba de manera similar a los SmartTags que Microsoft pretendió incluir en el SO XP.

¿Cómo funciona TopText?, al igual que la tecnología SmartTags de Microsoft, escanea el contenido de una página web e incorpora hiperenlaces, sin permiso del webmaster de la página ni del usuario de la máquina que la navega, bajo determinadas palabras clave.

Por ejemplo, y continuando con el mismo ejemplo anterior de bebidas carbonatadas, TopText podría cada vez que aparece en una página web la palabra 'Bebida' incluir de manera artificial un hiperenlace que apuntase a la página de Cocacola.

La cosa puede llegar a ser bastante más grave que el ejemplo anterior, pues se podría llegar a incluir enlaces de páginas porno dentro de páginas que nada tiene que ver con ello, por ejemplo.

La situación puede ser hasta más grave, pues se puede llegar a sustituir hiperenlaces por otros, por lo que lo que en realidad está haciendo es cambiando los contenidos de una página sin permiso de nadie, de hecho la legalidad de este tipo de programas está actualmente en entredicho, aunque en realidad lo más importante es que alteran los contenidos de las páginas que visitamos sin ningún tipo de permisos.

Curiosamente, existe otra definición del término Scumware, que dicta: “es todo programa que evita a toda costa ser desinstalado, valiéndose de protecciones para no permitirlo, de esta manera se convierte en un programa molesto y malicioso.”

Crimeware

Es un software diseñado específicamente para cometer crímenes del tipo financiero o similar, intentando pasar desapercibido por la víctima. Por extensión, también hace referencia a aplicaciones web con iguales objetivos.

Un crimeware puede robar datos confidenciales, contraseñas, información bancaria, etc. y también puede servir para robar la identidad o espiar a una persona o empresa.

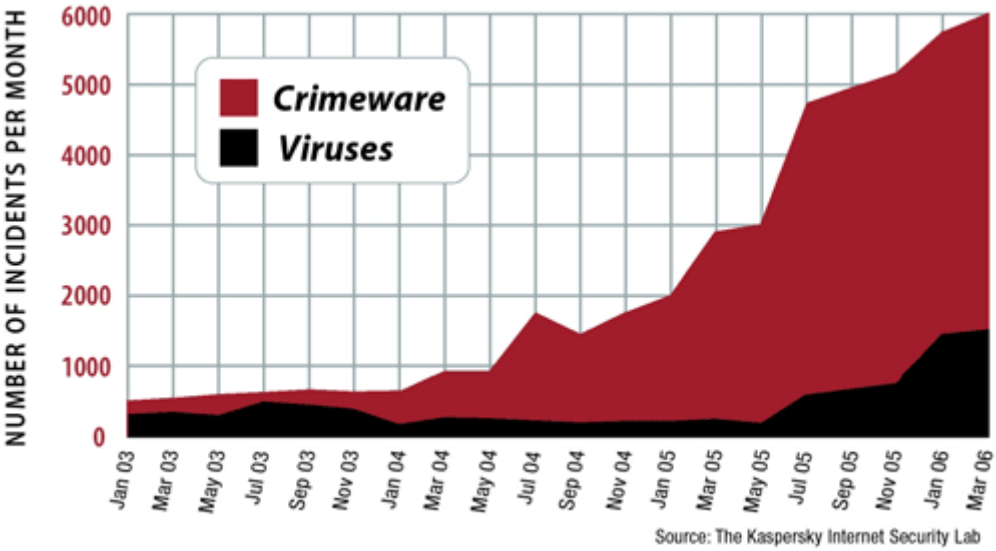
El término fue ideado por Peter Cassidy, secretario general del Anti-Phishing Working Group, para distinguir este tipo de programas de otros malignos como malwares, spywares, adwares, etc. (aunque muchas veces éstos emplean técnicas similares para propagarse o actuar).

