Tendencias 2013: vertiginoso crecimiento de malware para móviles

Índice

Autor:

Laboratorio de ESET Latinoamérica

Introducción

Cada fin de año, el Laboratorio de ESET Latinoamérica prepara un documento sobre las tendencias de los códigos maliciosos, el cibercrimen, y otros tipos de ataques informáticos, en base a lo observado y analizado durante el año en curso. Al respecto es importante señalar que una tendencia es una proyección que realiza la compañía de acuerdo al estado actual de las amenazas informáticas y el comportamiento de los cibercriminales.

Con todos estos antecedentes, se realiza una investigación de modo tal de poder prever cómo evolucionará el campo de la seguridad de la información durante el próximo año. Siguiendo esta línea, desde que se redacta este informe, las tendencias han ido cambiando. Por ejemplo, para 2010 la proyección principal fue "Madurez del crimeware", en 2011 "Las botnets y el malware dinámico", y para 2012, "El malware a los móviles". Si bien todos estos temas se relacionan entre sí ya que detrás de cada uno existe el interés de obtener rédito económico por parte de los cibercriminales, resulta particular que una misma tendencia experimente un crecimiento tan alto y en muy poco tiempo como lo ocurrido con el fenómeno de *malware mobile*.

Durante 2012 se pudo observar cómo los códigos maliciosos diseñados para Android se consolidaron como un objetivo fundamental para los ciberdelincuentes, quienes ante un mercado que crece a pasos agigantados, han comenzado a convertir con mayor celeridad a estos dispositivos en blancos de sus amenazas. En este sentido, el sistema operativo de Google ha experimentado durante el primer trimestre de 2012 y de acuerdo a IDC[1], un crecimiento de un 145.0% con respecto a la tasa de mercado y ventas del mismo período en 2011.

Sumado a lo anterior, Juniper Research estima que para 2013, la cantidad de usuarios que utilizan servicios bancarios a través de teléfonos inteligentes aumentarán a 530 millones de personas[2]. De acuerdo al mismo estudio, en 2011 sólo existían 300 millones de individuos que accedían al banco utilizando este medio. Frente a esta situación de crecientes ventas, variación de tipos de usos, y considerando la rápida evolución que ha tenido esta tecnología y los códigos maliciosos para móviles en 2012, es posible establecer como **principal tendencia para 2013, un crecimiento exponencial de *malware mobile* como también, una mayor complejidad de éstos ampliándose así el rango de acciones maliciosas que realizan en el dispositivo**.

Otro hito que se podrá observar en 2013 es la consolidación de un cambio de paradigma que se viene gestando en los últimos años. Se trata del modo en cómo los códigos maliciosos son propagados por los cibercriminales y los medios que utilizan para ese fin. En este sentido, la propagación de *malware* a través de dispositivos de almacenamiento extraíbles está disminuyendo para dar paso al uso de un intermediario con el objetivo de obtener nuevas víctimas. Un intermediario es un servidor web comprometido por un tercero con el fin de alojar amenazas informáticas. Posteriormente, los ciberdelincuentes proceden a enviar hipervínculos que dirigen al usuario hacia el código malicioso en cuestión. A su vez, parte de esta metodología es que toda la información robada es almacenada en estos servidores vulnerados para evitar involucrar computadoras personales.

Considerando lo anterior, ¿Qué tendencias podrán observarse el próximo año? Este informe tiene como objetivo, aclarar y explicar aquella pregunta de tal modo que los usuarios tanto corporativos como hogareños puedan adoptar las medidas necesarias para protegerse adecuadamente de las últimas amenazas informáticas.

Importante aumento de *malware* para móviles

A partir de 2010, los códigos maliciosos para dispositivos móviles así como dicho mercado, empezaron a experimentar grandes cambios que marcarían la historia posterior de este tipo de amenazas. En primer lugar, Android comenzó a posicionarse como el sistema operativo *mobile* más utilizado dentro de la competencia. Por otra parte, en ese mismo año, *FakePlayer* se convertía en el primer código malicioso diseñado para la plataforma de Google. Luego, en 2011 el Laboratorio de ESET Latinoamérica vaticinaba que este sistema operativo dentro de los móviles, se convertiría un año más tarde en el más atacado por códigos maliciosos… Y así fue. Un año después, la creación de códigos maliciosos y variantes para Android no solo aumentaron considerablemente sino que también la complejidad de estos ataques, el tiempo y recursos que destinan los ciberdelincuentes en el desarrollo de *malware* para *mobile*. Resulta lógico que un sistema operativo móvil con una tasa de participación de mercado del 64,1%[3] sea tan apetecible para los ciberdelincuentes, pues tienen una mayor probabilidad de obtener ganancias ilícitas en comparación con otro cuya cantidad de usuarios, sea inferior.

A continuación, el siguiente gráfico muestra la tasa de participación de los principales sistemas operativos móviles que existen en la actualidad:

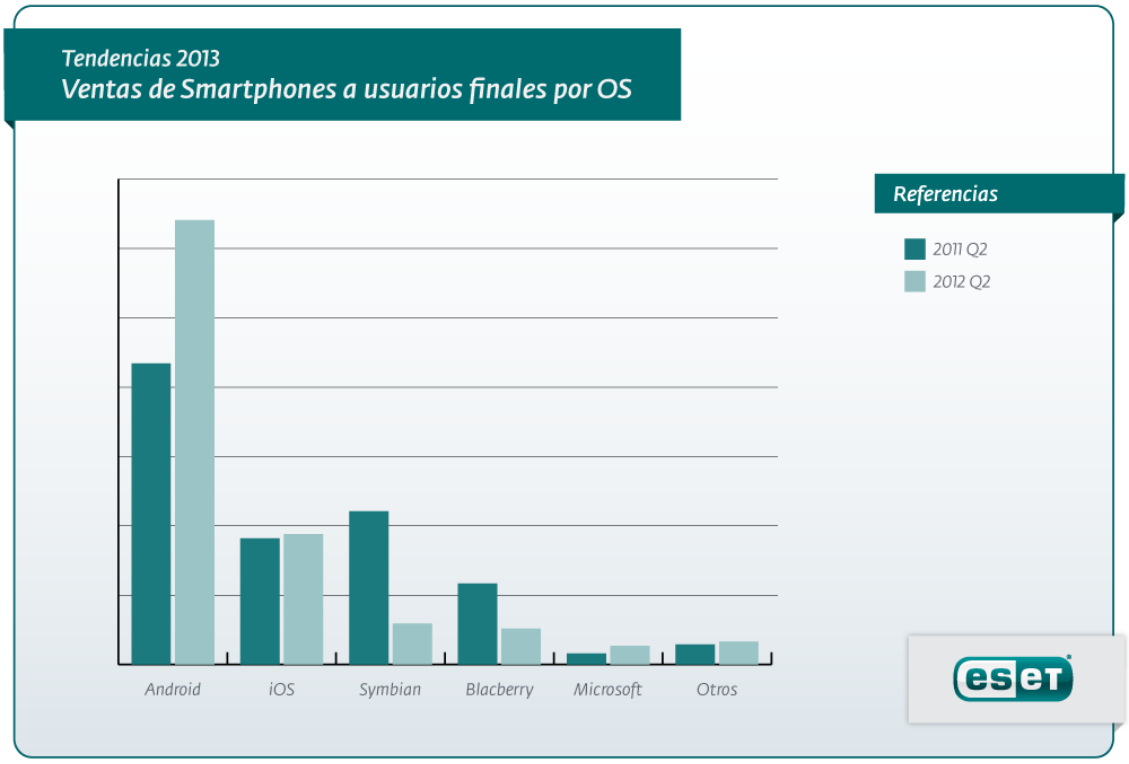
---

[1] De acuerdo a IDC, los smartphones con Android y iOS aumentaron sus cuotas de mercado en el primer trimestre de 2012. Disponible en http://www.idc.com/getdoc.jsp?containerId=prUS23503312.

[2] Juniper Research. Whitepaper: banca en cualquier momento y cualquier lugar. Disponible en http://www.juniperresearch.com/whitepapers/anytime_anywhere.

[3] Fuente: Ventas de smartphones a usuarios finales por sistemas operativos 2Q12, Gartner.

Disponible en http://www.gartner.com/it/page.jsp?id=2120015.



Fuente: Ventas de smartphones a usuarios finales por sistemas operativos 2Q12, Gartner.

Disponible en http://www.gartner.com/it/page.jsp?id=2120015

Al igual que en el mismo período que el año pasado (Q2), se puede notar que Android experimentó un crecimiento de 20,7%, iOS (Apple) un 0,6% y Microsoft 1,1%. Los demás sistemas operativos decrecieron con respecto a 2011. Symbian, sufrió una baja mayor (16,2%) y BlackBerry de 6,5%.

A medida que la cuota de mercado de Android crezca y los usuarios lo utilicen cada vez más para almacenar información personal y corporativa, realizar transacciones bancarias, o consultar cualquier otro servicio similar, los cibercriminales desarrollarán más *malware* para cumplir el objetivo de robar información y de ese modo, obtener ganancias ilícitas. En base a esto y al igual que los códigos maliciosos diseñados para computadoras, el principal motivo e interés de los ciberdelincuentes por crear este tipo de amenazas sigue siendo la obtención de dinero. Esto se reafirma con el descubrimiento del caso "Dancing Penguins" en donde a través del modelo de negocio ilegal pagar por instalar (PPI – *Pay Per Install*), cibercriminales cobran entre 2 y 5 dólares por instalar algún código malicioso en dispositivos Android.

