Tendencias 2012: el malware a los móviles

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

Índice

Autor:

Laboratorio de ESET Latinoamérica

Introducción

El informe de tendencias de ESET Latinoamérica se ha convertido en una costumbre para el equipo del Laboratorio de Análisis de Malware, que una vez más, finalizando el 2011, ha analizado lo ocurrido durante el año. Este documento presenta las tendencias para el próximo año, tanto en materia de códigos maliciosos, como así también, en general para otro tipo de ataques informáticos y el mundo del cibercrimen.

Las costumbres de los usuarios en cuanto al uso de tecnologías, siempre han influido y determinado el desarrollo de malware y, esta tendencia, seguirá estando vigente. Teniendo en cuenta este punto, el marcado crecimiento en la utilización de dispositivos móviles será determinante el próximo año, dado que estas plataformas ya no son un espacio de entrada prohibida para el malware debido a que los desarrolladores de códigos maliciosos han trabajado en los últimos años para poder infectar este tipo de dispositivos. En el presente documento describiremos cómo la migración de las amenazas para equipos de escritorio al mundo móvil está a la orden el día.

En ese contexto, las amenazas para dispositivos móviles, tanto en materia de nuevos códigos maliciosos como de estafas en Internet, entre otras; serán lo más relevante para el próximo año, además de la aparición de nuevos tipos de ataques, como así también de nuevas variantes de aquellas existentes.

Asimismo, la evolución de las tecnologías de seguridad en las plataformas existentes dará lugar a más y nuevas amenazas tecnológicamente complejas. Sin embargo, no dejarán de existir códigos maliciosos en el otro extremo, cuya sencillez no es proporcional al alto impacto que suelen tener en los usuarios.

¿Cuáles serán entonces las principales tendencias para el 2012? En las próximas secciones, esta pregunta se contestará para que el usuario esté al tanto de las próximas tendencias y pueda conocer de qué manera optimizar los mecanismos de protección tanto en entornos hogareños como corporativos.

Malware en dispositivos móviles

En los últimos años hemos asistido cómo, diversas amenazas, fueron apareciendo en las plataformas móviles. Previo al 2011, el surgimiento de distintos códigos maliciosos para plataformas como Symbian y Windows Mobile captó la atención debido a la novedad que representaban estos ataques.

No obstante, el 2011 confirmó la existencia de estas amenazas debido a la amplia adquisición que los usuarios hicieron de estos dispositivos y también a la aparición de Android como plataforma líder del mercado. En la actualidad, hay más de **5 mil millones de dispositivos móviles en todo el mundo** y más de 500 millones de estos están en países latinoamericanos. Por otro lado, uno de cada cuatro dispositivos móviles son teléfonos inteligentes (mejor conocidos como *smartphones).*

Según la consultora Gartner, a mediados del 2011, Android era el líder de plataformas móviles (con más de 400 millones de dispositivos móviles en todo el mundo, creciendo a raíz de 550 mil dispositivos por día):

