TENDENCIAS 2016

(IN) SECURITY EVERYWHERE

ENJOY SAFER TECHNOLOGY™

ÍNDICE

1

Introducción

1 INTRODUCCIÓN

Año tras año, desde los Laboratorios de ESET a nivel mundial hacemos un repaso de los sucesos más importantes del año y de su impacto tanto en el mundo corporativo como en la información de los usuarios hogareños. Al conversar, debatir y evaluar qué es lo que sucedió en el mundo de la tecnología, es difícil resumir todo en una sola frase. La velocidad con la que aparecen nuevas tecnologías, los reportes de ataques, nuevas familias de malware o fallas de seguridad de impacto global, hacen de la seguridad un desafío cada vez más importante para los negocios, las empresas, los gobiernos y los usuarios alrededor del mundo.

En los últimos años, hemos debatido sobre cómo la web se convirtió en uno de los principales canales de propagación de códigos maliciosos, el crecimiento y profesionalización del *crimeware*, la importancia de las botnet para el mundo del *cibercrimen* y la masificación del malware para dispositivos móviles. Estas tendencias tuvieron sus impactos en los años pasados, y en nuestro documento de "*Tendencias 2015: el mundo corporativo en la mira*" no solo remarcamos cómo diferentes empresas se volvieron objetivo de los ataques informáticos, sino también desglosamos el informe en temáticas diferentes.

Al marcar la diferencia entre las tendencias, nos dimos cuenta de un cambio más que circunstancial: cada vez hay más dispositivos, más tecnologías y un mayor número de desafíos en cuanto a cómo mantener la seguridad de la información, sea cual sea el ámbito de su implementación.

En "*Tendencias 2013: vertiginoso crecimiento de malware pare móviles*" incorporamos el primer apartado para malware en nuevas tecnologías, antes de que se hablara del Internet de las Cosas (IoT por sus siglas en inglés, *Internet of Things*), haciendo mención a Smart Tv y otros dispositivos inteligentes. Hoy, tres años después de aquel documento, la IoT está más presente que nunca, y en vistas de seguir creciendo no solo en el hogar, sino también en las industrias, las empresas y los gobiernos.

Cuando hablamos de IoT hacemos referencia a dispositivos que ya conocíamos y utilizamos pero con la capacidad de estar conectados a Internet, de generar y compartir información con miles de usuarios. La información que comparten es, ni más ni menos que la de los usuarios, ya sea mediante algo que se use y se lleve todo el día consigo (como un *smartwatch*), o mediante un electrodoméstico del hogar o de un sensor que recopila información en un lugar público.

Este nuevo desafío por asegurar la información que circula a partir de estos nuevos dispositivos tecnológicos, se suma a todas las otras áreas que ya están presentes desde hace años, extendiendo significativamente el nivel de protección y capacitación necesarias por parte de los equipos de IT.

2015 fue un año en donde el sector corporativo fue objetivo de diferentes incidentes de seguridad, en el que publicaciones de vulnerabilidades afectaron a millones de dispositivos móviles, además de que existieron reportes de ataques dirigidos, y en el que surgieron vulnerabilidades que afectaron a muchos dispositivos de IoT, desde autos hasta rifles de precisión. En este presente informe, repasaremos los

sucesos más importantes en materia de seguridad que han tenido lugar durante el último tiempo y en base a todo lo sucedido, plantearemos cuáles serán las tendencias y los desafíos para la seguridad de la información, ya sea dentro del ámbito empresarial como en los hogares.

A lo largo de las diferentes secciones de este artículo, repasaremos estado del *crimeware* y su impacto en empresas y usuarios, y revisaremos los ataques dirigidos y campañas de APTs que se presentaron en diferentes lugares del mundo. También daremos cuenta de los riesgos que enfrentan las víctimas del ransomware para recuperar su información, y cómo pueden protegerse de estas extorsiones. En definitiva, se hará un repaso de cada una de las temáticas más importantes del mundo de la seguridad, explicando por qué los cibercriminales atacan a cada vez más plataformas y tecnologías, y por qué en definitiva, la seguridad ya no es una problemática de unos pocos sino que abarca a cada vez más personas y por qué es necesario que progresivamente sea más parte de nuestras vidas.

Es un placer para nosotros presentarles el documento de los Laboratorios de ESET para saber qué sucederá y cuáles son los desafíos de cara al año próximo en materia de seguridad informática, ***"Tendencias 2016: (In) Security Everywhere".***

> CADA VEZ HAY MÁS DISPOSITIVOS, MÁS TECNOLOGÍAS Y UN MAYOR NÚMERO DE DESAFÍOS EN CUANTO A CÓMO MANTENER LA SEGURIDAD DE LA INFORMACIÓN.

2

Internet de las Cosas:
la seguridad del todo

- Wearables
- Interconectando el hogar
- Interconectvidad del todo
- Asegurar, después conectar

Autor
Pablo Ramos
Head of LATAM Research Lab

2 INTERNET DE LAS COSAS: LA SEGURIDAD DEL TODO

La Internet de las Cosas (IoT, por sus siglas en inglés de *Internet of Things*) es un tema que se popularizó hace ya algunos años, y que desde el primer momento generó polémica y debate, sobre todo dentro de la comunidad de la Seguridad Informática, puesto que su aparición supuso (y supone) grandes y novedosos desafíos.

Hace dos años, precisamente en el informe *Tendencias 2013: vertiginoso crecimiento de malware para móviles*, el laboratorio de investigación de ESET Latinoamérica ya hacía referencia a amenazas para dispositivos inteligentes basados en investigaciones, reportes y detecciones de 2012. Hoy, tres años más tarde, el avance de la tecnología continúa expandiendo los límites y capacidades de dispositivos de este tipo; hay cada vez más aparatos que se conectan a Internet y son más accesibles, por lo que la superficie de ataques creció, algo que se evidenció en casos de campañas maliciosas que lograron comprometer a millones de usuarios en todo el mundo. Como uno de los casos más relevantes, podemos mencionar a **Moose, un gusano que infectó a miles de routers en todo el mundo.**

Según un informe de la consultora Gartner, actualmente **existen 4.9 mil millones de dispositivos conectados a Internet y su número crecerá en 5 años hasta llegar a los 25 mil millones de dispositivos conectados a Internet para el 2020.** En pocas palabras, la IoT está aquí quedarse y durante los próximos años se incrementará la cantidad de dispositivos que generan, almacenan e intercambian datos con los usuarios para mejorar su experiencia y simplificar muchas de las tareas que realizan. (Tabla 1)

En pos de las proyecciones que presentó Gartner, es posible ver que el segmento del usuario (*consumer*) es el que más crecerá en los próximos cinco años. Ya sea por la aparición de nuevos *wearables* (dispositivos que se usan como accesorios en el cuerpo) como también de nuevos electrodomésticos para el hogar, es importante remarcar que habrá que protegerlos para evitar incidentes de seguridad.

Sin embargo, **la IoT no es solo para los usuarios; empresas y gobiernos están invirtiendo e incursionando en esta industria con el fin de mejorar la vida de la población.** Este proceso se conoce como la **Industria 4.0**; e incluso hay quienes creen que es el "cuarto paso de la revolución industrial", como el **Ministerio Federal de Educación e Investigación**

Tabla 1 Unidades de equipos de la IoT por categoría (en millones)

Categoría	2013	2014	2015	2020
Automotores	96.0	189.6	372.3	3,511.1
Usuarios	1,842.1	2,244.5	2.874.9	13,172.5
Negocios genéricos	395.2	479.4	623.9	5,158.6
Servicios (Vertical Business)	698.7	836.5	1,009.4	3,164.4
Total	**3,032.0**	**3,750.0**	**4,880.6**	**25,006.6**

Fuente: Gartner (Noviembre 2014)

de Alemania. Esto implica la creación de productos inteligentes a través de procesos y procedimientos inteligentes. De forma más sencilla: convertir la industria actual en una inteligente o "*Smart*", es decir, que se base principalmente en la IoT y los servicios. Algunas de las áreas afectadas más importantes son los proveedores de energía, la movilidad sustentable y el cuidado de la salud, entre otras.