Un programa crimeware puede actuar solo o teledirigido, pero su principal característica de funcionamiento es que intenta pasar desapercibido. Muchas veces para cumplir su objetivo, el crimeware debe ir combinado con la técnica de hackeo llamada ingeniería social. La ingeniería social hace referencia a la actividad de manipular o convencer de alguna manera a una persona, para que realice acciones que le servirán al cibercriminal para obtener datos importantes de esa misma persona. La mayoría de las personas suelen ser lo suficientemente ignorantes como para incluso dar sus propias contraseñas.

Los crimewares están diseñados para robar la identidad de una persona o usuario para acceder a las cuentas online de servicios financieros. En general, el propósito es robar el dinero de esas cuentas.

Un crimeware puede emplear diversas técnicas para lograr su objetivo criminal, la más común es instalarse ocultamente en una computadora, para capturar información importante del usuario como claves, nombres de usuario y tarjetas de crédito.

A continuación se presenta un gráfico que muestra el crecimiento del crimeware a través de los últimos años.



Una vez más vale aclarar que el Crimeware es una categoría en la cual se pueden etiquetar diversos Malware. Queda claro también que muchas veces, los diseñadores de códigos maliciosos actúan de manera específica sobre una víctima, preparando tal vez un coctel de malware (programas con varias características de malware) con el objetivo de llevar a cabo la acción criminal.

Un ejemplo clásico de Crimeware es un *troyano-keylogger-backdoor* que guarda las teclas oprimidas por el usuario y envía esta información al delincuente, para su posterior uso en el crimen cibernético.

Ransomware también se puede incluir dentro de esta categoría.

Grayware

En pocas palabras, grayware es otra forma de denominar a los spyware, adware, dialers, toolbars y keyloggers. Entonces, si grayware resulta ser una manera general de llamar al anteriormente mencionado conjunto de malware, los síntomas que indican su presencia en el ordenador son los mismos:

-Bajo rendimiento del equipo.

-Secuestro del navegador. Se cambia la página de inicio sin posibilidad de restaurarla.

-Ventanas emergentes de publicidad se despliegan incluso si estamos desconectados.

-Las herramientas de seguridad han dejado de actuar sin razón aparente.

ORGANIZACIONES ANTI-MALWARE

Además de los programas habituales de antivirus y antimalware a los cuales estamos acostumbrados, existen otros esfuerzos por combatir el efecto nocivo de estos programas, son las llamadas organizaciones anti-malware. El objetivo de cada una de estas organizaciones difiere en varios puntos, pero todas tienen una finalidad común: disminuir o frenar el avance frenético de los Malware.

CME (Common Malware Enumeration)

La CME tiene como iniciativa proveer de un identificador común y único a cada nueva amenaza de virus que se presenta, así también como para las amenazas más conocidas que se esparcen por la Red.

Administrado y mantenido por la Miter Corporation, CME no es un intento de resolver los problemas relacionados con los esquemas de nombramientos de de virus y otras formas de malware. En lugar de ello, es un esfuerzo para facilitar la adopción de una capacidad de indexación neutral de malware.

A través de la adopción del presente método de identificación compartido y neutral, la iniciativa CME procura:

- Reducir la confusión del público en referencia amenazas durante incidentes de malware.
- Mejorar la comunicación entre los fabricantes anti-virus.
- Mejorar la comunicación y el intercambio de información entre los fabricantes anti-virus y el resto de la comunidad de seguridad de la información.

CME reduce la confusión mediante la asignación de un identificador CME único a una amenaza particular para que los anti-virus, así como otros sistemas relacionados con la seguridad de las entidades, pueda incluirlo junto con su información de propiedad. De esta manera, el público podrá hacer una referencia cruzada del virus con nombres dispares a través de un identificador común. Estos identificadores CME comunes, se publican para el uso del público en la Lista CME del sitio web de CME.

A los efectos de la iniciativa CME, todas las amenazas de malware y los virus son descubiertos por las organizaciones que son miembros de la *CME Sample Redistribution Group* y subidos al *CME Submission Server* para la asignación de un identificador CME.