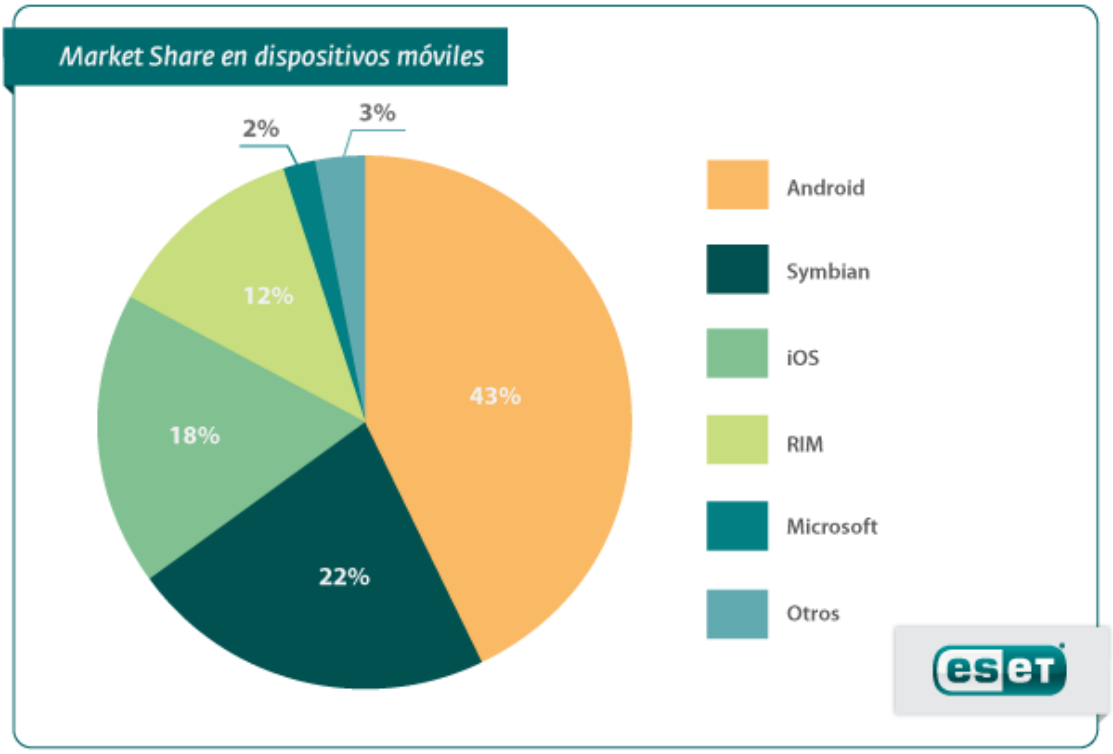

Imagen 1: market share de sistemas operativos para móviles

Esta tendencia fue acompañada por el desarrollo de códigos maliciosos tal como puede verse en el siguiente gráfico. En el mismo se detallan las principales variantes de malware que fueron llegando a los dispositivos Android durante los últimos dos años, cuando apareció FakePlayer, el primer código maliciosos para esta plataforma (el gráfico puede observarse en mayor tamaño al final del documento, junto a sus referencias):

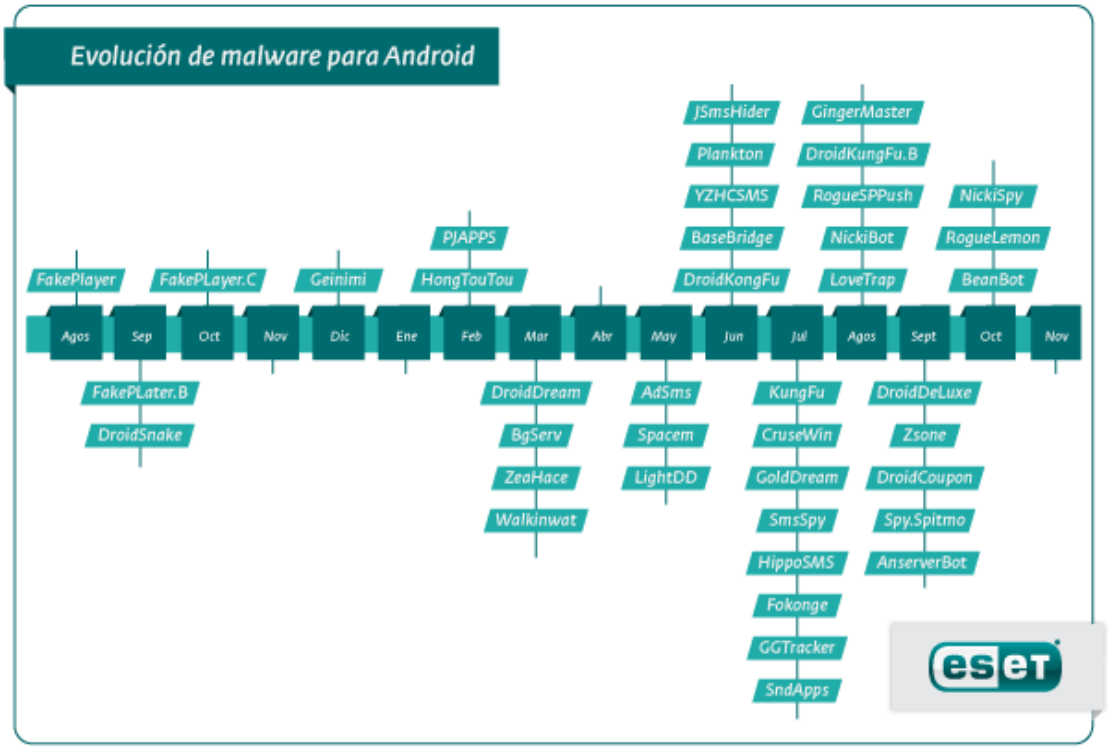

Imagen 2: Surgimiento de malware para Android

Es interesante observar la cantidad de variantes de malware y los años tenidos en cuenta para el análisis. De los **41 códigos maliciosos analizados, tan solo 5 aparecieron en el 2010**, perteneciendo estos solo a tres familias distintas de malware. Esta tendencia continuó durante el primer semestre del 2011 ya que aparecieron tan solo 7 nuevas variantes, lo cual evidencia una importante concentración de amenazas para esta plataforma en los últimos seis meses de 2011, destacando las **amenazas para Android como principal tendencia para el año 2012**.