En lo que refiere a la a Industria 4.0, existen algunas barreras que todavía mantienen reticentes a varias empresas. Como se puede ver en el siguiente gráfico, la protección y seguridad de los datos es uno de los mayores obstáculos a superar para profundizar el cambio y la aceptación de nuevos dispositivos para bienes y servicios dentro de esta nueva revolución industrial. (Gráfico 1)

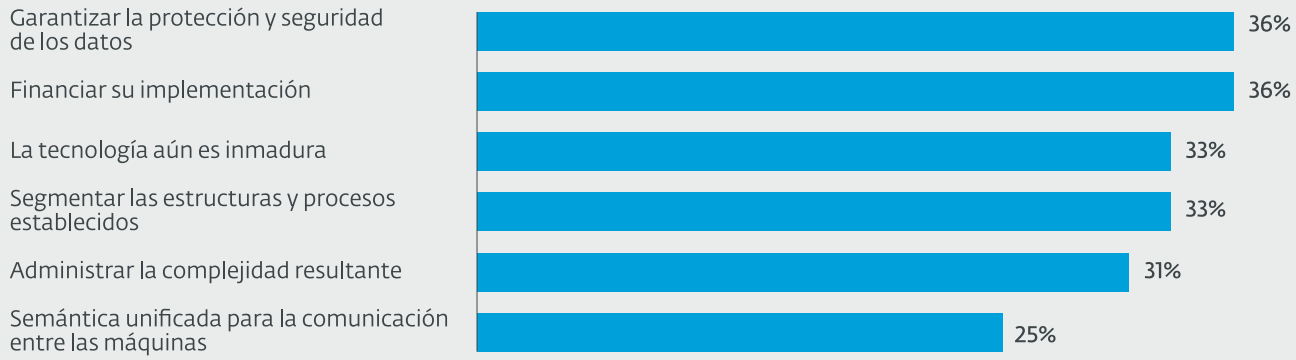
Cada vez que surge una nueva tecnología, los investigadores la ponen a prueba para entender cómo funciona y, en algunos casos, observar cómo se puede vulnerar su seguridad. A lo largo de 2015, se han visto múltiples reportes de vulnerabilidades en dispositivos de IoT, desde monitores para bebés, hasta el control remoto de un auto a través de Internet. Tanto **usuarios como empresas se están preocupando y ocupando de la seguridad de IoT,** y en vistas a 2016, la seguridad de estos dispositivos será uno de los mayores desafíos para los equipos de Seguridad Informática.

Wearables

Durante 2015 se realizaron muchos reportes sobre vulnerabilidades en los *wearables*, en donde se desarrollaban casos que permitirían a un atacante **robar y filtrar información desde el mismo dispositivo.** Entre los vectores de ataques utilizados, se han encontrado fallas en las aplicaciones y en el uso de las tecnologías de comunicación, como en el caso de **Bluetooth y los códigos pin de seis dígitos.**

Bluetooth Smart está ampliamente aceptado en la industria de IoT y, por lo tanto, su seguridad es un factor clave para la interconexión de los dispositivos. Desde

Gráfico 1 Barreras para la implementación de la Industria 4.0



Fuente: IDC 2014 – Solo empresas que están familiarizadas con el concepto de "Industria 4.0"

los relojes inteligentes hasta las pulseras que miden indicadores físicos durante actividades deportivas, utilizan esta tecnología para comunicarse con otros equipos, como los *Smartphones*. Cualquier falla de seguridad en el protocolo permitiría a los atacantes leer en texto plano la información que se intercambia entre ellos.

Algunos de estos sucesos llamaron la atención de los usuarios, en particular con la salida al mercado del **Apple Watch.** En este sentido, se vieron desde fallas de software hasta la posibilidad de que un **cibercriminal pudiera reinicializar un Apple Watch** y volver a conectarlo a otro iPhone sin ningún inconveniente, independientemente de que se haya establecido un pin de seguridad.

Interconectando el hogar

Los avances en IoT permitieron que cada vez más dispositivos se puedan interconectar entre ellos y con una misma red en el hogar. De esta manera, los usuarios pueden utilizar sus *Smartphones* y computadoras para gestionar y comunicarse con otros aparatos del hogar conectados a las redes, lo que mejora la experiencia con la tecnología y la usabilidad de los equipos. Por otro lado, ante una mayor interconexión se deberá incluir una mejor seguridad en la privacidad de los datos, protocolos de comunicación y actualizaciones de los aplicativos y sistemas operativos.

En septiembre de 2014, durante la **conferencia Virus Bulletin en la ciudad de Seattle, Jeong Wook Oh de HP,** presentó una investigación completa sobre diferentes dispositivos existentes en los hogares y la viabilidad de que sean comprometidos por un atacante. Actualmente, en los hogares se pueden encontrar televisores, termostatos, cámaras IP y otros dispositivos que se pueden conectar a Internet y ante una falla de seguridad la información personal de los miembros del hogar, o sus sistemas pueden quedar expuestos.

Esta investigación también contó con casos de diferentes dispositivos de los hogares, y en base a lo que se reportó durante los últimos años, es posible identificar esta tendencia en IoT.

En esta misma línea, SmartTVs de diferentes fabricantes fueron objeto de estudio por parte de los investigadores desde la conferencia **BlackHat 2013,** y en la actualidad se continúan realizando informes sobre fallas en este tipo de dispositivos. En reportes recientes, puede observarse cómo una **heladera puede convertirse en la puerta de entrada para que cibercriminales roben credenciales de Google.** Más aun, cómo un **monitor para bebes puede ser controlado remotamente para reproducir música** o, incluso, acceder a la red a la cual esté conectado.

Ante la rápida evolución de la tecnología, es de esperarse a que surjan fallas en la seguridad de los dispositivos, o que su implementación dentro de una red hogareña no sea la más óptima. Sin embargo, no es algo a lo que se deba temer; por el contrario, es importante tomar conciencia e informarse al respecto.

En la actualidad, las redes hogareñas cuentan con más dispositivos conectados que hace cinco o diez años, y en base a ello, todas las compañías enfocadas en la Seguridad de la Información comprenden el desafío que esto genera, es-

→
No es algo a lo que se deba temer; por el contrario, es importante tomar conciencia e informarse al respecto.

pecialmente para lograr ayudar a todos los usuario a proteger las redes de sus hogares de una manera sencilla y segura. Ya sea a través de **consejos, guías o manuales** los usuarios deberán repasar la seguridad de sus dispositivos cada vez más inteligentes.

Interconectvidad del todo

De cara al futuro inmediato, el desafío de la seguridad en IoT no se orienta únicamente al hogar. La tecnología sigue avanzando y continuamente se puede ver cómo los gobiernos, las industrias y los mercados en general se encuentran virando más hacia la interconectividad de todos los equipos, sistemas y servicios. Desde investigaciones de mercado hasta sistemas de tráfico, todo se está interconectando a través de tecnologías ya conocidas y, en ciertas ocasiones, sin la correcta implementación de los protocolos de seguridad.

En el informe *"Tendencias 2015: el mundo corporativo en la mira"* del Laboratorio de Investigación de ESET Latinoamérica, se menciona que uno de los objetivos de IoT es la generación de ambientes autónomos que provean de información y servicios a través de la interacción con la tecnología. Para llevar adelante este objetivo, diferentes empresas comenzaron a adoptar programas de recompensas a los especialistas de seguridad para que reporten fallan de seguridad, como un camino para proveer a sus clientes una mayor y mejor seguridad, privacidad y usabilidad de los dispositivos.

