Disfrazando códigos maliciosos: Ingeniería Social apliacada al malware

Autor: Jorge Mieres, Analista de Seguridad de ESET para Latinoamérica

Fecha: Jueves 20 de septiembre del 2007

ESET, LLC 610 West Ash Street, Suite 1900
phone: (619) 876 – 5400, fax: (619) 437 – 7045
sales@eset.com, www.eset.com

Introducción

A esta altura de la batalla, está muy claro que todo el malware, desde el momento en que se presenta ante el usuario, disfruta de su esencia maliciosa de provocar algún daño o molestia en la computadora que infecta. También es muy claro, que siempre utiliza alguna técnica de Ingeniería Social[1], sin discriminar el medio por el cual se vale para su propagación y eventual infección.

Bajo esta visión, la evolución de los medios tecnológicos y la proyección que mantuvo Internet a lo largo del tiempo, auxiliaron no sólo a la masificación de nuevas tecnologías sino que también facilitaron el nacimiento de nuevos, y cada vez más sofisticados vectores de infección que hacen uso de técnicas y metodologías cada vez más difíciles de combatir, detectar y, por consiguiente, de erradicar.

Pero como sucede con la gran mayoría del malware actual, estas técnicas y metodologías de infección no representan casos de innovación en lo que a códigos maliciosos se refiere; por lo tanto, existen similitudes comunes entre todos ellos, que fundamentalmente se basan en dirigir a los usuarios menos atentos y con menos conocimientos hacia un potencial engaño. Esta última observación, constituye uno de los principales vectores y objetivos que los autores y diseminadores de este tipo de programas aprovechan, a la hora de elegir víctimas de sus creaciones.

Por otro lado, el correo electrónico, las redes de intercambio de archivos tipo P2P, sitios web y aplicaciones de mensajería instantánea, constituyen los canales más utilizados para la diseminación de cualquier tipo de código malicioso ya que estas tecnologías, por ser utilizadas en forma masiva, establecen blancos perfectos a explotar por los creadores de malware.

Sin embargo, a pesar de todos estos malos pronósticos, existen herramientas básicas y fáciles de utilizar que, sumadas a una serie de buenas prácticas, consiguen un alto grado de eficacia a la hora de hacer frente al malware.

[1] **Ingeniería Social:** Técnica que a través del engaño persigue obtener, en forma voluntaria, datos confidenciales de los usuarios.

Metodologías comunes de infección

Las metodologías más utilizadas por los códigos maliciosos, dentro de las diferentes técnicas de Ingeniería Social, son las que se fundan en la filosofía intrínseca de todo programa malicioso. Es decir, fingir ser un programa o archivo benigno, inofensivo o divertido cuando en realidad no lo es y cuya finalidad consiste en provocar daños de diferente índole y magnitud tanto a los equipos informáticos como a la información de las personas que hacen uso de esos equipos comprometidos.

En otras palabras, el principal propósito del malware es intentar infectar un equipo en forma totalmente inadvertida, "disfrazándose" con alguna extensión, icono o imagen que no represente, a la vista de los usuarios, una amenaza o un potencial riesgo de infección.

En este sentido, los programas con características maliciosas han ido creciendo no sólo en número sino también en cuanto al potencial daño que pueden producir una vez que logran infectar con éxito, un equipo o un sistema informático.

Consecuentemente, los recursos más utilizados, se centran particularmente en todo aquello que conquiste la curiosidad, que, de alguna manera, genere suficiente impacto o atractivo en los usuarios o que le infrinjan algún tipo de temor o amenaza.

Una popular frase dice que "una imagen vale más que mil palabras" y a través de la siguiente captura, se pretende dar por válido su significado mostrando, en una sola imagen, aquellas formas comunes en las cuales se disfrazan los códigos maliciosos a la hora de intentar engañar a lo que en seguridad se define como el eslabón más débil de la cadena, el usuario.