Continuando con el análisis de los principales códigos maliciosos para Android, resulta interesante prestar atención al modo de propagación de los mismos ya que 12 de las variantes identificadas estuvieron disponibles para su descarga desde el Android Market. En este aspecto, que el 30% de las amenazas puedan ser descargadas desde el repositorio oficial del fabricante, indica la importancia que tendrá esta plataforma en el futuro y la necesidad de mayores esfuerzos por parte de los fabricantes para minimizar este tipo de incidentes. De todos modos se ha identificado que la mayoría de las amenazas fueron descargadas desde repositorios no oficiales (7 de cada 10) lo que indica que aún es muy **importante que los usuarios** estén concientizados sobre la importancia de **descargar software desde sitios web oficiales**.

Otros datos a destacar es que 15 de las 41 aplicaciones analizadas fueron identificadas como **troyanos SMS**, una de las principales amenazas para dispositivos móviles, y que el 60% de los códigos maliciosos analizados, poseían alguna característica del tipo **botnet**, es decir, control remoto del dispositivo que al ser infectado se convierte en un zombi.

Finalmente, tomando justamente las redes botnet, también es posible identificar al malware para plataformas móviles como tendencia. Durante el 2011 se pudo observar una marcada aparición de las variantes de las principales botnet para dispositivos móviles, años después de que ya están infectando sistemas de escritorio. Por ejemplo, Zeus apareció en el año 2007, y tres años después surgió su versión para móvil. Para 2011, ya tenía variantes para cuatro importantes plataformas móviles.
En la siguiente tabla se observan todas las fechas de descubrimiento de las variantes de Zeus y SpyEye, tanto en sus versiones de escritorio como móviles (ZITMO y SPYTMO respectivamente):

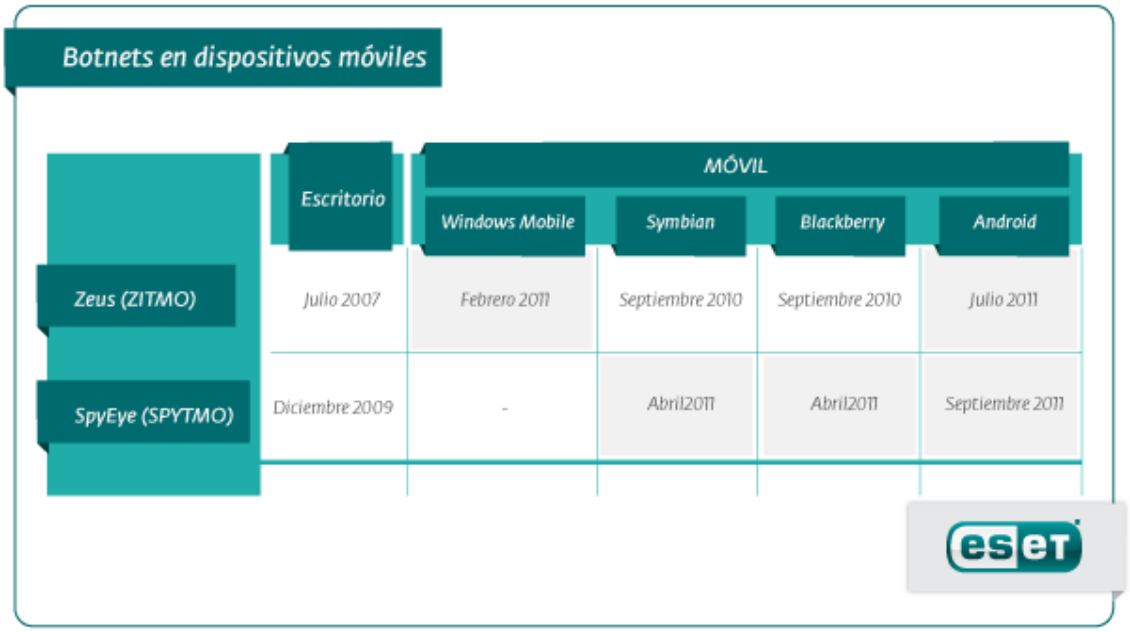

Imagen 3: Surgimiento de Zeus y SpyEye para equipos de escritorio y móviles

Claramente distintas variantes de malware han estado migrando durante el 2011 a versiones móviles. La tendencia es que esto continúe, y una vez aparecidos los primeros casos para un tipo de código malicioso específico, el siguiente paso lógico sería la creación de variantes que pueden comenzar a masificarse lentamente.

