Tendencias 2011: las botnet y el malware dinámico

ESET Latinoamérica | *info@eset-la.com* | *www.eset-la.com*

Índice

Autor:

Laboratorio de ESET Latinoamérica

Introducción

En función al análisis de los hechos más relevantes ocurridos durante el presente año en materia de ataques informáticos y la industria de desarrollo de malware, el equipo de ESET, desde su Laboratorio de Investigación y Análisis de Malware ubicado en Latinoamérica, ha desarrollado el presente informe donde se describen las **principales tendencias para el 2011** respecto a códigos maliciosos y seguridad antivirus.

El crimeware (malware relacionado a los delitos informáticos y el lucro económico), presentado un año atrás como la principal tendencia para este 2010, ha confirmado su nivel de madurez siendo cada vez mayor la cantidad de códigos maliciosos relacionados a este modelo, así como también ha crecido la proporción entre malware de este tipo y otros convencionales.
Relacionadas al cibercrimen y el malware aparecen las botnet: redes de computadoras zombis que son controladas por un atacante para el uso de sus recursos. Para el próximo año, y en este contexto del crimeware, las redes botnet serán protagonistas, afirmando la tendencia observada durante el presente 2010: mayor cantidad de malware de este tipo; aumento en la cantidad de redes activas y más cantidad de equipos zombis. Asimismo, el monto recaudado por los administradores de estas redes también aumentará; se verán innovaciones en las tecnologías de las mismas y habrá una mayor preocupación por parte de la comunidad en dar de baja este tipo de redes delictivas.

A continuación se brindan más detalles sobre esta, y otras tendencias relevantes al malware para el 2011.

Botnet: el fin del malware estático

Muchos años atrás, un desarrollador de malware decidía al momento de crear un código malicioso cuáles serían las tareas que realizaría el mismo luego de infectar un sistema: qué archivos serían modificados, qué claves de registro serían alteradas, qué información sería capturada o a qué dirección del atacante sería enviada la misma, entre otros. Con el surgimiento de los troyanos del tipo backdoor [1] aparecen los primeros indicios de **malware dinámico**. Se entiende por código malicioso dinámico aquel que primero infecta el sistema y luego a través de algún acceso remoto al equipo afectado, el atacante puede realizar diversas tareas mientras el equipo no sea desinfectado.

Los troyanos del tipo backdoor han dejado el lugar en los últimos años a aquellos del tipo bot, diseñados para armar redes de computadoras infectadas. Las **botnet** [2] son la **confirmación del malware dinámico** en conjunto con el **negocio delictivo**: los equipos zombis pueden ser utilizados en cualquier momento por el administrador de la red para realizar diversas tareas que por lo general están asociadas a diversos delitos informáticos, tales como el robo de información, ataques a través de Internet o envío de spam, entre otros.

¿Qué se espera para el 2011? Mayor cantidad de redes botnet implicará el aumento en malware del tipo bot. Por lo tanto, se observará un crecimiento en la cantidad de usuarios afectados por esta amenaza, así como también en la proporción que representan los códigos maliciosos de este tipo por sobre el total de malware existente. Cuando se trate de un usuario con malware, cada vez será más frecuente que este tenga una infección de una botnet. Es decir, **un equipo infectado será probablemente un equipo zombi**.
Según las estadísticas brindadas por ThreatSense.Net, el servicio de Alerta Temprana de ESET NOD32 Antivirus, los códigos maliciosos de este tipo han aumentado durante el año 2010, a la espera de que esta tendencia continúe y se afirme durante el próximo 2011. Por ejemplo, si se compara el mes de octubre de 2009 con el mismo del 2010, se puede observar cómo la familia de códigos maliciosos identificada bajo la firma *IRC/SdBot*, que representó el 0,24% del total de las detecciones de malware de ESET NOD32 durante octubre del 2009, un año más tarde representa para el mismo mes el 0,49%. Es decir que mientras en 2009, durante un mes determinado, 1 de cada 400 usuarios recibían dicha amenaza en su sistema, para el 2010 ya son **1 de cada 200 usuarios los que vieron dicha variante de botnet** en su sistema, siendo detectada a través de su software antivirus.

La siguiente tabla explica cómo diversas firmas han visto aumentado el porcentaje de detección entre el año 2009 y 2010, según las estadísticas de detecciones indicadas por ThreatSense.Net:

Firmas	Detecciones de malware	
	2009	2010
IRC/SdBot	0,24%	0,49%
Win32/IRCBot *	0,15%	0,24%
Win32/Zbot	0,09%	0,23%
Win32/AutoRun.IRCBot *	0,03 %	0,18 %

