

Informe sobre malware en América Latina



Autor: Laboratorio de ESET para Latinoamérica
Fecha: Jueves 14 de febrero del 2008

Objetivos del Laboratorio de ESET para Latinoamérica

ESET cuenta con un Laboratorio de investigación y análisis de malware en sus oficinas de América Latina, el cual recibe constantemente distintas muestras de códigos maliciosos provenientes de usuarios de Internet.

La importancia del Laboratorio en América Latina radica en la focalización del análisis de muestras específicas de la región, lo que genera una mayor cobertura y velocidad de detección de códigos maliciosos que tienen como objetivo a los usuarios de habla hispana.

Durante el 2007, las amenazas en el idioma en español y completamente focalizadas en América Latina se masificaron, y por eso cobra aún más importancia la localización de un laboratorio de investigación, ya que genera tiempos de respuesta mucho menor.

La conjunción entre el Laboratorio de virus de ESET ubicado en Eslovaquia y los Laboratorios de Investigación de América Latina y Gran Bretaña, logran mejorar constantemente tanto la velocidad de generación de nuevas firmas específicas -firmas genéricas para una base de códigos maliciosos de funcionamiento similar- como la de los métodos de detección proactiva a través de la Heurística Avanzada de ESET NOD32 Antivirus y ESET Smart Security.

Además, el Laboratorio latinoamericano es una constante fuente de generación de contenido informativo a través de sus artículos técnicos y en el Blog del Laboratorio, en donde se escribe sobre distintas amenazas informáticas, las principales técnicas y en donde también se apunta a explicar el funcionamiento del malware intentado educar a los usuarios.

Este informe tiene como objetivo analizar las tendencias y las técnicas utilizadas por los códigos maliciosos recibidos durante el 2007 en el Laboratorio de América Latina. Para ello, es necesario aclarar primero que se considera una muestra a cualquier archivo dañino que es reportado al Laboratorio y analizado posteriormente para determinar si debe ser detectado como malware por las soluciones de ESET.

Se debe tener en cuenta que en este reporte estadístico sólo se contemplan archivos ejecutables (DLL, EXE, SCR, etc.) sin considerar los lenguajes de script (como JS ó VBS) de programación web como HTML, ya que estos, en última instancia, descargan un archivo ejecutable al equipo del usuario.

Si se contemplaran los lenguajes web, sin duda la situación sería totalmente distinta, ya que las infecciones por esta vía se han transformado en una de las formas más importantes de propagación y de las principales tendencias futuras [1].

Ingeniería Social

La gran diversidad y cantidad de metodologías de ataque y canales de infección utilizados por los creadores de malware durante el año 2007, comparten una serie de características que, mediante el engaño al usuario, logran instalar a una amplia variedad de malware en los equipos de los usuarios.

El principal factor, que por lo general comparte el malware, es la utilización de metodologías de Ingeniería Social [2] al momento de llevar a cabo su propagación y concretar sus infecciones.

Estos factores pueden ser discriminados dependiendo de las particularidades propias de los códigos maliciosos, desprendiendo así, por un lado, información particular de cada uno de ellos; y por otro lado, información general que en definitiva permite describir las características más comunes del malware.

Tipos de engaños utilizados

A continuación se muestran los distintos tipos de engaños utilizados durante 2007 por el malware según las muestras recibidas en el Laboratorio de América Latina. Cada uno de estas llegaba al usuario a través de un correo electrónico que lo incitaba a descargar algún tipo de archivo dañino.

Estas son las fechas aproximadas de aparición y no significa que este tipo de engaños se haya dejado de utilizar, simplemente muestran la evolución y perfeccionamiento de los mismos.

Tipo de engaño	Periodo
Noticias actuales / Miedo	Diciembre 2006 – Mayo 2007
Tarjetas de felicitaciones	Junio – Agosto
Tarjetas virtuales	Agosto
Soporte Técnico	Agosto
Programa Beta tester	Agosto
Videos	Agosto – Septiembre
Eventos	Septiembre (National Football League)
Descarga de juegos	Septiembre – Octubre

Es interesante notar que la mayoría de estas técnicas han sido explotadas por el gusano Nuwar (también conocido por gusano Storm), en algún momento del año. Más información disponible en:

<http://blogs.eset-la.com/laboratorio/2007/07/20/tarjetas-virtuales-nuwar/>

Tipos de amenazas

Desde un punto de vista general, los troyanos fueron los más propagados durante el 2007 con casi el 60% del total, agrupando a distintas variantes tales como:

- **Troyano Downloader:** troyano que descarga otros malware luego de la instalación en el sistema
- **Troyano Keylogger:** troyano que registra las teclas pulsadas para enviar la información al creador del malware
- **Troyano Banker:** troyano destinado a robar información privada del usuario, generalmente relacionada con cuentas bancarias
- **Troyano Clicker:** troyanos responsable de simular clics en sitios de publicidad
- **Troyano Bot:** los troyanos botnets, son utilizados para controlar al equipo infectado y crear redes de equipos zombis (botnets).