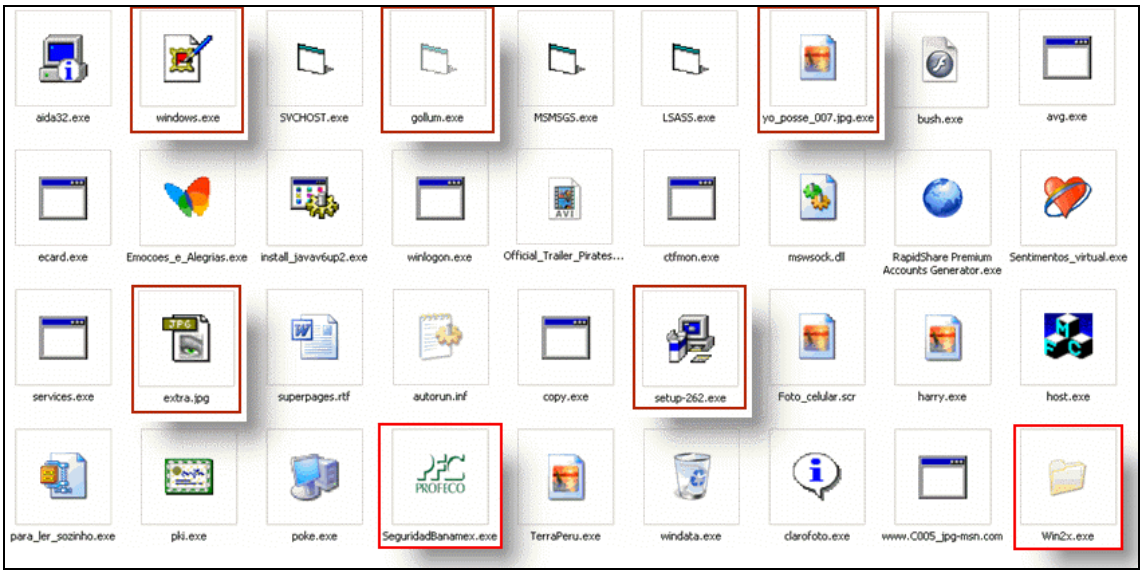

Imagen 1 – Alguna de las "formas" de malware

Se pueden encontrar algunas de las variedades de códigos maliciosos más habituales y, aunque parezca una extensa lista de variantes, estas pocas muestras constituyen una insignificante fracción de lo que realmente representa el malware a nivel mundial.

Breve análisis de los casos más comunes de encontrar

Como se anticipó en un principio, la mayoría de las infecciones provocadas por la extensa gama de códigos maliciosos se puede prevenir con simples configuraciones o herramientas que forman parte del mismo sistema operativo.

Esto de ninguna manera significa que dichas herramientas y configuraciones sean suficientes para alcanzar el grado de prevención que debería tener el equipo; sin embargo, constituyen utilidades prácticas que los usuarios pueden, y deberían, tener en cuenta al momento de verificar la integridad de aquellos archivos que sean motivo de sospechas.

A través de los siguientes ejemplos, se pretende describir casos comunes sobre aquellas formas con las que habitualmente se suelen presentar los códigos maliciosos ante los usuarios con ánimo de persuadirlos a infectar sus equipos:

- Un detalle que debería llamar poderosamente la atención, es la incompatibilidad entre los iconos y las extensiones, ya que más allá de los nombres que reciban los archivos e imágenes que tengan sus iconos, la extensión de la mayoría de los archivos es "`.exe`". No obstante, las imágenes asociadas a los mismos no son de aplicaciones válidas para la extensión que poseen. Esta es una característica que, a priori, indica que se está frente a un potencial riesgo de infección.

Imagen 2 – Incompatibilidad entre iconos y extensiones

- Sin embargo, en muchos casos, los creadores de estos particulares programas maliciosos acuden a otros tipos de ardides para aspirar a una "exitosa" infección. Un común ejemplo de ello lo constituyen los archivos que poseen atributos de "`oculto`" en donde con sólo seleccionar la opción "`Mostrar todos los archivos y carpetas ocultos`" del menú "`opciones de`

carpeta", se pueden visualizar aquellos archivos que gozan de estas particularidades, evitando que se infiltren en el equipo en forma totalmente subrepticia.

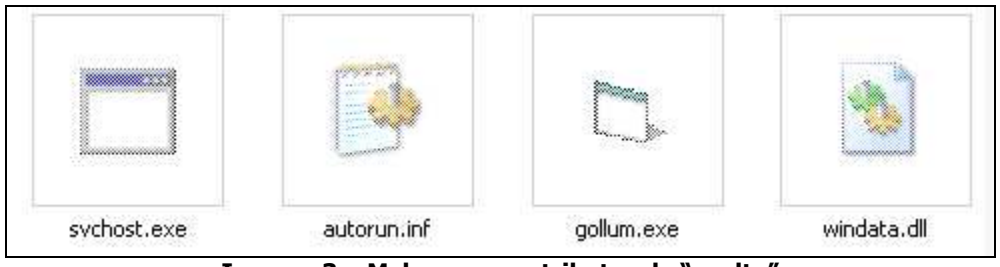

Imagen 3 – Malware con atributos de "oculto"

- Otro recurso muy empleado, es utilizar archivos con doble extensión. Su funcionamiento básicamente se concentra en simular una extensión asociada a la imagen de su icono. Los archivos están formados por un nombre y una extensión que se separan a través de un punto ".";
de esta manera se puede formar el nombre de un archivo ejecutable ".exe" incorporando en el mismo nombre del archivo la falsa extensión; por ejemplo, *mis_fotos.jpg.exe*. Si se tiene habilitada la opción "ocultar las extensiones de los archivos para tipos de archivos conocidos", el código malicioso con doble extensión pasaría desapercibido como si se tratase de un archivo genuino. Acorde al primero de los ejemplos, un archivo de MS Word cuando en realidad se trata de un programa dañino.