Adicionalmente se puede citar otras organizaciones que están abocadas al mismo fin que la CME, como por ejemplo la CARO Malware Naming Scheme.

AMTSO

La AMTSO (Anti-Malware Testing Standards Organization) fue fundada en mayo de 2008 como una asociación sin fines de lucro que se centra en la necesidad mundial de hacer frente a la necesidad de mejorar la objetividad, la calidad y la pertinencia de las metodologías de puesta a prueba de anti-malware. La membresía de AMTSO está abierta a personas de los ambientes tanto industriales como académicos, que trabajan en el entorno de la lucha contra el Malware.

El esquema preliminar de AMTSO se centra en las siguientes 5 áreas:

- Proporcionar un foro para los debates relacionados con la prueba de anti-malware y productos relacionados.
- El desarrollo y la difusión de normas objetivas y las mejores prácticas para la prueba de anti-malware y productos relacionados.
- La promoción de la educación y el conocimiento de las cuestiones relacionadas con la prueba de anti-malware y productos relacionados.
- Proporcionar herramientas y recursos a la ayuda basada en estándares y metodologías de prueba.
- Proporcionar análisis y revisión de las actuales y futuras de las pruebas anti-malware y productos relacionados.

A pesar de su corta existencia, esta organización tiene como objetivo, como se puede observar, mejorar y formalizar el entorno de los productos anti-malware estableciendo normas objetivas y sugiriendo mejores prácticas. Este esfuerzo se encamina a una mejor protección otorgada por dichos programas antimalware.

TENDENCIAS EN EL 2008

ESET, compañía líder en detección proactiva y desarrollador del multipremiado antivirus ESET NOD32, publica un informe sobre las tendencias que se esperan para el 2008 en códigos maliciosos y seguridad antivirus. Tal y como ESET adelantó en el 2007, el malware sigue llevando adelante sus acciones dañinas, ampliando sus frentes de ataque y mejorando su efectividad.

Es así que en la actualidad, la variedad de los tipos de malware, como así también las dimensiones que abarcan sus efectos, han ido en aumento destacándose ciertas cuestiones que hacen de este tipo de programas, las amenazas más importantes y más difíciles de combatir en cualquier entorno informático.

Cristian Borghello, Technical & Educational Manager de ESET para Latinoamérica, preparó el informe a continuación donde se explican las tendencias que se esperan para el 2008 de los códigos maliciosos y los creadores de malware.

Abuso de confianza del usuario

La "Ingeniería Social" sigue siendo el elemento más explotado para engañar e infectar al usuario. Esto queda demostrado con la aparición de gran cantidad de malware que utilizan las tarjetas virtuales y los eventos de gran envergadura para incitar al usuario a que descargue un archivo dañino. La realización de los juegos olímpicos durante 2008 seguramente será una importante red para cazar usuarios desprevenidos.

La formación de grandes comunidades online (como MySpace, Orkut, FaceBook y diferentes juegos en línea) también se ha convertido en un importante punto para abusar de la confianza de los usuarios. Actualmente, ya existe gran cantidad de malware disponible para robar los datos privados a los usuarios que participan de estas comunidades. Como siempre, este año Asia ha marcado el rumbo de lo que cabe esperar dentro de poco para este lado del mundo.

También es válido lo mencionado anteriormente para los ataques de phishing, cuyos anzuelos se perfeccionan y se hacen más eficaces. Técnicas antiguas, como por ejemplo pharming local, siguen siendo utilizadas masivamente y los principales bancos latinoamericanos (y sus usuarios) se están convirtiendo en el epicentro de estos ataques, a través de correos masivos y troyanos.

Un ejemplo de perfeccionamiento de estas técnicas son los casos en donde los ataques de phishing no implican la clonación de páginas web para robar información sensible de los usuarios sino que, contrariamente a ello, utilizan metodologías mediante las cuales superponen, en la zona de acceso al Home-Banking, una imagen similar a la real.

Por otro lado, los kits de construcción de phishing, si bien tuvieron su auge durante los primeros meses del año 2007 y luego fueron decayendo, no dejan de ser amenazas latentes.