Ocupando el segundo puesto de los códigos maliciosos más propagados, se encuentran los programas tipo adware y spyware, ambos con casi el 20% de la totalidad. En este sentido, el adware **Virtumonde**, que posee funcionalidades típicas de spyware, es uno de los más representativos del año. Un estudio de este adware fue publicado por ESET en noviembre del 2007 [3].

Debe prestarse especial atención ante este tipo de amenaza, ya que muchas veces los usuarios no reportan el adware para su detección, debido a que millones son infectados con este tipo de archivos, pero desconocen esta situación. Esto se debe a la forma de actuar que poseen y a que suelen modificar zonas del sistema a los que el usuario promedio no conoce cómo acceder.

En tercer lugar, los gusanos son los códigos maliciosos de más propagación con el 16% del total, y la familia de gusanos Nuwar fue la más propagada durante el año, valiéndose de las técnicas de Ingeniería Social continuamente actualizadas.

El último lugar es ocupado por los virus propiamente dichos, con una cifra sumamente baja (4%) si es comparado con los otros malware representados en la imagen. Si bien poseen un bajo porcentaje no por ello dejan de ser peligrosos y de hecho, en el último semestre, un virus con capacidades polimórficas bautizado por ESET con el nombre de **Virut**, fue la prueba de que no han desaparecido.

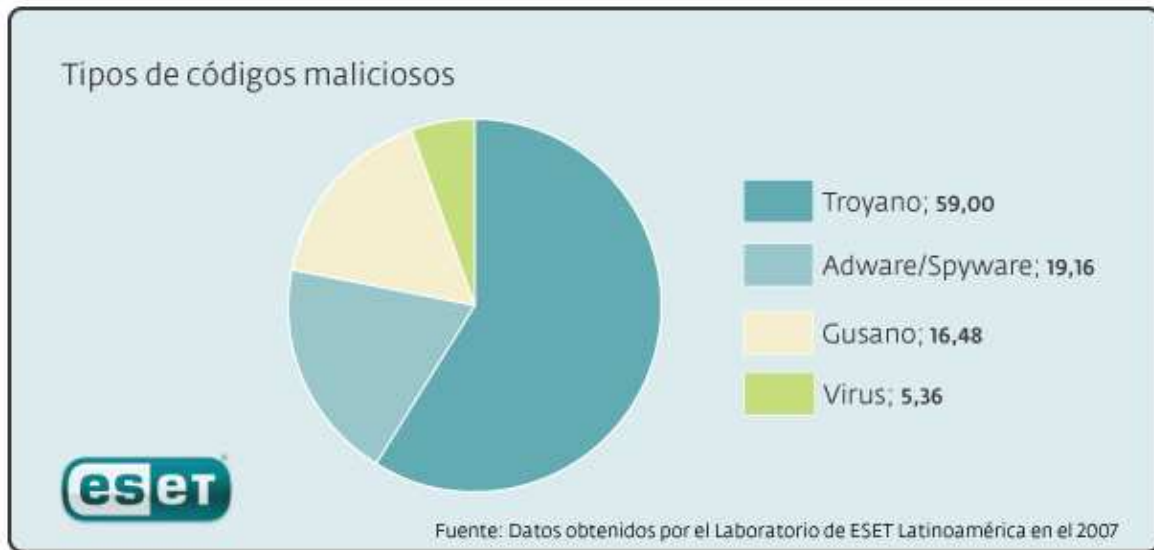


Gráfico 1 – Tipos de Códigos Maliciosos

Tamaño de archivos maliciosos

En lo que respecta al tamaño de los archivos propagados e identificados como malware, este peso oscila entre los 3KB y los 7.0 MB y por supuesto, las funcionalidades son distintas en cada caso contemplado. El promedio se establece en los 260 KB que coincide con el tamaño de la mayoría de los archivos dañinos recibidos por spam.

Por ejemplo, el tamaño del gusano Nuwar es aproximadamente 111 KB, por su parte el del adware Virtumonde oscila en los 130 KB dependiendo las variantes de cada uno.

En el caso de los virus, hay que tener en cuenta que los mismos infectan archivos genuinos del sistema, agrandando el tamaño del archivo original, pero generalmente el tamaño del virus en sí mismo raramente supera los 20 KB. A modo de ejemplo, el virus Virut anteriormente mencionado tiene un tamaño promedio de 13 KB según la versión.

Lenguajes de programación

Los lenguajes de programación elegidos por los autores de malware para la región, siguen siendo los más comunes que pueden encontrarse actualmente en el marco mundial.