De acuerdo a una encuesta realizada por ESET Latinoamérica sobre el uso que le dan los usuarios a los dispositivos móviles, se pudo determinar que aunque el almacenamiento de información privada y contraseñas no es la tarea que más realizan las personas por el momento, sí posee un porcentaje bastante considerable. A continuación, se muestra el gráfico con las estadísticas al respecto:

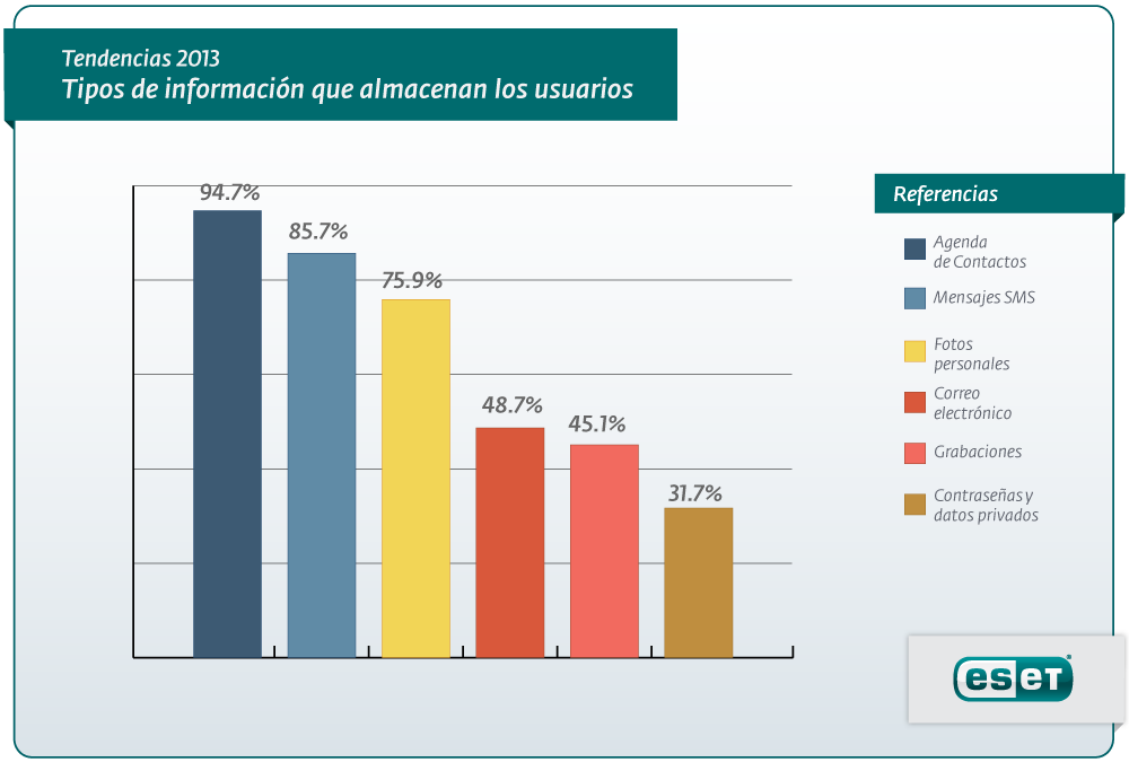


Gráfico 1 Tipo de información que almacenan los usuarios en dispositivos móviles

Como se puede observar, la información más utilizada por los usuarios en estos dispositivos es la agenda de contactos. En base a esto, existen códigos maliciosos para Android diseñados con el fin de robar este tipo de datos. Esto le resulta útil a los ciberdelincuentes para poder obtener nuevas víctimas. Las **contraseñas e información privada ocupan un 31,7%** de las preferencias, estadística que seguirá aumentando a medida que los teléfonos inteligentes sigan evolucionando tecnológicamente, y los servicios se adapten a esta tendencia desarrollando aplicaciones y sitios web optimizados específicamente para *smartphones*.

Crecen detecciones de *malware* para Android

La primera estadística que avala este vertiginoso aumento de *malware* para móviles, y que además, permite establecer como **tendencia para 2013 un crecimiento exponencial de códigos maliciosos para Android**, es que en 2012 la cantidad de detecciones únicas crecieron **17 veces a nivel global** con respecto a 2011**.** En relación a los países que experimentaron el mayor crecimiento de detecciones de *malware* para Android, expresado en cantidad de veces, se destacan Ucrania con 78 veces, Rusia 65, e Irán 48. En cambio, si se considera la cantidad de detecciones ocurridas en 2012 independientemente de lo acontecido el año anterior, China, Rusia e Irán figuran entre los tres primeros con más cantidad de detecciones a nivel mundial. En sexto lugar aparece México, lo que lo posiciona como el país de Latinoamérica más afectado en cuanto a detecciones de códigos maliciosos para la plataforma móvil de Google. De acuerdo a estos antecedentes, se puede aseverar que **el crecimiento de códigos maliciosos para Android en 2013 seguirá aumentando con mayor vertiginosidad.**

En relación a la cantidad de familias de *malware* para Android, es decir, códigos maliciosos lo suficientemente distintos como para poder ser clasificados de forma única, el año pasado existían 51 familias en comparación con 56 que se han reportado hasta noviembre de 2012. Aunque esta cifra no subió considerablemente durante 2012, más adelante en el documento se puede observar cómo la **cantidad de firmas y variantes sí aumentaron considerablemente**, por lo tanto, **el número de amenazas para Android seguirá creciendo independientemente del total de familias,** de forma similar a lo que ocurre con Windows. Es importante tener en cuenta que a los ciberdelincuentes les resulta más sencillo modificar un código malicioso previamente conocido (variante) que crear uno desde cero. En la siguiente página aparecen agrupadas las familias de acuerdo al año y mes de descubrimiento.

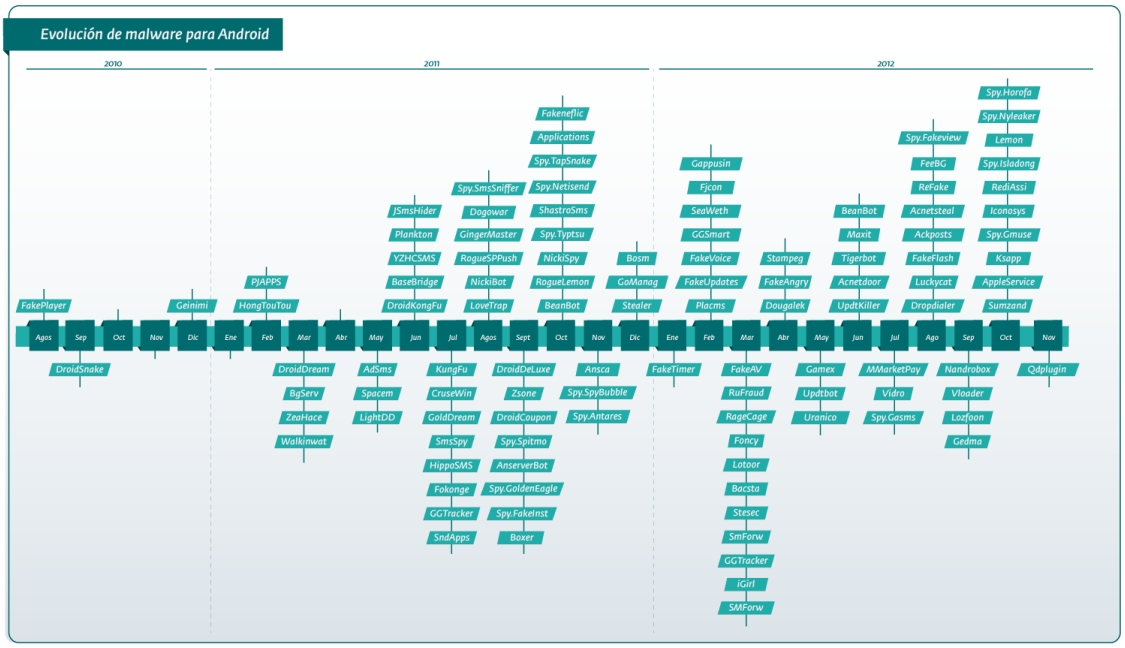


Imagen 1 Surgimiento de familias de *malware* para Android

De acuerdo a las familias anteriormente mencionadas y a la acción maliciosa (*payload*) que realizan estos *malware* en dispositivos con Android, es posible clasificar dichos comportamientos en: robo de información (Spyware), envío de mensajes SMS a números Premium, y la transformación de los equipos en zombis. De acuerdo a esto, se obtiene el siguiente gráfico:

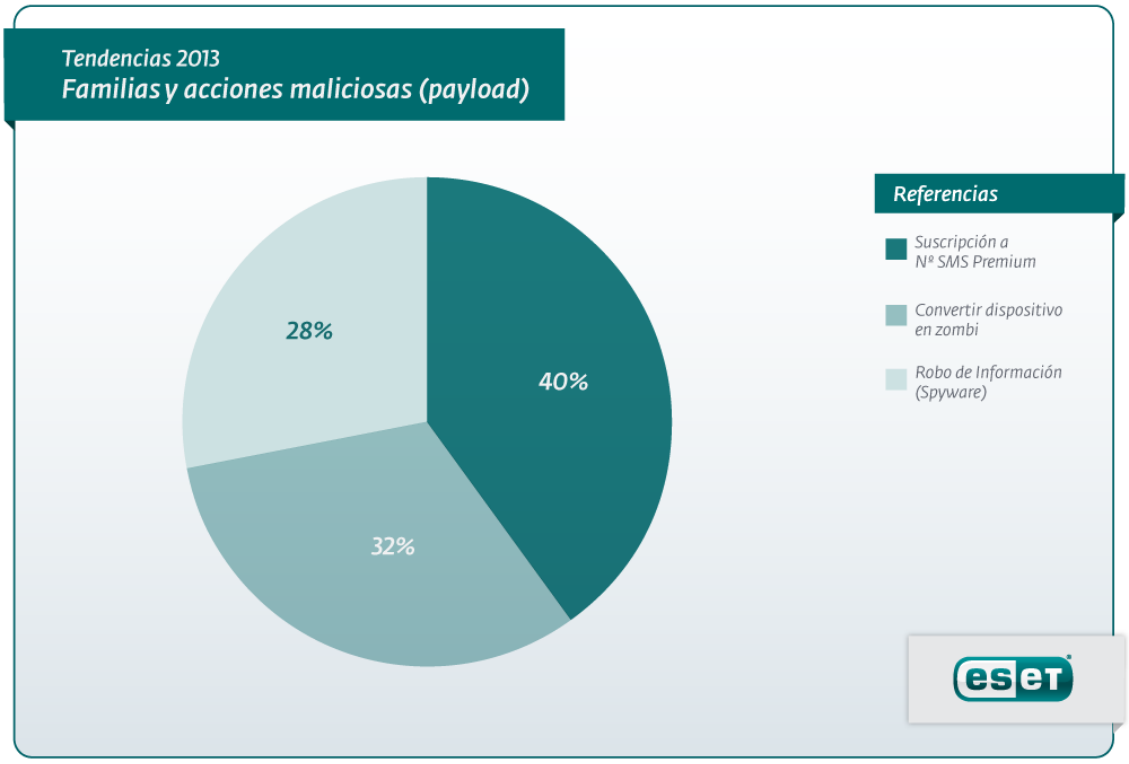


Gráfico 2 Familias de 2010, 2011 y 2012 y las acciones maliciosas que realizan.