Los desafíos de IoT fueron tema de discusión durante todo el año 2015, por lo que a través de diferentes comunicados, las organizaciones han comenzado a trabajar en reglas y normativas para incorporar la Internet de las Cosas a las industrias, ciudades y diferentes sectores con el objetivo de mejorar el estilo de vida de sus habitantes.

Algunos ejemplos de esto son las intenciones de inversión del Gobierno alemán y la ya mencionada Industria 4.0, y también la colaboración de la **Agencia Europea de Seguridad de la Información y las Redes (ENISA)** para ayudar al desarrollo de las buenas prácticas en **las infraestructuras críticas inteligentes emergentes.**

Asegurar, después conectar

2016 será un año con desafíos de seguridad para los nuevos dispositivos que se conecten a la red o que permitan diferentes maneras de comunicarse entre sí. Ya sea un **auto que se pueda controlar de manera remota** y fallas de seguridad en los drones, hasta las formas en las que los usuarios protegen sus redes hogareñas. Cualquier dispositivo que esté conectado deberá ser revisado para garantizar su protección y correcta configuración para asegurar la privacidad, seguridad y confidencialidad de usuarios, empresas y gobiernos de cara al futuro.

Existen diferencias entre cómo los usuarios y las empresas protegerán su información en todos aquellos dispositivos en los que no se pueda instalar una solución de seguridad, y haciendo de la red en sí un factor crítico a proteger. En el caso de una red hogareña, uno de los puntos más importantes a tener en cuenta es el router, el dispositivo que brinda acceso a Internet, y que muchas veces se lo deja

de lado, no se lo actualiza e, incluso, no se le cambian las contraseñas que tiene por defecto.

Si el dispositivo que brinda acceso a Internet en un hogar, que está conectado las 24 horas del día, no es seguro, esto puede llevar a que la red se vea comprometida, como se reportó desde el Laboratorio de ESET con el caso de **Linux/Moose** que modificaba el comportamiento de las redes afectadas. En contraparte, en el mundo corporativo la incorporación de nuevos dispositivos inteligentes conectados a la red deberá ser un punto a contemplar por los equipos de IT para garantizar que no sean la puerta a terceros no autorizados que puedan generar incidentes y brechas de seguridad.

En el panorama actual de la seguridad, hemos debatido y presentado los incidentes de mayor impacto a nivel mundial que van desde ataques dirigidos hasta casos masivos de infección por códigos maliciosos. Si tomamos en cuenta los incidentes que vemos suceder y las fallas de seguridad que suelen explotar los atacantes, podemos llegar a la conclusión que, si se agrega una nueva gama de dispositivos inteligentes conectados a una red corporativa, el rol que tomará la seguridad será aún más importante y relevante de lo que ya es ahora.

Asegurar cualquier dispositivo que se conecte en un entorno corporativo es una tarea más que difícil para los equipos de seguridad y de cara al futuro próximo, y con el rol de la IoT, su relevancia será cada vez mayor para aquellas empresas que vean la seguridad de la información como un rol clave para la continuidad del negocio.

> LAS ORGANIZACIONES HAN COMENZADO A TRABAJAR EN REGLAS Y NORMATIVAS PARA INCORPORAR LA INTERNET DE LAS COSAS A LAS INDUSTRIAS, CIUDADES Y DIFERENTES SECTORES CON EL OBJETIVO DE MEJORAR EL ESTILO DE VIDA DE SUS HABITANTES.

3

Ransomware:
primero los archivos... ahora los dispositivos completos

- La variedad de estilos del ransomware
- El aumento en la cantidad de variantes
- La evolución de las amenazas
- De la computadora al televisor
- Conclusión: el mismo objetivo para otra amenaza

Autor
Camilo Gutiérrez Amaya
Sr. Security Researcher

3 RANSOMWARE: PRIMERO LOS ARCHIVOS... AHORA LOS DISPOSITIVOS COMPLETOS

Dentro de la Seguridad Informática, una de las principales amenazas son los códigos maliciosos. De hecho, a lo largo de los años se ha posicionado como uno de los principales causantes de incidentes de seguridad; al principio con los virus, hasta llegar a amenazas sofisticadas como el ransomware. Y precisamente este tipo de malware que, si bien no es nuevo, es el que más dolores de cabeza ha causado en los últimos años tanto para empresas como para usuarios hogareños.

La variedad de estilos del ransomware

En el último año, los casos de ransomware han cobrado relevancia en el campo de la Seguridad Informática debido a su crecimiento en la cantidad de víctimas, un hecho que se debe a los importantes niveles de ganancias que los cibercriminales obtienen de este tipo de campañas maliciosas.

Este formato de ataque puede parecer algo novedoso, pero como se dijo anteriormente, no lo es. De hecho, el primer caso de ransomware **se remonta 25 años atrás;** se trataba de un malware que ocultaba los directorios y cifraba los nombres de todos los archivos de la unidad C, haciendo inutilizable el sistema. Luego, se le solicitaba al usuario "renovar su licencia" con un pago de 189 dólares. Desde ese momento se han identificado nuevas versiones de programas que buscaban extorsionar a los usuarios, que a diferencia del cifrado simétrico de ***PC Cyborg,*** utilizaban algoritmos de cifrado asimétrico con claves cada vez de mayor tamaño. Por ejemplo, en 2005 se conoció ***GPCoder,*** y sus posteriores variantes, que luego de cifrar archivos con extensiones específicas solicitaba un pago de entre 100 y 200 dólares como rescate de la información.

Pero este tipo de códigos maliciosos va más allá, y de hecho hay grupos cibercriminales que lo ofrecen como un servicio. El *Ransomware as a Service (RaaS)* se ha descubierto a través de una herramienta denominada ***Tox,*** la que permite crear este tipo de malware de manera automática, independientemente de los conocimientos técnicos de quien la utiliza. De la misma manera, con la reciente noticia de la publicación de **Hidden Tear, el primer ransomware de código abierto,** se abre una nueva ventana para el desarrollo de este programa malicioso y sus variantes, donde es posible pronosticar la creación de malware cada vez más sofisticado y masivo.

El aumento en la cantidad de variantes

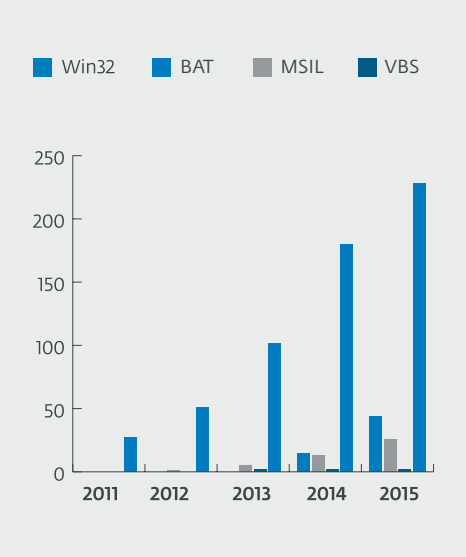
Una de las características salientes del ransomware es el crecimiento en la cantidad de variantes vistas en los últimos años para diferentes tipos de plataformas y tecnologías. En el siguiente gráfico se puede observar, como era de esperarse, que las familias relacionadas con Windows son las que más se han visto con un crecimiento año a año en la cantidad de detecciones. (Gráfico 2)

Pero además de Windows, también se han diseñado variantes para otros sistemas operativos. Tal es el caso de OS X, ya que durante 2015 se detectaron variantes de familias de filecoders exclusivas para estos sistemas.

→ **Este tipo de malware es el que más dolores de cabeza ha causado en los últimos años tanto para empresas como para usuarios hogareños.**

Gráfico 2

Crecimiento de variantes detectadas de la familia Filecoder en los últimos 5 años



Otras tecnologías como *VBS*, *Python*, *BAT* y *PowerShell* también son algunas de las utilizadas por los cibercriminales para infectar usuarios y obtener ganancias económicas.