* *Todas las variantes asociadas*

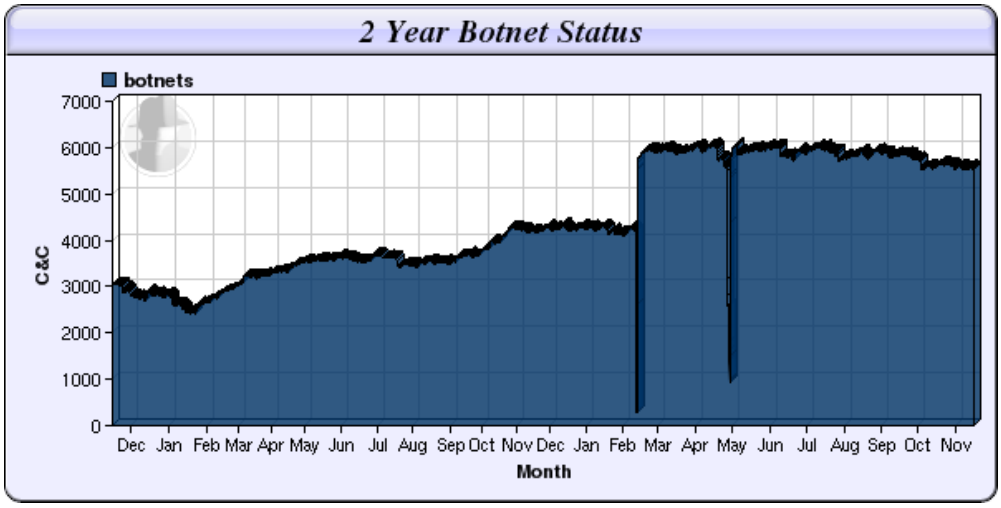
En consecuencia se puede observar a través de estos datos que, entre los usuarios de las soluciones de seguridad de ESET, también ha aumentado la cantidad de veces que fueron detectadas determinadas amenazas a lo largo del año, presentándose a continuación el porcentaje de aumento año a año:

Firmas	Aumento en cantidad 2009 a 2010
IRC/SdBot	98%
Win32/IRCBot *	66%
Win32/Zbot	130%
Win32/AutoRun.IRCBot *	139%

* *Todas las variantes asociadas*

Los datos de malware coinciden con las estadísticas publicadas por la fundación dedicada al análisis de amenazas digitales Shadow Server [3], que realiza seguimiento de redes botnet y publica estadísticas de forma periódica a disposición de la comunidad.

Los datos indican que a noviembre de 2010 son detectados unas **cinco mil quinientos botnet** (habiendo llegado durante el año a seis mil en meses como mayo o julio), contra los pocos más de cuatro mil a finales del año anterior. El crecimiento de las redes botnet activas detectadas por Shadow Server en los últimos dos años puede observarse en el siguiente gráfico:



Tomando estos 24 meses, se estima un crecimiento en la cantidad de botnet activas de aproximadamente un 85%. A partir de estos valores, **es posible esperar para el próximo 2011 más de siete mil redes botnet activas**.

Esto representa millones de usuarios afectados por esta amenaza. Este valor es obtenible tan solo si se toman simplemente tres de las botnet que han sido dadas de baja durante 2010 (ver sección siguiente): Waledac (80 mil usuarios afectados), Mariposa (13 millones) y Bredolab (30 millones).

Costos

¿A qué se debe tal cantidad de botnet y de usuarios afectados? Esencialmente al dinero: el escaso monto necesario por parte de los delincuentes para obtener paneles de administración o malware del tipo bot, y el importante dinero que obtienen estos por los servicios delictivos brindados por estas redes.

En el ciclo de comercialización explicado por el informe publicado por ESET Latinoamérica en abril de 2010 [4], se presentaron algunos de los costos asociados a estas tecnologías maliciosas:

- Por entre **U$S 80 y U$S 200** mensuales un atacante podría obtener un servidor destinado a alojamiento de malware, *exploits* o botnet, entre otros.
- El paquete de administración de botnet conocido como Eleonore Exploit Pack tiene un costo de **U$S 1000** (en su versión 1.3). Alquilar una red botnet de entre 10 y 20 mil equipos administrada por este mismo paquete tiene un costo promedio de **U$S 40 diarios** (lo que representa que un administrador podría recuperar la inversión realizada ¡en 25 días!).
- Otros kits de administración de botnet manejan diversos costos, según sus características y popularidad:
    - Zeus kit v1.3: U$S 3.000 / 4.000
    - YES Exploit System v3.0: U$S 1.150
    - Fragus v1.0 : U$S 980

En la siguiente imagen puede observarse directamente cómo en un foro ruso se comercializa la contratación de un **ataque de denegación de servicio**, por **costos a partir de los 25 dólares**, y con la posibilidad de realizar una **prueba gratuita de 10 a 20 minutos** (la imagen dispone de la traducción del sitio al español):

Pueden conocerse más costos de este tipo leyendo el informe completo “Costos del negocio delictivo encabezado por el crimeware” [4].

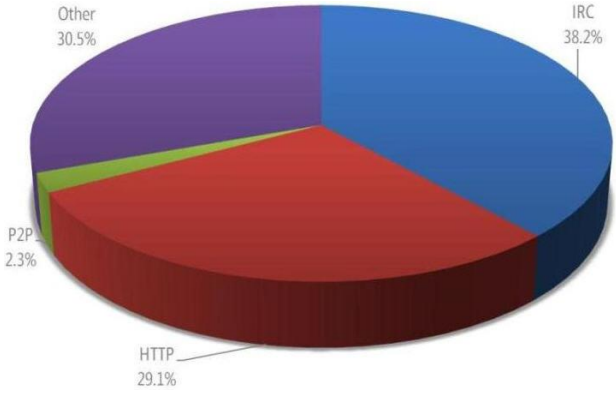
A su vez, la ganancia obtenida por los administradores de estas redes aumenta día a día, potenciando tanto la creación de estas, como su uso cada vez mayor por parte de los atacantes. Por ejemplo, un reciente estudio revela que la botnet **Koobface ha obtenido una ganancia de más de dos millones de dólares** entre junio de 2009 y junio de 2010. En países como Rusia, donde las botnet poseen mayor propagación que en el resto del mundo, diversos estudios indican que incluso una pequeña red botnet ha logrado obtener **ganancias superiores al millón de dólares en el transcurso de un mes**. Es decir que, no solo los costos para utilizar estas redes son relativamente bajos, sino también que las potenciales ganancias obtenidas son valores por demás elevados para cualquier negocio en la actualidad.