Como puede notarse, la mayoría de estas familias tienen como objetivo suscribir a la víctima a números de mensajería Premium. Por otra parte, existen amenazas que transforman estos dispositivos en zombis, es decir, que quedan a merced de ciberdelincuentes, quienes pueden realizar acciones de forma remota como instalar otros códigos maliciosos, robar determinada información, modificar parámetros de configuración, entre otras. En tercer lugar, están aquellos códigos maliciosos que roban información como contactos telefónicos, mensajes de texto, o datos que sirven para identificar el dispositivo, como el número IMEI. A diferencia de los que transforman el teléfono inteligente en zombi, los que roban información no le entregan el control total del equipo al ciberdelincuente. Finalmente, existen casos particulares como *Android/Stampeg* cuya función es insertar una imagen extra en los archivos JPG que se encuentren almacenados en el *smartphone*, lo que puede producir el colapso de la tarjeta de memoria. Por su parte, *Android/MMarketPay* es capaz de adquirir aplicaciones pagas de un mercado chino sin el consentimiento del usuario mientras *Android/FakeFlash*, simula ser un *plugin* de Flash que redirige al usuario hacia un sitio web determinado.

Considerable aumento de variantes

La cantidad de variantes de códigos maliciosos para Android también aumentó considerablemente en 2012. Una variante es una modificación de un *malware* específico y conocido. Los ciberdelincuentes modifican la estructura y el código de una amenaza para crear una nueva (basada en la anterior) con el fin de añadir novedosas funcionalidades maliciosas o evadir la detección de los antivirus. Asimismo, puede suceder que otro cibercriminal obtenga una amenaza existente y la modifique para obtener rédito económico para sí mismo. A continuación se muestra un gráfico con cuatro familias de *malware* para Android y la cantidad de variantes que aparecieron en 2011 y 2012. Es importante destacar que para cada variante nueva que aparece, los laboratorios de ESET le asignan una letra que va incrementándose de acuerdo al abecedario y la cantidad respectiva. Por ejemplo, dos variantes de un supuesto código malicioso se catalogarían como *Amenaza.A* y *Amenaza.B*. En el caso de superar el número de letras disponibles, se repite el abecedario: .AA, .AB, etc.

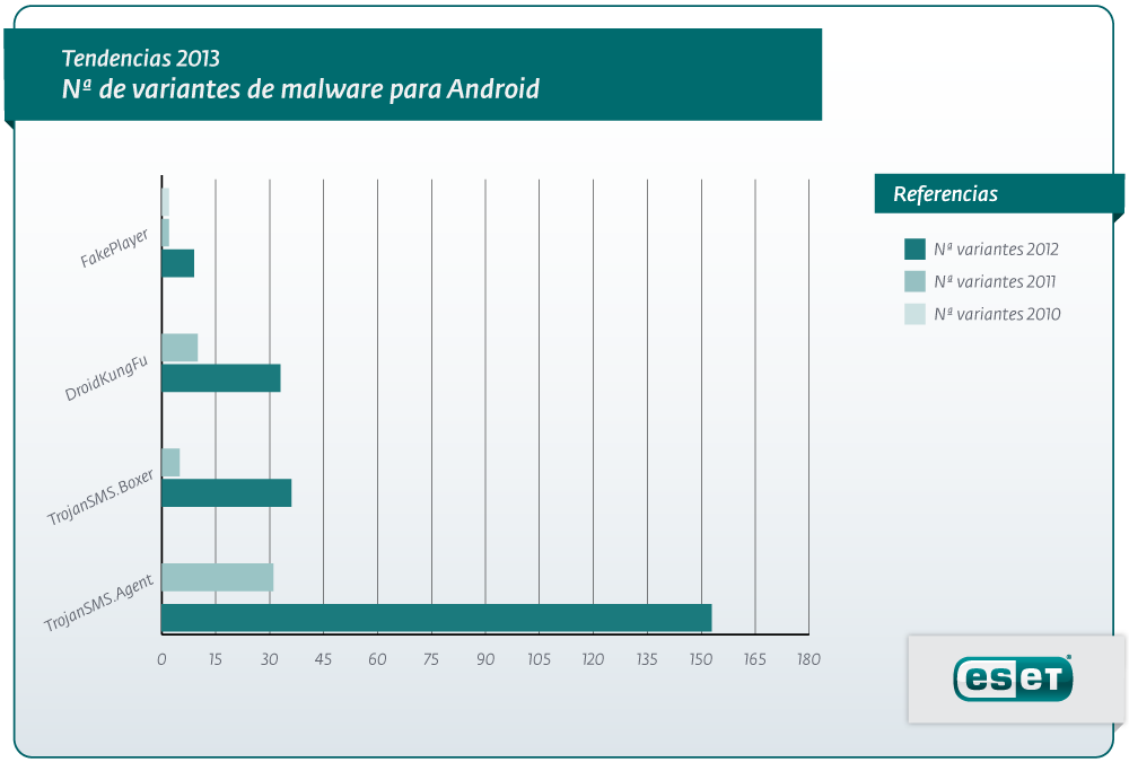


Gráfico 3 Número de variantes de códigos maliciosos para Android

Como se puede apreciar, el troyano que experimentó el mayor crecimiento en 2012 con respecto a 2011 y la cantidad de variantes es *TrojanSMS.Agent*. Éste corresponde a una numerosa familia de códigos maliciosos distintos entre sí pero que tienen como objetivo común, suscribir a la víctima a números de mensajería Premium. En 2011 aparecieron tan solo 31 variantes en comparación a 2012 cuya cantidad alcanza 153 modificaciones. Le sigue otro troyano SMS denominado *Boxer*. Tanto este *malware* como algunas particularidades serán explicadas en este documento más adelante, sin embargo, es importante notar que en 2011 esta familia estaba conformada por 5 variantes. En la actualidad, la cifra aumentó a 36. Con *DroidKungFu* sucedió algo similar, 10 variantes en 2011 y 33 en 2012. Finalmente está el caso de *FakePlayer*, el primer *malware* para Android. En 2010 aparecieron dos variantes, en 2011 también, y 2012, 9.

Mayor cantidad de firmas para detectar *malware* móvil

La cantidad de firmas desarrolladas por ESET en 2011 con respecto al 2012 para detectar variantes de ocho familias de códigos maliciosos diseñados para Android, también avalan este importante aumento de *malware* para *mobile*. Asimismo, esto se debe al vertiginoso crecimiento que experimentaron las variantes de este tipo de códigos maliciosos como pudo apreciarse anteriormente. A continuación se muestra un gráfico con cuatro familias. Para cada una, se expresa la cantidad de firmas desarrolladas en 2011 y 2012. Al respecto, es importante señalar que una firma es una porción de código destinada a detectar una o más amenazas, por lo tanto, si el número de firmas aumenta, es por la necesidad de detectar correctamente todos los *malware* nuevos que aparecen a diario.

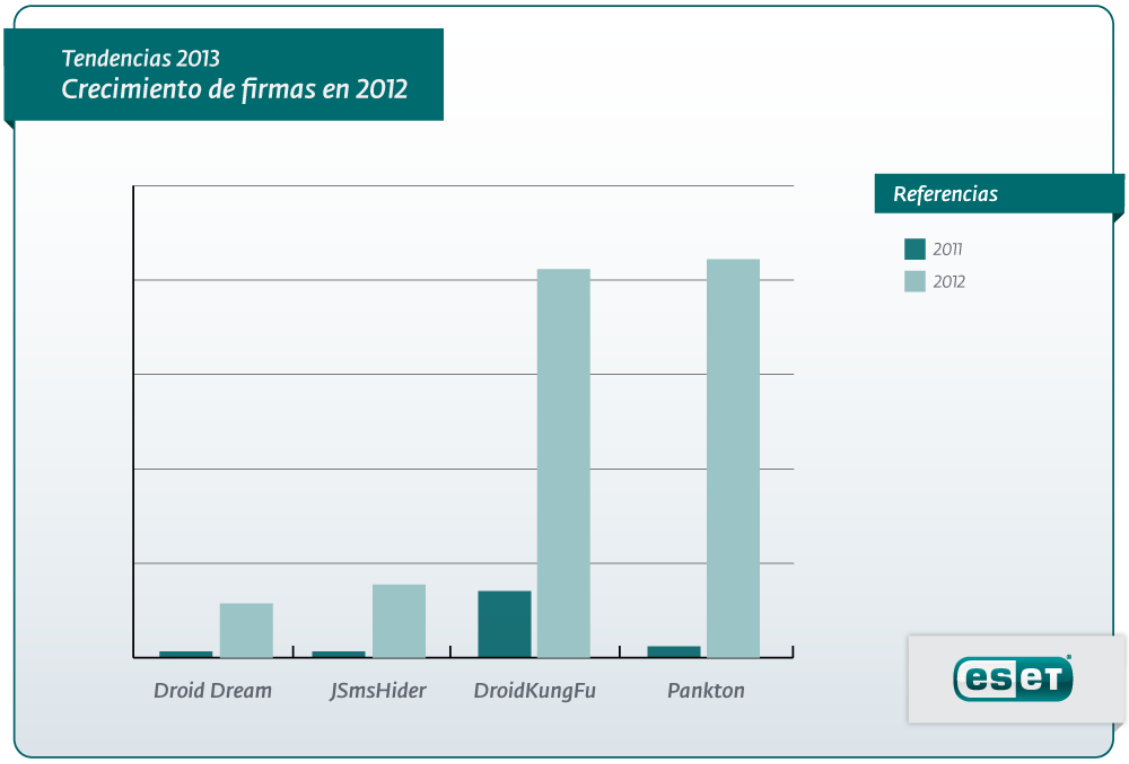


Gráfico 4 Crecimiento de firmas en 2012 en comparación a 2011

De acuerdo al gráfico anterior, la familia de troyanos que experimentó el mayor crecimiento en 2012 con respecto al año pasado y la cantidad de firmas necesarias para detectar todas las modificaciones, fue Plankton. **Esta amenaza creció 35 veces con respecto al año pasado**. Le sigue JSmsHider con 12, DroidDream con 9, y DroidKungFu con 6 veces respectivamente. Otras amenazas experimentaron un aumento menor como BaseBridge que creció 3 veces, LightDD 2, y GoldDream y Geinimi una vez con respecto a 2011 y la cantidad de firmas agregadas.

Troyanos SMS: las amenazas más comunes para *smartphones*

Con respecto al tipo de código malicioso más común para dispositivos Android, y considerando que los mayores aumentos en el número de variantes fueron protagonizados por dos amenazas de este tipo, se destacan los troyanos SMS. Durante 2012, de la totalidad de reportes de detecciones únicas de *malware* desarrollados para el sistema operativo de Google , el troyano *Android/TrojanSMS.Boxer.AQ* encabeza la lista. Luego, le sigue *Android/Plankton.H* y *Android/TrojanSMS.Agent.BY.Gen*[4]. En la siguiente página, se muestra una infografía que explica el funcionamiento general de este tipo de código malicioso para móviles:

[4] .Gen son aquellas firmas diseñadas para detectar modificaciones menores de una variante de forma genérica, es decir, sin la necesidad de contar con firmas específicas para cada amenaza.