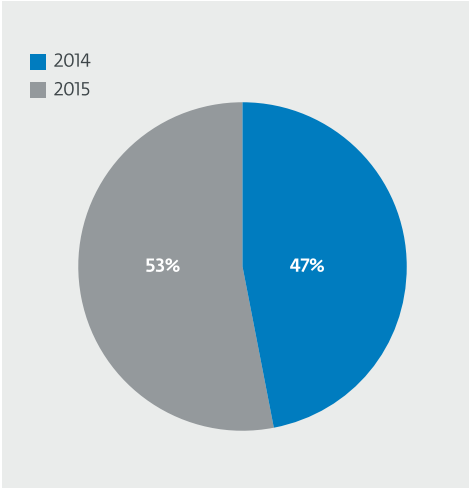
La evolución de las amenazas

Si bien hasta ahora se habló de sistemas operativos para equipos de escritorio o laptops, estas no son las únicas plataformas que están expuestas a esta amenaza. También se encontraron casos de ransomware para afectar dispositivos móviles, particularmente para Android, ya que es el sistema operativo móvil con mayor cantidad de usuarios en el mundo.

Tras el descubrimiento de las primeras familias, que incluían antivirus falsos con la capacidad de bloquear las pantallas de los dispositivos, en 2014 fue descubierto **Simplocker, el primer ransomware para Android activado en Tor que directamente cifra los archivos del usuario.** De hecho, la cantidad de familias que se fueron detectando desde 2014 ha crecido durante 2015.

Gráfico 3

Distribución de la cantidad de variantes detectadas de Simplocker en los últimos dos años



Durante 2015, investigadores de ESET descubrieron el **primer tipo de ransomware de bloqueo de pantalla para Android** que modifica el código de desbloqueo del teléfono para impedir el acceso. Esto es una diferencia considerable con respecto a los primeros troyanos de bloqueo de pantalla para Android, que lo que hacían era poner constantemente en un primer plano la ventana de pedido de rescate en un bucle infinito.

Como este mecanismo no contaba con una gran complejidad técnica, era fácilmente descartable por parte de los usuarios con cierta información, por lo tanto los cibercriminales redoblaron sus esfuerzos y crearon nuevas familias de ransomware que bloquean el acceso al dispositivo. Estas nuevas familias, detectadas por ESET como *Lockerpin*, impiden que los usuarios

tengan una forma efectiva de recuperar el acceso a sus dispositivos sin los privilegios de raíz o sin una solución de administración de seguridad instalada.

Sin embargo, Android no es la única plataforma en la que el ransomware ha evolucionado. En 2013 se conoció la relevancia de **CryptoLocker** debido a la cantidad de infecciones generadas en distintos países. Entre sus principales características se encuentra el cifrado a través de algoritmos de clave pública RSA de 2048 bits, enfocado únicamente en algunos tipos de extensiones de archivos, así como en comunicaciones con el Centro de Comando y Control (C&C) a través de la red anónima Tor.

Durante 2015 se identificó una nueva oleada de ransomware con la aparición de **CTB-Locker,** con la particularidad de que podía ser descargado al equipo de la víctima utilizando un *TrojanDownloader,* es decir, un troyano que secretamente descargaba esta amenaza. Entre sus distintas versiones, **una estaba enfocada a los países hispanoparlantes,** con mensajes e instrucciones para realizar los pagos escritos en español. Estos hechos llevan a pensar que el ransomware aún no ha encontrado un límite en cuanto a la cantidad de víctimas que podría alcanzar y a la complejidad que podría obtener su código y formatos de ataque. No obstante, sí parece que esta familia de códigos reapareció para quedarse y seguramente seguirá mutando en los próximos años.

De la computadora al televisor

Hasta ahora, es evidente la evolución de esta amenaza en cuanto a una mayor cantidad variantes, con mecanismos cada vez más complejos y que hacen casi imposible recuperar la información, a menos de que se realice el pago al cibercriminal -una práctica no recomendable- o se tenga algún tipo de respaldo.

De la misma manera, su diversificación también ha ido en aumento. En los últimos meses de 2015 se ha registrado un importante crecimiento de ransomware que se enfoca en equipos asociados a la Internet de las Cosas (IoT, por sus siglas en inglés de *Internet of Things*). Distintos dispositivos, como relojes o televisores inteligentes, son susceptibles de ser afectados por software malicioso de este tipo, principalmente aquellos que operan en Android.

Pero la IoT abarca más que relojes y televisores; desde automóviles hasta refrigeradores ya tienen la capacidad de conectarse a Internet y basar toda su operatividad en una CPU. Si bien aún no se han encontrado amenazas para estos aparatos, al existir un componente de software y una conexión a Internet, es viable que los atacantes se sientan atraídos para comprometerlos y obtener algún tipo de información valiosa de ellos.

Ya se han realizado pruebas de concepto en las que, por ejemplo, se toma con éxito el control total de un automóvil de forma remota. Por este motivo, de no tomarse las medidas de precaución necesarias por parte de fabricantes y usuarios, nada impediría que un atacante lograra secuestrar las funciones de un dispositivo y exigiera dinero para devolver su control. Tal vez no sea una amenaza que se masifique en los años venideros, pero es necesario no perderla de vista para no tener problemas serios más adelante.

→
En los últimos meses de 2015 se ha registrado un importante crecimiento de ransomware que se enfoca en equipos asociados a la Internet de las Cosas

Conclusión: el mismo objetivo para otra amenaza

Durante los últimos años, el secuestro de la información de usuarios y empresas en diferentes plataformas fue una de las tendencias más destacadas. El impacto que puede tener para un usuario, al no poder acceder a toda su información por haberse infectado por un código malicioso, es una preocupación y uno de los incidentes de seguridad más importantes ya que deja al descubierto la falta de copias de seguridad o la vulnerabilidad del negocio de una compañía.

Lamentablemente, el éxito de este tipo de ataques para los cibercriminales, los ha llevado a extenderse no solo a los sistemas con Windows o dispositivos móviles, sino que también ha generado un impacto más que considerable y es una de las mayores preocupaciones de los usuarios y empresas. Durante 2015, hemos visto campañas de ransomware de gran tamaño y en múltiples lenguajes, como el caso de **CTB-Locker en enero de 2015,** el cual no puede ser tomado como un hecho aislado. Los cibercriminales buscan convencer a los usuarios de abrir sus amenazas, cifrando sus archivos y secuestrando su información, y es algo que probablemente continúe sucediendo.

Acompañando la evolución de la tecnología, las protecciones contra amenazas como el ransomware han mejorado en base a la experiencia, y deben ser acompañadas por la gestión y la educación de los usuarios. Sin embargo, no todos los dispositivos se pueden proteger con una solución de seguridad, y esto lo convierte en un riesgo de cara al futuro para usuarios y empresas. Basados en estos puntos, y de cara a 2016, continuaremos viendo campañas de ransomware, intentando incorporar nuevas superficies de ataque que prohíban a los usuarios acceder a su información o servicios. La creciente tendencia de que cada vez más dispositivos cuenten con una conexión a Internet le brinda a los cibercriminales una mayor variedad de dispositivos a atacar.

Desde el lado de la seguridad, el desafío se encuentra en cómo garantizar la disponibilidad de la información, además de la detección y eliminación de este tipo de ataques. En el futuro próximo, la seguridad de las redes, el bloqueo de exploits y la correcta configuración de los dispositivos tomará una mayor importancia para prevenir este tipo de ataques, para así permitirle a los usuarios disfrutar de la tecnología: estamos en **camino a quintuplicar la cantidad de dispositivos conectados a Internet en cinco años, llegando a los 25 mil millones en línea,** por lo que el desafío es protegerlos correctamente ante este tipo de ataques.