Imaginando el lugar de un desarrollador de malware, atacante o delincuente; y luego de la observación de los números presentados: ¿cuál es el sentido de desarrollar nuevas variantes de malware estático si es posible utilizar los códigos maliciosos del tipo bot ya existentes en el mercado, a costos rentables y con ganancias extraordinarias? La respuesta, es el principal justificativo por el cual las botnet seguirán aumentando durante el próximo año y serán cada vez más frecuentes las infecciones de este tipo por sobre otras.

Administración de botnet

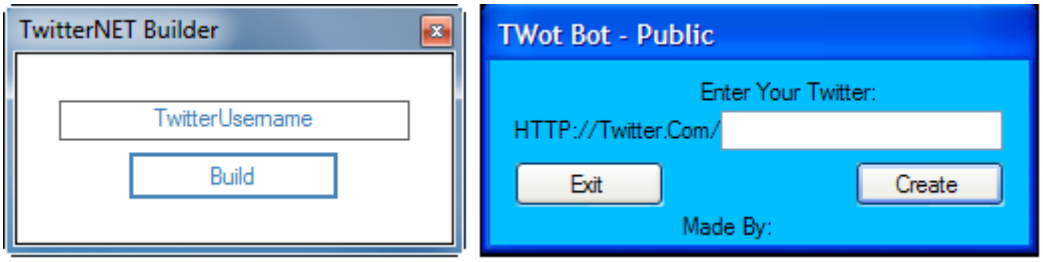
Durante 2010 se mostraron también nuevas formas de administrar redes botnet, además de las clásicas por protocolos como IRC y P2P, o las más modernas por HTTP. Mientras que las primeras se han logrado mantener, se ha notado una clara tendencia al uso del protocolo web e incluso nuevos formatos en la administración de botnet. Según lo reportado en el Blog de Laboratorio de ESET Latinoamérica durante el año, cada vez son menos las botnet que utilizan canales que en otras épocas fueron más populares, como el P2P.

Estadísticas de Microsoft [5] concuerdan con el comportamiento observado y reportado por el Laboratorio de ESET Latinoamérica durante el 2010: los protocolos más utilizados para la administración de estas redes son IRC y HTTP, como se indica en el siguiente gráfico:



Sin embargo, además de la baja en las redes botnet por *peer-to-peer*, también puede observarse un elevado porcentaje (30%) de métodos de administración no convencionales, un valor que probablemente aumentará durante el próximo año, especialmente con métodos de administración a través de redes sociales.

A lo largo del 2010, el Laboratorio de ESET Latinoamérica detectó dos herramientas para la creación de malware del tipo bot, que permitían **controlar los equipos zombis a través de Twitter** [6]. Los códigos maliciosos, detectados por ESET NOD32 como *MSIL/Agent.NBW* y MSIL/TwiBot.A respectivamente, permiten que el sistema infectado (equipo zombi) espere instrucciones a partir de la lectura de los contenidos en Twitter publicados por un determinado usuario, indicado al momento de la creación del malware con estas herramientas:



De esta forma, el atacante puede publicar contenidos en su cuenta de Twitter y lograr así que todos los zombis sigan las instrucciones indicadas, que pueden permitir el envío de spam, la ejecución de archivos o ataques de denegación de servicios, entre otros [7]. Incluso a través de este formato, se facilita la posibilidad que un administrador de una botnet envíe instrucciones a los zombis directamente desde un dispositivo móvil, pudiendo lanzar ataques, campañas de correo masivo u otros delitos directamente desde la palma de su mano.

Es de esperarse que el próximo año se observen con mayor frecuencia este tipo de botnet, controladas a través de métodos no convencionales, especialmente a través de redes sociales, ya que difícilmente estas estén bloqueadas en la conexión a Internet de la víctima.

Desmantelamiento de botnet

El crecimiento de las botnet despierta otra problemática: cómo terminar con esta amenaza. Teniendo en cuenta la cantidad de redes existentes (presentadas en secciones anteriores), es complejo prácticamente imposible concretar la baja de todas ellas, y por ese motivo es que es importante que el usuario se mantenga protegido para evitar la infección de su sistema. Sin embargo, con aquellas botnet con gran cantidad de usuarios, o un impacto importante en el escenario delictivo, es posible realizar diversas acciones que permitan dar de baja la red botnet, proceso que se conoce como *takedown*.