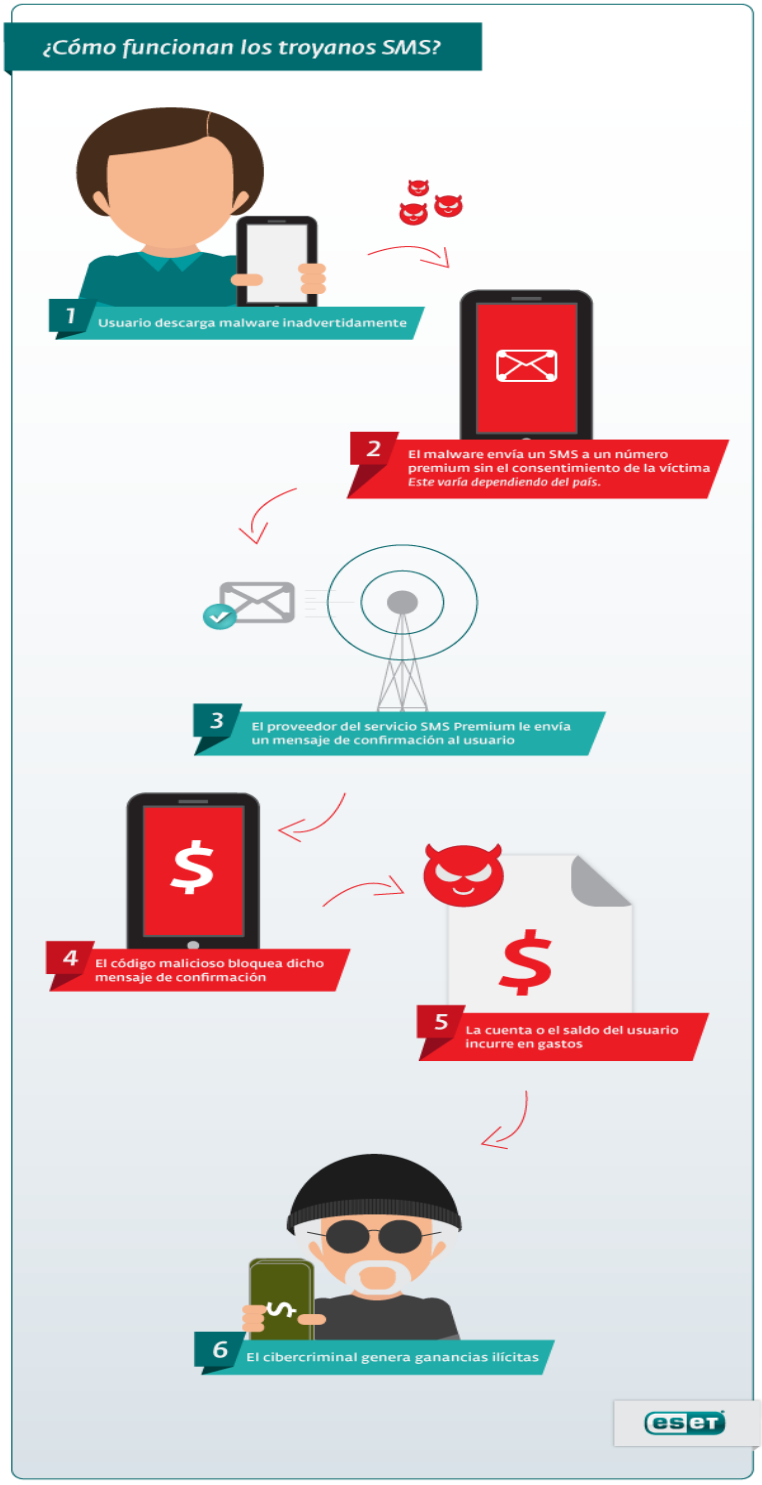


Imagen 2 Funcionamiento de troyanos SMS

Mientras este tipo de negocio fraudulento siga siendo rentable y fácil de implementar por parte de los ciberdelincuentes, es probable que los troyanos SMS sigan siendo la categoría de amenaza móvil más común durante 2013.

¿Qué sucede con América Latina?

Pese a que China, Rusia e Irán son los tres países cuyos índices figuran entre los más altos del mundo en la detección de este tipo de códigos maliciosos, países latinoamericanos como México, Argentina, Perú y Chile también se vieron afectados por este fenómeno. En la siguiente tabla se muestra este crecimiento expresado en cantidad de veces que aumentó en 2012 con respecto a igual período de 2011:

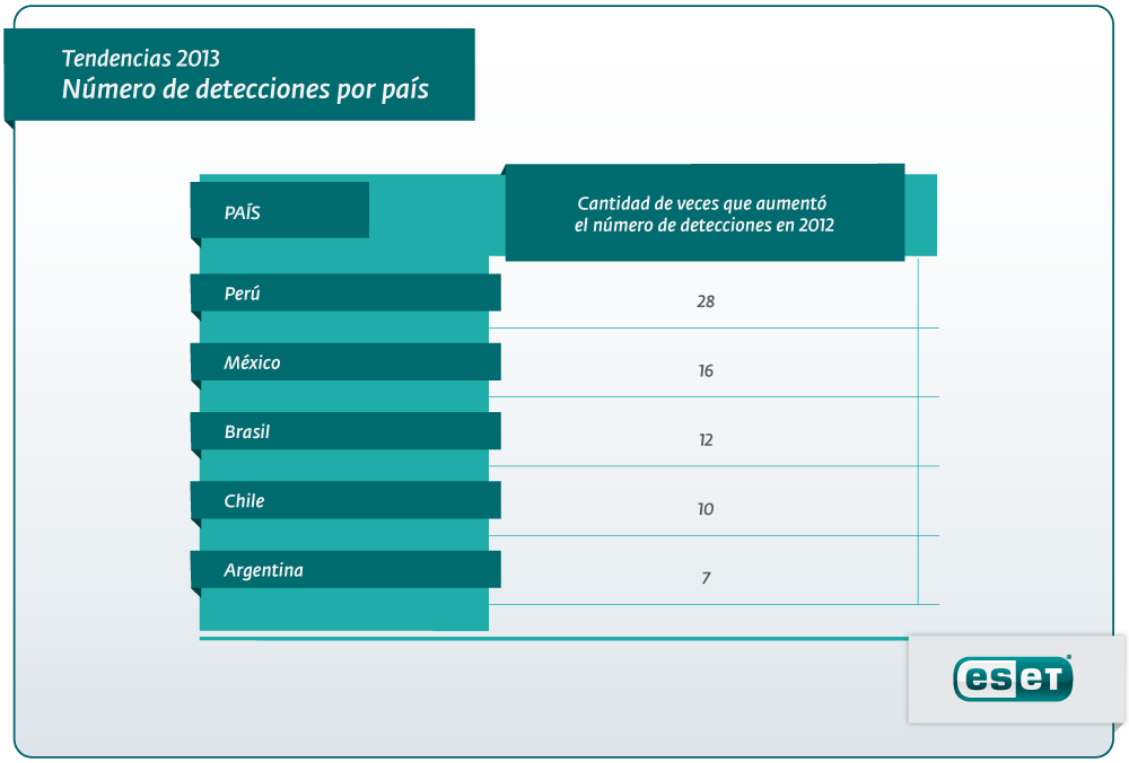


Tabla 1 Países latinoamericanos y cantidad de veces que aumentó N° detecciones 2012 vs 2011

De los países de América Latina, Perú fue el más afectado por esta tendencia de progresivo aumento con un crecimiento de 28 veces en comparación con 2011. Le sigue México (16) y Brasil (12). Aunque Chile y Argentina no registraron un alza tan considerable como las otras naciones (10 y 7 veces respectivamente), continúan siendo de los países de la región con mayores índices de detección de *malware* para Android.

Boxer: troyano SMS afecta a Latinoamérica

Otro hito importante que marcó el desarrollo del *malware* móvil durante 2012 fue el descubrimiento de una variante de *Boxer*, un troyano SMS que tiene como objetivo suscribir a la víctima a variados números de mensajería premium con el fin de generarle ganancias ilícitas a los ciberdelincuentes. Esta amenaza posee dos particularidades con respecto a otros códigos maliciosos similares: es capaz de afectar 63 países alrededor del mundo y dentro de esa lista, 9 pertenecen a Latinoamérica (**Argentina, Brasil, Chile, Perú, Panamá, Nicaragua, Honduras, Guatemala y México**). Asimismo, *Boxer* fue encontrado en 22 aplicaciones pertenecientes a Google Play. Si el usuario no es precavido y se infecta con dicha amenaza, el código malicioso procede a detectar el país y la compañía de telefonía móvil a la cual pertenece el dispositivo. Posteriormente, procede a enviar tres SMS a números premium correspondientes al país en cuestión. A continuación, se muestra un gráfico con los nueve países de América Latina que afecta Boxer:

Gráfico 5 Nueve países de Latinoamérica que ataca Boxer

Pese a que es común encontrar troyanos SMS que afecten países determinados o incluso una región como Europa del Este, *Boxer* es capaz de afectar a Europa, Asia y América, por lo tanto, es uno de los códigos maliciosos para teléfonos inteligentes con mayor potencial de propagación que se haya encontrado.

Para saber más sobre este *malware*, puede consultar y descargar el informe Troyano SMS Boxer.
Como puede notarse en las páginas anteriores, el fenómeno de los códigos maliciosos para teléfonos inteligentes con Android experimentará un alza considerable en el mundo y América Latina. Sin embargo, no es la única tendencia que crecerá en 2013. El año 2012 ha estado marcado entre otras cosas, por algunos casos de espionaje industrial como los ocurridos en el mundo con *Flamer* y *Gauss* tal como aparece en el Blog del Laboratorio de ESET Latinoamérica. No obstante, el primer reporte de un ataque dirigido fue *Stuxnet*, gusano que afectó mayoritariamente a las plantas de enriquecimiento de uranio de Irán. Aunque dichos ataques se han concentrado principalmente en Oriente Medio, se reportó uno que afectó a un país de Latinoamérica como se describe más adelante en este documento.

Propagación de *malware* vía sitios web

Con la introducción de la primera versión comercial de Windows XP en 2001, y la masificación de los dispositivos de almacenamiento extraíbles (*pendrive*), se comenzó a gestar una era marcada por los gusanos que se propagan a través de estos medios aprovechándose de una vulnerabilidad de diseño del Windows XP (*Autorun*). Gracias a que este problema fue solucionado en 2009, y que los usuarios han migrado hacia nuevas versiones de Microsoft Windows, la cantidad de códigos maliciosos que continúan utilizando esta técnica han ido disminuyendo en los últimos años.

