Tendencias 2014: El desafío de la privacidad en Internet

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

Índice

Autor:

Equipo de Investigación de ESET Latinoamérica

Introducción

Como es tradición, cada fin de año el Laboratorio de Investigación de ESET Latinoamérica redacta el informe Tendencias en donde se abarcan diversos temas relacionados a la Seguridad de la Información. El objetivo es concientizar a la comunidad sobre el estado actual de las amenazas informáticas y, en base a esto, proyectar la posible evolución que podrá observarse en los próximos años. En esta línea, durante 2011 se pudo notar una consolidación en cuanto a las botnets y el *malware* que persigue fines económicos[1]. En 2012 la principal tendencia tuvo relación directa con las amenazas diseñadas para plataformas móviles[2]. Un año más tarde, el tema principal fue el crecimiento vertiginoso de códigos maliciosos para *mobile*[3] y actualmente, si bien tales amenazas continúan creciendo, el principal tópico está centrado en el aumento de la preocupación manifestada por los usuarios con respecto a la privacidad en Internet.

En este sentido, casos como el acontecido con Edward Snowden y la Agencia Nacional de Seguridad de los Estados Unidos (NSA) influyeron en el incremento de la preocupación de la privacidad en Internet. No obstante, dicha tendencia no ha significado una disminución con respecto a los casos de personas afectadas por algún código malicioso u otro tipo de amenaza informática. Se puede afirmar que la preocupación por privacidad, es un buen punto de partida en el sentido que el interés por parte del usuario existe, sin embargo, es fundamental que las personas se concienticen sobre la Seguridad de la Información, de lo contrario, no se logrará mitigar el impacto de las amenazas informáticas. Esta situación equivaldría a una persona que se muestra intranquila por la seguridad de su hogar, pero si no instala un sistema de alarma, deja las ventanas abiertas y deja pasar a desconocidos, lo más probable es que se convierta en víctima de algún incidente.

Otra tendencia observada durante 2013 y que se consolidará en los próximos años tiene que ver con el aumento en cuanto a número y complejidad de códigos maliciosos diseñados para Android. Los cibercriminales están comenzando a aplicar metodologías clásicas de ataques pero que son novedosas con respecto a las plataformas para móviles. En esta línea, el descubrimiento de vulnerabilidades críticas y su posterior explotación a través de códigos maliciosos representan una evolución del cibercrimen que afecta a la tecnología *mobile*. Por otro lado, el incremento en la complejidad de botnets, amenazas de 64 bits y códigos maliciosos que intentan lucrar con el robo de monedas electrónicas, son otros temas que han cobrado protagonismo en el último tiempo. Finalmente, la diversificación de dispositivos no tradicionales como autos inteligentes, consolas de juegos, Smart TV y otros, plantea la posibilidad de que en un futuro, se puedan observar amenazas diseñadas para este tipo de tecnología.

Considerando los puntos anteriores, ¿será posible la privacidad en Internet?

[1] Tendencias 2011: las botnet y el malware dinámico
[2] Tendencias 2012: El malware a los móviles
[3] Tendencias 2013: Vertiginoso crecimiento de malware para móviles

Pérdida de privacidad y mecanismos para proteger la información en Internet

En los últimos años, la tecnología de almacenamiento en la nube ha experimentado un crecimiento considerable en cuanto al número de usuarios finales y empresas que la utilizan. Si antes era común ver que las personas compartían información a través de disquetes, medios ópticos (CD/DVD), dispositivos de almacenamiento extraíbles USB, u otros, en la actualidad es posible observar una clara tendencia hacia el uso masivo de la nube en detrimento de otros medios "tradicionales". Las ventajas que ofrece la nube son considerables ya que, por ejemplo, facilita el acceso a la información puesto que los archivos están disponibles desde prácticamente cualquier lugar que cuente con conexión a Internet. Asimismo, en caso de realizarse un *backup*, no será necesario tener que elegir un lugar físicamente seguro en donde guardar el soporte de respaldo. Todas esas ventajas han provocado que la nube sea una tecnología cada vez más popular entre todo tipo de usuarios. En este sentido, Gartner aseguró que en 2011 solo un 7% de la información de los usuarios finales fue almacenada en la nube, sin embargo, se espera que para el año 2016 dicho porcentaje aumente a un 36%[4]. Por otro lado, la publicación "Global Cloud Index" de Cisco, estima que en 2017 los usuarios de América Latina habrán almacenado una cantidad de 298 exabytes de información en la nube (1 billón de gigabytes)[5]. A continuación, se muestra una tabla en donde se proyecta el crecimiento de la nube en varias regiones del mundo y la cantidad de datos almacenados (expresados en Exabytes):

CRECIMIENTO DEL TRÁFICO EN LA NUBE POR REGIONES

REGIÓN	2012	2013	2014	2015	2016	2017	CRECIMIENTO PORCENTUAL 2012-2017
AMÉRICA LATINA	77	117	159	203	249	298	31%
ASIA PACÍFICO	319	505	736	1.042	1.415	1.876	43%
EUROPA CENTRAL Y ORIENTAL	69	101	140	191	253	325	36%
ORIENTE MEDIO Y ÁFRICA	17	31	51	77	112	157	57%
NORTEAMÉRICA	469	691	933	1.211	1.526	1.886	32%
EUROPA OCCIDENTAL	225	311	400	501	623	770	28%

Tabla 1 Crecimiento del tráfico en la nube por regiones (expresado en Exabytes)

[4] Gartner Says That Consumers Will Store More Than a Third of Their Digital Content in the Cloud by 2016. Disponible en http://www.gartner.com/newsroom/id/2060215.

[5] Cisco: Global Cloud Index (GCI). Disponible en http://www.cisco.com/en/US/netsol/ns1175/networking_solutions_solution_category.html#~Overview.

En base a la tabla anterior, es posible observar que en todas las regiones la tendencia indica un crecimiento en al almacenamiento de información en la nube, es decir, el uso de esta tecnología por parte de los usuarios va aumentando conforme pasa el tiempo. En el caso de América Latina, el crecimiento porcentual que se proyecta para 2017, en comparación a los años anteriores, es de un 31%.Pese a este incremento y a las ventajas que conlleva para los usuarios, es importante considerar que esta tecnología no está exenta de riesgos asociados a la seguridad de la información.

Esta tendencia de "ir hacia la nube" por supuesto que tiene implica a la seguridad de la información, pero además existe una cuestión que en los últimos años ha sufrido algunas modificaciones dado el uso que las personas le han dado a la tecnología, y es el tema de la privacidad. En este sentido, es necesario comprender que el humano es un es ser social que utiliza distintos métodos para comunicarse con los demás, como el lenguaje oral o gestual, entre otros. El objetivo de la comunicación es poder compartir emociones, opiniones y otros aspectos de la vida en sociedad. Si se lleva este caso al ámbito de la tecnología, es posible vincularlo con las redes sociales, servicios que facilitan la interacción entre personas a través de una plataforma en línea. Sin embargo, pese a esta esfera social y/o pública que caracteriza a la humanidad, también existe otra de igual relevancia que se relaciona con el ámbito de lo privado. En esta línea, Internet no es la excepción. Tal como una persona guardaría un secreto profesional o personal, en el mundo virtual también existe información confidencial que no debe ser accedida por terceros no autorizados. Si alguien necesitara proteger escrituras legales o cualquier objeto de valor, lo más probable es que pensara en una caja fuerte u otro lugar seguro.

A pesar de que en Internet los usuarios se enfrentan al mismo escenario, los mecanismos para proteger los datos adecuadamente no siempre son conocidos o implementados correctamente. Si bien esta problemática ha estado presente desde el momento en que comenzó a masificarse esta tecnología, casos como el acontecido con la Agencia de Seguridad Nacional de los Estados Unidos (NSA por su sigla en inglés) han provocado en cierto modo, un interés de los usuarios por proteger la información almacenada en la nube.

El caso de la NSA y el debate de la privacidad

A partir de la masificación de Internet y algunos servicios de valor agregado, como buscadores, redes sociales, *webmail*, entre otros, el tema de la privacidad de la información comenzó a adquirir mayor trascendencia para la comunidad en general y no solo para los expertos del área de seguridad informática o las empresas. Ya en 2004 fue posible observar que junto con el lanzamiento de Gmail, el servicio de correo electrónico de Google, algunos usuarios se mostraron preocupados por la privacidad del mismo[6]. La razón de esto, se debe a que la empresa puede analizar el contenido del correo para mostrar publicidad que sea acorde a los intereses de las personas.

Partiendo por la base de que las acciones que se realizan en Internet pueden tener consecuencias (positivas o negativas) tangibles, varios países han aplicado normativas para regular actos cuyos resultados puedan perjudicar temas y aspectos de interés social como la piratería, fraude electrónico (códigos maliciosos, *phishing*, *scam*, etc.), pedofilia, seguridad nacional, entre otros. Precisamente, el último punto es el tema principal del incidente y debate mediático que se gestó a partir de las revelaciones dadas a conocer por Edward Snowden a la opinión pública. Nacido en Estados Unidos, Snowden se desempeñó como técnico de la NSA a través de una empresa contratista hasta que, en junio de 2013, filtró masivamente información de inteligencia relacionada al control que ejerce el gobierno estadounidense sobre la privacidad de los datos de los ciudadanos y el mundo en general[7]. Este hecho generó un debate mundial entre los países que no apoyan este tipo de control y Estados Unidos, que lo entiende como una acción para prevenir ataques terroristas.

Más allá del legítimo debate ideológico, legal y moral que se genera en torno a este tema, también existen implicancias que abordan directamente el campo de la Seguridad de la Información. Desde esta perspectiva, es importante entender que las medidas de seguridad que debe adoptar un usuario mitigan el impacto y ocurrencia de varios ataques informáticos como intrusiones, códigos maliciosos, robo de información, etc., pero no tienen la misma eficacia al momento de resguardar la privacidad de la persona en determinados escenarios, como el acaecido con la NSA. En este sentido, si una empresa proveedora de algún servicio tecnológico establece en su política de privacidad cláusulas que mencionan posibles usos para la información almacenada, los mecanismos "tradicionales" de protección implementados por los usuarios no podrán impedir que esa información sea utilizada con algún propósito establecido en el contrato. Por ejemplo, algunos proveedores continúan almacenando los archivos del usuario incluso si se cancela el servicio, por lo tanto, los datos podrían resultar comprometidos en caso que esa empresa sea víctima de algún incidente informático.

[6] Electronic Privacy Information Center – Gmail Privacy FAQ. Disponible en http://epic.org/privacy/gmail/faq.html#1.
[7] Wikipedia – 2013 mass surveillance disclosures. Disponible en http://en.wikipedia.org/wiki/2013_mass_surveillance_disclosures.

Con respecto a los mecanismos "tradicionales" de protección, una solución de seguridad resguarda al usuario de diversos códigos maliciosos, un *firewall* de las intrusiones, la doble autenticación de ataques que puedan comprometer la contraseña y así sucesivamente. Sin embargo, en el caso que los datos del usuario se encuentren almacenados en un sistema cuyo uso depende de la aceptación de políticas de privacidad, es la propia empresa prestadora del servicio quien puede hacer un uso determinado de dicha información, por lo tanto, se requieren de otras medidas para aumentar la privacidad. En este contexto, un aspecto primordial es leer detenidamente el contrato de uso de los servicios y programas que se utilizan. Es importante considerar que cuando una persona acepta este tipo de contratos, está aceptando explícitamente todos los puntos que allí se detallan sin importar si estos fueron leídos o no.

Mayor preocupación de los usuarios por la privacidad en la nube

Como se mencionó anteriormente, los problemas relacionados a la seguridad y privacidad de los datos almacenados en la nube existen a partir del momento en que esta tecnología comenzó a masificarse, sin embargo, lo acontecido con la NSA provocó que más usuarios empezaran a preocuparse por la Seguridad de la Información. La primera estadística que corrobora este aumento tiene relación con el incremento del tráfico web del buscador DuckDuckGo[8]. Este sitio se caracteriza por ofrecerles a los usuarios un nivel de privacidad mayor al posibilitar la búsqueda de contenido en Internet sin que se registre información del internauta. De este modo, cualquiera que realice una búsqueda en DuckDuckGo obtendrá el mismo resultado independiente de los intereses, locación y otros factores de personalización. En este sentido, el tráfico promedio que registra el portal aumentó considerablemente luego que se filtrara información con respecto a los programas de vigilancia de la NSA. A continuación, se muestra un gráfico que evidencia lo expuesto anteriormente:

Gráfico 1 Promedio de consultas por mes de DuckDuckGo

Tal como se observa en el gráfico, en mayo se registró un promedio de 1.755.121 consultas. Cabe destacar que en aquella fecha todavía no se había filtrado masivamente información sobre los planes de vigilancia de la NSA. El aumento de consultas quedó evidenciado a partir de junio, cuando Snowden, dio a conocer algunos detalles de cómo opera la NSA. A partir de ese momento, el promedio de visitas mensuales de DuckDuckGo experimentó un aumento sostenido de más del 200%, siendo que de 1.755.121 consultas promedio en mayo se pasó a un total de 3.890.084 en septiembre. Aunque estos

[8] Detalles del tráfico de DuckDuckGo. Disponible en https://duckduckgo.com/traffic.html.

números son considerablemente menores a los de Google, demuestran que la cantidad de usuarios que se preocupan por la privacidad en Internet aumentó a partir de la filtración de información que realizó Edward Snowden.