Durante 2010, se realizó el desmantelamiento de tres importantes redes de equipos zombis:

- **Waledac** [8], la red botnet de envío de spam del tipo farmacéutico que tuvo casi dos años de vida, fue dada de baja en febrero de 2010, a partir del cierre de 277 dominios que utilizaba la misma. El mismo fue ordenado y forzado por el juzgado federal de Virginia, en Estados Unidos [9], y en el proceso **ESET participó a través de sus profesionales e investigadores brindando información** a las fuerzas de seguridad locales.

- El mismo mes, la Guarda Civil española desmanteló una red de equipos zombis conocida por el nombre de **Mariposa**, que era administrada por tres ciudadanos españoles [9].
- El 25 de octubre de 2010 el gobierno holandés dio la baja de la botnet conocida como **Bredolab**, conocida por su orientación al robo de credenciales bancarias. La misma acumuló a lo largo de los años más de 30 millones de usuarios afectados [10]. De todas formas, se estima que a partir de nuevas variantes sus creadores lograron mantener viva, al menos parcialmente, parte de la estructura de la red [11].

Asimismo, también se han hecho trabajos "parciales" contra servidores de otras botnet importantes, como es el caso de Koobface en noviembre del presente año [12].

En el futuro, será más frecuente la colaboración entre empresas de seguridad, investigadores u organizaciones independientes y las fuerzas de seguridad de los países, con el ánimo de realizar este tipo de campañas con las redes botnet más importantes. A la fecha, ESET y la industria ya están colaborando con algunas fuerzas de seguridad, brindado información relacionada a redes botnet en actividad.

Malware multi-plataforma

A lo largo de 2010 diversas plataformas se vieron afectadas por variantes de malware. A pesar de que Windows sigue siendo la plataforma más explotada por los códigos maliciosos (un **84,3% de los usuarios se infectó con malware** durante el año [13]), hubo otras que también sufrieron algunos incidentes de malware durante el año:

- El sistema operativo libre más popular, **Linux**, sufrió algunos ataques de malware tales como un troyano simulando ser un protector de pantalla en sitios de repositorios [14], o un troyano del tipo *backdoor* que estuvo activo por más de 6 meses en el repositorio oficial del software Unreal IRC [15], entre otras variantes.
- Los dispositivos móviles no han sido ajenos a esta tendencia, y sistemas operativos en crecimiento se han visto afectados con primeras versiones de malware; como fue el caso de Android, para el cual fue reportado su primer troyano SMS [16] en agosto del presente año. Según investigaciones de ESET, el **malware para móvil ha aumentado un 95% entre 2009 y 2010**.

Como alternativa más rentable para los desarrolladores de malware aparece la creación de **códigos maliciosos multi-plataforma**, archivos que pueden afectar a diversas plataformas con un mismo fin, o bajo un mismo modelo de infección. Un ejemplo de esta tendencia se observó a principio de año con un experimento realizado para crear botnet en plataformas móviles con iPhone y Android, obteniendo más de 8 mil dispositivos afectados [17].

Esta tendencia fue ratificada a finales del año, con la aparición de una nueva variante del troyano Koobface, conocida como Boonana e identificada por ESET con la firma **Java/Boonana.A** ***[18]. La misma implicó la primer versión multi-plataforma de este troyano que está en actividad desde finales de 2008, y que dos años después de su creación ha comenzado su propagación más allá de sistemas Windows, infectando también sistemas Linux y Mac OS.***

En este contexto, las redes botnet son una de las mejores alternativas para el malware multi-plataforma. ¿Qué importancia tiene para el atacante si el envío de spam es realizado desde un sistema Windows o Linux? ¿Qué diferencia existe para el administrador de la botnet si las credenciales son robadas a un usuario de Mac OS desde su computadora portátil, o a un usuario de Symbian accediendo al *home banking* desde su dispositivo móvil?

En la siguiente imagen se puede observar cómo una red botnet posee equipos infectados de diversas plataformas, en diferentes proporciones que ratifican lo ya mencionado:

Operation Systems:	Totals:
Windows XP	23529
Windows 7	4060
Windows Vista	1585
Linux	168
Mac OS	162
Windows 2000	115
Windows 2003	111
Mobile phone	76
Unknown OS :(	25
Power PC	25
Windows 98	22
Symbian OS	15
iPhone OS	11
Windows ME	5
Windows 95	3
Bots	2
Windows NT 4	1
PlayStation	1
Nintendo Wii	1

Nótese también como incluso la botnet en cuestión posee dos equipos conformados por un sistema PlayStation y Nintendo Wii. Aunque no se han observado ejemplares de estos propagándose por la red, la imagen demuestra que los atacantes ya están trabajando en extender aún más las plataformas que pueden convertirse en zombis.

El malware multi-plataforma permite a los atacantes que sus códigos maliciosos infecten con éxito, independientemente de la plataforma que utilice la víctima, y es de esperarse que siga aumentando la tendencia durante el próximo año.