Abuso de recursos de Internet

Teniendo en cuenta este escenario, hoy se continua siendo testigo de que la natural evolución del malware seguirá en aumento y seguirá perfeccionándose con técnicas y metodologías de todo tipo pudiendo alcanzar niveles preocupantes. Por ejemplo, durante el 2007 diversos países ya habían denunciado ciberataques llevados a cabo por troyanos orientados a robar documentación secreta.

Con relación al correo electrónico no deseado y no solicitado -comúnmente denominado spam- se percibe un gran avance en las metodologías de engaño que utilizan los creadores de malware para acaparar la atención de los usuarios; por ejemplo la masificación de mensajes conteniendo imágenes y el nacimiento del spam en archivos PDF y MP3.

El robo de inmensas bases de datos de diferentes organizaciones mundiales permite ataques dirigidos a usuarios a través de spam y de phishing personalizado. Por esto, se volverá más común encontrar que el spam sea dirigido a una persona con nombre y apellido, e incluso en el idioma nativo del propietario de las cuentas de correo.

Por otro lado, aprovechando las nuevas tecnologías de comunicación de las comunidades online ya mencionadas, el spam común y corriente se está trasladando a estas comunidades en formato de splog (comentarios en blogs enlazando a sitios dañinos).

La aparición de servicios gratuitos tipo mash-up, en donde un sitio web no vulnerable “recibe” servicios de otros que pueden ser vulnerables, se está afianzando y cada vez es más normal encontrar enlaces a sitios conocidos que contienen servicios de terceros que apuntan a código dañino. Esto incluso sucede en cualquier buscador y con cualquier tema de referencia.

Vulnerabilidades

Un apartado especial se merecen los errores que todo software tiene como común denominador. La explotación de vulnerabilidades a través de los navegadores es una de las técnicas que más se ha perfeccionado durante el 2007 y día a día surgen nuevos exploits y nuevos scripts (generalmente ofuscados para evadir a las herramientas de seguridad) que aprovechan determinadas debilidades en los sitios web comprometidos y que permiten la instalación de malware en los equipos de los usuarios.

La fusión entre diferentes códigos maliciosos, las diferentes técnicas y la diversificación de las metodologías serán una constante durante el 2008 por permitirle a los delincuentes mayores posibilidades de efectuar alguna estafa con la información de los usuarios, obtenida a través del malware.

Debe remarcarse que la tendencia actual de los creadores de malware es infectar a una gran cantidad de usuarios en forma totalmente silenciosa a través de códigos ocultos en sitios web, para pasar desapercibidos. Sin duda, esta técnica resulta más eficiente que un ataque masivo y rápido que alerta a los usuarios y a las compañías de seguridad.

Por otro lado, la creación de servidores web con contenido malicioso, así como el enlace de los mismos desde sitios web conocidos y previamente comprometidos dieron origen a un "nuevo" concepto: Malware 2.0. Esta analogía hace clara referencia a la Web 2.0, donde cada componente dañino posee un rol dinámico que se apoya también en el comportamiento del usuario ante un sitio web.

Nuevas tecnologías

El aprovechamiento de las nuevas tecnologías sigue creciendo al igual que sus vulnerabilidades y formas de explotación. En este sentido, tecnologías como voz sobre IP no fueron la excepción y también terminaron siendo explotadas por el malware.

Asimismo, se debe hacer referencia a la creación de programas dañinos para productos de reciente aparición como nuevas versiones del iPod y el iPhone. Si bien las infecciones no han sido masivas, son las suficientes como para marcar el camino en este aspecto.

Por otro lado, la utilización de clientes de mensajería instantánea y las redes P2P para propagar malware son moneda corriente, e incluso han alcanzado niveles de infección elevados en Latinoamérica.

La diseminación y posterior infección por intermedio de dispositivos de almacenamiento extraíbles (USB, memorias, flash, etc) que aprovechan las bondades de ejecución automáticas de los sistemas operativos, se ha ido

acrecentando desde mediados del 2007 y todo indica que seguirá creciendo aún más.