Otro estudio que avala el aumento de la preocupación de las personas con respecto a la privacidad en Internet, es la encuesta realizada por ComRes, una consultora de investigación de Gran Bretaña. Esta investigación arrojó que de un total de 10.354 entrevistados que viven en nueve países distintos (Brasil, Gran Bretaña, Alemania, Francia, España, India, Japón, Corea del Sur y Australia), el 79% manifestó estar preocupado por su privacidad en la red[9]. Asimismo, los países que se mostraron más alarmados por este fenómeno son India (94%), Brasil (90%) y España (90%). A continuación, se muestra una tabla que resume los principales hallazgos de la investigación. Los datos se encuentran divididos en base a los nueve países que contempló el estudio[10]:

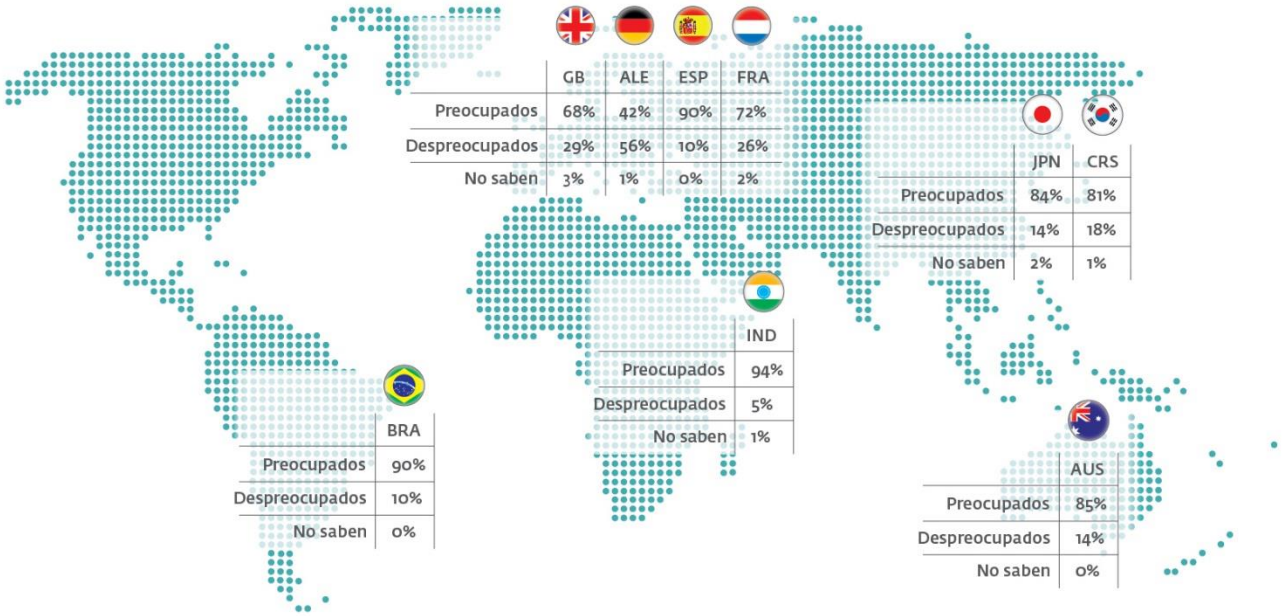


Gráfico 2 Resumen de la investigación por países

De acuerdo a la información recopilada sobre los países que contempló la investigación, Alemania es el menos preocupado por la privacidad en Internet. El resto de las naciones comparten una visión más uniforme sobre la importancia de proteger adecuadamente el ámbito íntimo de las personas en la red.

Más allá de casos puntuales, la tendencia global que se observa en la actualidad es hacia una mayor preocupación con respecto a cómo las empresas y los gobiernos almacenan, controlan y utilizan información privada de los usuarios en Internet. En esta línea, es posible que lo acontecido con la NSA y Edward Snowden[11] hayan contribuido a que muchas personas alrededor del mundo estén más conscientes, y a la vez más interesadas, sobre su privacidad en línea. Pese a esta preocupación, que se extendió prácticamente alrededor de todo el mundo, y más allá del extenso debate social y mediático que generó todo el tema de la NSA, las medidas de protección que adoptan los usuarios para resguardar la privacidad y seguridad de los entornos informáticos que utilizan (computadores, teléfonos inteligentes, tabletas, entre otros) son, en varias ocasiones, insuficientes. Asimismo, producto de la falta de concientización, las personas suelen actuar de un modo riesgoso desde el punto de vista de la Seguridad de la Información. Por ejemplo, una encuesta aplicada por ESET Latinoamérica arrojó que el 67% de los usuarios que recibió el "gusano de Skype", terminó infectándose con la amenaza en cuestión. Dicho código malicioso se propagaba utilizando mensajes sugestivos, enlaces acortados y Skype; una combinación de técnicas de Ingeniería Social que demostraron ser eficientes para propagarse en números impresionantes.

Dicho porcentaje de afectados se contradice con la tendencia que indica que las personas están cada vez más preocupadas por su privacidad en Internet. Esto se da porque los códigos maliciosos son amenazas que suelen ser desarrolladas precisamente para robar información, "invadiendo" de ese modo la esfera de privacidad de aquellos que resultan infectados. Aunque a simple vista se trata de una contradicción *per se*, se puede explicar por el hecho de que muchos

[9] New Research: Global Attitudes to Privacy Online. Disponible en http://www.bigbrotherwatch.org.uk/home/2013/06/new-research-global-attitudes-to-privacy-online.html.
[10] Big Brother Watch – Online Privacy Survey. Disponible en http://www.slideshare.net/fullscreen/bbw1984/global-privacy-research/3.
[11] Más información disponible en Wikipedia – Edward Snowden.

usuarios aun adoptando tecnologías de seguridad, como soluciones antivirus, *firewalls* y otras herramientas, no le prestan la importancia suficiente a la concientización. De hecho, la educación resulta fundamental para proteger correctamente un entorno informático y, de ese modo, mejora la privacidad del usuario en Internet. Este antecedente queda de manifiesto si se analizan los resultados del informe ESET Security Report Latinoamérica 2013[12]. En dicho documento, es posible observar que las empresas que adoptan planes de concientización en Seguridad de la Información son menos propensas a ser víctimas de ataques informáticos, en comparación con aquellas que no implementan ese tipo de prácticas o lo hacen esporádicamente. Cabe destacar que la concientización en seguridad, ya sea corporativa o personal, debe ser constante y sostenida en el tiempo debido a que es un campo que evoluciona rápidamente. El siguiente esquema tiene como objetivo mostrar que si bien la instalación de una solución de seguridad otorga una capa de protección adicional, la concientización es vital para lograr un nivel de protección adecuado:

Esquema 1 Mayor preocupación no es sinónimo de más privacidad

Tal como se puede apreciar en el esquema, existe una mayor preocupación por resguardar la privacidad en Internet, sin embargo, la falta de concientización sigue siendo uno de los principales obstáculos al momento de proteger adecuadamente la información y privacidad. Otra encuesta que corrobora esta tendencia es la que aplicó ESET Latinoamérica en julio de 2013. En aquella instancia, se abordó el tema del uso de las redes sociales. Frente a la pregunta sobre cuán seguros creen los usuarios que están sus datos en los servidores de las redes sociales, un 52,2% piensa que están ligeramente inseguros, es decir, más de la mitad de los encuestados considera que es posible que dicha información pueda ser obtenida por un tercero.

Antes de explicar los factores que pueden afectar la privacidad en línea de una persona, es imprescindible entender qué rol juega el usuario en todo este proceso. En una primera instancia, es él quien decide qué información publicar y cuál no, una decisión que puede aumentar o disminuir el nivel de su privacidad en Internet. A simple vista, este proceso puede verse como algo sencillo, no obstante, es necesario ser prudente y comprender correctamente los verdaderos alcances que puede llegar a tener una publicación en Internet.

En un intento por aminorar este problema, algunas redes sociales como Facebook han implementado métodos más sencillos para restringir lo que la persona publica, como por ejemplo botones para configurar la visibilidad de algo que se transmite. En esta configuración se puede seleccionar que el contenido sea público, solo para los amigos del usuario o exclusivamente para la persona en cuestión. Por otro lado, Facebook también implementó un nuevo menú que permite gestionar fácilmente la privacidad del usuario. Para mitigar la problemática que se observa en esta primera instancia, es importante que el usuario conozca este tipo de control y que también piense en la trascendencia que puede llegar a tener toda esta situación. Un caso podría ser, la posibilidad de que un tercero malintencionado pueda obtener datos personales si la potencial víctima hace pública información como su dirección física, números de teléfono, lugar de trabajo, etc.

La nube y el almacenamiento de información en otros países

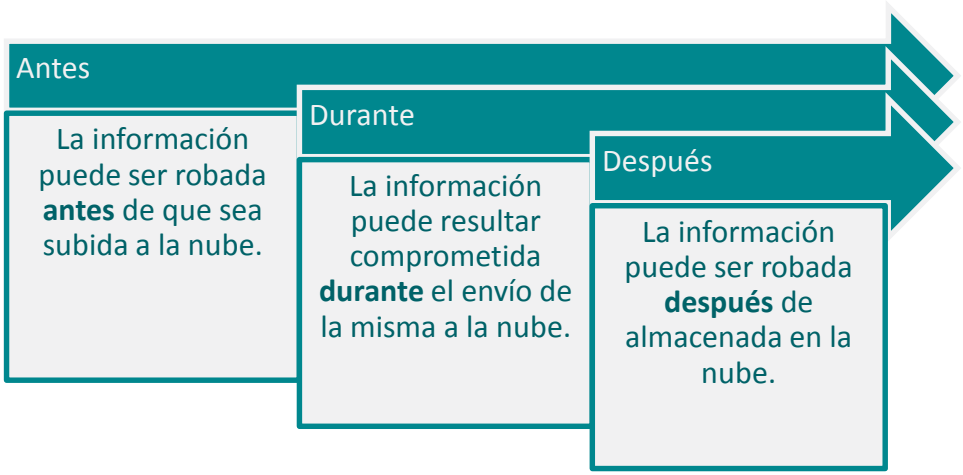
Como se mencionó anteriormente, la nube es una tecnología de almacenamiento en línea que no es nueva, sin embargo, su flexibilidad ha provocado, con el transcurso de los años, una masificación relevante tanto entre usuarios hogareños como corporativos. De acuerdo a un estudio de Gartner que proyecta el estado de la nube entre 2011 y 2016 con respecto a varios aspectos, Latinoamérica no es la región que más ha invertido en términos económicos en esta tecnología (lo es Estados Unidos con el 59% de las inversiones), sin embargo, algunos países de América Latina como Argentina, México y Brasil son las naciones que registran las tasas de crecimiento más altas de servicios en la nube[13].

Pese a dicho crecimiento y a la flexibilidad que otorga un servicio de este tipo, la nube continúa generando controversias e incertidumbres en lo que respecta a la seguridad y privacidad de los datos almacenados. En este sentido, algunos usuarios

[12] ESET Security Report Latinoamérica 2013. Disponible en http://www.eset-la.com/pdf/prensa/informe/eset-report-security-latinoamerica-2013.pdf.

[13] Gartner Says Worldwide Public Cloud Services Market to Total $131 Billion. Disponible en http://www.gartner.com/newsroom/id/2352816.

manifiestan su preocupación debido a que esta tecnología no permite un control directo sobre los datos como sí lo posibilita un servidor local o el sistema propio del usuario. Para dilucidar este tema, es necesario comprender algunos aspectos de la tecnología en cuestión. Primero, se debe considerar que la información o plataforma que se almacenará en la nube puede ser comprometida antes, durante o después de la transmisión de datos. El siguiente esquema muestra las tres etapas mencionadas anteriormente:



Esquema 2 Etapas donde puede ocurrir robo de información en la nube

En base al esquema anterior, la primera instancia en que la información podría resultar comprometida es antes que esta sea almacenada en la nube. Por ejemplo, una empresa cuyos sistemas se encuentran infectados con un código malicioso, se expone a que los datos sean robados antes de que sean subidos a la nube. Por otro lado, la información también puede correr riesgo si la organización transmite los datos a través de una conexión insegura. En este sentido, el robo de información ocurriría durante la transmisión de datos producto de ataques como *sniffing* o robo de paquetes. En la tercera instancia, la seguridad que adopta el proveedor del servicio en la nube como cifrado de datos, política de uso y seguridad, etc., también determina la probabilidad de que la información almacenada en la nube pueda ser vulnerada mediante un ataque en contra del proveedor de los servicios.

Asimismo, el país en el que reside el servidor que almacena la información también es un aspecto crítico que puede influir en la seguridad y privacidad de dicha información. Cada país tiene un marco normativo distinto con respecto a la protección de datos personales en entornos informáticos, por lo tanto, una legislación más estricta puede favorecer el nivel de protección de los datos. Sin embargo, un sistema legal menos riguroso o la inexistencia de una norma específica podría afectar negativamente la privacidad de la información.

Mayor regulación legal y políticas de privacidad más claras

La vía legal es uno de los métodos que emplean los países para regular el uso de Internet penalizando actos como el robo de información, fraude, pedofilia, piratería, entre otros. En concordancia, durante 2013 Perú impulsó una ley que busca penalizar determinadas actividades que pueden atentar directa o indirectamente sobre la privacidad de los usuarios en Internet. En este caso, el congreso peruano aprobó la Ley de Delitos Informáticos. La norma busca sancionar la pedofilia y los fraudes electrónicos. Por ejemplo, en caso de violación de la privacidad, la ley contempla una pena de seis años de prisión.

Por otro lado, a raíz del caso de la NSA, la presidenta de Brasil, Dilma Rousseff, se mostró preocupada por la privacidad de los ciudadanos que utilizan Internet. Por lo mismo, planteó la posibilidad de que las empresas sean obligadas a almacenar todos los datos de los brasileños en servidores locales[14], es decir, sistemas informáticos que se encuentren físicamente establecidos en ese país de tal modo que las leyes brasileñas sobre dicha materia puedan ser aplicadas. Precisamente, ese punto sobre el lugar de ubicación de un sistema informático y las normativas que rigen ese país es una de las problemáticas de la nube y que se explica en mayor detalle en las siguientes páginas. Como puede inferirse, tanto el cibercrimen como los eventos ya mencionados han provocado que la privacidad de los usuarios en Internet sea una preocupación prioritaria para la sociedad en su conjunto.

[14] El Financiero México - Google y Facebook, en la mira de Dilma Rousseff. Disponible en http://www.elfinanciero.com.mx/secciones/internacional/32329.html.

Las empresas son actores que tampoco se han mantenido al margen de toda esta situación. La tendencia que se observa al respecto es un aumento por dar a conocer y simplificar las políticas de privacidad de servicios como Facebook, LinkedIn y Pinterest. En el caso de Facebook, la empresa introdujo cambios en la Política de uso de datos y la Declaración de derechos y responsabilidades que rige a los usuarios de dicho servicio. Las actualizaciones buscan esclarecer algunos aspectos y también entregar consejos enfocados en la privacidad como el hecho de eliminar aplicaciones de Facebook que ya no sean utilizadas. En el caso de LinkedIn, el objetivo también apuntó a la simplificación de las políticas de privacidad para facilitar su comprensión. Pinterest, por su lado, implementó un sistema que ofrece contenido personalizado y que puede modificar los parámetros de configuración relacionados a la privacidad de la cuenta[15].

Con todos estos cambios es posible afirmar que existe una tendencia por transparentar las políticas de privacidad y sensibilizar a las personas sobre la temática. Asimismo, de forma paulatina algunos países de la región comienzan a mostrar mayor interés por reglamentar Internet y la privacidad de los usuarios.

¿Cómo proteger la información en Internet?