> EL DESAFÍO SE ENCUENTRA EN CÓMO GARANTIZAR LA DISPONIBILIDAD DE LA INFORMACIÓN

→

Durante 2015, hemos visto campañas de ransomware de gran tamaño y en múltiples lenguajes

4

Ataques dirigidos, implicaciones, razones y objetivos

- ¿Kits para el ciberespionaje?
- Ataques a usuarios y sistemas específicos
- ¿Son las APT las armas del futuro?

Autor
Pablo Ramos
Head of LATAM Research Lab

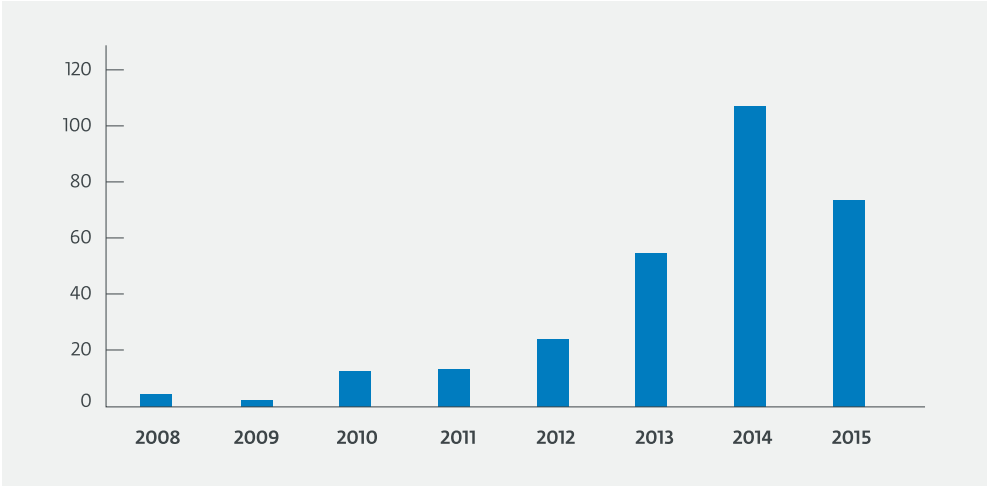
4 ATAQUES DIRIGIDOS, IMPLICACIONES, RAZONES Y OBJETIVOS

Desde hace unos años se vienen reportando una serie de ataques con el término **APT (por sus siglas en inglés de *Advanced Persistent Threats*),** y cada vez que aparece un informe con esta terminología, significa que no estamos hablando de campañas comunes y corrientes de códigos maliciosos en las que se apunta a lograr infecciones lo más masivas posible, sino que se trata de algún objetivo más específico. En el informe de ***"Tendencias 2015: el mundo corporativo en la mira",*** se relevó el impacto que las APT tienen para la seguridad de las empresas y cómo se convirtió en uno de los mayores desafíos a los que una organización se puede enfrentar en términos de Seguridad de la Información.

Este 2015 continuó con la tendencia, y los reportes de ataques dirigidos, APTs y *"sponsored malware"* (esto es, campañas en donde hay un gobierno o entidad detrás del ataque) fueron temas que generaron debate en diferentes lugares alrededor del mundo cuando aparecía un nuevo informe. **APTNotes,** un repositorio de **GitHub** creado y mantenido por la comunidad, recopila los informes sobre los ataques dirigidos publicados desde el 2008. En base a la última actualización en agosto del 2015, se han reportado 291 campañas dirigidas contra alguna empresa, institución o gobierno, siendo 73 de ellas correspondientes a 2015, más del doble que en el mismo período del año anterior, y en una cantidad similar al último semestre del 2014. (Gráfico 4)

Más allá del crecimiento en los reportes de APTs o ataques dirigidos, 2015 tuvo su impacto en determinados ataques que generaron controversia en base a la información que se filtró. Uno de los casos más relevantes dentro de este ámbito fue el de ***Hacking Team*, cuando aproximadamente 400GB de información fueron filtrados desde sus servidores,** generando un gran revuelo respecto al listado de clientes y herramientas que la empresa comercializaba. Las consecuencias de este hecho continuaron llamando la atención con la incorporación por

Gráfico 4 Cantidad de reportes de APTs



Fuente: https://github.com/kbandla/APTnotes

parte de diferentes grupos cibercriminales de varios exploits de Hacking Team filtrados, como fue el caso del **grupo de *APT Sednit*, quienes incorporaron estos exploits a su arsenal en muy poco tiempo,** así como también lo hizo el ***grupo Webky.***

Además de este incidente, **el caso de Ashley Madison** y la filtración de **los datos de 37 millones de sus usuarios** también generaron un gran impacto que trajo consigo muchas consecuencias para los clientes de este servicio. La estrategia de ***Impact Team,*** quienes perpetraron este ataque, fue extorsionar a la empresa para que diera de baja sus servicios y ante la falta de respuesta a sus exigencias, **publicó todos los datos de los usuarios en la web,** dando inicio a una serie de **campañas extorsivas y de propagación de amenazas a las víctimas.**

Las campañas de ataques dirigidos tienen diversos objetivos, que varían según los actores que estén detrás de cada incidente. Desde los Laboratorios de ESET se reportaron casos de escala global, dirigidos contra determinados países, regiones u organizaciones. Entre los sucesos más importantes de 2015 aparecen sucesos como ***Potao Express, Animal Farm, Terracota VPN,*** *Mumblehard* y ***Carbanak*** entre otras.

¿Kits para el ciberespionaje?

El primer caso que se mencionó fue ***Operación Potao Express,*** una campaña de malware específica con múltiples herramientas para ciberespionaje. Los objetivos de Potao se centraron principalmente en Ucrania, pero también incluyeron a otros países de la CEI, incluyendo a Rusia, Georgia y Bielorrusia. Entre sus objetivos se podían encontrar a diferentes secciones del gobierno ucraniano, entidades militares de ese país e incluso agencias de noticias.

Esta familia de códigos maliciosos, conocida con *Win32/Potao,* cuenta con una estructura modular que permite a los atacantes elegir diferentes herramientas según la acción que decidan realizar en base a su objetivo. Las diferentes campañas de Potao se remontan a 2011, cuando fue visto por primera vez, pero tomó más repercusión durante 2014 y continuó con campañas a lo largo de 2015. El incremento de sus detecciones está relacionado con la incorporación de infecciones a través de unidades USB, funcionalidad que se observó por primera vez en octubre de 2013.

Continuando con reportes de amenazas o campañas dirigidas, también puede nombrarse lo ocurrido con el grupo denominado *Animal Farm,* a quienes se les atribuyó la creación de familias de malware conocidas como ***Dino, Casper, Bunny*** y ***Babar.*** Cada una de estas familias de códigos maliciosos fue reportada a lo largo de 2015 e identificadas en campañas dirigidas que **se remontan a abril de 2014, tal como lo indicó Joan Calvet, uno de los investigadores del Laboratorio de Investigación de ESET.** En algunos casos en particular, como el de Babar, los informes al respecto se remontan hasta 2009, lo que claramente demuestra lo persistente de este tipo de ataques y/o campañas dirigidas.

El conjunto de las cuatro familias de códigos maliciosas se relacionó en base a los hallazgos reportados en abril de 2015, sobre las relaciones en el código ***Babar*** y ***Bunny*** que luego se complementaron con *Casper* y *Dino*, develando lo que podría ser una operación que tuvo **como objetivos sistemas en Irán y Siria.**

→
Las campañas de ataques dirigidos tienen diversos objetivos, que varían según los actores que estén detrás de cada incidente.