Como ejemplo más reciente, a finales de octubre, también los códigos maliciosos del tipo rogue (falsas aplicaciones de seguridad) aparecieron para Android, tal como lo reportó el Blog de Laboratorio de ESET Latinoamérica.

Impacto masivo

Otro componente que ubica a los códigos maliciosos para dispositivos móviles como principal tendencia para el próximo año, es el crecimiento del impacto causado por malware. Es aquí donde **DroidDream** resulta el caso más ejemplificador, ya que esta amenaza tuvo más de **250,000 descargas desde el Android Market** (que a julio de 2011 contenía el mismo número de aplicaciones disponibles). El caso tuvo tanto impacto que Google decidió desinstalar remotamente la aplicación de todos los sistemas infectados por dicho código malicioso. Todos los usuarios cuyo dispositivo móvil había sido comprometido fueron notificados a través de un correo electrónico.

Entre los principales objetivos de DroidDream se encuentra el robo de información que permite identificar de manera unívoca al dispositivo como así también la capacidad de instalar otros códigos maliciosos. Entre las particularidades de este malware hay que remarcar que para evitar ser identificado por el usuario, se ejecutaba durante la noche, corroborando la hora, cualidad que le dio su nombre.

De esta forma, **DroidDream quedará en la historia como el primer código malicioso para dispositivos móviles de impacto masivo**, lo cual certifica y abre lugar a la concreta posibilidad de que se observen más incidentes de este tipo el próximo año.

Android: ¿el nuevo XP?

Durante muchos años hemos observado cómo los desarrolladores de software malicioso para sistemas operativos de escritorio focalizaron sus esfuerzos en Windows. Aunque en los últimos años se han observado múltiples amenazas para otras plataformas (como Linux o Mac OS) el sistema operativo de Microsoft siempre fue el foco de atención de quienes escriben malware.

A pesar de las distancias existentes entre el mundo del móvil y el de los equipos de escritorio, en cuanto a cantidad de dispositivos y a la cantidad de amenazas, hoy en día los creadores de aplicaciones maliciosas están encontrando en Android muchas de las características que años atrás encontraron en Windows XP, no solo por las características propias de la plataforma, sino también por los usos y costumbres de la masa de usuarios.

El crecimiento en el market share, las características técnicas del sistema operativo, la posibilidad de propagar el malware en repositorios (oficiales o no) y otras características, posicionarán a Android como la prioridad para crear malware para cualquier desarrollador de códigos maliciosos, y **allí estará puesto el foco de códigos maliciosos para estas plataformas durante el 2012**.

Nuevas tecnologías, nuevas amenazas

Según las estadísticas **publicadas por la consultora Gartner**, para fines del 2011 Windows 7 se convertirá en el sistema operativo para equipos informáticos más utilizado a nivel mundial, con el 42% del *market share*. Este suceso, que desplazará a Windows XP del primer puesto, marca también algunos cambios en las amenazas desarrolladas por los cibercriminales. Las mejoras en los mecanismos de seguridad provistas por los nuevos sistemas operativos conllevan el desarrollo de códigos maliciosos tecnológicamente más avanzadas, con el objetivo de evadir las protecciones provistas, como por ejemplo en Control de Acceso a Usuarios (UAC). Estas amenazas serán más complejas desde el punto de vista tecnológico, ya que en la era de Windows XP muchas amenazas únicamente sobrescribían una entrada de registro o escribían un archivo para hacer daño en el sistema, mientras que en la actualidad los nuevos códigos maliciosos deberán incorporar también cuestiones más complejas, destinadas a lograr la ejecución en el sistema, antes del daño propiamente dicho.

Además de estos mecanismos de protección muchos sistemas de 64 bits (la mayoría de los equipos de escritorio modernos) cuentan con protecciones de seguridad desde el inicio del sistema operativo, de forma tal de evitar amenazas como los *rootkits,* códigos maliciosos que ocultan su ejecución al sistema operativo. No obstante, a lo largo del 2011 se han propagado nuevas variantes de códigos maliciosos que cuentan con funcionalidades para evadir estos mecanismos de protección. La aparición de una nueva variante de una amenaza conocida en su última versión como **TDL4**, demostró que el desarrollo de malware más complejo es una realidad. Esta nueva variante, es un *rootkit* del tipo botnet que permite infectar y saltear mecanismos de autenticación en sistemas operativos de 64 bits, especialmente diseñada para Windows Vista y Windows 7.