Partiendo por la premisa de que la preocupación por la Seguridad Informática de las personas es algo perceptible y medible, se hace necesario comprender los diversos factores que pueden comprometer la privacidad de una persona en Internet. Del mismo modo, es fundamental conocer qué tecnologías permiten mitigar el impacto de esta problemática. En esta línea, la siguiente tabla expone los distintos factores que pueden comprometer la privacidad del usuario. También se enumeran de forma resumida, las tecnologías y medidas de protección que se pueden adoptar para reducir tal impacto:

[15] Pinterest Español.Net - Nueva política de privacidad y Pins más personales. Disponible en http://pinterestespanol.net/nueva-politica-de-pivacidad-y-pins-mas-personales/.

FACTORES QUE PUEDEN COMPROMETER LA PRIVACIDAD DEL USUARIO

FACTORES	Descripción	Tecnologías y medidas de protección
AMENAZAS INFORMÁTICAS 1	Amenazas como códigos maliciosos, phishing, scam, vulneración de servidores y contraseñas, entre otras, suelen robar información confidencial de la víctima.	> Implementar tecnologías de seguridad (antivirus, *firewall*, doble autenticación, etc.) > Adoptar un comportamiento seguro y precavido. > Concientizarse sobre las últimas tendencias en ataques informáticos.
POLÍTICAS DE PRIVACIDAD POCO CLARAS O ABUSIVAS 2	Algunos programas y servicios incluyen políticas de privacidad poco explícitas o abusivas que pueden repercutir en la privacidad del usuario.	> Antes de instalar un *software* o utilizar un servicio en particular, leer atentamente la Política de Seguridad. Es importante considerar que cuando un usuario utiliza algunos de esos productos, está aceptando las cláusulas de privacidad.
ACCESO INDEBIDO POR PARTE DE TERCEROS 3	Considerando que ningún sistema informático está exento de sufrir ataques, es posible que la información del usuario sea accedida por terceros si la empresa proveedora del servicio no adopta las medidas necesarias.	> El cifrado (encriptación) de datos es una técnica que consiste en hacer ilegible una información en caso de que no se ingrese la contraseña de descifrado correcta. Se recomiendan aplicaciones de código abierto y cuya clave sea de 1024 ó 2048 bits.

Tabla 3 Factores que pueden comprometer la privacidad del usuario

En la tabla anterior también se mencionan algunas medidas concretas que el usuario puede aplicar para aumentar la seguridad y privacidad en Internet. Algunas acciones en particular, como el cifrado de datos y la doble autenticación, se abordarán en detalle en las siguientes páginas.

Cifrado (encriptación) de datos

Otra medida de seguridad que resulta eficaz en este contexto es el cifrado (encriptación) de datos. Se trata de un método que, en términos sencillos, hace ilegible la información de tal modo que sea necesario el uso de una llave (contraseña) para poder descifrar los datos y hacerlos legibles nuevamente. En este caso, la información podría ser obtenida por un tercero, no obstante, al estar cifrada no podrá leerla sin la contraseña necesaria. Sin embargo, como toda medida de protección informática, no es infalible. El nivel de seguridad que otorga el cifrado depende de la robustez del algoritmo de encriptación, es decir, del modo en que cifra la información para hacerla ilegible. Aunque suene paradójico, leer el contrato de uso nuevamente adquiere protagonismo puesto que si el *software* o servicio de cifrado contempla dentro de las políticas compartir la llave o algoritmo de descifrado, la información del usuario podría quedar expuesta nuevamente.

A continuación, se muestra un esquema que resume el funcionamiento del cifrado de datos:

Esquema 3 Funcionamiento del cifrado de datos

Tal como se aprecia en el esquema, en el primer cuadrado (1) es posible observar que la información se encuentra en texto plano, es decir, descifrada. Posteriormente, se cifra la información y se protege mediante una llave (2). Luego, cualquier usuario que intente acceder a los datos cifrados y no posea la llave adecuada, se verá imposibilitado de acceder a la información de forma legible (3). Finalmente, aquellas personas que sí posean la llave podrán descifrar los datos (4) y acceder al mensaje original (5).

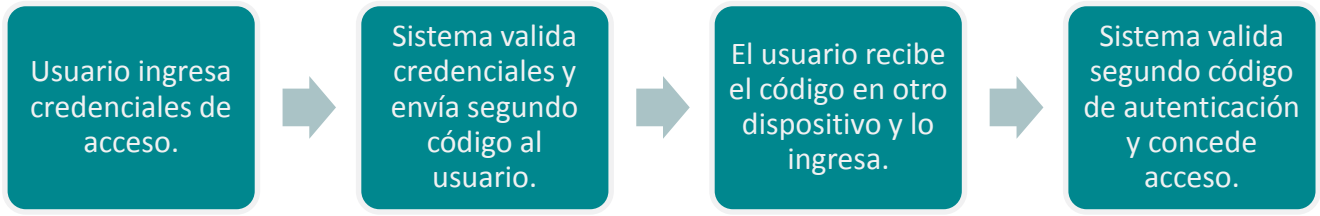
En base a esto, es recomendable cifrar siempre la información antes de subirla a la nube. De este modo, los datos no podrán ser descifrados y accedidos por terceros. Asimismo, tecnologías como Microsoft BitLocker permiten cifrar los archivos almacenados en el sistema de forma local (en el propio equipo del usuario), por lo tanto, cifrar la información tanto de forma local como en la nube mitiga considerablemente la posibilidad que un atacante pueda hacer mal uso de esos datos.

Robo de información y doble autenticación como mitigación de ataques

Tal como se abordó en el documento Tendencias 2013: Vertiginoso crecimiento de malware para móviles, casos de fuga de información producto de ataques perpetrados por terceros han continuado ocurriendo a lo largo de 2013. Casos como el de Burger King, en donde atacantes vulneraron la contraseña de la cuenta de Twitter de esa franquicia de comida rápida y publicaron publicidad de su competencia, como también las diversas amenazas informáticas que intentan robar contraseñas (códigos maliciosos, fuerza bruta, ataque a servidores y phishing), han demostrado empíricamente que la autenticación simple a través del factor de conocimiento (uso de un usuario y contraseña) es una medida insuficiente para reducir el impacto de los ataques.

En esta línea, la doble autenticación es una metodología que implementa un segundo factor de autenticación, de modo que atenúa los riesgos ante un ataque. Por ejemplo, cuando un usuario accede a su cuenta (de correo, red social, banco, etc.), aparte de ingresar las credenciales de acceso (autenticación simple) tendrá que escribir un segundo código de verificación que suele ser enviado al teléfono inteligente por medio de un mensaje de texto o una aplicación. De este modo, si un atacante logra obtener un nombre de usuario y contraseña, no podrá comprometer la privacidad del usuario porque desconocerá el segundo factor de autenticación.

El siguiente esquema simplifica y aclara el funcionamiento de este sistema:



Esquema 4 Funcionamiento de la doble autenticación

Una tendencia que quedó de manifiesto durante 2013 es el aumento de empresas que han implementado sistemas de doble autenticación como forma de mitigar algunos ataques informáticos. Excluyendo entidades financieras que llevan más tiempo trabajando con esta tecnología, dicho sistema de protección ha sido adoptado por organizaciones como Facebook, Apple, Twitter, LinkedIn, Evernote, Google, Microsoft, entre otras. Por lo general, para mejorar la usabilidad de este método, solo solicitan el ingreso del segundo factor de autenticación en caso que la persona inicie sesión desde un dispositivo nuevo o desconocido (que no haya sido añadido previamente como un equipo de confianza). Esto evita que el usuario tenga que estar ingresando el segundo código de comprobación cada vez que desee utilizar el servicio. Asimismo, en la actualidad, varios servicios facilitan el uso de este tipo de protección utilizando Google Authenticator, aplicación disponible para plataformas móviles y que genera un código aleatorio que puede ser ingresado como segundo factor de autenticación en cuentas de Microsoft, Google, Facebook, Amazon Web Services, Evernote, entre otras. En consonancia, ESET lanzó al mercado ESET Secure Authentication, solución diseñada para implementar un sistema de doble autenticación en redes VPN y servidores de correo electrónico corporativo.

Pese a la tendencia en el aumento de compañías que ofrecen este método de protección, el desconocimiento de esta tecnología por parte de los usuarios dificulta la mitigación de algunos ataques informáticos. Tal situación se ve agravada si se considera que, en muchas ocasiones, la doble autenticación viene desactivada por defecto siendo necesaria la activación y configuración manual por parte del usuario. Para poder medir qué tan sensibilizados están los usuarios con respecto a la doble autenticación, ESET Latinoamérica aplicó una encuesta que abordó dicha temática. De acuerdo a los datos obtenidos, más del 64% de los usuarios en América Latina desconoce qué es la doble autenticación. Queda en evidencia la falta de concientización del usuario con respecto a este mecanismo. Ciertamente la usabilidad es un tema vital en la adopción de un sistema de seguridad por parte de los usuarios, sin embargo, algunas empresas han demostrado que esta característica sí es considerada al momento de implementar un sistema de doble autenticación.

Teniendo en cuenta que la preocupación por una mayor privacidad en Internet es un tema de interés social, es posible que en un futuro se observe una tendencia de los usuarios por activar este tipo de protección doble y se lleven a cabo campañas de concientización que contemplen este tema. En esta línea, ESET Latinoamérica publicó el documento ¿El fin de las contraseñas? La autenticación simple cada vez más amenazada. En el texto citado es posible ahondar en el funcionamiento de este método de validación y cómo activarlo en algunos servicios.

Cibercrimen

Como se explicó en las páginas anteriores, la preocupación que manifestaron los usuarios con respecto a la privacidad de la información en Internet ha ido aumentando, sin embargo, ciertas amenazas informáticas, como los códigos maliciosos, continúan siendo una de las principales causas de robo de información y pérdida de privacidad. Si bien la falta de concientización por parte de los usuarios cumple un rol fundamental en el "éxito" de estos ataques, el mundo del cibercrimen mejora y actualiza constantemente sus técnicas para obtener rédito económico.

Tal como se mencionó en el documento **Tendencias 2013: Vertiginoso crecimiento de malware para móviles**[16], el incremento tanto de amenazas informáticas para dispositivos Android como para el mercado móvil en general han continuado evolucionando a un ritmo acelerado. En esta línea, y de forma similar a lo ocurrido en 2013, la cantidad de detecciones, familias, variantes y firmas para detectar códigos maliciosos diseñados para Android continúan creciendo rápidamente.

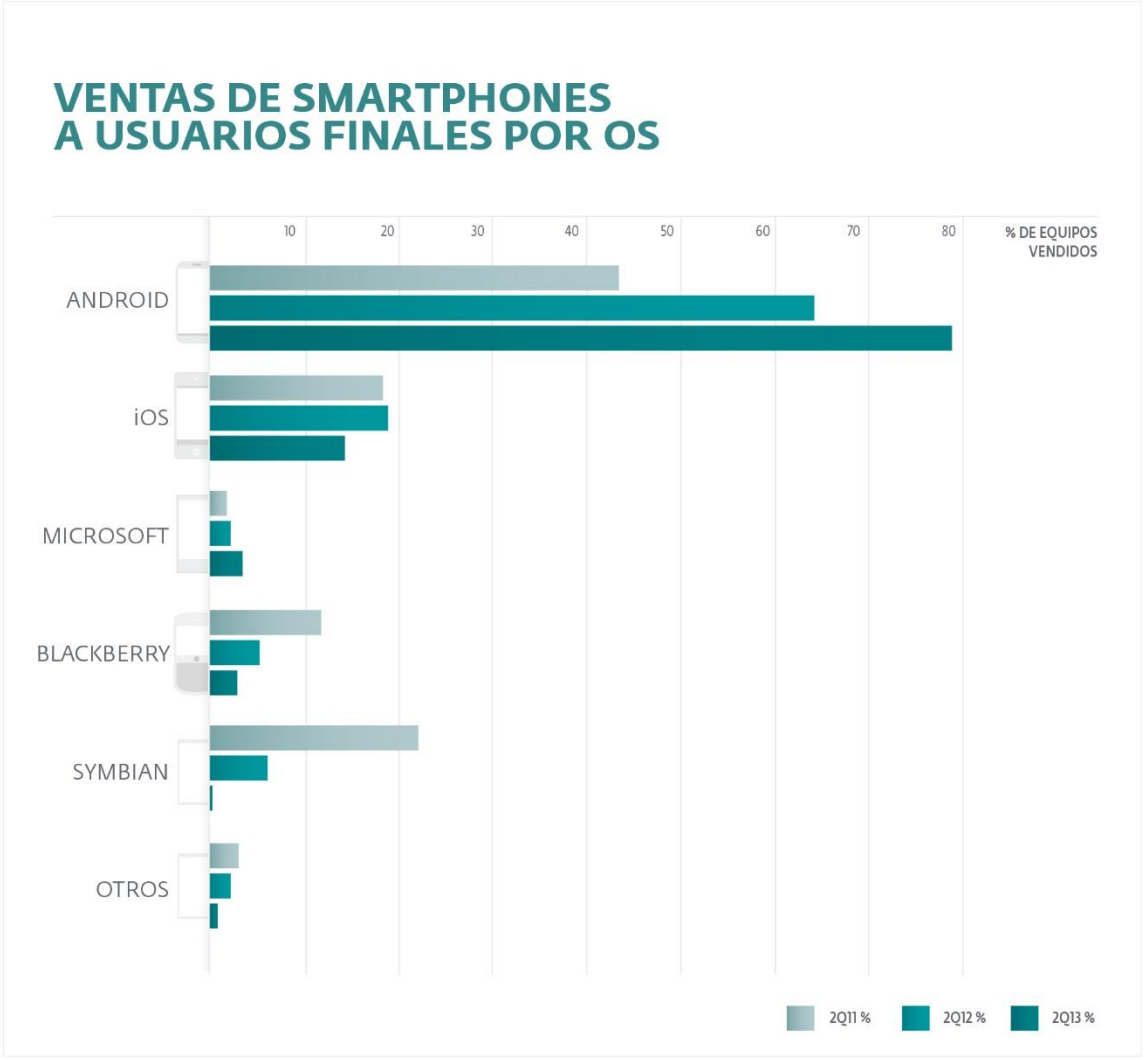
Más allá de las tendencias planteadas en los párrafos anteriores, también se ha podido notar una evolución técnica de ciertos tipos de códigos maliciosos. La primera categoría tiene relación con las amenazas diseñadas para formar botnets, es decir, redes de computadores comprometidos (zombis) que son manipulados por un atacante. En segundo lugar, el *malware* diseñado para plataformas de 64 bits que también se ha ido complejizando en el último tiempo. Finalmente, cabe destacar que la extorsión utilizando malware (*ransomware*) como método de obtención de rédito económico se ha vuelto cada vez más frecuente en América Latina, dejando de ser una técnica que se aplicaba casi exclusivamente en países como Rusia y Estados Unidos.