Imagen 4 – Malware con doble extensión

- Códigos maliciosos más "elaborados" fusionan eficazmente la imagen del icono con la extensión utilizada, logrando un efecto mucho más inteligente y mucho más peligroso para los usuarios menos experimentados. En estos casos, con sólo renombrar el archivo sospechoso con la extensión .txt *(bloc de notas)* se puede precisar, a través de su identificador (headers), si la extensión mostrada corresponde al archivo que aparenta ser. Este identificador no es variable, por lo que para los archivos con extensión `.exe` el identificador es siempre `MZ`, tal como se aprecia en la imagen.

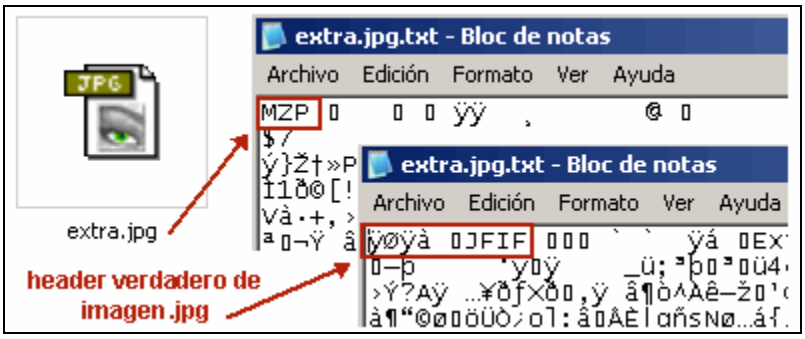

Imagen 5 – Identificadores de archivos

Si bien esta sencilla manera de verificar los archivos es muy útil para establecer rápidamente y con precisión si tal archivo constituye una amenaza para un sistema, en muchos casos no será válida su utilización.

La peligrosidad de sencillas técnicas

Dejando a un costado la generalidad de estas metodologías, se intentará focalizar la atención en la particularidad que presenta el tipo de técnica que se muestra en la siguiente imagen:

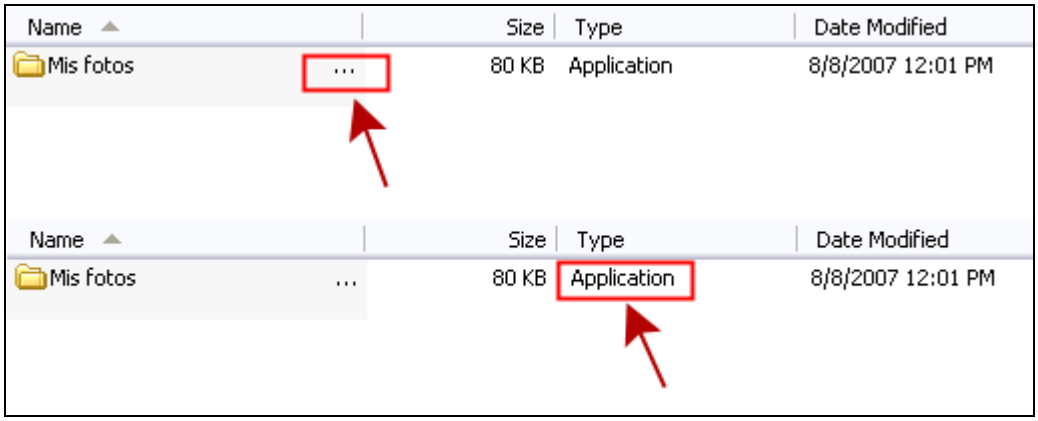

Imagen 6 – Malware simulando ser una carpeta

En este punto, es necesario aclarar que la estructura de toda carpeta en un sistema Windows está formada por un nombre, mientras que los archivos, como se mencionó líneas arriba, están formados por una identificación (el nombre del archivo) más una extensión (formada por tres caracteres) que establece el programa asociado a ese archivo en particular.

En este caso, los tres puntos marcados indican que el nombre de esa supuesta carpeta continúa. En este sentido, una buena recomendación es visualizar los archivos en modo "`detalle`", lo que se consigue configurándolo desde el menú "`ver`". Con esta opción, es posible visualizar, rápidamente, una serie de datos relacionados al archivo en cuestión, como por ejemplo: su peso, los datos de creación y el tipo de archivo.

La columna referida a "`tipo de archivo`" es muy importante, ya que muestra la verdadera asociación del archivo. Como se observa en la imagen, se trata de una "`aplicación`", por ende, haciendo doble clic sobre la supuesta carpeta se estará activando en realidad un archivo ejecutable, en este caso, un malware.