Para el 2012 aparecerán también más códigos maliciosos con capacidades de vulnerar los sistemas de firmado digital con los que también cuentan los sistemas operativos más modernos. Un caso de este tipo fue el de Mebroni, un código malicioso que **infecta la BIOS del sistema**, comprometiendo el mismo desde antes del inicio, y siendo un tipo de **amenaza más persistente** ya que al infectar la BIOS del sistema, ante cada reinicio del mismo, puede sobrescribir memorias de inicio de sesión de la computadora (MBR y VBR) y de esa manera comprometer la seguridad del equipo.

Códigos maliciosos firmados digitalmente con certificados robados, como fue el caso de Stuxnet a finales del 2010, serán cada vez más frecuentes durante el próximo año. De hecho, hacia finales del 2010 la entidad Diginotar, dedicada a la generación de certificados, se vio afectada por la exposición y utilización de sus certificados con fines maliciosos, lo que llevó a la empresa a **decretar la quiebra**.

Finalmente, el legado de Stuxnet seguirá presente. Tal como pronosticó el Laboratorio de ESET en su informe “Tedencias 2011: botnets y malware dinámico”, durante el presente año no se observó un crecimiento masivo de códigos maliciosos que ataquen sistemas SCADA, aunque la tendencia seguirá siendo creciente a paso lento, y es probable que el próximo año puedan aparecer algunas amenazas de este tipo.

La desaparición de Conficker

Otra de las consecuencias de la migración como sistema operativo líder de Windows XP a Windows 7, es la desaparición de Conficker. Este gusano informático apareció en noviembre de 2009 y desde aquel entonces se convirtió en el gusano más importante de los últimos años, ubicándose mes a mes entre las tres amenazas más detectadas durante 3 años, según los reportes mensuales de amenazas de ESET Latinoamérica.

No obstante, la tendencia de detección de este código malicioso es decreciente, tal como presentan las estadísticas de ThreatSense.Net, el sistema de alerta temprana de ESET:

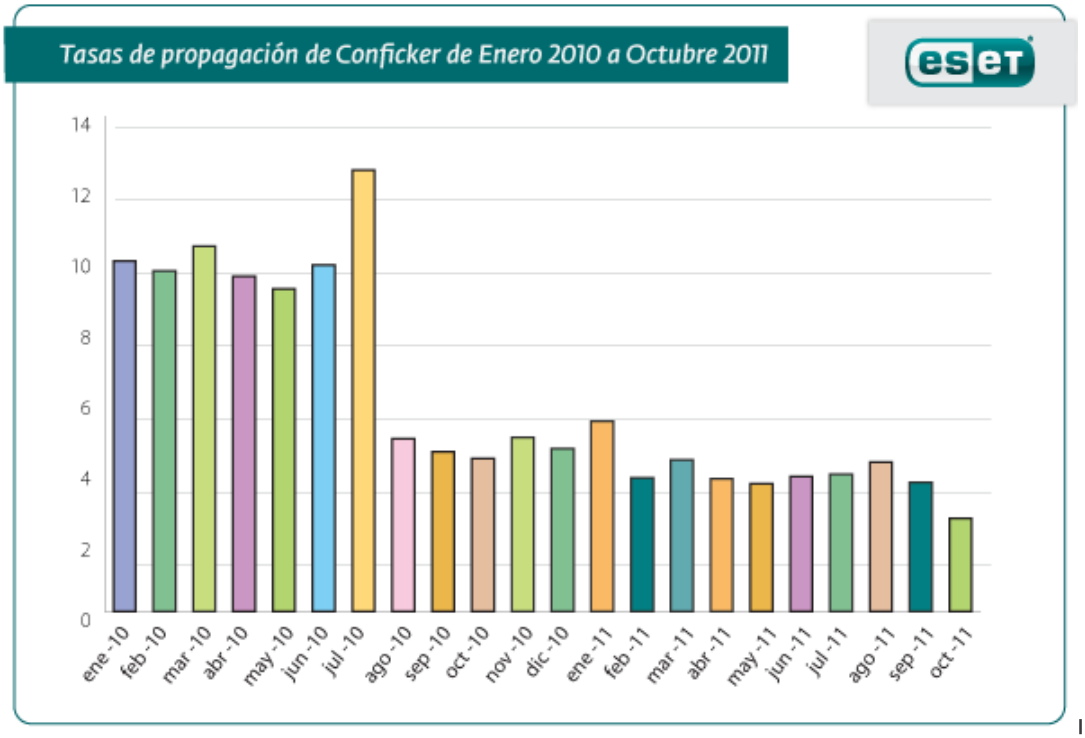

Imagen 4: Tasas de propagación de Conficker de enero 2010 a octubre 2011

Como se puede observar, los índices de detección del gusano están disminuyendo mes a mes, habiendo promediado un **3,90% de detección en el 2011** (hasta octubre inclusive), una disminución muy notoria respecto al año anterior, en el que el promedio era del 7,83%. Asimismo, durante el 2010 Conficker se ubicó como el código malicioso más detectado según ESET durante 7 de los 12 de meses del año; mientras que en el 2011 solo logró esa posición en el mes de enero (con el 5,38% de las detecciones), valores que disminuyeron notoriamente a octubre del presente año (tercero, con el 2,63%; el valor más bajo desde su lanzamiento).

¿A qué se debe esta disminución en las cifras obtenidos sobre este gusano? Es necesario mencionar dos factores importantes que impactan sobre las tasas de detección de este malware. En primer lugar, la declinación natural en el ciclo de vida de cualquier código malicioso (que de hecho, en el caso de Conficker fue extremadamente extenso), generado por los usuarios que instalaron los parches de seguridad para cortar los circuitos de propagación, o usuarios que actualizaron sus soluciones antivirus para mejorar la detección. Sin embargo en el caso de Conficker, las variantes que se propagaban por USB fueron aquellas que continuaron generando un alto impacto en los usuarios. No obstante, durante el 2011 ocurrieron algunos hechos significativos: por un lado, el crecimiento de Windows 7, plataforma en la cual Conficker no puede propagarse automáticamente a través de dispositivos USB. Por otro lado, en febrero del 2011 Microsoft lanzó una actualización para deshabilitar la funcionalidad de Autorun de dispositivos USB en los equipos con el sistema operativo Windows XP (parche que ya estaba disponible pero de forma optativa para los usuarios, desde el año anterior). De esta forma, cada vez más usuarios tienen bloqueados los circuitos de propagación del gusano Conficker.

Por lo tanto, podemos esperar que para el 2012 los niveles sigan disminuyendo y esta amenaza, (que afectó a gran cantidad de usuarios durante tantos años y batió tantos records en cuanto a impacto causado, velocidades de propagación, y otros) **irá desapareciendo lentamente de la primera plana del escenario de malware mundial**.

Botnet *takedowns*

Durante el 2011 se observó, tal como pronosticó un año atrás ESET Latinoamérica, cómo empresas de seguridad, compañías proveedoras de servicios de Internet y organismos públicos unieron sus esfuerzos para dar de baja redes de equipos zombis, también conocidas como botnets.

Este procedimiento conocido como **takedown**, consiste en cortar algún circuito de funcionamiento de la red y, de ser posible, encontrar a los responsables de la administración de la misma. Durante el 2011 se hicieron públicas las bajas de importantes redes como Kelihos (desmantelada por Microsoft en septiembre), Coreflood y Koobface, entre otras. Es interesante el caso de Bredolab, ya que la misma fue desmantelada con el total apoyo del gobierno holandés, factor clave en el éxito de esta operación.

Teniendo en cuenta el importante crecimiento de las redes botnet durante el 2011 (según ShadowServer, hay casi seis mil redes activas a octubre de 2011), estos esfuerzos deberán multiplicarse, no solo para evitar que redes de grandes magnitud operen, sino también para que aquellas cuyo impacto no es tan mediático pero que logran infectar miles de equipos, también puedan ser dadas de baja.

Consecuentemente, durante el próximo año los takedown de botnets seguirán siendo frecuentes, muchos de ellos con exposición pública cuando la magnitud sea la suficiente.

La sencillez: rogue y greyware

Más allá del crecimiento que se espera de amenazas más complejas desde el punto de vista tecnológico, durante el 2011 se ha observado paralelamente un crecimiento importante de otros códigos maliciosos que representan el otro extremo: **sus rutinas son tecnológicamente muy sencillas**. No obstante, debido a la efectividad de la Ingeniería Social, logran propagarse de manera muy efectiva.

Entre los códigos maliciosos sencillos se encuentran por ejemplo, los troyanos bancarios del tipo Qhost que al ejecutarse en el sistema, modifica un archivo de texto que es suficiente para que el atacante robe las credenciales bancarias de los usuarios.

En esta misma categoría de amenazas, hay dos que se destacan por el alto impacto que están comenzando a tener en los sistemas de los usuarios: **el rogue y el greyware**.