De hecho, en el transcurso de 2012 aquellas detecciones relacionadas con esta vulnerabilidad de diseño (*INF/Autorun* y otras) han ido decreciendo sostenidamente. Por otro lado, detecciones genéricas como *HTML/ScrInject.B*, *HTML/Iframe.B*, *JS/Iframe* y *JS/TrojanDownloader.Iframe.NKE* comenzaron a ocupar el segundo lugar y otros puestos respectivamente, en el Ranking de propagación de amenazas mensuales que prepara ESET Latinoamérica. Todas esas firmas tienen como objetivo detectar diversos sitios web que han sido comprometidos y modificados por un atacante para propagar *malware*. En la mayoría de los casos, son páginas legítimas que pertenecen a empresas de diversos rubros y que, producto de alguna vulnerabilidad, protección insuficiente, o configuración inadecuada, han sido modificadas por un ciberdelincuente que ha logrado obtener acceso al servidor en donde se encuentran alojadas. Posteriormente, los cibercriminales proceden a inyectar *scripts* maliciosos o etiquetas *Iframe* que redirigen al usuario hacia la descarga de alguna amenaza. En algunos casos la información que roban también la suben a este servidor comprometido con el fin de evitar utilizar computadoras personales y de ese modo, dificultar la identificación de estos individuos.
En la siguiente tabla se pueden observar los crecimientos porcentuales que han experimentado durante 2011 y 2012, algunas firmas genéricas utilizadas para detectar códigos maliciosos que se propagan a través de dispositivos de almacenamiento extraíbles y sitios web comprometidos.

Tendencias 2013
Crecimiento promedio de Autorun y firmas para detectar web comprometidas

FIRMAS	Crecimiento promedio 2011	Crecimiento promedio 2012	Tendencias para 2013
INF/Autorun	5.8%	5.3%	↓
HTML/Scrinject.B	1.7%	4.3%	↑
JS/TrojanDownloader.Iframe.NKE	0.9%	1.2%	↑
JS/Iframe	0.6%	1.7%	↑
HTML/Iframe.B	1.5%	3.0%	↑

Tabla 2 Crecimiento promedio de Autorun y firmas para detectar web comprometidas 2011 vs 2012.

En la tabla anterior, es posible dilucidar cómo Autorun decreció en 2012 y todas las otras firmas relacionadas a sitios comprometidos aumentaron. Es importante destacar que los números anteriores corresponden al promedio de las detecciones mensuales para cada año y en algunos casos, existen detecciones que no estuvieron presentes durante todos los meses del año
A continuación, se presenta un gráfico que comprende todo 2011 hasta septiembre de 2012 en lo que respecta al porcentaje de detecciones asociadas a gusanos Autorun y amenazas que son propagadas a través de un servidor web vulnerado. Con el fin de simplificar la interpretación de la información, las firmas relacionadas a sitios web comprometidos han sido clasificadas en "JS" (JavaScript) y "HTML", y se ha omitido la nomenclatura "INF" de la firma Autorun.

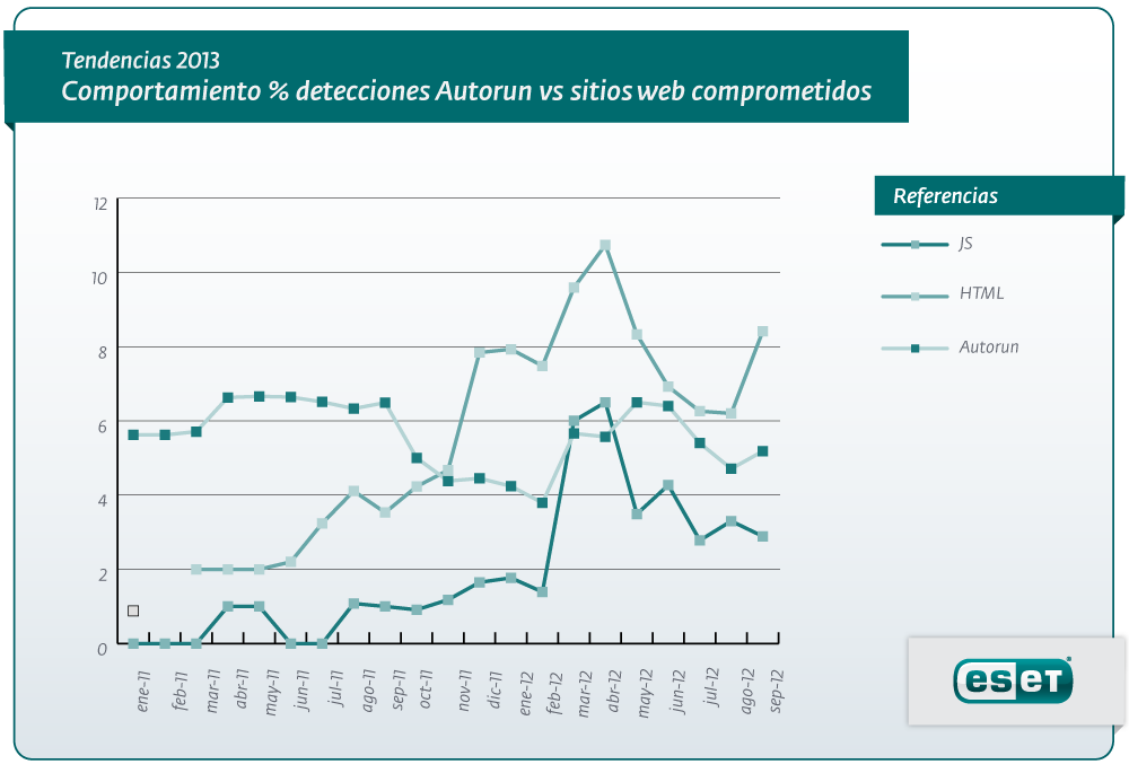


Gráfico 6 Comportamiento porcentual de detecciones Autorun vs sitios web comprometidos (2011-septiembre 2012)

Como puede observarse, a principios de 2011 las firmas relacionadas a sitios web comprometidos eran prácticamente nulas. Conforme fue avanzando el año pasado, la detección Autorun comenzó a disminuir hasta que en septiembre de 2011, fue superada por las detecciones tipo HTML. Asimismo, tanto HTML como JS han ido experimentando un crecimiento considerable a través del tiempo. Esto permite establecer como **segunda tendencia para 2013, un aumento sostenido en el uso de esta técnica para infectar potenciales víctimas** y por ende, un decrecimiento en el uso de gusanos que se aprovechan de los dispositivos de almacenamiento extraíbles con este fin.

Antes de esta tendencia de cambio en los métodos de propagación de códigos maliciosos, los cibercriminales propagaban directamente el *malware* a través de algún medio (correo, redes sociales, recursos corporativos, dispositivos de almacenamiento extraíble, entre otros) hacia la computadora de la víctima tal como puede apreciarse en el siguiente esquema:

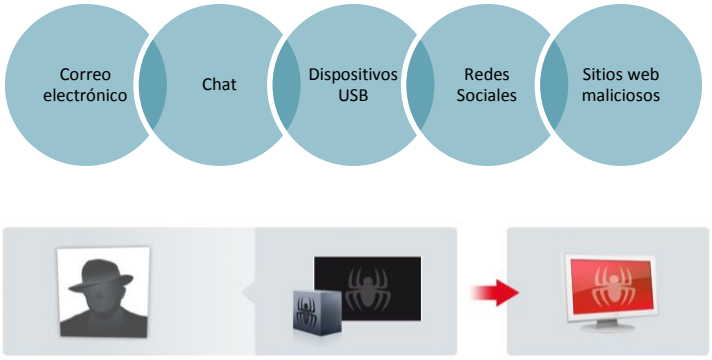


Imagen 3 Método tradicional de propagación de *malware*

Con este nuevo paradigma de distribución de *malware* utilizando sitios web comprometidos, los ciberdelincuentes recurren a un intermediario (servidor comprometido) para infectar a las víctimas como puede verse a continuación:

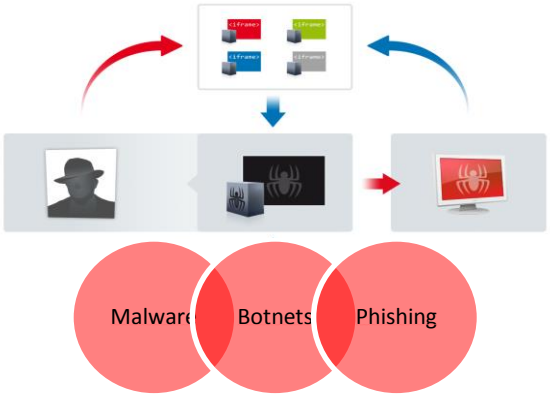


Imagen 4 Propagación utilizando un intermediario

Para que esta situación de propagación vía sitios web ocurra, los cibercriminales recurren a las siguientes etapas:

1. El ciberdelincuente explota una vulnerabilidad presente en un servidor web. Allí modifica el sitio original para poder inyectar código malicioso.
2. Comienza a propagar el enlace que dirige hacia la amenaza alojada en el servidor comprometido. El hipervínculo es enviado a una lista de usuarios a través del correo electrónico, redes sociales, o cualquier medio que le sirva para dicho fin.
3. El usuario visita este sitio y descarga el *malware*. En algunos casos, la información que se le roba a la víctima también es almacenada en ese intermediario.

Antes de esta tendencia, los cibercriminales omitían todo este proceso y propagaban el código malicioso directamente hacia las potenciales víctimas. Asimismo, la información que robaban era almacenada en sus propias computadoras.

Por otro lado, sumada esta nueva técnica de propagación también puede considerar la táctica Black Hat SEO. Mediante esta técnica, los cibercriminales posicionan ilícitamente los sitios web maliciosos dentro de los primeros resultados de una búsqueda realizada en un buscador. Por lo general utilizan palabras claves (*keywords*) relacionadas a tragedias o temas de interés masivo, para que las potenciales víctimas sientan curiosidad y visiten dichas páginas con facilidad. Finalmente, es importante destacar que los ataques de

phishing suelen ser desplegados a través de un intermediario como también, aquellos centros de comando y control (C&C) pertenecientes a una red botnet.

Otras tendencias

En conjunto con un vertiginoso aumento en la cantidad de códigos maliciosos diseñados para Android, y la propagación de *malware* utilizando un intermediario o servidor comprometido, se suman otros temas de interés relacionados a la Seguridad de la Información. Por ejemplo, el Laboratorio de ESET Latinoamérica en 2012 descubrió el primer caso conocido de espionaje industrial en la región. Por otro lado, las botnets, la nube, casos de fuga de información y hacktivismo, continúan siendo tópicos recurrentes que de una u otra forma, se han ido consolidando con el paso del tiempo. Asimismo, los códigos maliciosos diseñados para otras plataformas más allá de los sistemas operativos comunes, también han ido apareciendo durante el transcurso de 2012. En las siguientes páginas se explican cada uno de estos temas.