Otra posibilidad, es extender la columna de visualización. Con esta acción se logrará observar el nombre completo del archivo, pudiendo de esta manera, apreciar su verdadera extensión. Tal como se observa en la siguiente imagen:

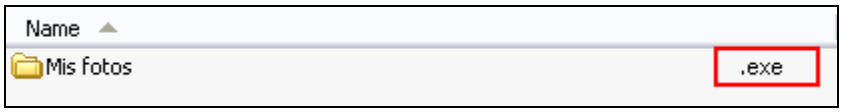

Imagen 7 – Extensión real del archivo

Esta metodología de engaño suele, lamentablemente, tener serios efectos que muchas veces son difíciles de evitar y, que en la mayoría de los casos, logra concretar el objetivo de sus autores: comprometer el equipo a través de la infección provocada por el malware.

Esto se debe a que cualquier usuario puede ejecutar involuntariamente este tipo de archivos. Por tanto, estos engaños son un factor a tener en cuenta, sobre todo por aquellos usuarios que forman parte de redes corporativas ya que, en forma inconsciente pueden comprometer, no sólo su equipo, sino toda la red.

En este aspecto, resulta de capital importancia el nivel de conocimientos que posean los usuarios, ya que a través del conocimiento se obtiene un importante horizonte de prevención al adquirir buenos hábitos o "buenas practicas".

El correo electrónico como vía de infección

Cualquiera de las metodologías aplicadas a la simulación de archivos que hasta aquí fueron presentadas, suelen ser utilizadas en combinación para su diseminación con cualquiera de los medios masivos de comunicación.

En este aspecto, el correo electrónico constituye uno de los canales de comunicación elegidos por los delincuentes informáticos debido a la instantaneidad con que se distribuyen los mensajes, sin mencionar su facilidad de uso.

Durante el 2007, se vienen experimentando casos de masiva recepción de mensajes de correo electrónico en los que un archivo adjunto contiene la publicidad de determinados productos; siendo esto un claro ejemplo de hasta dónde es capaz de llegar la imaginación de los delincuentes informáticos en pos de evadir los controles y filtros de seguridad.

A modo de ejemplo, se pueden citar dos de los casos más comunes y representativos de la utilización del correo electrónico como vía de infección.

En primer lugar, una metodología bastante antigua que consiste en la recepción de correos electrónicos con archivos maliciosos adjuntos al mensaje; y en segundo lugar, la descarga de archivos maliciosos a través de enlaces incrustados en el cuerpo del correo electrónico donde diferentes tipos de malware aprovechan de forma activa y eficaz.

A través de la siguiente imagen se puede advertir un ejemplo de esta metodología de infección:

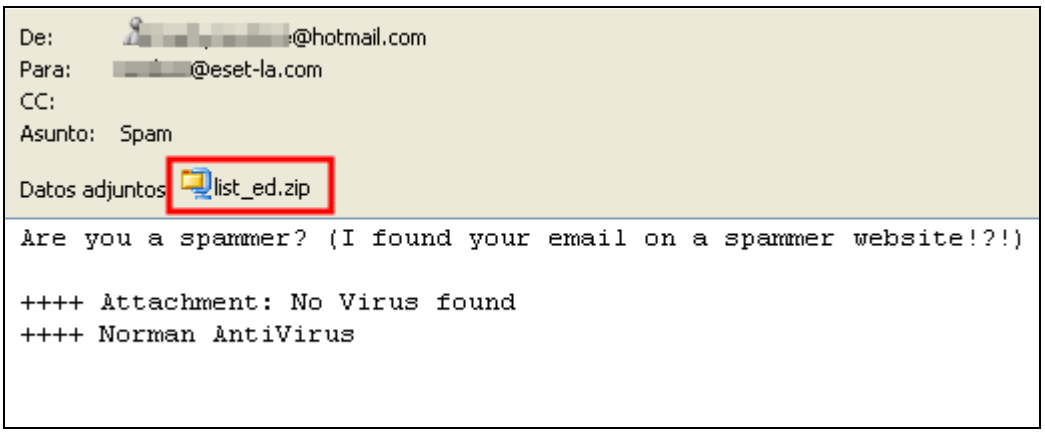

Imagen 8 – Correo malicioso con archivo adjunto

Básicamente, en estos casos el correo electrónico de tipo spam, llega a la casilla del destinatario conteniendo un archivo adjunto (el malware) con un asunto y mensaje lo suficientemente astuto como para lograr que la potencial víctima, al verse tentada por la curiosidad o por el interés en el asunto y el mensaje (Ingeniería Social), ejecute el archivo que acompaña al correo; es decir, que ejecute el código malicioso.