Android: líder del mercado y el más atacado

En el documento Tendencias 2013 quedó de manifiesto que el sistema operativo Android de Google se consolidó como la plataforma móvil más utilizada. En este sentido, la tendencia imperante, en cuanto a la porción del mercado que ocupa Android, es hacia una tasa de uso cada vez mayor, lo que permite explicar el aumento y consolidación de diversas amenazas informáticas que afectan a esta plataforma y que serán explicadas más adelante. Siguiendo con la revisión del mercado de móviles, se puede observar que Apple iOS continúa siendo el segundo sistema operativo más popular. A continuación, se presenta un gráfico que muestra la evolución experimentada por las diversas plataformas móviles existentes. Para ello se utilizaron dos estudios de Gartner[17] que contemplan estadísticas de mercado del segundo trimestre de 2011, 2012 y 2013:

[16] Tendencias 2013: Vertiginoso crecimiento de malware para móviles. Disponible en http://www.eset-la.com/centro-amenazas/articulo/Tendencias-2013-Vertiginoso-crecimiento-malware--moviles/2863.

http://www.gartner.com/newsroom/id/1764714 y http://www.gartner.com/newsroom/id/2573415.



Fuentes: Ventas de Smartphones a usuarios finales 2Q11 y 2Q12-13, Gartner

En base a los resultados publicados por Gartner, en el segundo trimestre de 2011 Android poseía el 43,4% del mercado. Un año más tarde, dicho porcentaje aumentó a un 64,3% y en la actualidad alcanza el 79%. Este crecimiento va acompañado de un aumento directamente proporcional de la cantidad de códigos maliciosos que se desarrollaron para Android. Asimismo, la evolución de algunas amenazas para este sistema operativo y el descubrimiento de ciertas vulnerabilidades, demuestran el creciente interés de los cibercriminales por atacar este segmento.

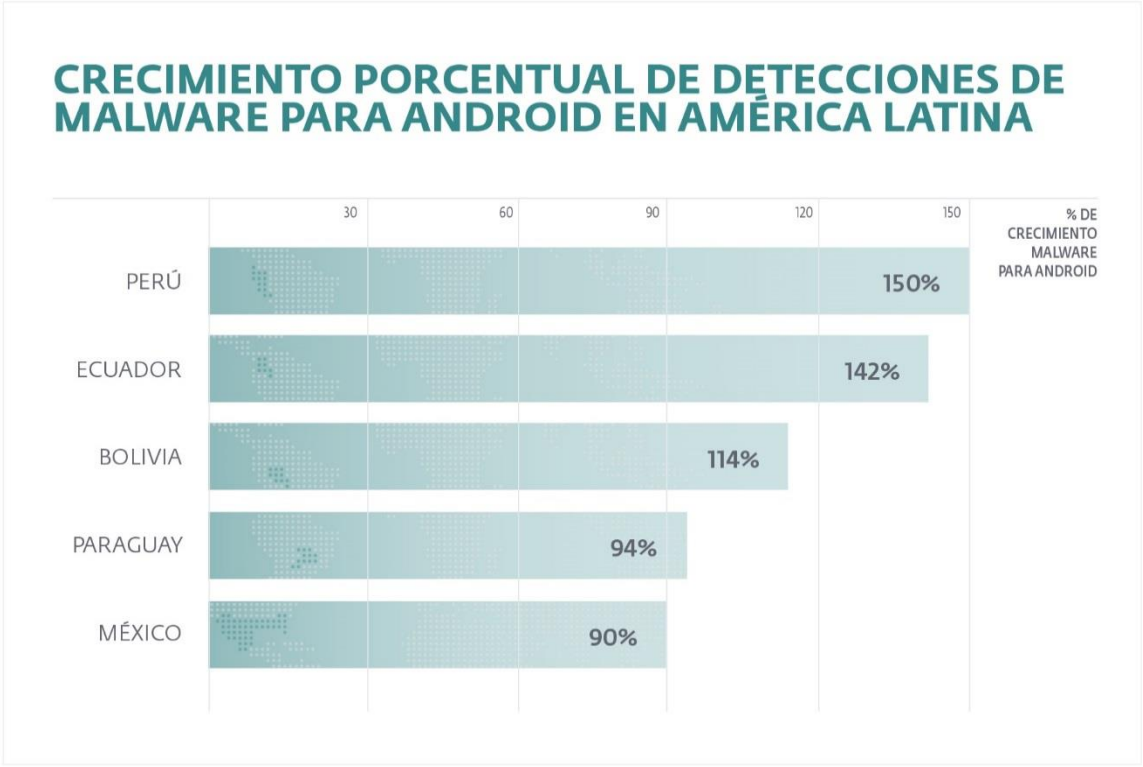
Con respecto a los demás sistemas operativos, iOS mantiene su posición pese a algunos vaivenes, como la segunda plataforma más popular del mercado. Windows Phone experimentó un leve aumento, mientras BlackBerry y Symbian sufrieron un decrecimiento.

En las siguientes páginas se abordará el crecimiento que han experimentado algunas amenazas para plataformas móviles en cuanto al número de detecciones, complejidad y otros factores. Posteriormente, en la tercera sección, se explicará la tendencia en la diversificación de dispositivos "no tradicionales" que ejecutan Android y otros sistemas operativos, y el consiguiente riesgo para la seguridad y privacidad que esto puede significar para los usuarios.

Las amenazas informáticas para Android continúan aumentando

Tal como se vaticinó en el documento Tendencias 2013, el crecimiento de códigos maliciosos para Android continúa aumentando a un ritmo vertiginoso. La primera cifra que permite corroborar este punto tiene relación con la cantidad de detecciones únicas. Si se comparan las detecciones ocurridas en 2012 y 2013, es posible establecer que se incrementaron un 63% a nivel mundial. Cabe destacar que se está contemplando todo el año 2012 y solo parte de 2013 (desde el 1 de enero hasta el 22 de octubre). Aun así, el crecimiento es considerable.

Los países que registran el mayor crecimiento en el número de detecciones de *malware* para Android son Irán, China y Rusia. Por otro lado, si se consideran los cinco países de América Latina que registraron el mayor incremento porcentual de detecciones comparando 2012 y 2013, se destacan Perú (150%), Ecuador (142%), Bolivia (114%), Paraguay (94%) y México (90%). A continuación, se muestra un gráfico con los porcentajes expresados anteriormente:

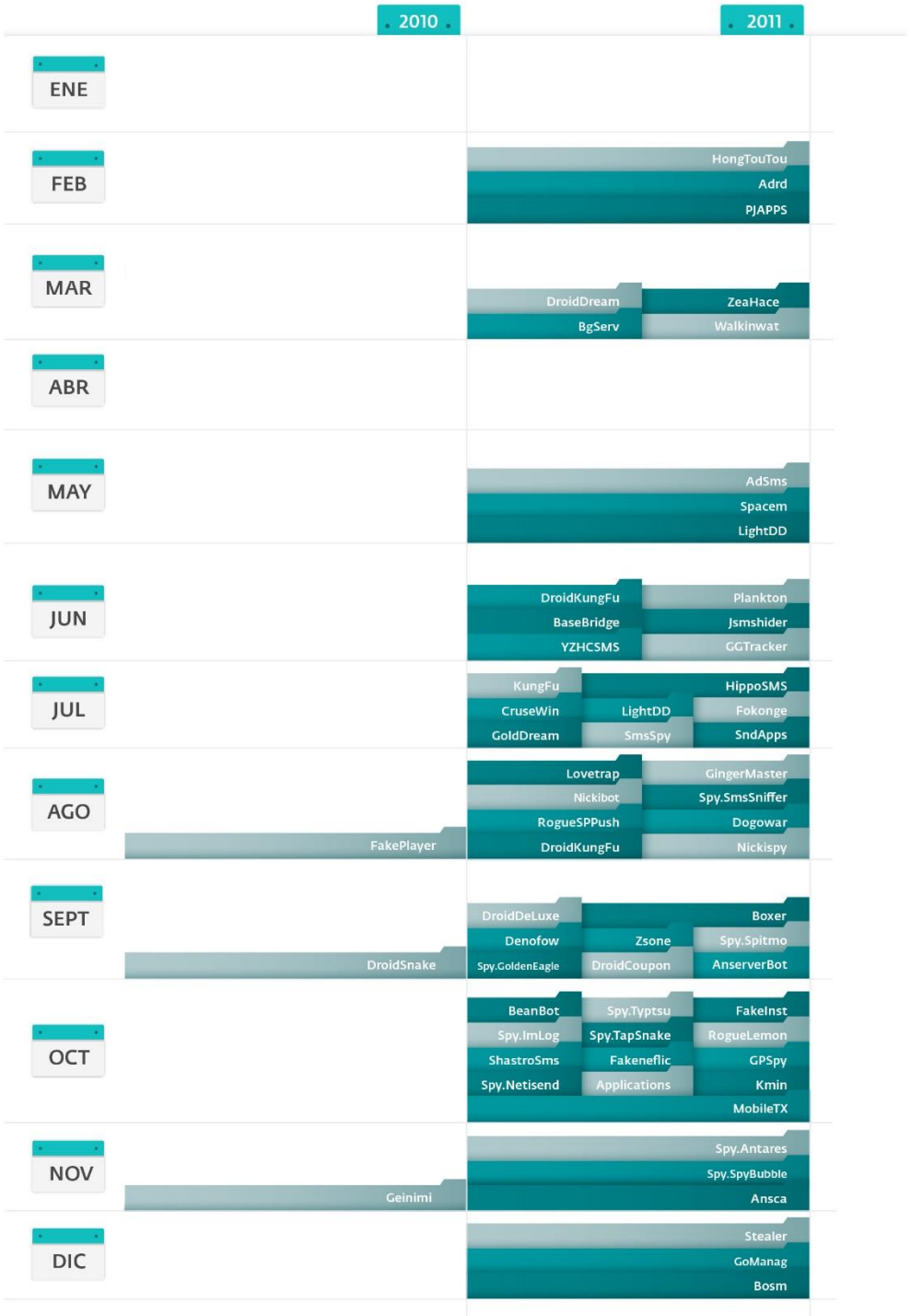


Si se comparan las cifras de este año con las expresadas en el documento Tendencias 2013, Perú y Ecuador continúan liderando este ranking. Debajo quedan Colombia (63%), Chile (17%) y Argentina (20%) dando paso a Bolivia, Paraguay y México.

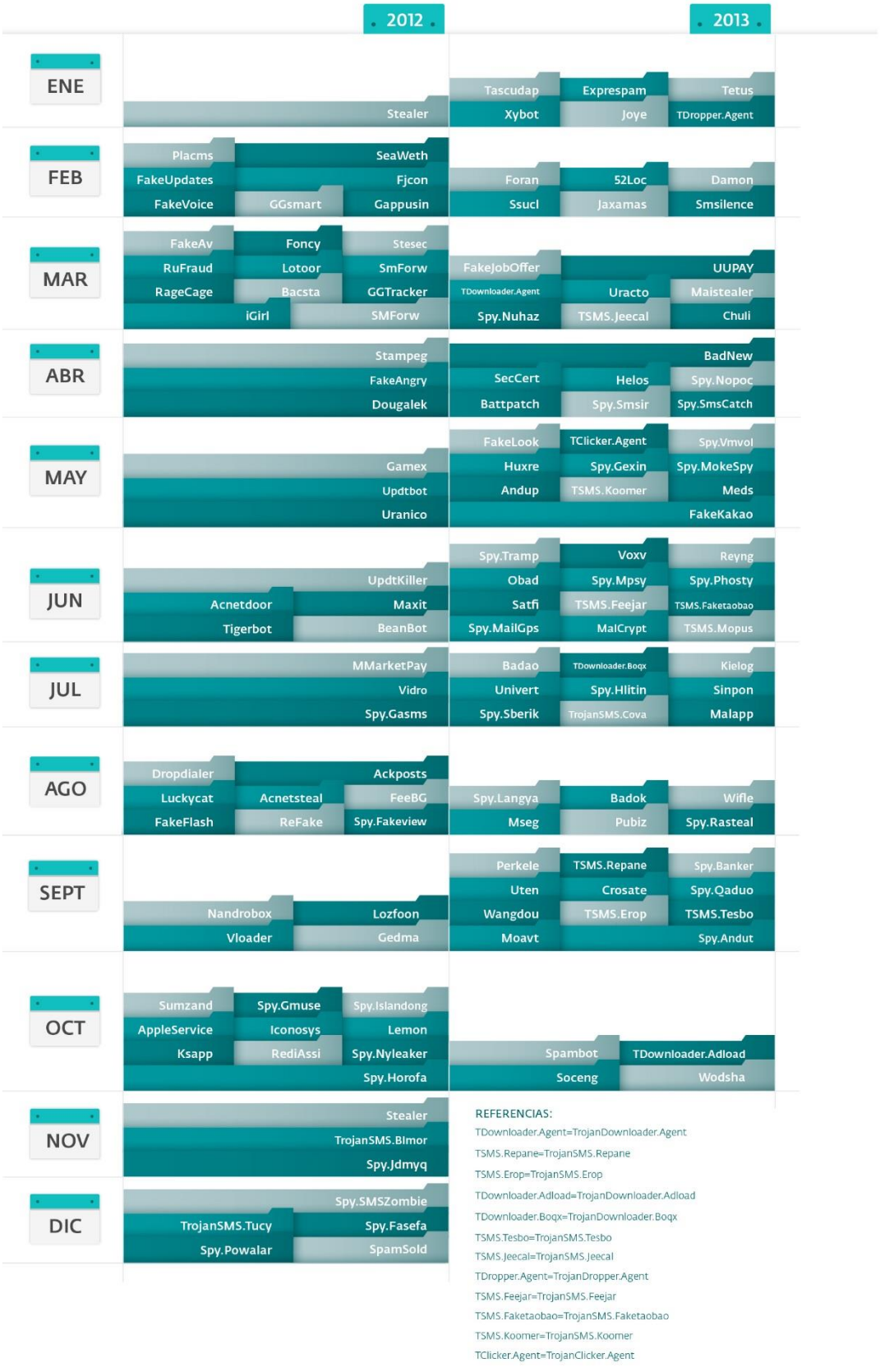
Nuevas familias y tipos de malware para Android

En conjunto con el crecimiento del porcentaje de las detecciones de códigos maliciosos para Android, también se ha podido notar un aumento en el número de familias de *malware* para este sistema. Cabe destacar que una familia es un conjunto de códigos maliciosos que comparten algunas características en común. A continuación, se muestra un diagrama que contempla las familias que aparecieron en los últimos cuatro años (2010-2013):