Operación Medre: espionaje industrial en Latinoamérica

A partir de febrero de 2012, ESET Latinoamérica notó un significativo aumento en la tasa de detección de un código malicioso un tanto particular: *ACAD/Medre*. Otra arista novedosa de este caso era que la gran mayoría de estas infecciones provenían principalmente de un país específico de América Latina, Perú. De acuerdo a información recopilada por el sistema de alerta temprana ESET Live Grid, el 96% de dichas detecciones provenían de esa nación. Una investigación posterior permitió determinar que este gusano diseñado para robar planos y proyectos realizados con AutoCAD, logró sustraer aproximadamente 10.000 archivos pertenecientes a empresas del Perú. Por esa razón, la **Operación Medre se convirtió en el primer caso conocido de espionaje industrial en afectar la región de Latinoamérica**.

Imagen 5 Mapa de detección de ACAD/Medre

Es posible que durante el transcurso de 2013, se descubran más casos de espionaje industrial en América Latina, sin embargo, no necesariamente se tratarán de nuevos ataques. Esto se debe a que en algunas oportunidades, al ser códigos maliciosos diseñados específicamente para atacar empresas o países en particular, su descubrimiento, detección y solución puede tardar bastante tiempo en concretarse. Dicha situación podría reducirse si se realizara un esfuerzo en conjunto con las organizaciones y la industria de la seguridad de la información. Para mayor información, es posible consultar el informe Operación Medre: ¿espionaje industrial en Latinoamérica?

Botnets en alza

A partir de 2010, los códigos maliciosos diseñados con el objetivo de robar información y generarles ganancias económicas a los ciberdelincuentes comenzaron a consolidarse con ímpetu. Durante 2011 se pudo observar un aumento de estas amenazas y en el presente año han continuado aumentando sostenidamente tanto a nivel mundial como en Latinoamérica. El gusano *Dorkbot* es sin dudas una de las amenazas más prolíficas de la región, capaz de convertir el equipo de la víctima en zombi. Un ejemplo del alcance de esta amenaza es que los integrantes del Laboratorio de Análisis e Investigación de ESET Latinoamérica encontraron una botnet compuesta por más de 80.000 equipos zombis pertenecientes principalmente a Chile (44%), Perú (15%) y Argentina (11%). *Dorkbot* ha sido propagado utilizando diversos temas que aprovechaban la Ingeniería Social, tales como supuestos videos de accidentes sufridos por Jennifer López, Hugo Chávez, Lionel Messi y Alexis Sánchez. Asimismo, han recurridos a falsos concursos y premios con el fin de

conseguir nuevas víctimas. Técnicamente, algunas variantes de esta amenaza se propagan mediante dispositivos de almacenamiento extraíble, redes sociales, Windows Live Messenger y otros canales. Además esta amenaza roba información confidencial como usuarios y contraseñas de cuentas de correos electrónicos, entre otros datos. Por ejemplo, en este caso se pudo determinar que el 88% de las cuentas de correos que robaron los cibercriminales utilizando Dorkbot, pertenecen a empresas. El 12% restante son de servicios como Gmail, Hotmail o Yahoo!. En la siguiente página se muestra un gráfico con la cantidad de equipos zombis (bots) y tipos de usuarios de acuerdo al sistema operativo.

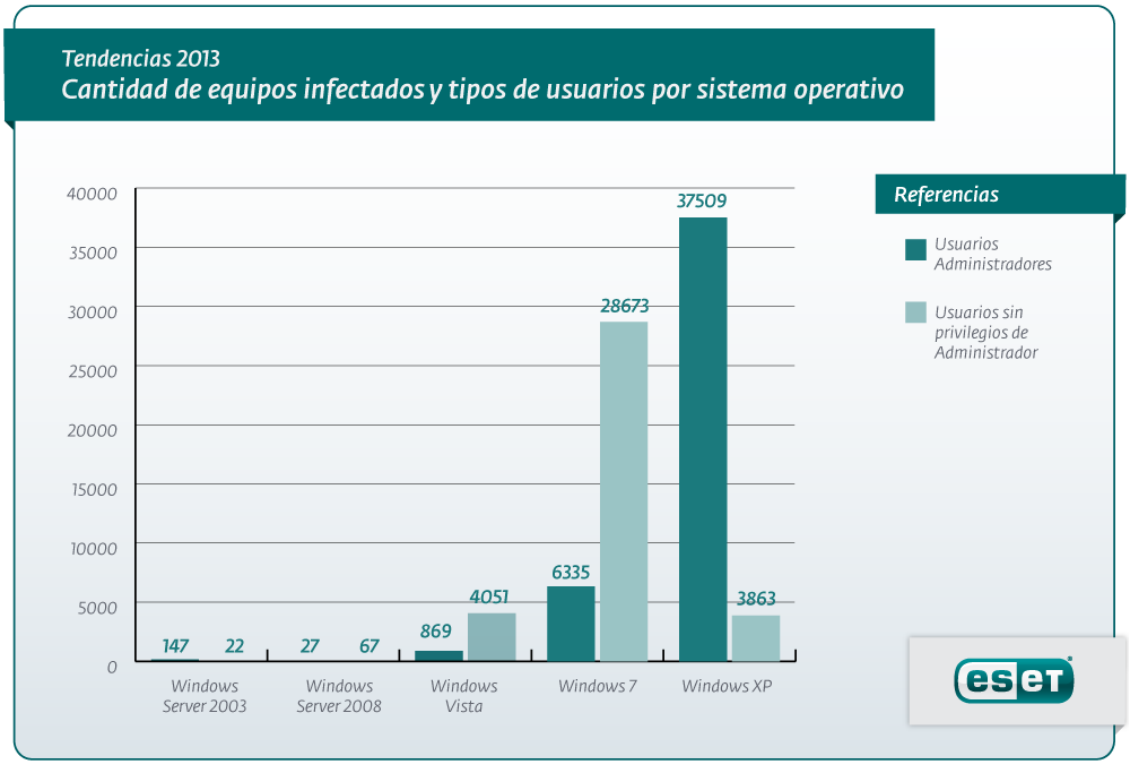


Gráfico 7 Número de sistemas infectados y tipos de usuarios por sistema operativo.

En base a dicho gráfico, se puede apreciar que la mayoría de los usuarios infectados todavía posee una versión de Windows XP y utiliza una cuenta de usuario con privilegios de administrador. Aunque esta amenaza es capaz de funcionar bajo cualquier tipo de cuenta, es importante que las personas se limiten a utilizar perfiles con permisos restringidos para el uso diario de sus equipos, de este modo, algunos códigos maliciosos son incapaces de ejecutarse, o si lo hacen, su funcionamiento se ve limitado. Debido a la complejidad de Dorkbot, la limpieza de un sistema infectado consta de algunos pasos extras que debe seguir el usuario. Al respecto, se recomienda consultar en nuestro Blog de Laboratorio ESET: ¿Cómo eliminar Win32/Dorkbot de mi equipo?

Otro código malicioso con características de botnet reportado en 2012 fue *Flashback*. A diferencia del resto del *malware* de este tipo, que suele estar diseñado para funcionar bajo Windows, este troyano afectaba equipos con el sistema operativo Mac OS X de Apple. De acuerdo a información recopilada por ESET, Flashback logró infectar alrededor de 750.000 usuarios de Mac, de los cuales, **40.000 equipos pertenecen a Latinoamérica**. Entre los países de la región más afectados por esta amenaza se encuentran México (45%), Brasil (17%) y Chile (13%). Esta situación demuestra una vez más que el usuario debe adoptar patrones de conducta segura sin importar el sistema operativo que utilice. Asimismo, seguramente las botnets seguirán aumentando en 2013 debido a la flexibilidad que le otorgan a los cibercriminales, con el objetivo de obtener rédito económico mediante el envío de instrucciones remotas.

La nube y casos de fuga de información

El almacenamiento en la nube es otra tendencia que ha ido creciendo durante 2012. Según Gartner[5], el aumento en la adopción de dispositivos con cámaras fotográficas, como tabletas y teléfonos inteligentes, influirá proporcionalmente en las necesidades de los consumidores por almacenar más archivos en la nube. Otros acontecimientos como la inundación de las fábricas de discos duros sufrida por Tailandia en la primera mitad de 2012, también influyeron en el crecimiento de esta tecnología. En base a este informe, Gartner estima que en 2011 sólo se guardó un 7% de archivos pertenecientes a usuarios finales, aunque sin embargo proyectan un

[5] Gartner predice que los consumidores almacenarán en la nube más de un tercio de sus contenidos digitales para 2016. Disponible en http://www.gartner.com/it/page.jsp?id=2060215.

incremento del 36% para 2016. A pesar que esta tecnología facilita aspectos como el acceso de la información desde prácticamente cualquier dispositivo que cuente con acceso a Internet, eso también hace susceptible a ataques informáticos que pueden comprometer la seguridad de esos datos y provocar una fuga de información. Esto quedó demostrado cuando atacantes obtuvieron acceso a algunas cuentas de Dropbox al obtener credenciales de ingreso de este servicio en otros lugares. Pese a que no fue una falla del sitio en sí, este incidente permitió mejorar la seguridad del mismo. No obstante, y al igual que otros sistemas informáticos, la nube no está exenta de peligros. Es posible afirmar que a medida que esta tecnología crezca en cuanto a su uso, mayor será el interés de los cibercriminales por vulnerar estos servicios para intentar generar algún rédito económico.

Otros portales que también se vieron afectados por incidentes de fuga de información durante 2012 fueron LinkedIn, Yahoo! y Formspring. Por otro lado, las prestigiosas empresas de tarjetas de crédito Visa y MasterCard tuvieron que emitir una alerta cuando un sistema de procesamiento de pagos sufrió una fuga de información. Este incidente afectó a un total de 56.455 cuentas de ambas compañías, de las cuales 876 fueron utilizadas para cometer algún fraude.

Hacktivismo

En los últimos tiempos se ha podido observar un aumento en las protestas y manifestaciones que hacen ciudadanos pertenecientes a varios países como Grecia, España, Chile, Argentina, entre otras naciones, producto de algún descontento social. Como la tecnología y el mundo de la computación acompañan la vida cotidiana de muchas personas, esta tendencia de activismo también se ha consolidado utilizando medios informáticos (hacktivismo). A comienzos de 2012, integrantes del grupo Anonymous atacaron varios sitios en rechazo al cierre del portal Megaupload. Como consecuencia, el sitio del FBI estuvo fuera de línea y también se hizo pública información confidencial de Robert Müller, director de este organismo de los Estados Unidos. Además, Sony Music Entertainment también fue blanco de ataques hacktivistas cuando el mismo grupo decidió protestar en contra del apoyo explícito de esta compañía a proyectos de leyes de derecho de autor. En este caso, Anonymous obtuvo acceso a material multimedia de artistas y películas pertenecientes a esta firma que luego publicaron en Internet.