Conforme al ejemplo, otra de las metodologías de engaño utilizadas en este aspecto esta constituida por aquella que intenta convencer al usuario de hacer clic sobre un enlace incrustado en el cuerpo del mensaje, nuevamente se recurre a la Ingeniería Social. Tal como se aprecia en la siguiente imagen:

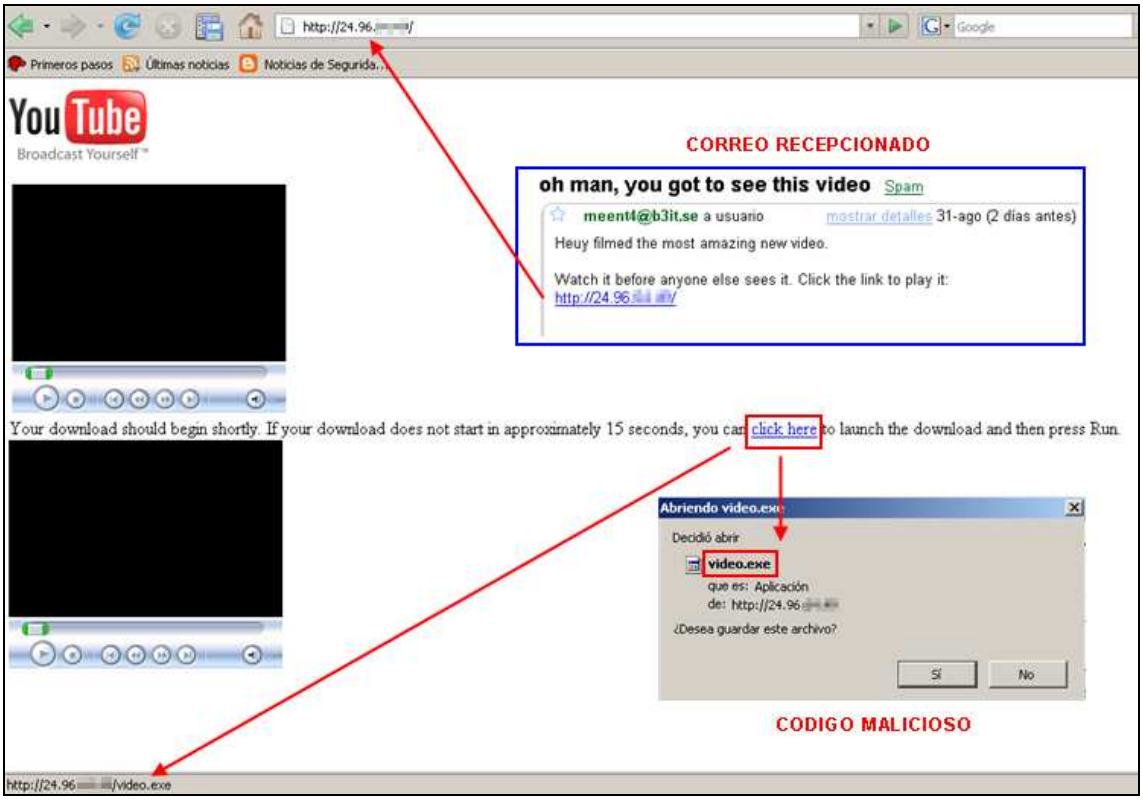

Imagen 9 – Correo electrónico con enlace incrustado

En esta oportunidad, el diseminador malicioso ofrece al usuario un enlace ubicado en el cuerpo del mensaje desde el cual se podría observar un supuesto video, pero que en realidad, el enlace redirecciona

al usuario hacia la descarga de un archivo ejecutable: el malware que se intenta diseminar a través de esta metodología.

Si bien en ambos casos la técnica empleada es la misma (Ingeniería Social), las metodologías utilizadas difieren en cuanto al modo de aplicarlas. Sin embargo, coinciden en el intento por intimar a los usuarios para que descarguen el código malicioso, ya sea a través de un archivo adjunto o por intermedio de un vínculo incrustado en el cuerpo del correo electrónico.

Clientes de Mensajería Instantánea como medios de transmisión del malware

De la misma manera que sucede con los mensajes de correo electrónico, las aplicaciones de mensajería instantánea tales como *Yahoo Messenger y MSN Messenger/Windows Live Messenger* conforman otro importante grupo de vectores que habitualmente son explotados con fines maliciosos.

En relación con ello, durante este año vienen proliferando aquellos códigos maliciosos que utilizan este tipo de programas para distribuirse masivamente, alcanzando picos de infección realmente preocupantes en Latinoamérica.

En la mayoría de los casos, resultan ser variantes de otros códigos maliciosos que atacantes con menos conocimiento modifican para intentar engañar con nuevos artilugios a aquellos usuarios menos atentos o menos informados.

En este aspecto, el objetivo que se persigue con la constante modificación en sus códigos apunta a evadir la detección de los programas antivirus con capacidades de heurísticas débiles.