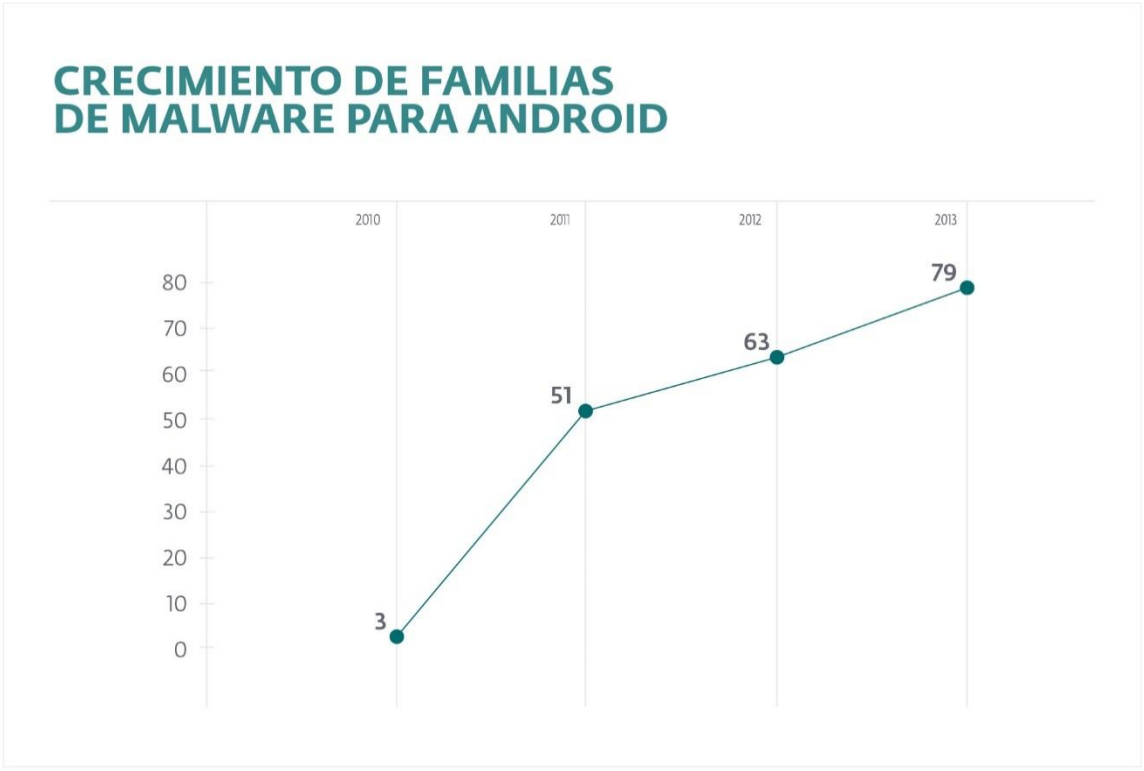
EVOLUCIÓN DE MALWARE PARA ANDROID



EVOLUCIÓN DE MALWARE PARA ANDROID



A través del gráfico, se puede observar que en 2010 solo existían tres familias. Conforme pasaron los años, dicha cifra fue incrementándose de tal modo que en 2011 se reportaron 51 familias, en 2012 63, y hasta octubre de 2013, 79. El siguiente gráfico muestra esta tendencia:



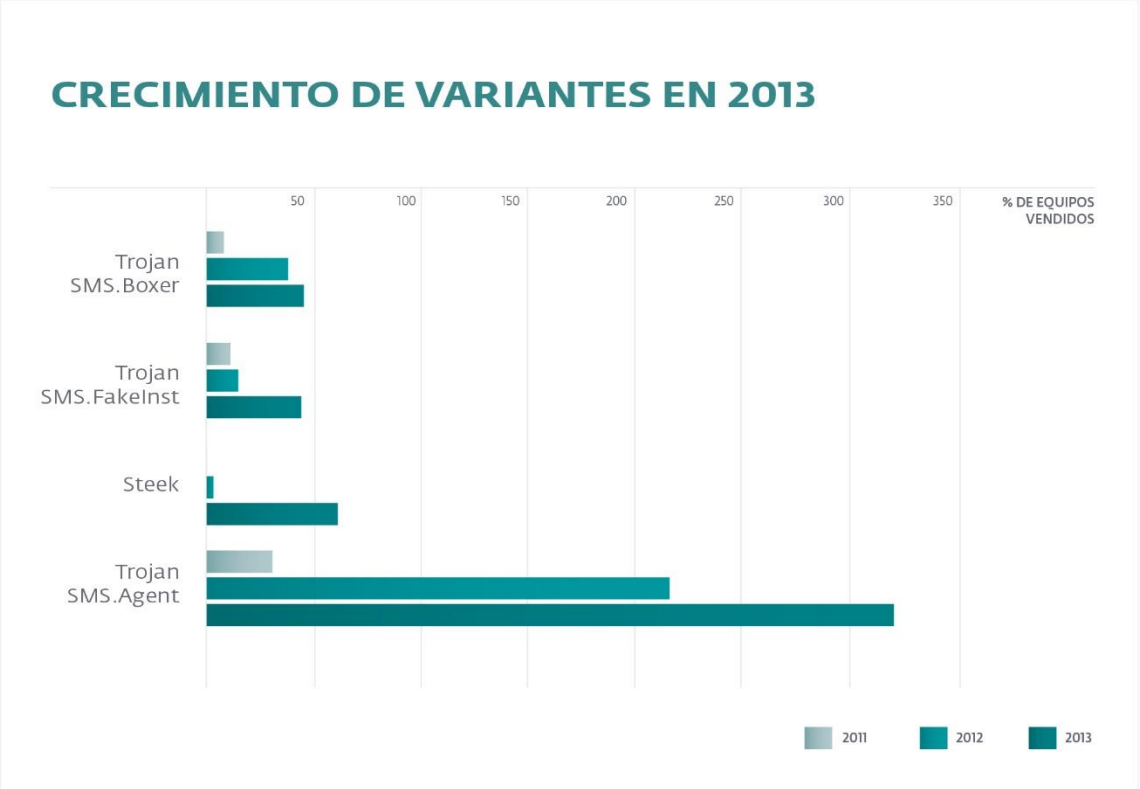
Cabe destacar que en 2013 se reportaron la mayor cantidad de familias de *malware* para Android, incluso considerando solo diez meses. Si se compara el mismo período de tiempo (de enero a octubre), en 2012 aparecieron 55 familias y en 2013 79. Esto representa un 43,6% de crecimiento durante 2013. Otro aspecto interesante de analizar con respecto a las familias, es el descubrimiento de nuevas categorías de troyanos para Android. Hasta hace un año, era común observar troyanos espías (*Spyware*), SMS y aquellos que buscan convertir el dispositivo en zombi. Sin embargo, en 2013 se reportaron cuatro subcategorías de troyanos que antes solo se observaban para Windows y otras plataformas "convencionales":

1. Troyanos *Downloader*: buscan descargar otras amenazas desde Internet para posteriormente instalarlas en el equipo.
2. Troyanos *Dropper*: instalan otras amenazas que el propio troyano incluye dentro de su código.
3. Troyanos *Clicker*: el objetivo es generar tráfico en un sitio o aviso publicitario con el fin de aumentar artificialmente el número de "clics". Esto permite que el atacante genere una ganancia superior.
4. Troyanos bancarios: busca robar específicamente datos relacionados a entidades financieras y bancos.

La tendencia dominante no solo tiene relación con el crecimiento de amenazas para la plataforma móvil de Google, sino también con la aparición de subtipos de troyanos que antes solo afectaban a sistemas operativos "tradicionales". Es probable que en el futuro aumenten la cantidad de familias de troyanos que componen cada una de estas subcategorías.

Las variantes de malware también aumentan

Otra cifra que aumentó nuevamente es la cantidad de variantes que componen cada familia, es decir, modificaciones relativamente menores de un código malicioso conocido. Los atacantes suelen desarrollar nuevas variantes con el objetivo de evadir la detección de las soluciones de seguridad y para añadir nuevas funcionalidades maliciosas. 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. El siguiente gráfico contempla cuatro familias de códigos maliciosos para Android; para cada una se incluye el número de variantes que aparecieron en 2011, 2012 y 2013 según corresponda:



Nuevamente, la familia que experimentó el mayor crecimiento en cuanto a variantes es *TrojanSMS.Agent*. La primera variante de este *malware* data de 2011 y en aquel momento llegó a estar conformada por tan solo 31 variantes. En 2012 se descubrieron 214 variantes y un año más tarde, 324. Le sigue el troyano Steek cuya primera variante se descubrió en 2012. En la actualidad, dicho código malicioso está conformado por 61 variantes en comparación a las tres que se detectaron en 2012. Boxer y FakeInst también aumentaron en 2013 con 45 y 48 nuevas variantes respectivamente.

Vulnerabilidades en plataformas móviles

Las vulnerabilidades son errores de programación que bajo determinadas circunstancias pueden ser aprovechadas por atacantes para comprometer un sistema y robar información. En este sentido, la tecnología móvil no está exenta de este problema, pues son dispositivos que también utilizan *software* y *hardware* que pueden contener fallas. Pese a esto, en la actualidad se observan más casos de explotación de vulnerabilidades que afectan a sistemas "tradicionales" y no plataformas mobile, sin embargo, en 2013 ha quedado de manifiesto que los cibercriminales están comenzando a enfocarse cada vez más en explotar agujeros de seguridad en sistemas operativos para móviles como Android.

Una prueba de la afirmación anterior es el descubrimiento del troyano Obad. Este código malicioso puede ser manipulado por un tercero a través de mensajes SMS y posee la capacidad de descargar otras amenazas y de robar información sensible, como los contactos de la víctima. Aunque tales características no lo convierten en un troyano novedoso, lo que sí lo hace es la explotación de dos vulnerabilidades hasta ese momento desconocidas. La primera radica en el programa dex2jar, *software* que es utilizado por la industria de la seguridad para analizar estáticamente códigos maliciosos diseñados para Android. La segunda vulnerabilidad explotada por Obad reside específicamente en Android.

Antes de explicar este aspecto, es necesario comprender que Android posee una lista visible para el usuario y que incluye aquellas aplicaciones instaladas que necesitan permisos de administrador para funcionar. Esta lista puede ser accedida en algunos dispositivos ingresando a Ajustes → Seguridad → Administradores de dispositivos. En esta línea, un agujero de seguridad permitió que este código malicioso se ejecutara con privilegios sin aparecer en la lista de programas que solicitan tal permiso. De este modo, para la víctima resultaba imposible visualizar a Obad como aplicación que requiere permisos de administrador. Si bien esta situación, en donde códigos maliciosos explotan vulnerabilidades *0-day* (desconocidas hasta aquel entonces), no es novedosa en plataformas como Windows, sí lo es en Android. El descubrimiento de Obad demuestra que los cibercriminales están buscando nuevas vulnerabilidades en sistemas operativos, como Android, con el objetivo de perpetrar fácilmente ataques informáticos.

Por otro lado, investigadores de Bluebox Labs encontraron una grave vulnerabilidad que afecta a casi todas las versiones de Android (desde la 1.6 a la 4.2). Denominada por sus descubridores como "Master Key" (llave maestra), este error facilita que un atacante pueda desarrollar códigos maliciosos que roben información o conviertan el dispositivo en zombi y camuflarlos como aplicaciones genuinas. La explotación de esta vulnerabilidad afecta el modo en que Android comprueba la llave criptográfica de las aplicaciones[18]. En otras palabras, cada aplicación legítima posee una llave única que permite comprobar la autenticidad de la misma. De este modo, si un tercero modifica arbitrariamente un programa, Android impedirá la instalación del *software*, sin embargo, mediante la explotación de este agujero de seguridad, un cibercriminal podría alterar una aplicación dejando intacta la llave criptográfica. Por lo mismo, el programa malicioso sería ejecutado sin ningún tipo de advertencia por parte del sistema operativo.

Tecnología NFC

La tecnología *Near Field Communication* (NFC) permite intercambiar información juntando físicamente dos dispositivos. Aunque puede ser utilizada para la transferencia de archivos, algunos países como Chile están adoptando este protocolo de comunicación para facilitar el pago de servicios como restoranes, centros comerciales, entre otros[19]. El objetivo es facilitar la vida cotidiana al evitar que las personas tengan que llevar consigo tarjetas u otros medios de pago. Sin embargo, es importante considerar que cualquier tecnología utilizada para realizar transferencias bancarias es un blanco potencial de ataques informáticos. En este sentido, es posible que a medida que esta tendencia de pago electrónico se consolide, será más probable encontrar códigos maliciosos que intenten robar la información de los medios de pago en cuestión.

En el caso de la tecnología NFC, el robo de información podría ocurrir en el momento en que el usuario realiza el pago, como también en el mismo dispositivo que implementa dicha tecnología. Por lo mismo, es fundamental que tanto los datos de pagos almacenados en el equipo como la transmisión de información que ocurre al momento de pagar, cuenten con un mecanismo de cifrado robusto.

Otras tendencias en cibercrimen

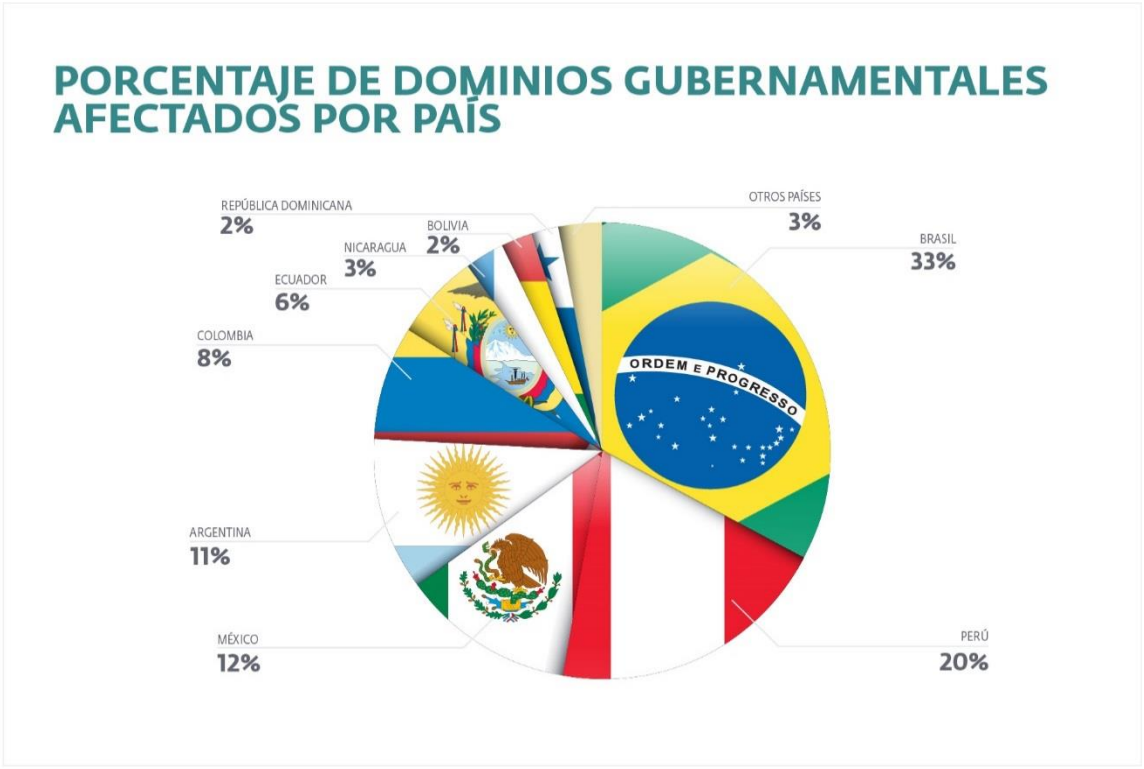
Vulnerabilidades – Java y sitios latinoamericanos

En el artículo Tendencias 2013, una de las principales tendencias que se analizó fue la propagación de códigos maliciosos utilizando un intermediario, es decir, un servidor web que ha sido vulnerado por atacantes para tal propósito. En aquel momento quedó de manifiesto que las estadísticas de detecciones relacionadas a este método de propagación experimentaron un aumento sostenido. En la actualidad, esta tendencia continúa consolidándose en América Latina, siendo los blogs uno de los servicios más vulnerados en la región. Estos representan el 47% del total de sitios afectados en base a una lista de páginas comprometidas.