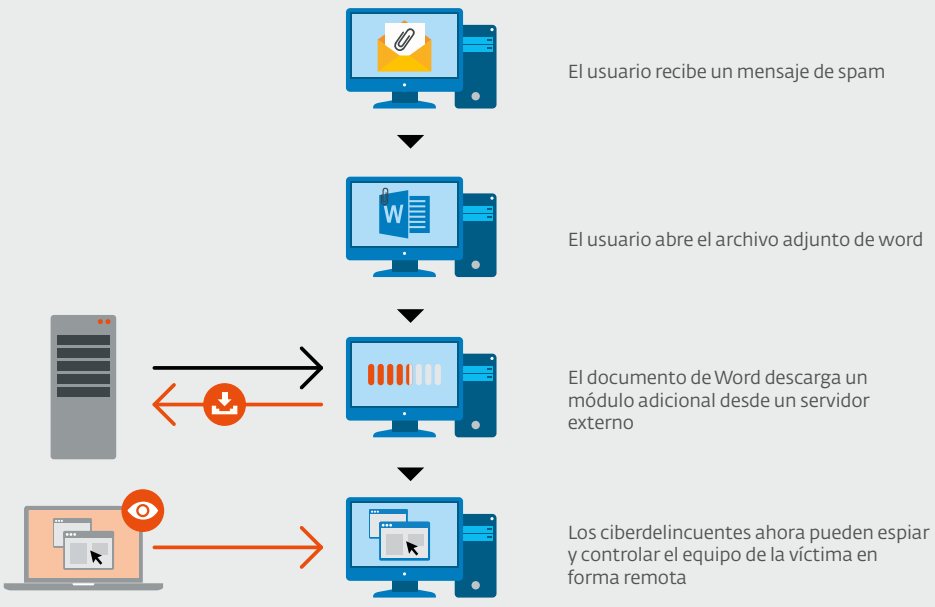
Ataques a usuarios y sistemas específicos

Otra de las investigaciones que causó un gran impacto fue ***Operation Buhtrap,*** cuyo objetivo fueron diferentes bancos de Rusia. En esta campaña, que fue descubierta a finales de 2014, los atacantes solo instalaban sus amenazas en aquellos sistemas que tuvieran definido al ruso como su lenguaje determinado. En este caso, los atacantes utilizaron como un vector de infección la explotación de una **vulnerabilidad en Microsoft Word** con más de tres años de antigüedad. En base al análisis de las detecciones de familias de malware asociadas a estas campañas, se puede observar que el 88% de las víctimas están en Rusia. Si bien el modo de operar era en parte similar a campañas más globales de malware, como el caso de la ***Operación Liberpy,*** los objetivos eran específicos. (Gráfico 5)

Durante los primeros días de noviembre de 2015 se volvieron a detectar campañas de propagación de las amenazas utilizadas en **Operación Buhtrap a través de un conocido sitio web.** En este último caso, el enfoque fue más general pero igualmente orientado a usuarios rusos, a través de técnicas de *spear phishing*. El primer malware que se detectó fue el **downloader Lurk,** distribuido el 26 de octubre. Luego aparecieron **Corebot** el 29 de octubre, Buhtrap el 30 y, finalmente, **Ranbyus** y el **RAT Netwire** el 2 de noviembre.

Hasta este punto, todas las campañas presentadas en esta sección, ya sean APTs o ataques dirigidos, se orientaron particularmente a sistemas basados en Windows y con la finalidad de robar información confidencial del usuario, espiar sus actividades o recolectar información. Sin embargo, esto no fue todo lo que pasó en 2015, ya que diferentes ha-

Gráfico 5 Estructura de una campaña de Buhtrap



llazgos e investigaciones han permitido identificar campañas con más de cinco años de antigüedad, cuyo **objetivo eran servidores basados en Unix, con la finalidad de enviar spam.** Bajo esta premisa se encontró ***Linux/Mumblehard,*** el código malicioso desarrollado en Perl y que contaba con dos componentes principales: el primero es un backdoor que otorga a los atacantes un acceso remoto, mientras que el segundo es un daemon encargado del envío de spam.

Cuando los investigadores de ESET analizaron su tamaño, llegaron a observar que al *sinkhole* se conectaron desde 8500 direcciones de IP únicas, y que a principios de abril de 2015 su tamaño era de aproximadamente tres mil equipos, principalmente servidores. En este sentido, en el informe de tendencias para 2015 ya se había hablado acerca de ***Operación Windigo*** y los más de 500 mil equipos afectados durante las campañas de propagación a lo largo de todo el mundo.

Campañas específicas contra servidores web u otros servicios que estén disponibles en la web, son parte de los objetivos de los cibercriminales para darle fuerza a sus ataques y muchas veces, para pasar desapercibidos y lograr así mantener sus actividades durante el período más extenso posible.

Además de los ataques descriptos en estas páginas, múltiples reportes de ataques dirigidos, en los que empresas, instituciones o gobiernos vieron su información comprometida, han llegado a las noticias más de una vez durante todo 2015, para combatir este tipo de sucesos, las empresas tiene que mejorar sus defensas y procesos de seguridad informática.

¿Son las APT las armas del futuro?

Cada vez que se habla de ataques dirigidos o campañas de malware específicas para un fin, siempre se disparan las alertas de las empresas, ya que quieren saber si han sido víctimas u objetivos de los ataques reportados. Es muy difícil de predecir cuándo o cómo una empresa se convertirá en el objetivo de un grupo de cibercriminales, y es en base a ello que siempre se deben preparar y proteger para ese momento, dado que el objetivo de los equipos de seguridad es proteger a las empresas de cualquier tipo de ataque, sea dirigido o no.

La seguridad de una empresa es un factor clave para su funcionamiento, y es algo cada vez más importante para el negocio, tal como quedó evidenciado en esta sección a partir del impacto que las filtraciones de datos han tenido sobre algunas empresas. Por tal motivo, el mejor enfoque que puede adoptar una empresa, organismo o gobierno de cara a la Seguridad Informática es la proactividad: evaluar sus defensas, capacitar a sus usuarios y entrenar a sus equipos son algunas de las medidas que se deben tomar para minimizar la exposición al riesgo en caso de que ocurra un incidente.

¿Pero cómo proteger a las empresas de un ataque que no se conoce? En el informe de tendencias para 2015 se expresó que las empresas son un objetivo cada vez más tentador para los atacantes, una predicción que a lo largo de 2015 se vio refrendada y que, en los hechos, generó un impacto más que considerable con la aparición de ataques como los mencionados anteriormente.

→

Es muy difícil de predecir cuándo o cómo una empresa se convertirá en el objetivo de un grupo de cibercriminales.

De manera constante se deben evaluar las tecnologías utilizadas para proteger los ***endpoints*** mediante una solución de seguridad, proteger el perímetro y los servidores. El cifrado ayuda a proteger la información confidencial, y no siempre es una defensa que las empresas chicas o medianas incluyan. Además de proteger los sistemas y la red, o apostar al cifrado de la información importante, sensible y/o confidencial, la gestión y la educación de los usuarios ayudan a proteger aún más a la organización.

En otras palabras, se necesita de una Gerencia que entienda el negocio y el rol de la seguridad, para garantizar su continuidad y de esta manera apostar a la inversión y utilización de los recursos tecnológicos para proteger su negocio. Además, se debe incluir a los usuarios en los procesos de seguridad de la información y capacitarlos en esta área a través de jornadas de *awareness*, cursos internos o prácticas para evaluar su nivel de seguridad con los activos de la empresa. La seguridad en una empresa se construye, y al incluirlo como parte de un proceso se identifican de manera continua aquellos riesgos, se los analiza y se define como eliminarlo.

En 2016 se seguirán viendo reportes e informes sobre **ataques dirigidos, orientados contra empresas, gobiernos, etnias y personas individuales,** que serán resultado del trabajo de los analistas de seguridad, que buscan proteger a las empresas de las técnicas utilizadas por los atacantes.