Diferentes tipos de códigos maliciosos como la familia de troyanos IRCBot y SdBot, buscan constantemente reclutar computadoras zombies[2] para alimentar sus botnets[3] logrando la infección de un número alarmante de equipos informáticos a nivel mundial durante el último tiempo.

En estos casos de propagación de códigos maliciosos a través de clientes de mensajería instantánea, la metodología empleada para diseminar los archivos maliciosos es básicamente similar a la empleada para los casos de correo electrónico.

---

[2] **Zombie:** Computadora que, luego de haber sido infectada por un malware, puede ser utilizada en forma remota por un atacante.
[3] **Botnet:** Red de robots. Conjunto de computadoras infectadas por algún malware que son utilizadas para realizar ataques en forma distribuida.

Es decir, un equipo comprometido envía mensajes maliciosos a cada uno de los contactos que encuentre en la computadora víctima, siempre sin que el usuario se percate al respecto.

En este punto, son dos las metodologías que comúnmente utiliza este tipo de malware. Por un lado, el mensaje malicioso puede contener una simple dirección web acompañada de un llamativo mensaje mediante el cual, en caso de tener el sistema operativo desactualizado, explota alguna vulnerabilidad por la que se ejecuta e instala de forma totalmente transparente, infectando en cuestión de segundos, el equipo del usuario desprevenido. Todo ello con sólo hacer clic sobre el enlace.

Imagen 10 – Mensaje malicioso con enlace incrustado

Por lo general, la página web maliciosa contiene en su código fuente un script ofuscado en el cual se encuentra el exploit que aprovecha la vulnerabilidad del sistema, permitiendo que el malware se ejecute en la computadora víctima.

Por otro lado, también mediante un mensaje malicioso que se envía a todos los contactos desde un equipo comprometido por el malware, se intenta persuadir al usuario de que descargue un archivo que supuestamente contiene algo llamativo para el común de los usuarios, por lo general algunas supuestas fotografías o algún atractivo juego.

Imagen 11 – Mensaje malicioso invitando a descargar el código malicioso

Para cualquiera de los casos, el malware intentará engañar al usuario mediante alguna técnica de Ingeniería Social que logre acaparar la atención de los usuarios curiosos para que lo descarguen; y respetando su condición de engañador y malicioso, será disfrazado de igual forma que cualquiera de los ejemplos antes expuestos.

Diseminación de programas maliciosos a través de redes P2P

Las redes de intercambio de archivo se han vuelto muy populares y en la actualidad constituyen otra de las fuentes más importantes, peligrosas y explotadas para la distribución de códigos maliciosos disfrazados de cualquier otro tipo de archivos.

El peligro principal que existe entre la relación de las redes P2P y los códigos maliciosos, se centra básicamente en el engaño a través de los diferentes nombres de archivo que se ponen a disposición para que los usuarios puedan descargar.

Bajo esta situación, conviven en un mismo ecosistema infinidad de posibilidades que los creadores y distribuidores de malware pueden manipular para concretar con éxito infecciones y diseminación a granel de todo tipo de códigos maliciosos utilizando simples metodologías.

Por otro lado, además de esta situación, otro gran peligro contemplado en las aplicaciones de intercambio de archivos (como por ejemplo BitTorrent, eMule, Imesh, KaZaa, entre muchas otras) es que en sus versiones gratuitas se suele incorporar algún código malicioso, por lo general del tipo adware y/o spyware que se instalan junto al programa P2P.

En este escenario, también se encuentra que la mayoría del malware suele incorporar en su código, módulos de ataque que le permiten realizar diferentes tareas; como por ejemplo crear, bajo diferentes nombres y tipos de archivos simulados, copias de sí mismo en las carpetas compartidas que por defecto son creadas por los programas P2P al momento de ser instalados.

Esto, puede que constituya una de las principales razones por la que gusanos ya antiguos como el Netsky (aparecido durante el 2004) se sigan propagando e infectando con un alto porcentaje de actividad.