Las amenazas de siempre potenciadas

Troyanos, gusanos y PUP (Potencial Unwanted Programs; o en castellano programas potencialmente no deseados) son cada vez más sofisticados a punto tal que incorporan capacidades defensivas que hacen que la tarea de análisis y remoción sea más complicada. Por ejemplo, muchos de ellos ya cuentan con la habilidad de detectar cuando son ejecutados en máquinas virtuales o cuando están siendo analizados.

Con respecto a los gusanos y troyanos que han tenido una actuación preponderante durante el 2007, no queda más que esperar su crecimiento debido a que son la herramienta fundamental para la creación de redes botnets , como así se demostró con la propagación de SDBot y Nuwar (también conocido como gusano Storm) cuyo único fin es crear redes con miles de nodos de equipos infectados. Los objetivos de estas redes, si bien se manejan múltiples hipótesis, aún se desconoce.

Conclusiones

Al igual que ESET adelantó en las conclusiones para el año 2007, se debe remarcar la gran actuación que tuvieron y tienen las redes organizadas para el crimen en todo este panorama: la interoperación de spammers, phishers, botmasters y creadores de malware hacen que a veces Internet se convierta en un lugar agresivo transformando a los usuarios en mulas (aquellos que mueven dinero sin saberlo y generalmente previamente engañados).

Además, hay un factor que permanece intacto y permanecerá así por mucho tiempo más, sin importar el tipo de amenaza que se trate ni las diferentes metodologías que utilice, un componente fundamental que ningún código malicioso desperdicia ni deja de monopolizar: la Ingeniería Social.

Pero a pesar de la utilización de esta técnica, los usuarios deben ser concientes de que cuentan con una herramienta mucho más sofisticada: la educación, que aplicada de forma oportuna, permite potenciar las posibilidades de no ser víctimas del malware en general o de cualquier amenaza que a nivel informático se presente.

Si a esta educación se suman herramientas de última generación como las soluciones de ESET, que se condicen con la evolución e innovación del malware, el usuario alcanzará altos niveles de protección en todo momento.

ROOTKITS EN SOFTWARE COMERCIAL

Rootkit en sistema anti-cheat de blizzard

(fuente www.rootkit.com)

Blizzard, subsidiario de Vivendi, desarrolla el popular juego llamado World of warcraft, el cual tiene millones de jugadores alrededor del mundo. Pero lo que estos jugadores no saben es que el juego contiene un software malicioso el cual indiscriminadamente lee el contenido de los datos de todos los programas que se encuentran en ejecución. El objetivo de este programa llamado Warden es el de verificar el cumplimiento del tratado de EULA y del TOS. Mientras varios jugadores agradecen la existencia de este mecanismo otros lo encuentran como una violación a su privacidad.

El hecho es que este software lee información de otros procesos, indistintamente de la posibles justificaciones, esto técnicamente cuenta como espionaje a los usuarios por lo que también se lo considera un spyware.

Por su parte Blizzard contesto a esto indicando de que el uso de este programa forma parte de su "Términos de uso" y que el jugador acepta los términos.