También durante el transcurso de 2012, diversos grupos de hacktivistas también protestaron por otros temas, atacando sitios pertenecientes a entidades gubernamentales argentinas, chilenas, venezolanas, bolivianas y una multiplicidad de otros países. En la mayoría de los casos, las páginas atacadas dejan de estar disponibles, imposibilitando que los internautas puedan acceder a las mismas. En otras oportunidades realizan un *defacement*, es decir, modifican el contenido original de una web por otro como forma de manifestación. También se han reportado ocasiones en que estos ataques tienen una repercusión todavía mayor como la obtención de 12 millones de UDID de iOS por parte de AntiSec; el desarrollo de un sistema operativo (Anonymous OS Live) basado en Linux y personalizado con herramientas destinadas a provocar ataques de denegación de servicio distribuidos (DDoS); el uso de una botnet propia en contra de GoDaddy; o la fuga de información de 200.000 dominios peruanos por parte de Lulz Security Perú, entre otras.
El hacktivismo desde el punto de vista de la seguridad de la información, ha demostrado que todavía existe mucho por hacer en cuanto a los sistemas de protección que implementan las organizaciones tanto a nivel de tecnología, gestión y educación. Por otro lado, se ha consolidado como una tendencia que frente a algún problema de carácter social, las personas no sólo se manifiestan a través de protestas presenciales tradicionales sino que también expresan su descontento utilizando diversos medios informáticos. Es muy probable que en 2013 frente a algún inconveniente, se puedan observar ataques de esta naturaleza como forma de manifestación cibernética.

Vulnerabilidades

Las vulnerabilidades suelen ser explotadas por los ciberdelincuentes para facilitar la propagación de códigos maliciosos. Mediante la explotación de ciertos agujeros de seguridad, es posible ejecutar un *malware* sin la necesidad de que haya una mayor intervención por parte del usuario. Por ejemplo, con tan sólo visitar un sitio web que se aproveche de este tipo de problema, es posible que un usuario resulte infectado sin la necesidad de que descargue y ejecute una amenaza. Prueba de aquello son algunas vulnerabilidades que fueron encontradas durante 2012. Mediante un exploit *0-day* que afectó a Java, se propagó un troyano detectado por ESET NOD32 Antivirus como *Win32/Poison*. Si un sitio alojaba un *applet* malicioso, el usuario resultaba infectado sin mayor intervención. El problema que reviste Java y los fallos de seguridad, es que se trata de una tecnología multiplataforma, por lo tanto, un agujero de seguridad podría propagar amenazas diseñadas para varios sistemas operativos. Otro software afectado por una vulnerabilidad crítica fue Internet Explorer. Esta debilidad permitió que ciberdelincuentes propagaran otra variante del troyano Poison. Ambos problemas fueron solucionados por las respectivas compañías. Como forma de optimizar estos ataques, los cibercriminales desarrollan kits de vulnerabilidades que incluyen varios agujeros de seguridad y el modo de explotarlos. Aunque esta tendencia no es nueva, la última versión 2.0 de *Blackhole* – conocido kit de exploits–, demuestra que los atacantes añaden de forma activa nuevos *exploits* y funcionalidades con el fin de facilitar la propagación de códigos maliciosos. Conforme se descubran fallos de seguridad nuevos, se optimizarán los métodos para poder aprovecharse de los mismos y propagar malware.

Otra vulnerabilidad que se destacó en 2012 y que tiene en cierto modo relación con el fenómeno de aumento de códigos maliciosos para Android, es el descubrimiento de una falla de seguridad que permite en algunos equipos con el sistema operativo de Google, restablecer los valores de fábrica y borrar información. Si un usuario visita un sitio malicioso que se aproveche de este problema, mediante la ejecución de números USSD, el atacante puede lograr dichos objetivos. Como forma de proteger a los usuarios, es posible instalar ESET USSD Control de forma gratuita. Esta herramienta está disponible en el repositorio de aplicaciones oficial Google Play.

Pese a que las vulnerabilidades para Android no son explotadas de forma tan activa como sucede con Windows, es posible que los ciberdelincuentes dediquen más tiempo a buscar agujeros de seguridad que afecten a estos dispositivos con tal de obtener algún beneficio económico.

Códigos maliciosos para nuevas tecnologías

A medida que la tecnología avanza, los inventos que antes eran más sencillos como televisores, automóviles, enrutadores (*routers*), tarjetas inteligentes, entre otros; se han ido modernizando para ofrecerle al usuario nuevas posibilidades. Por ejemplo, algunos televisores poseen la capacidad de conectarse a Internet con el fin de mostrar contenido personalizado, existen vehículos que implementan un sistema de GPS para ayudar en la búsqueda de rutas o lugares, etc. Aunque todas esas características utilizadas de forma correcta simplifican la vida de las personas, también posibilitan que los ciberdelincuentes desarrollen códigos maliciosos para dichas tecnologías. Cuando un dispositivo evoluciona, tanto sus funciones como complejidad aumentan y se computarizan, por lo tanto, se abre la posibilidad que exista alguna vulnerabilidad o error que permita la creación de una amenaza informática. En la actualidad, ESET Latinoamérica detectó un *malware* diseñado específicamente para atacar televisores inteligentes de una conocida marca coreana. El troyano detectado como *Perl/Agent.B,* procede a buscar los dispositivos que se encuentren conectados en red. Si detecta alguno, le muestra al usuario un mensaje en donde se le indica que debe instalar una supuesta actualización. En caso que acepte, el televisor se apaga. Aunque este código malicioso no produce ningún daño ni roba información, demuestra que es posible desarrollar amenazas para dispositivos que no sean computadoras, tabletas o smartphones.

Otro caso similar es el que se reportó en marzo de 2012 y cuya amenaza es detectado como *Linux/Hydra.B*. Se trata de un código malicioso destinado a crear una red de dispositivos zombis. A diferencia de otros tipos de *malware* desarrollados para formar una botnet, Hydra afecta sistemas operativos no tradicionales como aquellos de cámaras de vigilancia IP, *routers* domésticos (enrutadores), sistemas VoIP (Voz sobre IP), teléfonos inteligentes y tabletas. Cuando se descubrió Aidra, existían 11.000 bots reportándose al Centro de Comando y Control (C&C), lo que demuestra que este código malicioso logró el objetivo de reclutar dispositivos zombis no tradicionales. Siguiendo esta misma línea, el investigador Paul Rascagneres planteó un ataque que se basa en un *malware* cuyo propósito es permitir el acceso remoto a tarjetas inteligentes. Mediante la obtención del PIN y la exportación del dispositivo USB a un C&C, se logra dicho objetivo. Finalmente, otra investigación, expuesta en la conferencia de seguridad Blackhat 2011, planteó la posibilidad de afectar el sistema de seguridad de automóviles de última generación. En este caso puntual, se pudo vulnerar un auto que utilizaba tecnología inalámbrica para abrir automáticamente las puertas y encender el motor. Aunque esto fue solo una prueba de concepto y el fabricante fue informado del problema, demuestra que es posible atacar los sistemas computacionales de este tipo de tecnología.

Al igual que lo que sucedió con los teléfonos inteligentes, en donde este invento evolucionó de un simple celular para llamar y enviar mensajes a verdaderas computadoras de bolsillo, a medida que otros artefactos tradicionales experimenten un proceso de modernización similar, será posible observar códigos maliciosos diseñados para atacar a estos objetivos. Este problema se incrementa si se considera que Java es una plataforma capaz de funcionar en varios sistemas operativos además de ser un blanco muy atacado por los cibercriminales.

Conclusión: el *malware* móvil acompaña la tecnología

El fenómeno de los códigos maliciosos para dispositivos móviles y el crecimiento exponencial que experimentarán en 2013 tiene una explicación que trasciende el tema de la seguridad de la información. A partir del lanzamiento de dispositivos como BlackBerry y iPhone (2007), el mercado de los teléfonos inteligentes y tabletas ha ido evolucionando rápidamente en varios ámbitos como el tecnológico (mejor hardware y software más optimizado), de mercado (ventas, cantidad de usuarios, número de aplicaciones), y conectividad e infraestructura (3G y 4G LTE). Este sector ha experimentado un crecimiento considerable a diferencia de lo que ocurre con los equipos informáticos "tradicionales", cuyas ventas se han visto mermadas producto de lo anteriormente expuesto. Un ejemplo de esto es el crecimiento de tan solo un 0,9%[6] previsto para este mercado, mientras que con respecto a los teléfonos inteligentes y tabletas, la situación es distinta: de acuerdo a la misma consultora, el mercado de *tablets* ha experimentado un crecimiento de hasta 66.2%[7] si se compara el Q2 de 2011 y 2012. Estos números resultan favorables para que los cibercriminales enfoquen más tiempo y recursos en el desarrollo de amenazas para este tipo de dispositivos.

En conjunto con el aumento en las ventas de *smartphones*, la cantidad de aplicaciones móviles descargadas en Google Play y Apple Store también han crecido de forma importante con el pasar del tiempo. En julio de 2011 se registraron a nivel mundial, 15 mil millones de descargas en Apple Store, mientras que en marzo de 2012, esta cifra aumentaba casi al doble (25 mil millones) con un total de

[6] IDC prevé una disminución en las ventas de PCs en Q2 de 2012. Disponible en http://www.idc.com/getdoc.jsp?containerId=prUS23660312.

[7] IDC: ventas de Apple impulsan crecimiento del mercado de tabletas. Disponible en http://www.idc.com/getdoc.jsp?containerId=prUS23632512.

550,000 aplicaciones disponibles para iPhone, iPod, iPad, etc.[8] En el caso de Google Play, los números indican un comportamiento similar: en septiembre de 2012, este servicio alcanzó en el mundo, un total de 25 mil millones de descargas y una cantidad de 675,000 aplicaciones y juegos[9]. De forma paralela, se activan 1,3 millones de dispositivos Android por día[10]. El número de activaciones también aumentó considerablemente en comparación con 2011, ya que entonces alcanzaba tan sólo los 550 mil equipos a diario[11].
En lo que refiere al aspecto tecnológico, los dispositivos móviles (tabletas y teléfonos inteligentes) han ido evolucionando aceleradamente en cuanto a hardware y software. El mercado ofrece *smartphones* con procesadores de cuatro núcleos, 2 GB RAM, GPU (procesador gráfico) más avanzadas como la línea Nvidia Tegra, entre otras características que permiten realizar tareas más complejas que antes no eran posibles. Asimismo, las nuevas versiones de sistemas operativos como iOS, Android y Windows Phone han mejorado en áreas como la usabilidad, funcionalidad, rendimiento, y en algunos aspectos de seguridad. Frente a todo este fenómeno de vorágine tecnológica, la sociedad ha adoptado progresivamente estos equipos móviles con el fin de conectarse con familiares, amigos, trabajo; para consumir contenidos de entretenimiento o información, agilizar trámites bancarios, etc. Observando esta situación en su totalidad, y considerando que todas estas estadísticas seguirán creciendo en los próximos años, es posible establecer que los códigos maliciosos diseñados para dispositivos móviles y su consiguiente aumento responden a la velocidad que experimenta el fenómeno móvil *per se*. Es decir, si el mercado crece y la tecnología va mejorando, mientras que los usuarios que emplean estos equipos para almacenar cada vez más cantidad de información sensible no adoptan los resguardos necesarios, resulta lógico que los cibercriminales responsables de crear amenazas informáticas se aprovechen de dicha situación e intenten obtener rédito económico al igual que que sucedió alguna vez con las computadoras personales, pero a un ritmo completamente distinto dadas las circunstancias.