El primero, también conocido en algunas de sus variantes como falsos antivirus, se caracteriza por ser un código malicioso cuyas funciones, en muchos casos, no se extienden más allá de una sencilla animación. Su único objetivo es engañar al usuario, asustarlo y cobrar por un servicio inexistente. Los rogue son estafas puestas en formato de malware. No obstante, más allá de su sencillez, los niveles de rentabilidad demostrados para los atacantes son altísimos ya que más allá de lo rudimentario de los ataques, muchas de estas falsas soluciones se cobran por encima de los costos reales de la industria. Es de esperarse que los rogue en idioma español comiencen a surgir en Latinoamérica durante el 2012.

Finalmente, el **greyware** es otra amenaza de tendencia creciente: son archivos cuyas características maliciosas son tan sutiles que hacen los laboratorios de análisis de malware tengan dificultades en su detección. En esta categoría, se identifican muchas aplicaciones que incluyen, por ejemplo, el envío de información personal del usuario al atacante mediante la política de uso. De esta forma, muchos de estos desarrolladores de códigos maliciosos pretenden que las empresas de antivirus no puedan generar estas firmas para proteger el equipo. Cada vez es más frecuente encontrarse con estas amenazas, que seguirán creciendo el próximo año, y que están específicamente **focalizadas en el robo de información**.

Este tipo de amenazas, sencillas desde el punto de vista tecnológico, seguirán creciendo en cuanto a su relevancia en el escenario del malware mundial y latinoamericano.

Amenazas de Latinoamérica

Finalmente, ¿qué ocurrirá con los ciber delincuentes en Latinoamérica? Como ya es sabido, desde hace muchos años, las amenazas informáticas no solo “llegan” a la región desde otros países, sino que también existen desarrolladores de malware locales. Estos aprovechan los hechos más importantes que acontecen en América Latina, para utilizar técnicas de Ingeniería Social e infectar a miles de usuarios.
En ese contexto, las principales amenazas generadas en la región, que se destacarán son las siguientes:

- **Hacktivismo**: la utilización de ataques informáticos con fines ideológicos está creciendo de forma importante en la región. A partir del caso Wikileaks, y de la enorme popularidad de las acciones de Anonymous, muchas personas en la región se han identificado con estos movimientos y muchas organizaciones están comenzando a sufrir este tipo de ataques informáticos, especialmente organismos gubernamentales o personas asociadas a la política. Durante el 2011, muchos gobiernos de la región se vieron afectados por estos ataques, entre ellos Argentina, Chile, Colombia, Guatemala y El Salvador.
- **Privacidad y redes sociales:** Latinoamérica es una región con un alto uso de redes sociales. De los 200 millones de internautas que hay en la región, 162 millones tienen cuenta en Facebook. Por lo tanto la propagación de troyanos por estos medios (a través de Ingeniería Social), y especialmente el crecimiento de amenazas de fraude como el clickjacking (el negocio de los clics para los cibercriminales), el scam o las falsas aplicaciones para el robo de información, serán notorias durante 2012.
- **Troyanos bancarios y phishing.** Dentro del malware, los troyanos bancarios son sin lugar a duda la variante más emblemática desarrollada en Latinoamérica. El phishing, como amenaza relacionada, también se expandió de forma masiva durante el último año y dada su efectividad (estudios de ESET confirman que un delincuente en la región puede obtener **datos de siete tarjetas de crédito por hora con un ataque activo**), seguirán funcionando el próximo año. El seguimiento que realiza el equipo de Laboratorio de ESET Latinoamérica a atacantes brasileños que propagan troyanos bancarios, indica que durante el 2011 lanzaron más de 60 campañas de propagación y que en esos meses obtuvieron al menos 200 mil cuentas de correo para utilizar como spam con el fin de continuar el circuito de infección.

En resumen, los delincuentes latinoamericanos aún están centrados en las amenazas que, aunque son algo antiguas desde el punto de vista tecnológico, siguen siendo extremadamente eficientes para infectar a los usuarios de la región.

Conclusión: ¿una nueva era?

Durante muchos años los usuarios fueron testigos de una especie de estabilidad en lo que respecta a códigos maliciosos: gusanos y troyanos, distribuidos por correo electrónico y redes sociales, que infectaban a los usuarios y se concentraban en el robo de información.

Hoy en día, el mundo móvil y las nuevas plataformas dan lugar a más diversidad de códigos maliciosos dado que estos dispositivos generan nuevas costumbres en los usuarios, no sólo porque estos alojan mayor cantidad de información sensible, sino también porque desde estos dispositivos móviles se puede acceder a sistemas que antes se accedían desde equipos de escritorio. El robo de información en teléfonos inteligentes, ya no solo representa el acceso a una libreta de contactos, sino también a archivos confidenciales, imágenes privadas o incluso claves para sistemas sensibles.