http://www.worldofwarcraft.com/legal/termsofuse.shtml

Acknowledgments.
You hereby acknowledge and agree that:
1. WHEN RUNNING, THE PROGRAM MAY MONITOR YOUR COMPUTER'S RANDOM ACCESS MEMORY (RAM) AND/OR CPU PROCESSES FOR
UNAUTHORIZED THIRD PARTY PROGRAMS RUNNING CONCURRENTLY WITH WORLD OF WARCRAFT. AN "UNAUTHORIZED THIRD PARTY
PROGRAM" AS USED HEREIN SHALL BE DEFINED AS ANY THIRD PARTY SOFTWARE, INCLUDING WITHOUT LIMITATION ANY "ADDON" OR
"MOD," THAT IN BLIZZARD'S SOLE DETERMINATION: (i) ENABLES OR FACILITATES CHEATING OF ANY TYPE; (ii) ALLOWS USERS TO MODIFY OR
HACK THE WORLD OF WARCRAFT INTERFACE, ENVIRONMENT, AND/OR EXPERIENCE IN ANY WAY NOT EXPRESSLY AUTHORIZED BY BLIZZARD;
OR (iii) INTERCEPTS, "MINES," OR OTHERWISE COLLECTS INFORMATION FROM OR THROUGH THE PROGRAM. IN THE EVENT THAT THE
PROGRAM DETECTS AN UNAUTHORIZED THIRD PARTY PROGRAM, BLIZZARD MAY (a) COMMUNICATE INFORMATION BACK TO BLIZZARD,
INCLUDING WITHOUT LIMITATION YOUR ACCOUNT NAME, DETAILS ABOUT THE UNAUTHORIZED THIRD PARTY PROGRAM DETECTED, AND THE
TIME AND DATE THE UNAUTHORIZED THIRD PARTY PROGRAM WAS DETECTED; AND/OR (b) EXERCISE ANY OR ALL OF ITS RIGHTS UNDER
SECTION 6 OF THIS AGREEMENT, WITH OR WITHOUT PRIOR NOTICE TO THE USER.
2. WHEN THE PROGRAM IS RUNNING, BLIZZARD MAY OBTAIN CERTAIN IDENTIFICATION INFORMATION ABOUT YOUR COMPUTER AND ITS
OPERATING SYSTEM, INCLUDING WITHOUT LIMITATION YOUR HARD DRIVES, CENTRAL PROCESSING UNIT, IP ADDRESS(ES) AND OPERATING
SYSTEM(S), FOR PURPOSES OF IMPROVING THE PROGRAM AND/OR THE SERVICE, AND TO POLICE AND ENFORCE THE PROVISIONS OF THIS
AGREEMENT AND THE EULA.

3. Blizzard may, with or without notice to you, disclose your Internet Protocol (IP) address(es), personal information, and information about you
and your activities in response to a written request by law enforcement, a court order or other legal process. Blizzard may use or disclose your
personal information if Blizzard believes that doing so may protect your safety or the safety of others.
4. BLIZZARD MAY RECORD YOUR CHAT SESSIONS AND OTHER ELECTRONIC COMMUNICATION TRANSMITTED OR RECEIVED THROUGH THE GAME
AND YOU CONSENT TO SUCH MONITORING OR LOGGING.
5. You are wholly responsible for the cost of all telephone and Internet access charges along with all necessary equipment, servicing, repair or
correction incurred in maintaining connectivity to the Servers.

Symantec reporta uso de un rootkit en uno de sus productos

(Fuente, www.hackinthebox.org)

El producto de esta compania llamado SystemWorks incluye una característica llamada Norton Protected Recycle Bin que sirve de extensión a la papelera de reciclaje estándar de windows salvando copias de los archivos "borrados" los cuales no son capturas por la papelera estandar, por ejemplo los archivos eliminados en los procesos de desinstalación de programas. Estos archivos se guardan en un directorio llamado NPROTECT el cual es creado y administrado por el SystemWorks, por debajo de la

papelera de reciclaje de windows en el directorio RECYCLER de cada partición. Symantec estaba originalmente preocupado que los usuarios finales pudieran acceder a este directorio, y modificarlo.

Por lo cual el programa utiliza una mascara o filtro dentro del manejado del sistema de archivos, para esconder a NPROTECT de los usuarios. Lo que no advirtió Symantec fue que este directorio podría ser utilizado para almacenar cualquier otro tipo de datos, por por ejemplo codigo, ejecutables maliciosos.