BlackHat SEO Social

Hoy en día prácticamente ningún usuario de Internet pasa un día completo sin realizar una búsqueda en la web, o utilizar alguna red social. Este dato no es ni será ignorado por los atacantes durante el próximo año, que incorporarán nuevas tendencias basadas en los ataques ya existentes para estos dos servicios:

- **Redes Sociales**: el crecimiento en la cantidad de usuarios se ha visto reflejado en el crecimiento de amenazas en propagación por estas redes. Durante 2010, Facebook ha superado los 500 millones de usuarios y otras redes como Twitter o MySpace también se ubican por encima de los 100 millones, todas ante la expectativa de seguir creciendo. Diversas amenazas se propagan por las redes sociales [19], como malware, phishing, spam o scam; y continuarán haciéndolo en todas las redes sociales que sean populares o tengan usuarios dispuestos a seguir sus contenidos y enlaces.
- **Buscadores**: los ataques de BlackHat SEO [20] consisten básicamente en la aparición de sitios que contienen malware (u otros contenidos maliciosos) en los resultados de los buscadores. Se caracterizan por estar asociados a temáticas de interés general o a eventos y sucesos actuales de amplia difusión a nivel mundial o regional. Por ejemplo, durante 2010 el mundial de fútbol fue uno de los eventos que más fueron explotados por los ataques de BlackHat SEO [21]. El malware se encuentra estrechamente relacionado a esta amenaza, especialmente el rogue, que según Google representa el 60% del malware asociado a búsqueda de *keywords* [22].

¿Qué se espera en esta materia para el 2011? En primer lugar la optimización de las técnicas de BlackHat SEO por parte de los atacantes. Por un lado, en cuanto a lo que se conoce como tiempo de posicionamiento: la demora entre la ocurrencia de un evento, y la ubicación en resultados envenenados en buscadores por BlackHat SEO. Según diversas investigaciones, los atacantes pueden lograr posicionar sus primeros enlaces envenenados en los buscadores en menos de 24hs. después de la ocurrencia de un evento

extraordinario; y en eventos planificados incluso logran ubicarse resultados de este tipo antes de que se incrementen las búsquedas según el servicio para medir tendencias de búsqueda, Google Trends.

En segundo lugar, la combinación de BlackHat SEO con las redes sociales resultará en el envenenamiento de los resultados en estas últimas para enlazar a los usuarios a malware u otros ataques. La web social se está caracterizando en los últimos tiempos por la optimización de sus búsquedas, especialmente aquellas en tiempo real. Por otro lado, los buscadores están comenzando a mostrar no solo sitios web, sino también resultados en redes sociales (una página de Facebook, un *tweet* de Twitter, etc.). Así, aparece una nueva forma de BlackHat SEO basada en las redes sociales, donde ya no es necesario para los atacantes la creación de sitios web envenenados, sino que pueden hacerlo directamente con falsos perfiles en las redes sociales (o desde perfiles de usuarios infectados) generando contenidos que enlacen a malware.

Un claro ejemplo de estos es el uso de etiquetas (o *hashtags* en inglés) en Twitter para el seguimiento de eventos en tiempo real. Un atacante podría crear cientos de perfiles falsos de Twitter y generar cada 10 segundos contenidos con el *hashtag* en cuestión, apareciendo así en todas las búsquedas en tiempo real que se realicen en el mundo, e incluso probablemente logrando un buen posicionamiento en los resultados que muestren los buscadores. Este tipo de ataques serán más frecuentes en el 2011, conforme los buscadores y las redes sociales sigan optimizando su relación a nivel de búsquedas.

La concientización de los usuarios será fundamental en esta materia, dado que diversas encuestas realizadas por ESET Latinoamérica indican que la mitad de los usuarios consideran que no hay riesgos de códigos maliciosos al acceder a las redes sociales [23]. Lo social se está convirtiendo en el eje de Internet y los atacantes no están ajenos a este hecho, por lo que se encuentran diseñando sus ataques exclusivamente para que tengan efectividad entre los usuarios de estas redes.

Las tendencias “de siempre”