Esta labor se tendrá que acompañar con una mejor y mayor inversión en seguridad por parte de las empresas, haciendo más difícil para los cibercriminales el acceso a las redes, servidores o servicios críticos.

Todavía queda mucho trabajo por hacer: **las empresas han aumentado sus presupuestos de seguridad,** pero la educación, gestión y evaluación de los sistemas serán un desafío permanente para 2016 y los años venideros. Las empresas, gobiernos y fuerzas deberán responder ante el **accionar del cibercrimen,** minimizando los tiempos de respuestas y mediante la colaboración de múltiples actores al mismo tiempo, haciendo que los **resultados en la lucha contra el cibercrimen y los ataques dirigidos sean aún mejores.**

> PROTEGER UNA EMPRESA NO ES UN PROYECTO, ES UN PROCESO.

5

Crimeware, malware y campañas masivas alrededor del mundo

- Botnets, zombis y campañas globales
- Nuevas familias, nuevas técnicas, pero los mismos objetivos
- La colaboración es la clave para la lucha contra el cibercrimen
- ¿Hacia dónde vamos?

Autor
Pablo Ramos
Head of LATAM Research Lab

5 CRIMEWARE, MALWARE Y CAMPAÑAS MASIVAS ALREDEDOR DEL MUNDO

Dentro del mundo de la Seguridad Informática, una de las mayores preocupaciones que tienen tanto empresas como usuarios son los códigos maliciosos que pueden comprometer sus sistemas y/o redes de información. Esta preocupación no es para nada infundada ya que los casos de malware, ***crimeware*** e incidentes se repiten a diario y alrededor de todo el mundo; y la cantidad de reportes, detecciones y el número de amenazas que observan los diferentes de laboratorios antivirus crece constante y diariamente, con una diversidad cada vez mayor.

El 2015 no fue la excepción a esta situación, y no solo se observó un crecimiento del cibercimen a nivel mundial sino que, además, hubo un cambio en su agresividad y tipos de ataque, tal como se puede leer en la sección de este reporte dedicada al ransomware.

Desde **IOCTA (por sus siglas en inglés *Internet Organized Crime Threat Assessment),*** informaron acerca de un cambio en el accionar de los atacantes, haciendo foco en la ***confrontación*** como uno de los cambios más importantes en sus acciones. Desde las acciones de las redes de computadoras zombis que buscan infectar a sus usuarios con variantes de ransomware para extorsionarlos, hasta **cibercriminales que usaron la fuerza para intimidar a empresas de seguridad a que dejen de lado sus amenazas.**

Al hablar de campañas de malware no se hace referencia a los ataques dirigidos o APTs (por sus siglas en inglés, *Advanced Persisten Threats,* para referirse a las Amenazas Avanzadas Persistentes), sino a la propagación masiva de malware generalmente utilizado para robar información de usuarios y empresas. 2015 presentó diferentes desafíos para la identificación y bloqueo de campañas masivas de propagación de malware a través de canales como los correos electrónicos, dispositivos de almacenamiento masivo o mediante sitios web vulnerados que redirigen a sus visitantes a diferentes tipos de *exploits*. Las cada vez más rápidas variaciones de código, los volúmenes de amenazas que llegan a las empresas son algunos de estos desafíos que las empresas deben afrontar.

El ecosistema del cibercrimen tiene diferentes actores que abarcan un amplio marco de delitos que involucran los bienes y servicios que sirve como infraestructura para fines maliciosos. Este tipo de acciones, que involucran a los troyanos bancarios y a los RAT *(Remote Acess Tools)* fueron objetivo de múltiples investigaciones de las fuerzas de seguridad.

No obstante, los ciberdelincuentes siguen encontrando la manera de llegar a los usuarios. Tales son los casos de campañas de malware regionalizadas como la **Operación Liberpy** -que se propagó inicialmente a través de correos electrónicos-, la **Operación Buhtrap- que infectaba a sus víctimas mediante sitios web comprometidos que embebían malware en los instaladores-** y **Brolux**- el troyano que atacó a sitios de banca en línea Japoneses; y de casos globales como **Dridex.**

Cabe destacar que el impacto de estas campañas repercute tanto en usuarios hogareños, como en los negocios de pequeñas, grandes y medianas empresas. En base al último informe del **Ponemon Institute,** el costo promedio de estos

→

El ecosistema del cibercrimen tiene diferentes actores que abarcan un amplio marco de delitos

incidentes fue de 7,7 millones de dólares para el primer semestre de 2015. Algunas de las empresas que formaron parte del informe perdieron hasta 65 millones de dólares por los incidentes de seguridad que sufrieron.

Botnets, zombis y campañas globales

Las redes de computadoras zombis, también conocidas como botnets, son desde hace años los actores más importantes en el mundo del cibercrimen. El rol de las botnets en el mundo del cibercrimen es casi central, dentro de un modelo en donde facilitan la compra y venta de servicios, robo de información o campañas de propagación de **ransomware.** En otras palabras, cientos o **miles de computadoras que forman parte de este tipo de redes** son utilizadas para el envío de Spam, ataques de Denegación de Servicio y otras acciones maliciosas.

La amenaza de las redes de zombis o bots, han llevado a realizar profundos estudios **sobre cómo identificar su comportamiento,** es decir, identificar patrones que permitan a los equipos de seguridad bloquear y detectar conexiones dentro de sus redes. Más aun, existen soluciones de seguridad, como las de ESET, que incluyen funcionalidades capaces de reconocer estas comunicaciones para bloquearlas y prevenir la fuga o el robo de información.

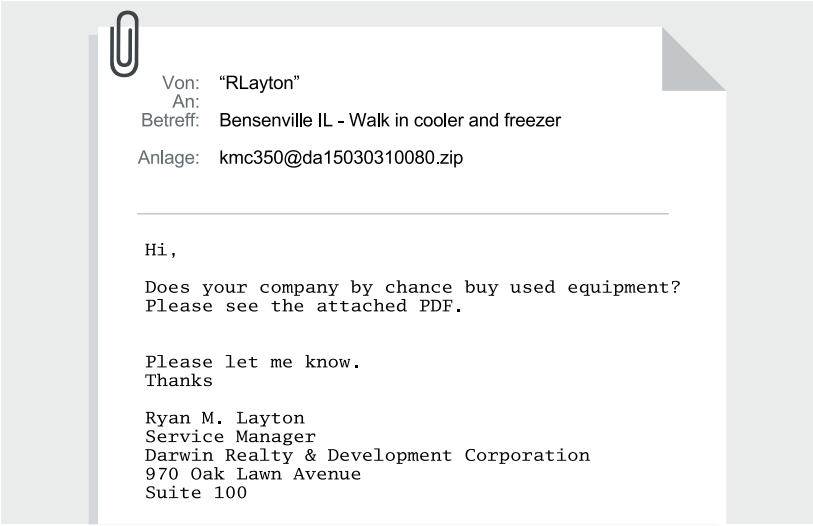
En cuanto a botnets dedicadas al robo de información, los Laboratorios de Investigación de ESET reportaron este año las acciones de la **Operación Liberpy, un *keylogger* que robó credenciales durante más de 8 meses en Latinoamérica y donde el 96% de las víctimas eran de un mismo país.** Esta amenaza, detectada como ***Python/Liberpy,*** se propagó inicialmente a través de correos electrónicos para luego continuar a través de dispositivos USB, aprovechándose de los accesos directos para infectar nuevos sistemas. El último método de propagación mencionado es similar al utilizado por otras familias como **Bondat, Dorkbot** o **Remtasu,** todas principalmente activas en América Latina.