En respuesta a esto, Symantec realizo un rediseño del sistema liberando una actualización, la cual se aprecia en el siguiente reporte.

http://securityresponse.symantec.com/avcenter/security/Content/2006.01.10.html

Rootkit en paquete propocionado por Kaspersky

(Fuente,http://blogs.technet.com)

Mark Russinovich, técnico experto y empleado de microsoft, quien descubrió la utilización del famoso rootkit por parte de sony, había comentado en su blog personal que sospechaba que el producto de seguridad Kaspersky utilizaba sistemas parecidos a los rootkits para implementar ciertas

políticas de seguridad. Por su parte Kaspersky Lab respondió a esto con un comunicado de presa negando tales acusaciones.

http://www.kaspersky.com/press?chapter=146335782&id=177718126
Kaspersky Lab responds to claims by Mark Russinovich regarding the use of rootkit technology in the company's products Mark Russinovich, an IT professional, has recently been reported as saying that Kaspersky Lab makes use of "rootkit" technology in its Kaspersky® Anti-Virus products.
Kaspersky Lab believes that the iStreams™ technology utilized in Kaspersky Anti-Virus cannot be exploited by a malicious user, and to call this technology a rootkit is incorrect.
iStreams™ technology was first implemented in the Kaspersky Anti-Virus 5.x product range almost two years ago and improves scanning performance. In basic terms, Kaspersky Anti-Virus products use NTFS Alternate Data Streams to hold checksum data about files on the user's system: if a checksum remains unchanged from one scan to another, Kaspersky Lab's products know the file has not been tampered with and do not, therefore, require a repeat scan.
NTFS Alternate Data Streams are not visible to the naked eye; special tools are required to view them. The fact that these data streams are not automatically visible does not mean technology which utilizes these streams is potentially exploitable or malicious.
Kaspersky Lab believes that the technology used is not vulnerable to exploitation for the following reasons:
1. If a Kaspersky Anti-Virus product is active, the streams are hidden and no processes (including system processes) have access to them.
2. If the product is disabled, the streams will be visible if viewed using the appropriate tools.
3. If a stream is rewritten with some (possibly malicious) data or code (for example, after rebooting in Safe Mode), when the system is next restarted, Kaspersky Anti-Virus will read the stream and not recognize the format. Kaspersky Anti-Virus will then begin to rebuild the checksum database. This means that potentially malicious code will be deleted.
Kaspersky Lab antivirus products utilize iStreams™ technology as it offers users a significant performance benefit.
The only drawback of this technology is that it increases the time taken to deinstall the product as the data streams have to be deleted. For this reason, and this reason alone, the next version of Kaspersky Anti-Virus will use an alternative mechanism to deliver the same performance benefits.
Eugene Kaspersky has commented further on this issue in the Kaspersky Lab Analyst's Diary.

Conclusión

La clasificación de los Malware queda como un tema en constante desarrollo, ya que como día a día aparecen nuevos tipos de programas maliciosos, la clasificación de los mismos debe adaptarse a estos nuevos ejemplares, que muchas veces utilizan las mismas características de varias categorías de los malware. De esta manera, el trabajo de etiquetar y catalogar las nuevas amenazas que aparecen se presenta como un gran esfuerzo que debe ser encarado con el mayor grado de objetividad y practicidad posible.

Con respecto a los esfuerzos existentes para contrarestar el efecto nocivo de los malware, es evidente que una buena educación del usuario final de los sistemas computacionales es necesario, más aún con el surgimiento de nuevas tendencias de comunicación (como las redes sociales, citadas en el informe anterior) que muchas veces dejan al usuario vulnerable a determinados ataques.

Finalmente se puede decir que hoy en día el tema del Malware es mucho más complejo que en sus inicios, ya que la motivación de estos programas maliciosos es en un 99% financiera, y en el resto de los casos se busca obtener alguna ventaja del usuario de manera ilegal.

BIBLIOGRAFÍA

- http://www.viruslist.com
- http://cme.mitre.org
- http://www.kaspersky.com
- http://es.wikipedia.org
- http://www.alegsa.com.ar
- http://www.webpanto.com
- http://www.seguridadpc.net
- http://news.softpedia.com/news/Pornware-Bad-Bad-Bad-40701.shtml