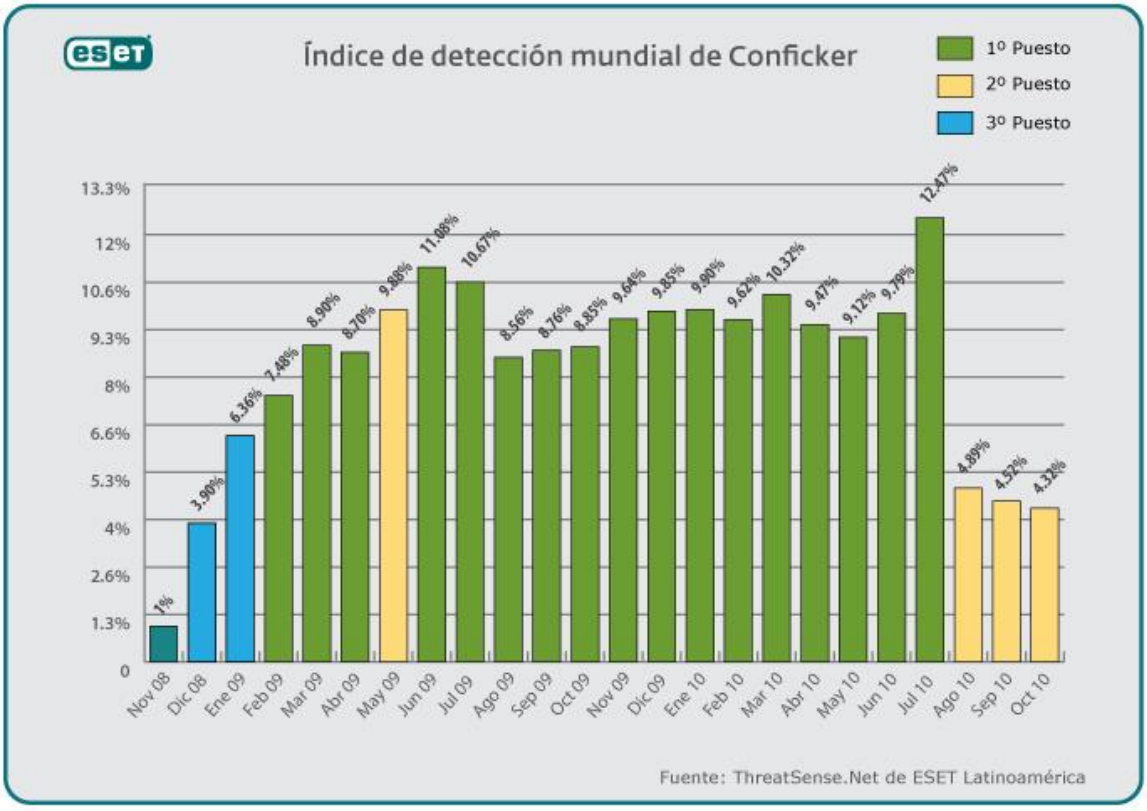
Mientras algunas tendencias aparecen basadas en nuevos ataques o tecnologías emergentes, otras se basan sencillamente en la continuidad de tipos de malware o vectores de ataques ya conocidos en años anteriores, pero que a pesar de ello seguirán siendo relevantes en el escenario de amenazas por su efectividad ante los usuarios.

Explotación de vulnerabilidades

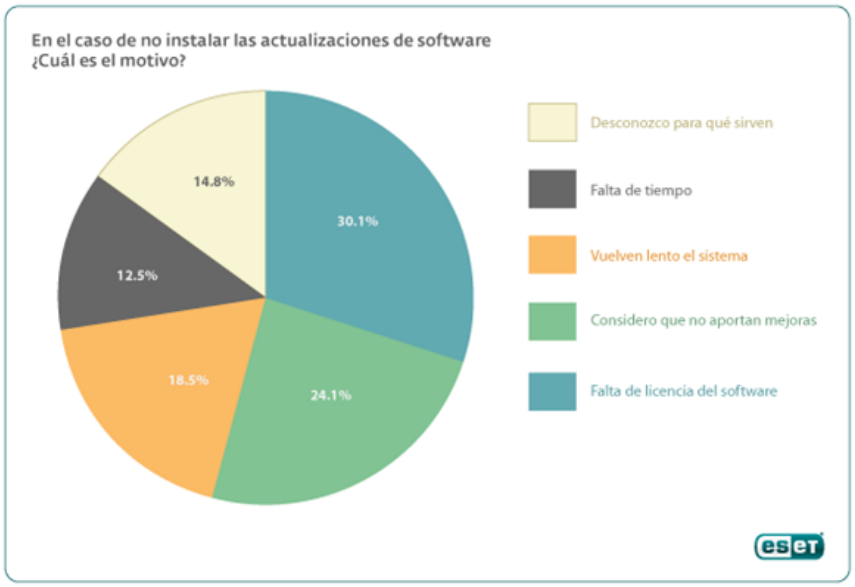
Las vulnerabilidades de software seguirán siendo uno de los vectores de infección más importantes para los creadores de malware, ya que permiten la ejecución de código sin la intervención del usuario, y por lo tanto la infección puede pasar desapercibida para la víctima hasta que no aparezcan síntomas en el sistema.

En este contexto, las vulnerabilidades del tipo 0-day (sin parche de seguridad disponible) representan una oportunidad para los atacantes, y que seguirá siendo aprovechada a medida que estas aparezcan. En casos ocurridos durante 2010, como el del gusano Stuxnet, ESET Latinoamérica detalló la cronología del ataque, indicando sus analistas que se concretaron “***16 días desde la publicación de la vulnerabilidad hasta la existencia de un parche*** *definitivo por parte del fabricante, ventana de tiempo durante la cual varios códigos maliciosos aprovecharon, causando numerosos problemas a entornos informáticos y atentando contra la seguridad de la información*” [25]. Solo aquellos usuarios que utilizaron software antivirus con capacidades proactivas de detección, como ESET NOD32, estuvieron protegidos durante esa “ventana de tiempo” en que la vulnerabilidad estuvo a disposición de los atacantes para propagar sus amenazas.