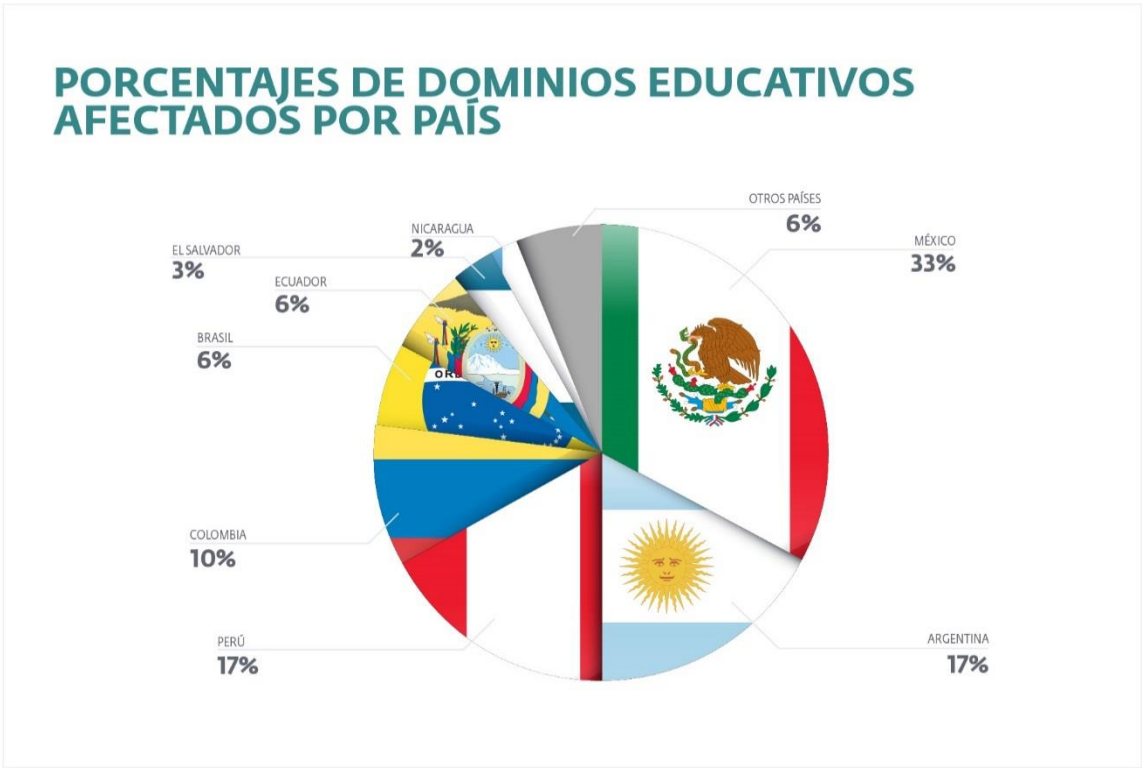
Por otro lado, el Laboratorio de Investigación de ESET Latinoamérica pudo determinar que Brasil, México y Perú tienen la mayor proporción de sitios de entidades oficiales y educativas que han sido comprometidos por terceros para propagar códigos maliciosos. De un total de 4.500 sitios comprometidos que fueron estudiados, el 33% correspondían a páginas gubernamentales brasileñas. Le sigue Perú con un 20% y México con 12%. A continuación, se muestra un gráfico con dichas estadísticas:

[18] Información de la vulnerabilidad CVE-2013-4787. Disponible en http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-4787.

[19] EMOL: Presentan programa piloto de pago con celulares usando tecnología NFC en Chile. Disponible en http://www.emol.com/noticias/tecnologia/2013/08/08/613576/presentan-programa-piloto-de-pago-con-celulares-usando-tecnologia-nfc-en-chile.html.



De los [códigos maliciosos que fueron alojados en dichos sitios], un 90% correspondían a troyanos y el 10% restante se repartía entre gusanos y *backdoors*. En lo que respecta a páginas comprometidas de entidades educativas, México lidera con un 33%. Le siguen Perú y Argentina con un 17% cada uno tal como se aprecia en el siguiente gráfico:



En base a la información expresada en los párrafos anteriores, es posible observar que la tendencia en el aumento del uso de un intermediario ha continuado creciendo en la región, sin embargo, esta problemática también ha evolucionado en términos técnicos. Esto se debe al aumento en la explotación de diversas vulnerabilidades en Java y al desarrollo de nuevos códigos maliciosos destinados a automatizar la vulneración de servidores web Linux y la propagación de amenazas informáticas.

El primer aspecto de esta evolución técnica se relaciona con el aumento en la explotación de vulnerabilidades en Java. Es importante considerar que Java es una tecnología multiplataforma (que funciona en varios sistemas operativos) y que posee la capacidad de agregar nuevas funcionalidades a sitios web, por lo tanto, reúne dos características que resultan provechosas para los cibercriminales. Por un lado, el hecho de que funcione en diferentes sistemas operativos facilita que los atacantes puedan comprometer distintos entornos; y por el otro, al ser una tecnología popular, los ciberdelincuentes se aseguran de poder afectar a un mayor número de usuarios.

La efectividad de ataques que explotan vulnerabilidades en Java quedó demostrada empíricamente cuando empresas como Facebook y Apple resultaron infectadas. Investigaciones posteriores revelaron que se trató de un código malicioso que logró ingresar a los sistemas de ambas compañías mediante la explotación de vulnerabilidades en dicho *software*. Para lograr tal objetivo, los atacantes vulneraron un sitio web que los empleados de Apple y Facebook solían visitar. En esa página, los ciberdelincuentes alojaron un *applet* malicioso (aplicación Java) que explotaba un agujero de seguridad. Finalmente, y tras la visita del sitio comprometido, la infección pudo concretarse sin mayor intermediación por parte de las víctimas. A continuación, se muestran las distintas etapas que hicieron factibles ambos ataques:

Esquema 5 Etapas involucradas en ataque a Apple y Facebook

El segundo aspecto de esta evolución técnica tiene que ver con el desarrollo de nuevos códigos maliciosos destinados a vulnerar servidores web que ejecutan Linux. Si antes los cibercriminales comprometían un servidor a través de la explotación de una vulnerabilidad para luego alojar un *malware*, en la actualidad ese procedimiento "manual" está comenzando a ser reemplazado por el uso de códigos maliciosos destinados a ese propósito, como Cdorked, Chapro y Snakso. En los tres casos, se trata de *malware* diseñado específicamente para comprometer servidores web Linux. Posteriormente, estas amenazas cumplen el objetivo de modificar los sitios y propagar otros códigos maliciosos diseñados para Windows, logrando finalmente automatizar todo el proceso de ataque.

Botnets

Tal como se mencionó en la publicación Tendencias 2010: la madurez del crimeware, los autores de amenazas informáticas comenzaron a desarrollar códigos maliciosos cuyo objetivo principal es la obtención de rédito económico. Dicha tendencia se ha mantenido constante en el tiempo y ha estado acompañada de *malware* que busca conformar botnets, es decir, redes de computadoras que una vez infectadas (zombi), quedan a merced de un grupo de ciberdelincuentes (botmasters) que las pueden utilizar para robar información, perpetrar ataques en contra de otros sistemas, almacenar contenido ilegal sin el consentimiento de la víctima, entre otras acciones maliciosas.

Si se considera que el principal objetivo es la obtención de ganancias económicas, resulta comprensible que los cibercriminales destinen recursos en la conformación de botnets debido a que mientras más computadoras infectadas controlen, mayor será la probabilidad conseguir dinero. En esta línea, no solo se ha podido observar un aumento de códigos maliciosos que poseen dicha capacidad, sino también técnicas que buscan aumentar la complejidad de este tipo de amenazas con el propósito de evitar que las autoridades u otros organismos desarticulen este tipo de redes. El primer caso observado en 2013 tiene que ver con el código malicioso detectado como *Win32/Rootkit.Avatar*. Dicha amenaza utiliza Yahoo! Groups como medio para controlar las computadoras zombis. Asimismo, este código malicioso posee técnicas para evadir análisis forenses, es decir, dificultar aquellos estudios que se realizan con el objetivo de poder determinar aspectos de la infección que son necesarios durante un proceso judicial.

Otra tendencia observada en torno a las Botnets, es la utilización de TOR como forma de ocultar el actuar de los ciberdelincuentes. Si bien no es una técnica novedosa *per se*, en los últimos meses se ha visto un incremento en el uso de esta metodología debido a los siguientes motivos: en algunas ocasiones, realizar un análisis de los datos que se transmiten desde y hacia una botnet permite determinar qué información se está robando; asimismo, facilita la desarticulación de la red y el posible reconocimiento de los responsables. Sin embargo, al utilizar TOR los atacantes dificultan considerablemente los objetivos mencionados anteriormente, ya que esta red fue diseñada específicamente para cifrar todos los datos transmitidos, por lo que realizar una captura de tráfico resulta una tarea bastante más compleja. A lo largo de 2013 también ha quedado de manifiesto que los cibercriminales además de utilizar variantes de códigos maliciosos ya conocidos, también desarrollan nuevas familias como Napolar, *malware* que afectó a países como Perú, Ecuador y Colombia. Dicha amenaza se propagó mediante Facebook y posee la capacidad de formar una botnet, realizar ataques de denegación de servicio (envío masivo de peticiones a un servidor con el objetivo de provocar un colapso y dejar sitios web fuera de línea), robar información de la víctima, entre otras acciones.

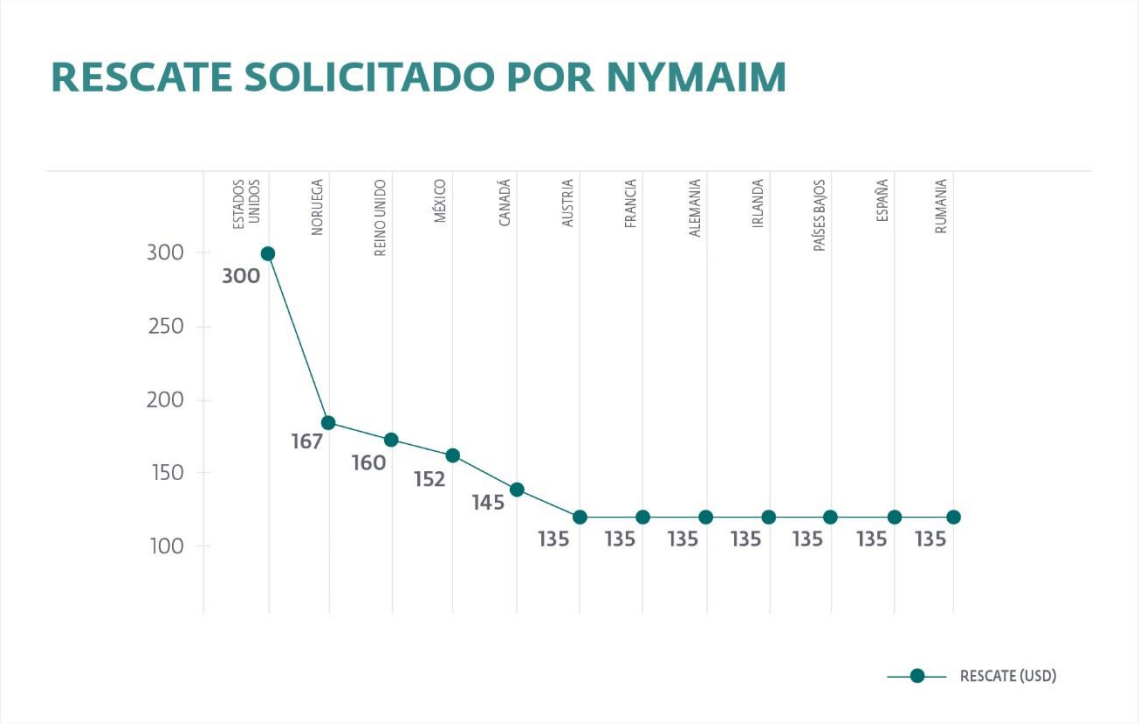
Por otro lado, pruebas de concepto como la creación de una red botnet conformada por 1.000.000 de navegadores, que fue presentada en el evento BlackHat 2013, reafirman la posibilidad de que en un futuro los ciberdelincuentes utilicen otras técnicas para continuar obteniendo rédito económico a través de redes de computadores zombi. Como se mencionó, el uso de estas metodologías obedece no solo al aumento de la complejidad y la consiguiente dificultad en el estudio de este tipo de amenazas, sino también al incremento en la efectividad de las soluciones de seguridad. En este sentido, a medida que los métodos de detección proactiva, como la heurística y las firmas genéricas, evolucionan, también lo hacen las amenazas. Es probable que en el futuro se detecten nuevos casos de códigos maliciosos y familias que estén destinadas a conformar este tipo de redes y que a la vez, implementen técnicas consignadas a perfeccionar el funcionamiento de dichas amenazas.

Ransomware en América Latina

Hasta hace algún tiempo, los códigos maliciosos del tipo *ransomware*, es decir, que solicitan dinero (un rescate) a cambio de la información que borran o cifran, afectaban principalmente a países como Rusia, no obstante, esta metodología de ataque está consolidándose en América Latina y ya existen varios usuarios que resultaron afectados. En el caso de los códigos maliciosos citados en las secciones anteriores, la obtención de ganancias económicas reside en el robo directo de la información, sin embargo, en el caso del *ransomware* la metodología es a través de la extorsión de la víctima.