Esto abre la puerta a que surjan nuevas modalidades y vectores de ataque, cobrando mayor importancia las plataformas móviles aunque sin dejar de lado las amenazas para equipos de escritorio. Los usuarios deberán estar conscientes del valor de la información que transportan día a día en sus dispositivos móviles y deberán comprender que no sólo pueden comprometer la confidencialidad de la misma mientras utilizan servicios web sino también con la pérdida y/o el robo de los equipos.

Esto no necesariamente representa una migración total del malware hacia los dispositivos móviles ni el surgimiento de una nueva era, pero sí implica una serie de cambios dentro del escenario del malware orientado al cibercrimen.

Además de la mayor relevancia de los dispositivos móviles, uno de los fenómenos que generan estos cambios es el resurgimiento de viejos conocidos, tal es el **caso de Induc** a finales del 2011, o la aparición de rootkits de BIOS. De esta forma, asistiremos al surgimiento de una mayor complejidad en cuanto a los códigos maliciosos que estarán cada vez más relacionados al cibercrimen y al mismo tiempo serán más diversos.

Asimismo, se seguirá observando un crecimiento en cuanto a la masividad de amenazas tecnológicamente sencillas. Por lo que, durante el 2012, los casos más importantes de malware estarán ubicados seguramente en alguno de los extremos desde el punto de vista de la complejidad técnica de las amenazas:

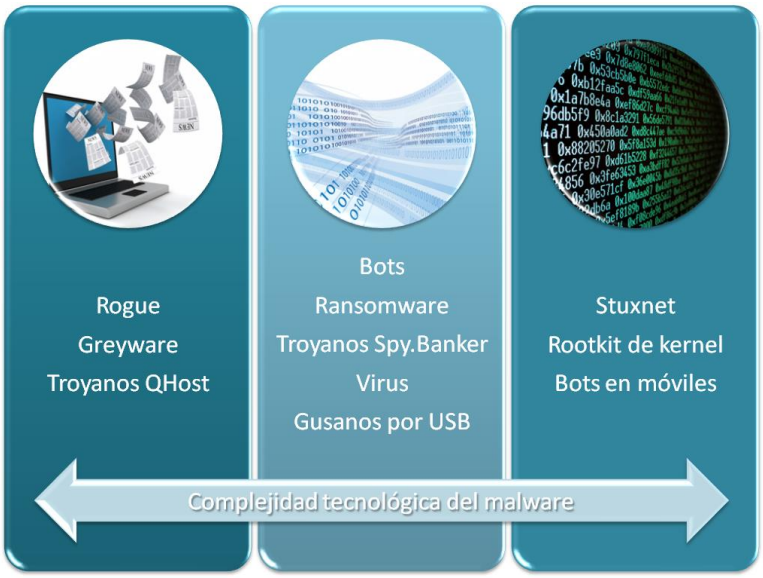

Imagen 5: Espectro de complejidad de amenazas

Esta polarización en cuanto a la complejidad técnica de la amenazas implica un mayor desafío para el usuario final dado que:

- Las amenazas más complejas aparecen con menor frecuencia pero su impacto puede ser muy alto.
- Las amenazas más sencillas son de fácil acceso para los desarrolladores malintencionados y suelen ser tener un nivel mayor de masividad.

Este segundo punto es de mayor importancia: ya no habrá botnet, o rogue en particular que representen una alta tasa de infección, o al menos serán cada vez más extraños. En cambio, presenciaremos la masificación de redes botnet en todo el mundo y de falsos antivirus que infectan a los usuarios. Sin embargo, esto estará complementado por una diversificación que implica que cada uno de ellos se propagará en valores bajos que son suficientes para generar rentabilidad a los criminales.

Por lo tanto, este contexto representará un riesgo para el usuario ya que la ausencia de amenazas que se destaquen puede generar una **falsa sensación de seguridad** cuando en verdad, los valores indican que los usuarios se siguen infectando. En 2011 el 80% de los usuarios encuestados por ESET Latinoamérica indicó haber sufrido una infección, valor apenas menor que en el 2010 (84%).
De esta forma, podemos concluir que la facilidad con la que los atacantes pueden multiplicar las variantes de las amenazas, representará un nuevo desafío para el 2012: estar protegidos de forma holística ante todo tipo de códigos maliciosos, independientemente de su complejidad técnica.