Sin embargo, no solo las vulnerabilidades 0-day son aprovechadas por los atacantes, sino también cualquier tipo de vulnerabilidad es una oportunidad para los desarrolladores de malware. Por ejemplo, el gusano Conficker está en actividad desde octubre del 2008, y más de dos años después sigue en actividad ocupando los rankings realizados por ESET Latinoamérica en cuanto a los códigos maliciosos más detectados mes a mes:



Es decir que más allá de la existencia o no del parche, las vulnerabilidades seguirán siendo explotadas por el malware. Los gusanos de este tipo serán probablemente las amenazas que se destaquen por altos índices de infección durante el próximo año.
En este aspecto, el rol del usuario y el uso de software no licenciado aparecen como componentes fundamentales para justificar este escenario. Según las estadísticas del año 2010, un **29,5% de los usuarios** indicó **no tener la costumbre de instalar las actualizaciones de seguridad**. Al consultar a estos por los motivos por los cuales no instalan los parches, se indicaron los siguientes [25]:



Es decir que el principal motivo por el cual no se instalan las actualizaciones de seguridad en las aplicaciones **es la falta de licencia de software**. Esto resulta muy relevante: **tres de cada diez usuarios no mantienen seguro su sistema por tener versiones del software no licenciadas**. En regiones como Latinoamérica, donde las tasas de piratería son particularmente altas, esto representa un riesgo más que importante para los usuarios de computadoras. Países como Venezuela se ubican en el primer lugar entre los países que utilizan sus aplicaciones sin licenciarlas, con una tasa del 89,7%, seguidas por otros como Paraguay (82%), Guatemala, Bolivia y El Salvador (todas con el 80%). Incluso países como Uruguay (68%) o Perú (70%) que se ubican entre las menores tasas, representan valores altos que superan la mitad de los usuarios.

Ingeniería Social

En concordancia con lo presentado en secciones anteriores, independientemente de la plataforma que se esté utilizando, detrás de la pantalla hay un usuario. Siempre existiendo la alternativa de aprovechar las vulnerabilidades de la plataforma, explotar al usuario es otra forma de propagar las amenazas, y la Ingeniería Social es el método más efectivo en este contexto.
Especialmente cuando se trate de asociación a hechos de relevancia, la utilización de estas técnicas seguirá siendo utilizada por los atacantes durante el 2011.

Para el próximo año ya se conocen algunos hechos que seguramente serán aprovechados por los creadores de malware, como la Copa América de fútbol, el Mundial de Rugby (los eventos deportivos suelen tener especial éxito para los atacantes) o eventos políticos, como las elecciones que se desarrollarán en Argentina y Perú el próximo año.

Privacidad y redes sociales

Otro aspecto que seguirá siendo foco de preocupación de los usuarios durante el año entrante es la privacidad expuesta en las redes sociales. Las aplicaciones y costumbres tendientes a exponer la información personal de los usuarios (con su propio consentimiento) seguirán aumentando, y la educación de los usuarios para el cuidado de su información será primordial en este aspecto.
Asimismo, los incidentes asociados a las redes sociales y la fuga de información [26] seguirán a la orden del día, y aquellos que resulten en la exposición de la información deberán ser atendidos por los usuarios para el cuidado de la información publicada, con la modificación de credenciales en caso de ser necesario.

Ataques desde Latinoamérica

Tal como anunciara el equipo de ESET Latinoamérica para el 2010, la región de Latinoamérica ya no es meramente una receptora de malware y ataques, sino también está en crecimiento el desarrollo de códigos maliciosos y otras amenazas en la región, otro aspecto que seguirá su desarrollo en los próximos años.

Durante 2010 se generaron ataques de todo tipo en la región, desde aquellos basados en la Ingeniería Social, como ocurrió este último semestre con los mineros chilenos (o a principio de año con el terremoto en el mismo país), o la situación política en Ecuador y Venezuela, todos ellos aprovechados para propagar malware [27]; la continuidad en la generación de troyanos bancarios en Brasil [28]; y también varios países de la región (como Argentina y Brasil) destacándose a nivel mundial en el envio de spam [29] e incluso la creación de botnet en países como México o Argentina [30].

El phishing es otra de las amenazas que crece particularmente en Latinoamérica, y que es desarrollado exclusivamente por atacantes locales o regionales, especialmente en casos en los que se intentan obtener credenciales bancarias de instituciones latinoamericanas. En países como Brasil, el phishing observado en el tercer trimestre del 2010 representó un **aumento del 150%** por sobre el mismo período del año anterior [31].

Los atacantes en la región están creciendo producto de los avances tecnológicos, el acceso a Internet y a la información, y el crecimiento de la comunidad delictiva digital, que seguirán presentes.

Conclusión

Como se pudo observar a lo largo del documento, todas las tendencias presentadas están de una u otra forma relacionadas: las botnet aumentarán al igual que el malware multi-plataforma, y justamente estas primeras son el principal recurso para llegar a distintos sistemas operativos. A la vez, se continúan detectando como tendencia la creación de botnet en Latinoamérica, que son generadores de spam donde, justamente, países de la región se destacan a nivel mundial. Por otro lado, también existen redes de equipos zombis creadas en la región, uso de técnicas de Ingeniería Social también regionales, e incluso relacionadas a nuevas tendencias tales como el uso de técnicas de BlackHat SEO en las redes sociales.

Estas relaciones resumen lo que ocurre con el malware en la actualidad: su estrecha relación con el negocio delictivo del cibercrimen, y su organización profesional a nivel mundial.

Algunas de estas afirmaciones que hace unos pocos años hubieran parecido incorrectas, son **y se afianzarán como certezas durante el 2011**:

1. La industria de desarrollo de malware está compuesta por profesionales que realizan sus códigos maliciosos con fines económicos y en relación con delincuentes.