Cuando un usuario ejecuta un código malicioso de estas características, puede suceder que el acceso al sistema sea bloqueado. Un ejemplo de este comportamiento es el que presenta la familia de *malware* LockScreen (Multi Locker) o el coloquialmente denominado "Virus de la Policía". En este caso, la persona no podrá acceder al equipo hasta que se remueva la amenaza del sistema. En otras ocasiones, la información es cifrada tal como lo realiza la familia de códigos maliciosos Filecoder, de este modo, se imposibilita el uso de esos datos. En ambos casos, los cibercriminales le solicitan a la víctima una suma de dinero a cambio del control de la computadora o el acceso a la información "secuestrada".

Con respecto a la tendencia en el aumento de amenazas *ransomware* en América Latina, se destaca México como el país más afectado por Multi Locker. En este sentido, las detecciones de LockScreen en dicha nación han aumentado casi tres veces con respecto a todo 2012. Asimismo, en 2012 México ocupaba la posición 37ª a nivel mundial de detecciones de LockScreen; en la actualidad, ascendió a la posición 11ª. Asimismo, Nymaim es otro código malicioso que afecta a ese país y que solicita una suma de dinero que asciende a los 150 dólares aproximadamente por el rescate del equipo. Cabe mencionar que el precio por el rescate varía de acuerdo a cada país. El siguiente gráfico muestra el monto solicitado en algunas naciones:



Con respecto a las estadísticas de Filecoder en la región, se destaca Perú como el país que registra el mayor índice de detecciones de América Latina durante 2013, siendo Rusia la nación más afectada del mundo. En relación a la complejidad técnica de esta familia de *malware*, es importante mencionar que en algunos casos la posibilidad de recuperar los archivos cifrados es factible debido a que el algoritmo utilizado no es lo suficientemente robusto, o la clave de descifrado se encuentra embebida dentro del código de la amenaza. Sin embargo, parte de la evolución de estos códigos maliciosos radica precisamente en el uso de algoritmos cada vez más complejos que imposibilitan o dificultan la recuperación de los archivos. Es posible obtener más información sobre los métodos de cifrado (encriptación) en la publicación Filecoder: dinero a cambio de información secuestrada.

Este tipo de metodología parte de la premisa de que los usuarios almacenan información valiosa y no siempre realizan los respaldos (*backup*) necesarios, por lo tanto, frente a esta situación de desesperación es posible que la víctima decida pagar por el "rescate". Dicha acción no hace más que incentivar tal modelo de negocio ilícito, por lo que no pagar y adoptar las medidas necesarias contribuye a prevenir y combatir este tipo de código malicioso.

Evolución del malware para 64 bits

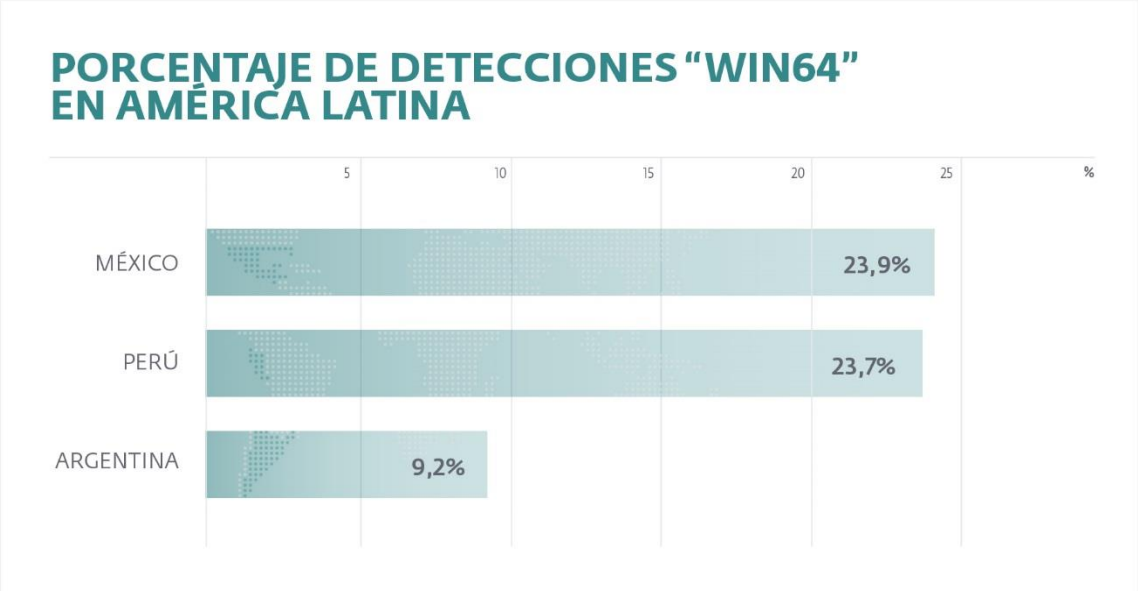
Las plataformas de 64 bits no son nuevas. De hecho, en 2005 Microsoft ya ofrecía una edición de Windows XP diseñada para funcionar en procesadores cuyo set de instrucciones es x86-64. Pese a esto, en aquellos tiempos era una tecnología poco adoptada por los usuarios, por ende, no formaba parte de los blancos de los cibercriminales. Tal situación ha ido cambiando con el tiempo y cada vez es más frecuente observar computadoras que incluyen una arquitectura de 64 bits de forma predeterminada. En este sentido, y de acuerdo a estadísticas publicadas por Microsoft, en junio de 2010 el 46% de las instalaciones de Windows 7 a nivel global fueron de 64 bits[20]. Asimismo, y en base a información publicada por Digital Trends, Gartner predice que para 2014 un 75% de las computadoras corporativas utilizarán alguna edición de 64 bits de Windows[21].

El aumento en el uso de arquitecturas de 64 bits resulta lógico si se considera que esta tecnología permite el uso de más de 4 GB de RAM, algo que de forma nativa la computación de 32 bits no puede manejar. Además, algunas aplicaciones complejas resultan beneficiadas en términos de rendimiento si son desarrolladas para sistemas de 64 bits. Considerando dicho contexto, los cibercriminales están comenzando a desarrollar más amenazas diseñadas específicamente para esta tecnología y que con el tiempo también han evolucionado técnicamente. El primer caso tiene relación con Expiro, virus

[20] Microsoft: 64-Bit Momentum Surges with Windows 7. Disponible en http://blogs.windows.com/windows/b/bloggingwindows/archive/2010/07/08/64-bit-momentum-surges-with-windows-7.aspx.
[21] Digital Trends: Most Corporate PCs to Run 64-bit Windows by 2014, Says Gartner. Disponible en http://www.digitaltrends.com/computing/most-corporate-pcs-to-run-64-bit-windows-by-2014-says-gartner/.

capaz de infectar archivos tanto de 32 como 64 bits, lo que lo transforma en una amenaza altamente versátil e infecciosa. Expiro tiene como objetivo robar datos que son ingresados por la víctima en diversos sitios web.

En consecuencia, los índices de detección de códigos maliciosos diseñados para plataformas de 64 bits también han aumentado en América Latina. Países como México, Perú y Argentina son los tres que han experimentado el crecimiento más importante de la región con respecto a esta tendencia. A continuación, se muestra un gráfico con los porcentajes para cada uno de estos tres países:



Tal como se puede apreciar, México (23,9%) y Perú (23,7%) son los países de la región más afectados por códigos maliciosos diseñados para plataformas Windows de 64 bits. En tanto, Argentina (9,2%) queda bastante por detrás, y otros países como Chile y Brasil se posicionan aún más abajo con el 5,9% y 5,4% respectivamente. En lo que atañe a los códigos maliciosos para 64 bits más detectados en México y Perú, destacan las familias *Win64/Sirefef* y *Win64/Conedex*.

En el futuro, es probable que esta tendencia se consolide todavía más. Asimismo, el lanzamiento de teléfonos inteligentes que utilizan sistemas operativos de 64 bits como el iPhone 5s, plantean la posibilidad de que en un tiempo se puedan detectar las primeras amenazas informáticas diseñadas para plataformas móviles de 64 bits.

Bitcoins

Las bitcoins representan una divisa electrónica relativamente nueva que carece de una entidad central que las regule. También permiten la compra de bienes "reales" y no necesariamente virtuales. Ambos puntos transforman esta moneda electrónica en un blanco para los cibercriminales. En esta línea, cada vez se desarrollan más amenazas capaces de aprovechar el poder de cálculo de la CPU y GPU de la computadora del usuario para obtener bitcoins. En este sentido, y considerando que las bitcoins son monedas electrónicas, los recursos de un sistema pueden ser utilizados para obtener dicha divisa. Sin embargo, el cálculo necesario para obtener una bitcoin es tan complejo que requiere de muchos recursos y tiempo de procesamiento, de modo que los ciberdelincuentes utilizan redes botnets para facilitar dicho objetivo. La ventaja del uso de varias computadoras en paralelo se resume en el siguiente esquema:

Esquema 6 Uso de computadoras zombis para obtener bitcoins

El método más utilizado por los atacantes para obtener rédito económico mediante estas divisas, es el cálculo del algoritmo que utilizan las monedas digitales. Entre los ejemplos de códigos maliciosos que utilizan dicho procedimiento, se encuentran Win32/Delf.QCZ y la cada vez más numerosa familia de *malware* CoinMiner. Pese a que bitcoin es la moneda electrónica más utilizada en la actualidad, existen otras alternativas que poseen características similares y que también se han transformado en blancos de los atacantes. Un ejemplo de esto es *MSIL/PSW.LiteCoin.A*.

Existe un segundo método por el cual los atacantes pueden obtener ganancias ilícitas de aquellos usuarios que utilizan estas divisas. Por lo general, se emplean billeteras electrónicas para almacenar este tipo de instrumento cambiario, por lo tanto, se han desarrollado códigos maliciosos diseñados para robar precisamente el archivo en donde reside este tipo de información. Esta metodología de obtención de rédito económico tampoco es nueva, sin embargo, la creciente popularidad de las monedas electrónicas permite inferir que un futuro estas amenazas aumentarán en número y complejidad. Para obtener más información sobre este tema se recomienda consultar la publicación "Bitcoins, Litecoins, Namecoins y cómo roban dinero electrónico en Internet".

Diversificación del *malware*: informatización de dispositivos electrónicos con acceso a Internet

Hace diez años, nadie hubiese pensando que un teléfono celular podría infectarse con un código malicioso. En aquel momento era comprensible, puesto que este tipo de dispositivos cumplían funciones básicas como llamadas telefónicas y el manejo de mensajes de texto (SMS), por lo tanto, era técnicamente difícil, o hasta imposible, que se descubrieran amenazas informáticas destinadas a estos equipos. Sin embargo, en la actualidad la situación es drásticamente distinta. La evolución experimentada por esta tecnología ha sido tal que los teléfonos inteligentes permiten realizar acciones similares a las de una computadora como la edición de fotografías, conexión a Internet de alta velocidad, trámites bancarios, juegos, etc. Este avance tecnológico ha sido tanto a nivel de *software* (aplicaciones y sistemas operativos cada vez más complejos) como *hardware* (procesadores de cuatro núcleos, mayor cantidad de memoria RAM, arquitectura de 64 bits, etc.).

Acompañada de esta evolución tecnológica, también se está evidenciando una tendencia no solo en el aumento de este mercado y las amenazas informáticas para móviles, sino también en la diversificación de dispositivos "no tradicionales" que utilizan Android como sistema operativo. En esta línea, productos como consolas de videojuegos (NVIDIA SHIELD), gafas inteligentes (Google Glass), refrigeradores (algunos modelos de Samsung), lavarropas (Lavarropas Touch Screen de Samsung), entre otros, ya se encuentran disponibles en algunos países. Aunque en América Latina y otras regiones este tipo de tecnología no se ha masificado, es probable que más adelante sí lo haga. Este antecedente plantea la posibilidad de que en un futuro se puedan observar amenazas informáticas diseñadas para electrodomésticos inteligentes y otros equipos que no sean directamente dispositivos móviles. Esta probabilidad aumenta si se considera que el sistema operativo de estos aparatos es Android, aspecto que facilita técnicamente el desarrollo de códigos maliciosos y otras amenazas.

Por otro lado, se debe considerar que Android no es el único sistema operativo que se está utilizando en dispositivos inteligentes. Otras empresas han optado por desarrollar plataformas propietarias, es decir, sistemas diseñados específicamente para un grupo de electrodomésticos inteligentes. En este caso, la facilidad con que se podrían desarrollar amenazas informáticas disminuye, sin embargo, en ningún caso es un aspecto que impide la creación de códigos maliciosos. Finalmente, y considerando lo acontecido con el mercado *mobile* y las amenazas para estos equipos, es posible inferir que los electrodomésticos de última generación y otros aparatos "no convencionales" se podrían transformar en blanco de los atacantes en base a tres factores. El primero tiene relación con la evolución tecnológica, luego la masificación en la utilización de estos aparatos, y finalmente el uso que le den los usuarios, es decir, que este pueda significar de algún u otro modo, un rédito económico para los cibercriminales.

A continuación, se mencionan algunos dispositivos "no tradicionales" que han evolucionado en términos informáticos. Asimismo, se explica en qué estado se encuentra la seguridad informática de estos aparatos:

Automóviles

En la actualidad, algunos automóviles incluyen sistemas informáticos cada vez más complejos que permiten la manipulación de ciertos parámetros a través de un teléfono inteligente y un *software*. Esto incluye la medición de la carga de combustible, niveles de aceite, kilómetros recorridos sistemas de entretenimiento a bordo, tecnologías de geolocalización (GPS), etc. Al tratarse de equipos complejos, la posibilidad de que se descubran vulnerabilidades y que estas sean explotadas por atacantes aumenta.

En esta línea, investigaciones recientes demuestran que los sistemas informáticos de algunos automóviles de última generación son vulnerables a un ataque informático. Producto de lo anterior, se ha demostrado, a través de pruebas de concepto, que es posible manipular remotamente un auto y encender el motor, abrir las puertas e incluso desactivar el sistema de frenado[22]. Es importante mencionar que estas pruebas de concepto han sido posibles mediante un enlace físico a través de un cable, no obstante, la capacidad de conexión a Internet que incluyen algunos automóviles podría facilitar un ataque de estas características.

[22] DEFCON: Hackeando autos y vehículos no tripulados. Disponible en http://blogs.eset-la.com/laboratorio/2013/08/03/defcon-hackeando-autos-y-vehiculos-no-tripulados/.