Nombre	Tamaño	Tipo
Magix Video Deluxe 5 beta.exe	29 KB	Aplicación
Matrix.mpg.exe	29 KB	Aplicación
Microsoft Office 2003 Crack b...	29 KB	Aplicación
Microsoft WinXP Crack full.exe	29 KB	Aplicación
MS Service Pack 6.exe	29 KB	Aplicación
netsky source code.scr	29 KB	Protector de pantalla
Norton Antivirus 2005 beta.exe	29 KB	Aplicación
Opera 11.exe	29 KB	Aplicación
Partitionsmagic 10 beta.exe	29 KB	Aplicación
Porno Screensaver britney.scr	29 KB	Protector de pantalla
RFC compilation.doc.exe	29 KB	Aplicación
Ringtones.doc.exe	29 KB	Aplicación
Ringtones.mp3.exe	29 KB	Aplicación
Saddam Hussein.jpg.exe	29 KB	Aplicación
Screensaver2.scr	29 KB	Protector de pantalla
Serials edition.txt.exe	29 KB	Aplicación
Smashing the stack full.rtf.exe	29 KB	Aplicación
Star Office 9.exe	29 KB	Aplicación
Teen Porn 15.jpg	29 KB	Acceso directo al pr...
The Sims 4 beta.exe	29 KB	Aplicación
Ulead Keygen 2004.exe	29 KB	Aplicación
Visual Studio Net Crack all.exe	29 KB	Aplicación
Win Longhorn re.exe	29 KB	Aplicación
WinAmp 13 full.exe	29 KB	Aplicación
Windows 2000 Sourcecode.d...	29 KB	Aplicación
Windows 2003 crack.exe	29 KB	Aplicación
Windows XP crack.exe	29 KB	Aplicación

Imagen 12 – Archivos maliciosos creados en la carpeta compartida del programa P2P

En la imagen, se muestra que los archivos creados en la carpeta compartida hacen uso de las técnicas explicadas en este artículo, como lo es la utilización de nombres de archivos llamativos, doble extensión, etc.

Contramedidas

A modo de lección y revisión, se propone una serie de pautas que ayudarán a todos los usuarios a crear nuevos y buenos hábitos para evitar una infección:

- Tener precaución al manipular archivos de procedencia dudosa verificando en cada uno de ellos, a priori y en forma visual, si la extensión es acorde al programa supuestamente asociado al archivo.
- Seleccionar la opción "`Mostrar todos los archivos y carpetas ocultos`" para evitar que archivos con atributos de oculto puedan inyectarse en el equipo de forma transparente.
- No seleccionar la opción "`ocultar las extensiones de los archivos para tipos de archivos conocidos`". Esto permitirá visualizar sin problemas, aquellos archivos que con doble extensión intenten pasar desapercibidos.

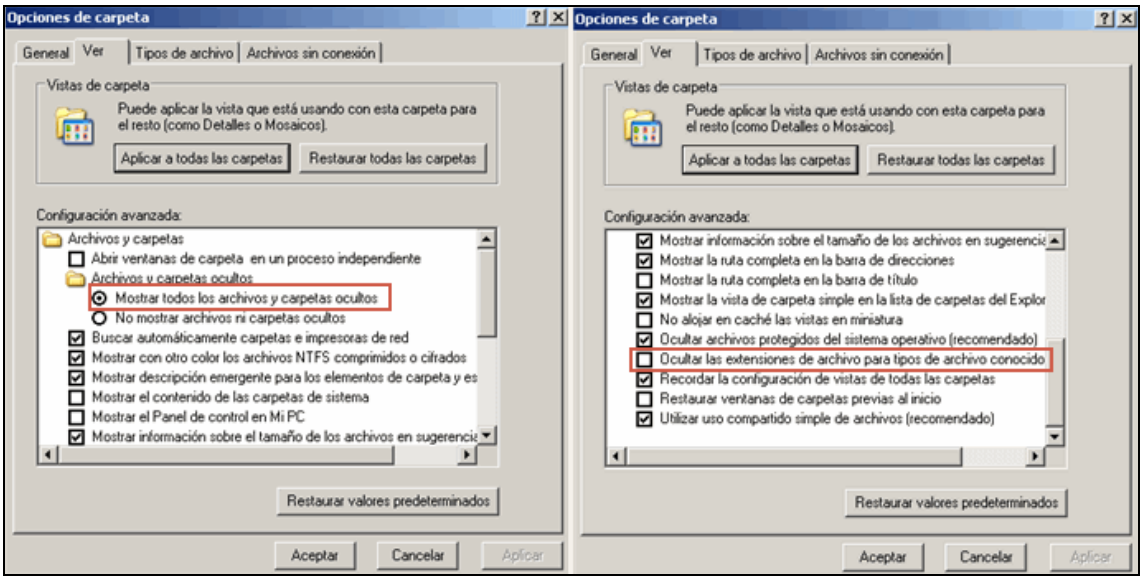

Imagen 13 – Configuraciones recomendadas para la visualización de archivos y extensiones

- La utilización del bloc de notas puede, en muchos casos, ayudar a visualizar el tipo correcto de un archivo dañino, tal y como se explicó anteriormente.

- Visualizar los archivos en modo "`detalle`" también forma parte de las sencillas configuraciones del sistema que se pueden utilizar.