El lenguaje de programación Visual Basic es el más elegido, ya que el 51% de los creadores de malware lo prefieren. Esto se asocia directamente con la cantidad de troyanos imitadores que simplemente son copias modificadas de otros códigos maliciosos. Por otro lado, el lenguaje Borland Delphi logra un 30% del total.

En cambio, la familia de lenguaje C se ubica tercero con el 15% y más abajo aparecen el Assembler y otros lenguajes menos comunes.

Empaquetadores (packers)

Con respecto a los empaquetadores [3] -es decir, a la compresión de los archivos ejecutables maliciosos- del análisis se desprende que UPX (Ultimate Packer for eXecutables) sigue siendo el empaquetador más elegido por los distribuidores de malware con un 40% de las muestras recibidas por el Laboratorio latinoamericano. Esto se debe a su característica de Open Source y a las posibilidades de modificación que ofrece el código fuente.

Otros empaquetadores conocidos y muy utilizados por los creadores de códigos maliciosos son: PECompact y ASPack con 9% de las detecciones cada uno, Yoda's Protector y tElock con el 5%, y MEW con el 4%.

Themida con el 11% de las detecciones, es uno de los empaquetadores comerciales más conocidos y si bien fue desarrollado con el fin de proteger software comercial, lamentablemente sus versiones crackeadas y pirateadas son utilizadas para empaquetar malware, dificultando la tarea de los laboratorios antivirus.

El resto de los archivos analizados han sido comprimidos con diferentes empaquetadores menos conocidos, los cuales pueden apreciarse en el siguiente gráfico:

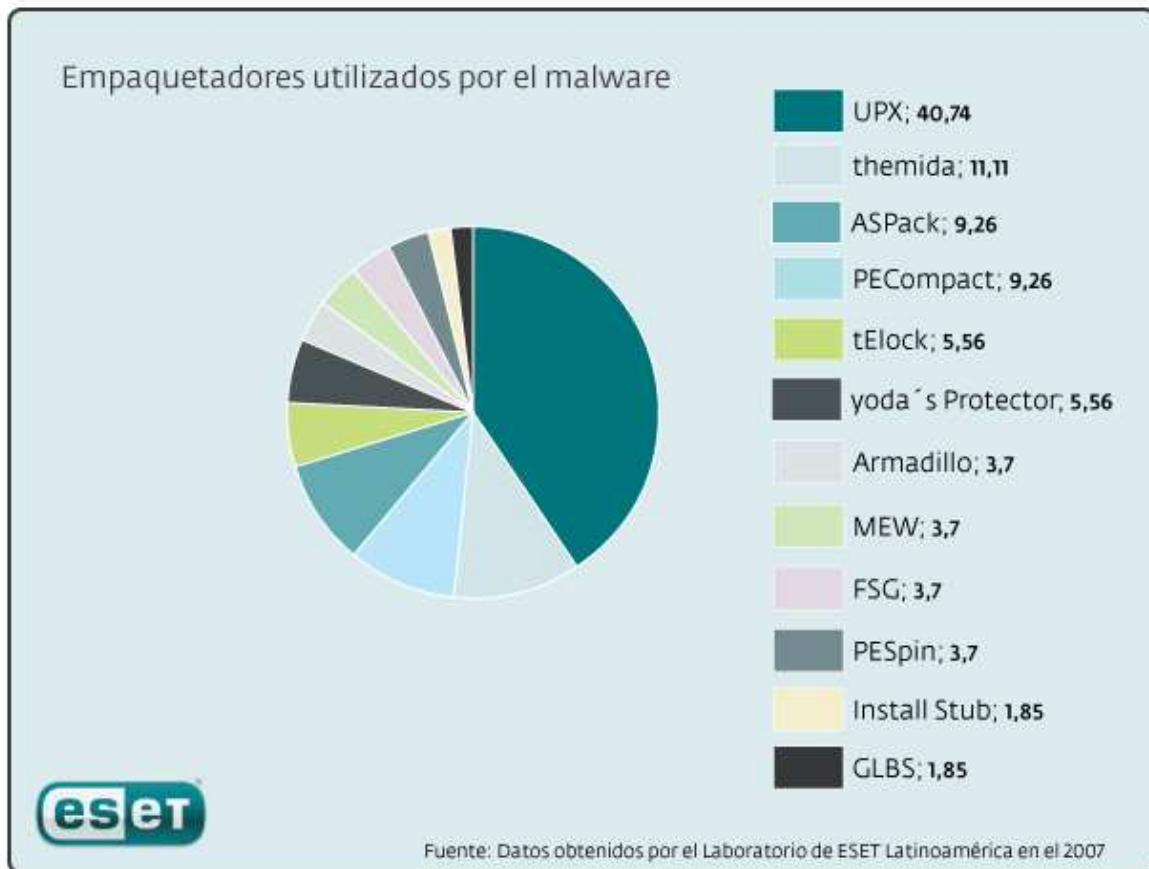


Gráfico 2 – Empaquetadores utilizados por el Malware

Es interesante remarcar que el 66% del malware analizado no se encontraba empaquetado, lo que confirma una tendencia importante de los autores a maximizar las creaciones en el menor tiempo posible sin importar el tamaño de los mismos.