Smart TV

Los televisores también han evolucionado en términos tecnológicos y algunos ya incluyen la posibilidad de conectarse a Internet para consumir contenidos. En este sentido, existe una prueba de concepto capaz de apagar el televisor, lo que demuestra la factibilidad de desarrollar códigos maliciosos para este tipo de equipos. Asimismo, la inclusión de una cámara frontal, que permite filmar de frente lo que sucede en un lugar, aumenta todavía más la posibilidad de que en un futuro estos dispositivos se conviertan en blanco de los cibercriminales. Una investigación presentada en BlackHat 2013 así lo demuestra: "Los Smart TV tienen prácticamente los mismos vectores de ataque que los teléfonos inteligentes"[23]. En esta línea, es posible que más adelante se puedan observar amenazas diseñadas para estos equipos, sin embargo, es posible que el foco esté puesto en la privacidad de la víctima y no necesariamente en la obtención de rédito económico.

Casas Inteligentes

La disciplina que hace posible el diseño e implementación de casas inteligentes se denomina domótica. En otras palabras, se trata de un conjunto de sistemas que posibilitan que una casa o espacio cerrado cuente con una gestión energética eficiente, elementos de confort, seguridad, bienestar, etc. También podría entenderse como la integración de la tecnología dentro de una casa, edificio, u otro tipo de construcción. Considerando la definición anterior, existen varios dispositivos convencionales que han evolucionado y que en la actualidad forman parte de un hogar inteligente, como por ejemplo, inodoros, heladeras, sistemas de iluminación, cámaras IP, entre otros.

En los siguientes párrafos se mencionan algunos de estos dispositivos y cómo un cibercriminal podría perpetrar un ataque informático en contra de estos aparatos tecnológicos:

Inodoros inteligentes

Los inodoros inteligentes también son vulnerables a ataques de seguridad. Algunos incluyen sistemas de limpieza, deodorización e incluso medidores de presión y glucosa en la sangre. Pese a tales características, investigadores de Trustwave lograron alterar el comportamiento normal de un excusado inteligente haciendo que este rocíe agua en la persona y que se abra y cierre automáticamente la tapa[24]. Aunque pueda parecer una acción que no trae mayores consecuencias, este tipo de retretes suelen ser parte de otros sistemas inteligentes, por lo tanto, que este componente de la casa sea comprometido puede significar que otros también estén expuestos a amenazas informáticas.

Sistemas inteligentes de iluminación

Con el avance tecnológico, los sistemas de iluminación también han evolucionado al punto de poder ser controlados utilizando una aplicación instalada en un teléfono inteligente con conexión a Internet. En el mercado ya existe un producto que cumple con dicha característica y que permite, además, cambiar la intensidad y color de la iluminación en base a las preferencias del usuario. Pese a la comodidad que puede otorgar un sistema como este, un investigador demostró mediante el desarrollo de un *exploit*, que puede robar las credenciales de la víctima para poder manipular el sistema de iluminación inteligente sin su consentimiento[25]. Dicha situación no solo puede convertirse en una molestia, sino también en un peligro para la seguridad física del lugar.

Heladeras

Algunos refrigeradores también cuentan con conexión a Internet. Esto posibilita que el usuario pueda conocer el estado y cantidad de los alimentos, buscar recetas en línea, entre otras acciones. Asimismo, empresas como LG han lanzado al mercado refrigeradores qure implementan Android para poder ofrecerle al usuario características "inteligentes" de valor agregado. Tales características posibilitan que un tercero pueda desarrollar códigos maliciosos diseñados para alterar el correcto funcionamiento de este tipo de tecnología. Un atacante podría, por ejemplo, abrir la puerta del refrigerador en la noche, modificar la lectura del estado y cantidad de alimentos, etc.

---

[23] BlackHat: ¿Es la hora de los Smart TV? Disponible en http://blogs.eset-la.com/laboratorio/2013/08/02/blackhat-es-la-hora-de-los-smarttv/.

[24] Here's What It Looks Like When A 'Smart Toilet' Gets Hacked [Video]. Disponible en http://www.forbes.com/sites/kashmirhill/2013/08/15/heres-what-it-looks-like-when-a-smart-toilet-gets-hacked-video/.

[25] Descubren vulnerabilidad en el sistema Philips Hue, ¿es seguro el Internet de las Cosas? Disponible en http://alt1040.com/2013/08/vulnerabilidad-philips-hue.

Cámaras IP

Otro dispositivo "no convencional" que puede convertirse en blanco de los cibercriminales son las cámaras IP. Este tipo de tecnología permite monitorear y ver en tiempo real a través de Internet, lo que está sucediendo en un lugar determinado. Investigadores de Core Security descubrieron diversas vulnerabilidades en una línea de cámaras IP que permitían que un atacante pudiera no solo obtener las filmaciones sin el consentimiento de la víctima, sino también la ejecución de comandos arbitrarios en la interfaz web de administración de estos dispositivos[26]. La vulneración de esta tecnología puede tener un gran impacto si se considera que un tercero podría acceder a filmaciones privadas que muestren los puntos de acceso de un lugar, el horario en que las personas se encuentran fuera de casa, etc.

Cerradura digital

En el mercado también es posible encontrar cerraduras digitales. Estas pueden incluir un registro de las personas que ingresan a un inmueble, facilitar el acceso al contemplar el uso de tarjetas electrónicas, entre otras características. Precisamente, el aumento en la complejidad de estos dispositivos hace posible ataques como la clonación de tarjetas de acceso, la apertura del cerrojo, etc. En esta línea, una investigación presentada en Black Hat 2013 demostró la factibilidad de que un tercero pueda capturar los paquetes que son transmitidos a través de Bluetooth cuando se utilizan algunos sistemas de cerraduras inalámbricas[27].

Google Glass y otros accesorios inteligentes

Uno de los dispositivos que sin dudas revolucionó el mercado durante 2013 fue Google Glass. Se trata de unas gafas que ofrecen la experiencia de la realidad aumentada y la posibilidad de conectarse a Internet a través de comandos por voz. Con respecto a la seguridad de estos dispositivos, un investigador descubrió una vulnerabilidad que posibilita el robo de información a través de una conexión Wi-Fi manipulada especialmente con dicho propósito[28]. Si el usuario utiliza Google Glass y envía información sin cifrar, esta podrá ser obtenida por un tercero.

Asimismo, otro agujero de seguridad, que ya fue solucionado, permitía que un código QR manipulado específicamente, conectara el dispositivo del usuario de modo automático a un Wi-Fi malicioso[29].

Si este dispositivo se masifica y empieza a ser utilizado para acceder al banco, pagar servicios, etc., es altamente probable que aparezcan códigos maliciosos diseñados para robar información. Este aspecto se agrava todavía más si se considera que, por el momento, Google Glass utiliza Android 4.0.4 como sistema operativo y no una versión más actualizada de esa plataforma.

Android en otros dispositivos (consolas, relojes, home appliance, entre otros)

Como se mencionó anteriormente, muchos de los dispositivos no convencionales utilizan Android como sistema operativo. Esto evita que las empresas tengan que desarrollar *software* propietario, por lo tanto, se disminuye el costo de producción de dichos aparatos. Asimismo, al implementarse un sistema operativo conocido, la disponibilidad de aplicaciones es mayor en comparación a una plataforma cuyo desarrollo está centrado para una compañía en particular. Tal característica, que resulta positiva con respecto a la disminución de los costos, la asequibilidad y la estandarización, también puede influir negativamente en la seguridad del usuario. Esto se debe a que el uso del mismo sistema operativo en una amplia gama de dispositivos diferentes, posibilita que un atacante pueda desarrollar códigos maliciosos capaces de funcionar en diversos aparatos tecnológicos.

---

[26] CORE-2013-0303 - D-Link IP Cameras Multiple Vulnerabilities. Disponible en http://seclists.org/fulldisclosure/2013/Apr/253.

[27] BLUETOOTH SMART: THE GOOD, THE BAD, THE UGLY, AND THE FIX! Disponible en http://www.blackhat.com/us-13/archives.html#Ryan.

[28] Google Glass still vulnerable to Wi-Fi attack. Disponible en http://www.computerworld.com/s/article/9240909/Google_Glass_still_vulnerable_to_Wi_Fi_attack

[29] Google Glass susceptible to poison-pill QR code. Disponible en http://www.networkworld.com/news/2013/071813-google-glass-271960.html.

Actualmente, el mercado ofrece relojes, heladeras, automóviles, cámaras fotográficas, teléfonos de línea fija, consolas de videojuegos, e incluso espejos que permiten consultar contenidos en línea. Todos estos dispositivos comparten una característica en común: utilizan Android como sistema operativo[30].

[30] Android Everywhere: 10 Types of Devices That Android Is Making Better. Disponible en http://www.androidauthority.com/android-everywhere-10-types-of-devices-that-android-is-making-better-57012/.

Conclusión: ¿es posible la privacidad en Internet?

A lo largo de este documento, quedó plasmado cómo ha aumentado la preocupación de los usuarios en torno a la privacidad en Internet. Asimismo, se abordó el tema de la evolución de las amenazas informáticas con respecto a la cantidad, complejidad y diversificación de ataques. Hasta este punto, es probable que el lector experimente una sensación de desconfianza con respecto al uso de las tecnologías informáticas, sin embargo, el objetivo fundamental es que los usuarios puedan utilizar Internet y otras herramientas de forma segura, y bajo ningún punto de vista dejar de emplearlas. Por lo mismo, ¿será posible la privacidad en Internet?

Hasta cierto punto sí, puesto que las personas pueden adoptar medidas que vayan encaminadas en pos de la seguridad y privacidad de la información, sin embargo, ningún sistema informático está exento de sufrir ataques. Algo similar ocurre con los automóviles: se puede adquirir la última tecnología de seguridad y también adoptar todos los resguardos necesarios en lo que respecta a una conducción prudente y segura, no obstante, la posibilidad de sufrir un accidente automovilístico continúa siendo una posibilidad.

Asimismo, el tema de la seguridad, en detrimento de la usabilidad, también plantea un desafío al momento de implementar tecnologías de protección y planes de concientización para aumentar el nivel de privacidad y seguridad en Internet. En este sentido, se podría adoptar un método de protección estricto que le pregunte al usuario frente a cualquier acción que pudiera poner en riesgo la integridad de la información, como la ejecución de programas, navegación en Internet, etc. Un sistema de estas características podría resultar altamente efectivo si la persona lee detenidamente cada mensaje y responde de la forma adecuada (sí o no dependiendo de la acción). Sin embargo, la falta de usabilidad y practicidad de un sistema como este probablemente provocaría que la mayoría de los usuarios lo desactivaran.

Algo similar ocurrió con UAC (*User Account Control*) que implementó Microsoft a partir de Windows Vista. Ese sistema de seguridad fue pensado para que todos los programas que ejecuta el usuario lo hagan con privilegios restringidos. Frente a aplicaciones que necesiten permisos administrativos, la persona se verá obligada a tener que permitir o denegar la ejecución del software. Es indiscutible que un sistema como este otorga un nivel de seguridad mayor, no obstante, fue tal la molestia experimentada por los usuarios que Microsoft se vio obligado a modificar UAC en Windows 7 para hacerlo menos "intrusivo"[31]. Si se toma el caso anterior como antecedente, se hace necesario plantear medidas que efectivamente puedan proteger al usuario, pero que al mismo tiempo no provoquen una "molestia" o se tornen invasivas.

Considerando los puntos planteados anteriormente, la primera medida efectiva para resguardar la privacidad de la información tiene que ver con el cifrado de los datos. En este caso, y tal como se abordó en profundidad en la sección "Privacidad", existen programas destinados a cifrar los archivos del usuario. La implementación de este método de protección puede lograrse a través de la instalación de programas destinados a tal propósito; asimismo, la seguridad de este método varía de acuerdo al nivel de robustez del algoritmo de cifrado.

Otra medida que se puede adoptar para mejorar la privacidad en Internet, es el uso de Tor, aplicación diseñada para navegar de forma anónima. Tal como aparece en el sitio del programa: "Tor es un *software* libre y una red abierta que le permite al usuario defenderse del análisis de tráfico, una forma de vigilancia que afecta la libertad personal, la privacidad de los usuarios y las empresas, y la seguridad de los Estados"[32]. En términos sencillos, el cliente de Tor consiste en una versión modificada del navegador Mozilla Firefox con ciertos parámetros y extensiones destinadas a otorgar un mayor nivel de anonimato mientras se navega por Internet. Otras de las funciones que incluye este programa es la posibilidad de navegar a través de la Deep Web[33] (Internet profunda).

En palabras simples, la Deep Web es todo el contenido de Internet que no forma parte de la superficie, es decir, sitios y contenidos que no son indexados por los motores de búsqueda como Google. Parte de la Deep Web la componen los pseudodominios .onion que se utilizan con el objetivo de facilitar el acceso anónimo a páginas que abarcan distintas temáticas como abusos, venta de estupefacientes, foros de cibercriminales y otros tópicos generalmente ilegales o que traspasan la barrera de lo ético y legal. Si bien Tor otorga un nivel de anonimato y privacidad mayor en comparación a un navegador "estándar", tampoco se trata de un sistema infalible. En esta línea, algunos documentos revelados por Edward Snowden afirman que la NSA ha intentado explotar vulnerabilidades encontradas en el cliente de Tor (no en la red),

[31] Aol Tech: User Account Control to be less annoying in Windows 7. Disponible en http://downloadsquad.switched.com/2008/10/09/user-account-control-to-be-less-annoying-in-windows-7/.
[32] Tor. Disponible en https://www.torproject.org/.
[33] Wikipedia: Internet profunda. Disponible en http://es.wikipedia.org/wiki/Internet_profunda.

permitiendo de este modo, revelar la identidad de algunos usuarios de dicha herramienta[34]. Por otro lado, los desarrolladores de Tor alertaron a la comunidad que algunas versiones antiguas del *software*, son vulnerables producto de un agujero de seguridad encontrado en versiones de Mozilla Firefox anteriores a la 17.0.7[35].

En este caso, actualizar Tor a la última versión es la solución a las vulnerabilidades mencionadas anteriormente, sin embargo, es posible que en un futuro se descubran nuevos agujeros de seguridad, por lo tanto, el uso de esta herramienta, como cualquier otra medida de seguridad, debe ser considerada como una forma de aumentar la privacidad pero no como una solución definitiva a esta problemática. Considerando todo lo mencionado en este documento, la privacidad en Internet es posible con algunos atenuantes, es decir, asumir que lo es en un 100% sería un error que atenta particularmente en contra de la seguridad del usuario.

[34] The Guardian: NSA and GCHQ target Tor network that protects anonymity of web users. Disponible en http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption.

[35] Tor security advisory: Old Tor Browser Bundles vulnerable. Disponible en https://blog.torproject.org/blog/tor-security-advisory-old-tor-browser-bundles-vulnerable.

Anexo: gráfico consolidado de la evolución de malware para Android de 2010 a 2013