2. El malware no afecta solo sistemas Windows, sino también a otros sistemas operativos e incluso otras plataformas como los dispositivos móviles.

3. Una vez infectado un equipo, este puede realizar diversas tareas delictivas, y el daño causado por un malware es dinámico e impredecible.

Lo más importante, y que ha sido destacado durante todo el documento, es que cada vez será más probable que esta última afirmación sea correcta: **un equipo infectado, es un equipo zombi**. Y este hecho inicial es el que permite el desencadenamiento del resto de las tendencias presentadas a lo largo del texto: el malware dinámico ofrece nuevas alternativas a los atacantes, mayores beneficios económicos y especial relación con los delitos informáticos desde los equipos infectados.

Referencias

[1] http://www.eset-la.com/centro-amenazas/amenazas/2136-Troyanos
[2] http://www.eset-la.com/centro-amenazas/1573-botnet-redes-organizadas-crimen
[3] http://www.shadowserver.org
[4] http://www.eset-la.com/centro-amenazas/2313-costos-negocio-delictivo-crimeware
[5] http://www.microsoft.com/security/sir/story/default.aspx#section_2_2_1
[6] http://blogs.eset-la.com/laboratorio/2010/05/14/botnet-a-traves-twitter/
http://blogs.eset-la.com/laboratorio/2010/08/27/twitter-mira-botmasters/
[7] http://www.youtube.com/watch?v=EoATrwF4DdM
[8] http://www.eset-la.com/centro-amenazas/2042-waledac-troyano-enamorado
[9] http://blogs.eset-la.com/laboratorio/2010/03/03/redes-botnet-desaparecen-adios-waledac-mariposa/
[10] http://blogs.eset-la.com/laboratorio/2010/10/29/gobierno-holandes-cierra-botnet-de-30-millones-de-victimas/
[11] http://blogs.eset-la.com/laboratorio/2010/11/03/bredolab-no-se-rinde-y-sigue-dando-pelea/
[12] http://blogs.eset-la.com/laboratorio/2010/11/15/piedra-libre-a-koobface/
[13] http://blogs.eset-la.com/laboratorio/2010/10/13/%C2%BFquien-se-salvo-del-malware-en-el-2010/
[14] http://blogs.eset-la.com/laboratorio/2009/12/10/troyano-para-linux/
[15] http://blogs.eset-la.com/laboratorio/2010/06/15/troyano-para-linux-activo-por-mas-de-6-meses/
[16] http://blogs.eset-la.com/laboratorio/2010/08/10/primer-troyano-sms-para-android/
[17] http://blogs.eset-la.com/laboratorio/2010/03/10/un-experimento-crea-botnet-en-dispositivos-moviles/
[18] http://blogs.eset-la.com/laboratorio/2010/10/28/koobface-llega-a-mac-os-y-linux/
[19] http://www.eset-la.com/centro-amenazas/2348-dudas_certezas_redes_sociales_empresa
[20] http://www.eset-la.com/centro-amenazas/2333-ataques-black-hat-seo
[21] http://blogs.eset-la.com/laboratorio/2010/05/28/buscadores-mundial-futbol-malwar/
http://blogs.eset-la.com/laboratorio/2010/05/20/mundial-futbol-2010-te-puede-infectar/
[22] http://blogs.eset-la.com/laboratorio/2010/04/20/60-malware-keywords-rogue/
[23] http://blogs.eset-la.com/laboratorio/2010/06/10/la-mitad-de-los-usuarios-consideran-que-no-hay-malware-en-redes-sociales/
[24] http://blogs.eset-la.com/laboratorio/2010/08/16/cronologia-de-un-ataque-0-day/
[25] http://blogs.eset-la.com/laboratorio/2010/09/24/actualiza-tu-software-licenciado/
[26] http://blogs.eset-la.com/laboratorio/2010/10/22/facebook-android-e-iphone-fugan-datos-de-usuarios/
[27] http://blogs.eset-la.com/laboratorio/2010/10/14/mineros-chilenos-malware-brasil/
http://blogs.eset-la.com/laboratorio/2010/07/14/caso-bruno-propagacion-malware/
http://blogs.eset-la.com/laboratorio/2010/11/08/politica-en-venezuela-usada-para-propagar-malware/
http://blogs.eset-la.com/laboratorio/2010/05/26/falsa-noticia-terremoto-chile-propaga-malware-bancatio/
http://blogs.eset-la.com/laboratorio/2010/02/28/terremoto-chile-japon-usado-propaga-malware/
[28] http://blogs.eset-la.com/laboratorio/2010/07/31/troyano-bancario-y-brasileno-%C2%BFsuena-conocido/
http://blogs.eset-la.com/laboratorio/2009/08/11/codigo-malicioso-made-in-brasil/
[29] http://blogs.eset-la.com/laboratorio/2009/08/13/spam-argentina-brasil-top-10/
http://blogs.eset-la.com/laboratorio/2010/06/25/crimeware-global/
[30] http://blogs.eset-la.com/laboratorio/2010/06/04/mariachi-botnet-latinoamerica-atacada-ciberdelincuentes-mexicanos/
http://blogs.eset-la.com/laboratorio/2010/11/15/nueva-botnet-argentina/
[31] http://www.nic.br/imprensa/releases/2010/rl-2010-23.pdf