Artículos técnicos y Análisis de Malware

El Laboratorio de ESET para Latinoamérica proporciona material diariamente a través de su Blog de Laboratorio (blogs.eset-la.com/laboratorio), que puede ser utilizado para prevenirse de los nuevos ataques o de las nuevas técnicas de ataque que evolucionan constantemente.

La idea del Blog de Laboratorio es informar sobre los malware en general, pero a su vez que sirva como una herramienta de educación y capacitación para sus lectores sin importar su nivel de conocimiento.

Además, ESET publica mensualmente artículos variados, entre los que se destaca el análisis de malware. Todo el material es publicado en la sección de Artículos del sitio de ESET para América Latina [5].

Tanto los artículos de ESET como su Blog de Laboratorio son de contenido técnico, pero escritos de forma sencilla para que la explicación sobre el funcionamiento del malware y sus técnicas de ataque sean comprendidas por todos los usuarios, ya que la capacitación y el conocimiento en estos tópicos son una herramienta fundamental para prevenirse de las amenazas informáticas.

Otros análisis

Dado que no todo concluye en la creación y posterior difusión del malware, es interesante destacar que uno de los principales objetivos del mismo está orientado a la formación de redes botnets y también al robo de información personal como nombres de usuario, contraseñas, números de tarjetas de crédito; entre otras.

Los ataques de phishing son, en general, cada vez más comunes y frecuentes y particularmente en Latinoamérica, se han vuelto moneda corriente por lo que cotidianamente se valen de diferentes metodologías, siempre orientadas al robo de información privada.

El pharming local –tipo de ataque que permite redireccionar un nombre de dominio a una IP distinta de la original modificando el archivo hosts del sistema- es uno de los ataques más utilizados para el robo de datos personales del usuario.

Los nombres e iconos elegidos para diseminar los códigos maliciosos son una característica fundamental del malware actual y que, como se mencionó al comienzo del documento, forman parte de la Ingeniería Social aplicada por los creadores de malware.

Durante el año 2007 el tiempo de respuesta de ESET fue variando entre 1 y 32 horas luego de que el malware comenzara su propagación. Es importante destacar que, en promedio, ESET no superó, en el 95% de los casos 24 hs para agregar un código malicioso a su base de firmas.

Conclusiones

Contar con un Laboratorio latinoamericano es algo que le viene permitiendo a ESET brindar una rápida respuesta a los incidentes reportados por los usuarios de Internet de la región, acelerando los procesos de detección del nuevo malware que aparece diariamente y brindando una veloz solución a los reportes recibidos.

Asimismo, permite ver cuál es la realidad latinoamericana de cerca, analizando las diferencias que pudieran existir con el resto de las regiones. Estos resultados, sumados a los reportes de ThreatSense.Net, permiten contar con la información necesaria para brindar la mejor protección posible a los usuarios locales.

Aunque se notan algunas diferencias con el malware que se reporta en otras regiones del mundo, las muestras analizadas demuestran que los principales vectores de ataque locales, así como los mundiales, están relacionados con la Ingeniería Social.

Entre lo reportado al Laboratorio latinoamericano, un alto porcentaje fue detectado directamente por ESET a través de firmas genéricas y heurística, lo que remarca la necesidad de contar con protección proactiva para lograr un alto nivel de seguridad contra el malware en la actualidad.

Brindar la más alta calidad tecnológica en detección de malware así como también ser una fuente de información confiable, son parte de los objetivos primordiales de ESET, y es por esto que el Laboratorio latinoamericano se suma a las iniciativas de ESET en materia de educación y divulgación con el fin de poder proveer las mejores herramientas para los usuarios de Internet.

Más Información:

[1] Tendencias

<http://www.eset-la.com/threat-center/1709-tendencias-2008>

[2] Disfrazando códigos maliciosos: Ingeniería Social aplicada al Malware

<http://www.eset-la.com/threat-center/1649-disfrazando-codigos-maliciosos>

[3] Virtumonde: Crónica de una muerte anunciada

<http://www.eset-la.com/threat-center/1674-analisis-tecnico-eset-virtumonde>

[4]Empaquetadores

http://es.wikipedia.org/wiki/Empaquetamiento_de_aplicaciones

[5] Sección de Artículos & White Papers de ESET Latinoamérica

<http://www.eset-la.com/threat-center/articles.php>