Otro factor que refuerza esta tendencia de crecimiento vertiginoso de *malware mobile* es BYOD (*Bring Your Own Device)* o "Traiga su propio dispositivo". Se trata de un fenómeno que está creciendo en varias regiones del mundo y que tiene directa relación con el desarrollo de dispositivos móviles cada vez más avanzados. BYOD consiste en que un empleado de una compañía lleve consigo y utilice equipos personales tales como computadoras portátiles, teléfonos inteligentes y tabletas dentro del entorno corporativo (lo que incluye acceso a redes inalámbricas Wi-Fi, VPN, archivos e impresoras compartidas, entre otros). Producto de esta situación, y si no se adoptan las medidas necesarias, BYOD podría convertirse en un serio problema de seguridad para las empresas. Por ejemplo, un empleado podría acceder a todos los recursos de la empresa a través de su smartphone infectado con algún código malicioso, que podría robar información confidencial de la organización. Otro problema que puede surgir como consecuencia de esta tendencia es el hecho que un dispositivo móvil sea robado o extraviado, y si este no se encuentra protegido correctamente, un tercero pueda acceder a datos sensibles.

De acuerdo a un estudio realizado por Gartner[12], los dispositivos que suelen conformar esta tendencia se distribuyen en teléfonos inteligentes (32%), tabletas (37%) y computadoras portátiles (44%). Asimismo, las empresas que suelen otorgar soporte técnico a estos equipos de los empleados varían de acuerdo a la región. El gráfico que se muestra página continuación compara los resultados obtenidos de aquellas compañías que sí prestan ayuda y consideran esta tendencia. Los porcentajes que se indican, corresponden a países pertenecientes al BRICS[13] (Brasil, Rusia, India, China y Sudáfrica) en comparación con el resto del mundo.

[8] Apple App Store alcanza 25 mil millones de descargas. Disponible en http://www.apple.com/pr/library/2012/03/05Apples-App-Store-Downloads-Top-25-Billion.html.

[9] Google Play alcanza 25 mil millones de descargas de aplicaciones. Disponible en http://techcrunch.com/2012/09/26/google-play-store-25-billion-app-downloads/.

[10] "Ha habido quinientos millones de activaciones de Android hasta la fecha. 1,3 millones se activan cada día". Andy Rubin, Vicepresidente Senior de móviles y contenidos digitales de Google. Disponible en https://en.twitter.com/Arubin/status/245663570812100608.

[11] Android alcanza un total de 130 millones de dispositivos. Cada día, se activan 500,000 nuevos. Disponible en http://www.theverge.com/2011/07/14/android-reaches-130-million-devices-growing-550000-day/.

[12] Fuente: Informe de Gartner revela que BYOD es una de las principales preocupaciones de las empresas con respecto a la seguridad móvil. Disponible en http://www.gartner.com/it/page.jsp?id=2048617.

[13] Países cuyo PIB y participación en mercados internacionales ha crecido y que además, poseen un extenso territorio y cantidad de habitantes.

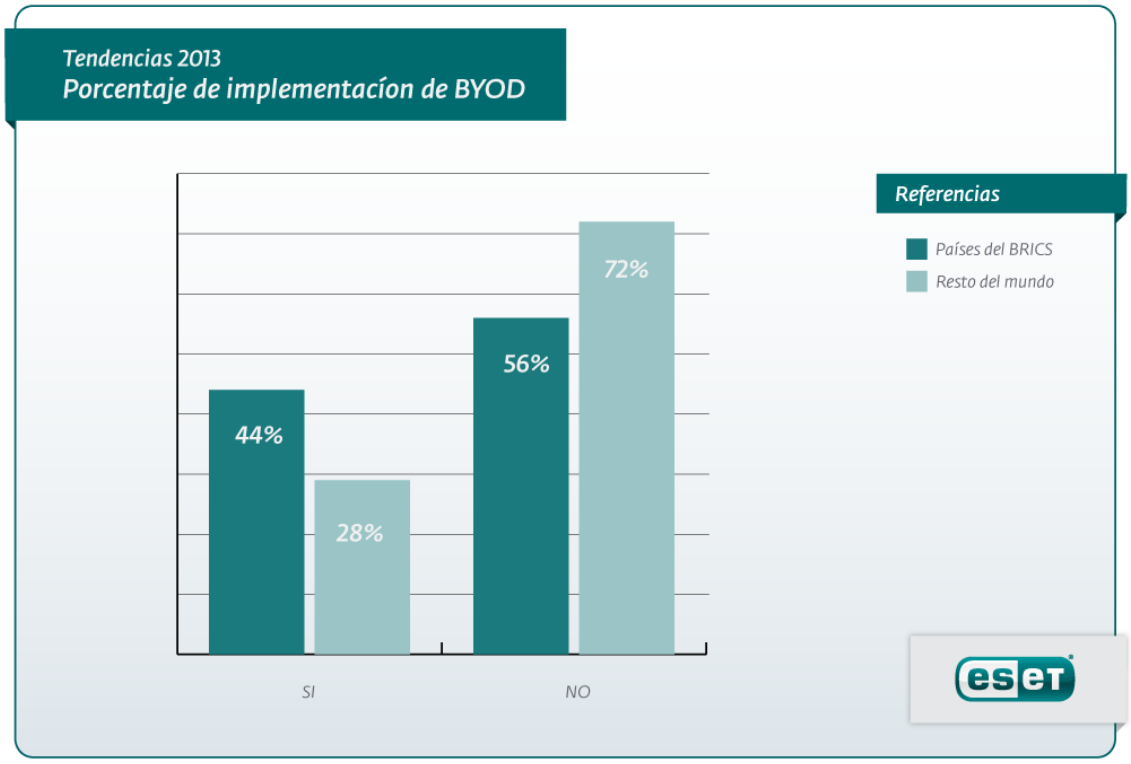


Gráfico 8 Empresas que consideran BYOD

Es posible afirmar que a medida que estos dispositivos se masifiquen con más rapidez en 2013, mayor será la cantidad de empresas y empleados que se verán involucrados con esta tendencia. Aunque algunas organizaciones han optado por prohibir el uso de estos equipos, existen algunas recomendaciones como el uso de redes Wi-Fi separadas del entorno informático principal, el uso de contraseñas de bloqueo para teléfonos inteligentes, la instalación de una solución de seguridad móvil, y la implementación de una política de seguridad empresarial que contemple tal situación que permiten minimizar los riesgos que se pueden presentar si BYOD no se adopta con el debido cuidado.

Toda esta rápida evolución ha influido en el desarrollo de amenazas para dispositivos móviles. FakePlayer, el primer código malicioso desarrollado para Android, fue reportado en 2010. Tan solo dos años después, la cantidad de *malware* para este sistema operativo ha crecido a una velocidad vertiginosa. Por ejemplo, la cantidad de variantes de códigos maliciosos para Android como TrojanSMS.Agent o TrojanSMS.Boxer aumentaron en más de un 700% con respecto a 2011. Además, es importante destacar que el porcentaje de firmas destinadas a detectar cada variante de una familia también aumentó cuantiosamente durante el presente año. Por ejemplo, en 2012 la cantidad de firmas destinadas a detectar diferentes variantes del código malicioso Plankton creció 35 veces con respecto al año anterior. Los códigos maliciosos para Android no solo seguirán aumentando de forma importante sino que también irán evolucionando hasta el punto de ser muy similares a sus pares de computadoras. Un caso de ello es la variante para *mobile* de *Zeus* (*Zitmo*, *Zeus In The Mobile*), conocido troyano capaz de convertir las computadoras y dispositivos móviles en zombis. Durante los últimos años, han ido apareciendo nuevas variantes de Zitmo capaces de ser controladas a través de mensajes SMS y burlar los sistemas bancarios de doble autenticación[14]. Considerando todo lo mencionado anteriormente, es posible afirmar que los códigos maliciosos móviles evolucionan y aumentan proporcionalmente de la mano de la tecnología, es decir, si esta última se ha masificado y hoy forma parte de la cotidianeidad, entonces las amenazas informáticas para tales dispositivos también lo harán.

Aunque los códigos maliciosos para Android son la principal tendencia en cuanto a amenazas informáticas para 2013, la propagación de *malware* utilizando sitios vulnerados también está aumentando considerablemente y de forma rápida, y por lo tanto se ha convertido en uno de los métodos de propagación más utilizados por los ciberdelincuentes. Al respecto, es importante considerar que aunque el mercado de las computadoras tradicionales no evolucione a la velocidad de las ventas de teléfonos inteligentes, los ciberdelincuentes seguirán desarrollando gran cantidad de códigos maliciosos diseñados para estos equipos, como también nuevas técnicas de ataques como lo demuestra la propagación vía web. Mientras los usuarios continúen utilizando computadoras de forma masiva, seguirán siendo blancos de amenazas informáticas. En este sentido, cualquier vector de infección que pueda facilitar el acceso no autorizado de un atacante a un sistema como por ejemplo vulnerabilidades, significará que los casos de espionaje industrial y las botnets seguirán creciendo en 2013. El desafío para los usuarios y la comunidad en general sigue siendo el mismo: no sólo adoptar soluciones de seguridad en equipos móviles y computadoras, sino también concientizarse en todo lo referente a la seguridad de la información en este tipo de tecnología. Tal como pueden facilitar la vida de una persona, estos equipos móviles también pueden convertirse en un

[14] Troyanos en Android: vulnerando sistemas de doble autenticación. Disponible en http://blogs.eset-la.com/laboratorio/2012/07/23/troyanos-en-android-vulnerando-sistemas-de-doble-autenticacion/.

serio problema para la seguridad de la información si no se utilizan con el debido cuidado, más considerando que los códigos maliciosos para Android continuarán aumentando significativamente durante el próximo 2013.