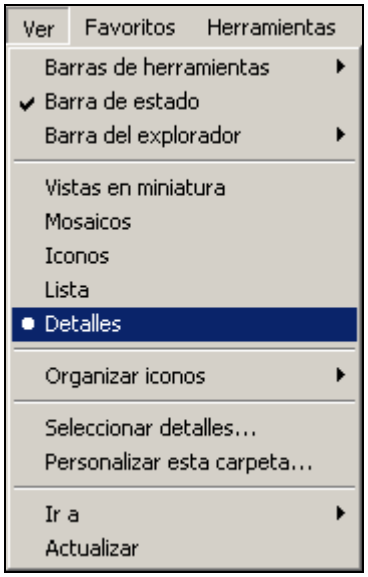

Imagen 14 – Mostrar información detallada de los archivos y carpetas

- Con relación a los programas de mensajería instantánea, jamás hacer clic sobre enlaces que acompañen a mensajes en otros idiomas o de los cuales se desconoce o se duda de su procedencia.
- De igual manera, se debe proceder en caso de recibir enlaces a través del correo electrónico.

- En relación con esto, una muy buena medida de prevención radica en, antes de hacer clic sobre el enlace, pasar el mouse sobre el mismo y verificar que en la barra de estado aparezca la dirección que propone el mensaje (ver imagen 15).

Imagen 15 – Redireccionamiento a página web falsa

- Se recomienda no ejecutar archivos que se reciban a través de programas de mensajería instantánea.
- Es aconsejable, preguntar al contacto que envía un enlace o archivo, si efectivamente está realizando dicha acción.

- Se recomienda no ejecutar archivos que a través de cualquiera de estas vía se reciba, contemplándose el mismo criterio para el correo electrónico.
- Verificar el origen de los archivos recibidos, tanto por clientes de mensajería instantánea como por correo electrónico y así también, que se encuentren libres de malware, mediante un producto antivirus con capacidades de detección proactiva como ESET NOD32.
- Eliminar el spam y tener la precaución de nunca contestar alguno de ello, esto evita confirmar la existencia de la dirección de correo.
- En cuanto a las redes P2P es importante que sus usuarios sean lo suficientemente precavidos al descargar archivos, ya que es muy normal que usuarios malintencionados “disfracen” código malicioso para simular ser programas o archivos muy buscados.
- También en cuanto a las redes P2P, verificar que sólo se estén compartiendo aquellos archivos y carpetas que se desee compartir.
- Observar el tamaño del archivo que se descarga, verificando que el peso del mismo sea razonable y acorde con lo que se pretende descargar. Si lo que se busca es un archivo .avi (película) pero el archivo que se esta descargando pesa sólo unos cuantos Kilo bites (KB) se debería sospechar de él, ya que puede estar tratándose de un malware.
- Implementar una solución antivirus con altos niveles de detección proactiva gracias a la Heurística Avanzanda. Mantenerlo actualizado del mismo modo que debería mantenerse actualizado el sistema operativo, para evitar que programas maliciosos exploten vulnerabilidades conocidas en el sistema.
- Por último, configurar al antivirus para que verifique la totalidad de los archivos que se descargan a través del correo electrónico, aplicaciones de mensajería instantánea y redes de intercambio de archivos.

Conclusión

En la actualidad, cualquier sistema informático es susceptible de sufrir el ataque de alguna variedad de código malicioso ya que, sin lugar a dudas, existen sistemas operativos y aplicaciones con más riesgos que otras debido a su mayor utilización en el mercado; lo que las convierte en atractivos blancos para los creadores de este tipo de amenazas.

Por otro lado, cualquiera de las situaciones planteadas fundamentan el importantísimo rol que juegan las acciones llevadas a cabo por una herramienta antivirus, ya que estas soluciones poseen una presencia primordial y necesaria para mantener cualquier sistema libre del alcance de los códigos maliciosos, sobre todo, soluciones como ESET NOD32 que utilizan técnicas de detección avanzada a través de una heurística inteligente, evitando que códigos maliciosos conocidos y desconocidos manipulen impunemente un sistema informático.

Resulta igualmente importante, mantener actualizado el antivirus, como así también el sistema operativo y cualquier aplicación que se encuentre instalada en la computadora.

Según lo analizado, se puede ver como los creadores de malware pueden ocultar o disfrazar sus creaciones en casi cualquier tipo de archivos o programas, generando de esta manera un sin número de posibilidades en cuanto a metodologías y técnicas que les permitan elaborar, con mayor eficacia, las tácticas tendientes a lograr sus objetivos de infección.

Cabe destacar el hecho de que si no se conjugan el conocimiento con un software antivirus de detección proactiva como ESET NOD32 para mantener un sistema informático fuera del alcance de códigos maliciosos, difícilmente se logrará incorporar el hábito necesario que permita evitar la proliferación y eliminación de toda forma de amenazas informáticas.

Más información:

Plataforma Educativa de ESET Latinoamérica
http://edu.eset-la.com/

Blog del laboratorio de ESET Latinoamérica
http://blogs.eset-la.com/laboratorio