Algunas campañas no son dirigidas a un país en particular, sino que su objetivo se basa en la infección de tantos sistemas como les sea posible. Uno de los casos que se reportaron durante 2015 fue **Waski, una campaña global que buscó instalar troyanos bancarios alrededor del mundo para infectar a los usuarios con una variante de *Win32/Battdil*.**

La campaña se inició con el envío de correos que de engañar al usuario, lo invitaban a abrir un documento que no haría ni más ni menos que infectar su sistema. (Gráfico 6)

Gráfico 6

Falso correo que infecta al sistema con Waski



Los correos electrónicos son uno de los principales vectores de propagación de códigos maliciosos y, al igual que en 2014, se vieron múltiples reportes de campañas de correos masivas, relacionadas con **troyanos bancarios como *Dridex*** a través de documentos de ofimática con macros maliciosas, o la propagación de **ransomware, como las oleadas de CTB-Locker a mediados de enero,** que llegaron a las bandejas de entrada de los usuarios.

Si bien durante 2015 hemos visto múltiples **acciones conjuntas entre fuerzas de seguridad,** empresas y gobiernos para desmantelar estas redes delictivas, más adelante veremos que continuarán siendo una amenaza y un riesgo para las organizaciones y usuarios alrededor del mundo durante el 2016.

Nuevas familias, nuevas técnicas, pero los mismos objetivos

A lo largo de 2015, se reportó la aparición de nuevas familias de códigos maliciosos o incluso la incorporación de nuevas funcionalidades a troyanos ya conocidos, como el caso de **CoreBot,** que agregó a sus capacidades la posibilidad de robar información bancaria de sus víctimas. **La evolución de las familias de códigos maliciosos** para incorporar nuevos módulos o herramientas es constante y parte del mundo del cibercrimen.

Las botnets no fueron la única área de innovación en la que aparecieron nuevas familias de códigos maliciosos. Tal como se comentó en el **documento de tendencias del año pasado,** el *Point Of Sale Malware* fue uno de los tipos de código malicioso en donde aparecieron nuevos actores, como el caso de **PoSeidon.** Este código ataca a los puntos de venta y busca infectar los terminales de cobro por tarjeta de crédito para revisar su memoria en busca de los datos de las tarjetas. Otro caso de PoS Malware fue el **Punkey,** que apareció un mes después que ***PoSeidon*** y se reportó en más de 75 direcciones IP diferentes, filtrando la información de las tarjetas de crédito.

Los incidentes con este tipo de amenazas-con los casos reportados durante el año pasado de **Home Depot, UPS** o Target-demostraron que los cibercriminales buscan acceder a grandes cadenas de *retail,* para infectar los puntos de ventas y así robar millones de tarjetas de crédito. Este tipo de incidentes aceleraron la reevaluación de **cómo se protegen los puntos de venta** y trajeron a la luz algunos casos curiosos, como que **ciertos fabricantes utilizaron durante 26 años la misma contraseña por defecto.**

En otras ocasiones, los cibercriminales han abusado de fallas en sitios web o incluso **páginas falsas de videojuegos, en donde alojaban las copias de sus códigos maliciosos.** A través de fallas en **plugins de los CMS *(Content Management System),*** los atacantes vulneraron la seguridad de miles de sitios web para alojar en ellos contenido dañino para los usuarios.

La colaboración es la clave para la lucha contra el cibercrimen

Agencias de seguridad y empresas de todo el mundo colaboran para combatir el cibercrimen y hacer de Internet un

→
Algunas empresas perdieron hasta 65 millones de dólares por los incidentes de seguridad que sufrieron.

lugar seguro. Durante 2015, más allá de los **anuncios de Europol sobre lo amenazante que se ha vuelto el cibercrimen,** se han realizado acciones en conjunto para poder desmantelar redes de computadoras zombis. Estas acciones, coordinadas y distribuidas alrededor del mundo, tuvieron éxito y culminaron con casos como la desmantelación de Dridex, **Liberpy, Ramnit** o el **arresto del creador del troyano Gozi.** Además de estas acciones directas contra ciertas familias de malware, las fuerzas de seguridad también lograron el arresto de diferentes cibercriminales asociados a foros ilegales, como el caso de **Darkode** donde 62 personas en 18 países fueron arrestadas por diferentes delitos informáticos.

¿Hacia dónde vamos?

Recapitulando los sucesos más importantes de los últimos tiempos en cuanto al malware de propósito más general, es posible observar que la barrera que lo separa de los ataques dirigidos se vuelve cada vez más delgada. Los cibercriminales continúan incorporando diferentes técnicas de propagación con el fin de infectar tantos sistemas como les sea posible, ya sea mediante la **incorporación de vulnerabilidades recientemente descubiertas a diferentes *Exploit* Kits o campañas de propagación de malware.**

En otras palabras, la evolución del cibercrimen continúa amenazando a los usuarios, y las campañas de propagación de malware han tomado escalas mayores y con diferentes niveles de eficiencia.

Para combatir estas acciones, la colaboración de los especialistas, las fuerzas de seguridad y otras entidades es clave para detener el cibercrimen y ayudar a que los usuarios puedan disfrutar de Internet sin tener que preocuparse.

Para 2016 se seguirán observando evoluciones de las familias de códigos maliciosos, ya sea en nuevas variantes o en la incorporación de funcionalidades que antes no tenían. El **cibercrimen se ha vuelto más amenazante, las empresas han aumentado la inversión en seguridad a nivel global en un 4.7%** y las agencias de seguridad están redoblando sus esfuerzos para dar de baja las botnets y poner a los cibercriminales tras las rejas.

→
La barrera que lo separa de los ataques dirigidos se vuelve cada vez más delgada.

EN OTRAS PALABRAS, 2016 SERÁ UN AÑO CON NUEVOS DESAFÍOS EN MATERIA DE SEGURIDAD, PERO CON UN ENFRENTAMIENTO MÁS ACTIVO Y ORGANIZADO EN EL COMBATE CONTRA EL CIBERCRIMEN.

6

Haxposición:
una amenaza emergente con importantes implicaciones

- Expuestos: daños a secretos corporativos y a empleados inocentes
- Las implicaciones de la haxposición
- Haxposición en 2016

Autor
Stephen Cobb
Senior Security Researcher

6 HAXPOSICIÓN: UNA AMENAZA EMERGENTE CON IMPORTANTES IMPLICACIONES

Hubo una amenaza informática en 2015 que, a pesar de no haberse propagado demasiado, merece nuestra atención por haber estado implicada en dos brechas de seguridad dirigidas a objetivos de alto perfil: *Hacking Team* y *Ashley Madison*. En ambos casos, los perpetradores de la infiltración no solo robaron información confidencial sino que también la dieron a conocer al mundo.

Esta combinación de robo de datos mediante ataques informáticos y divulgación pública de secretos internos representa en sí una amenaza emergente, a la que denominé "***haxposición***" (*hacking* + exposición de datos). Considero que una haxposición pertenece a una categoría diferente al robo de datos para su reventa, que es un tipo de ataque informático mucho más común. El robo de datos quedó tipificado por los ataques a tarjetas de pago de Target en 2013 y a la aseguradora Blue Cross en 2014 y 2015.

En esta sección analizamos en qué se diferencia la ***haxposición*** de otras amenazas, por qué puede empezar a ser más común y qué deben hacer las organizaciones para protegerse.

Expuestos: daños a secretos corporativos y a empleados inocentes

En julio de 2015, **se robaron y publicaron alrededor de 400 gigabytes** de información de la **empresa de seguridad italiana *Hacking Team*.** Ese mismo mes, en otro incidente no relacionado, un grupo que se hacía llamar *Impact Team* publicó una serie de datos de cuentas robados de la empresa canadiense **Avid Life Media,** que opera el sitio web ***Ashley Madison.*** Allí se ponen en contacto hombres y mujeres en busca de una aventura amorosa.

Los atacantes exigieron que se cerrara el sitio web, pero como desde la compañía no lo hicieron, en agosto publicaron más gigabytes de datos internos, lo que provocó la vergüenza de algunos individuos y proporcionó evidencia para hacer demandas judiciales contra la empresa. La publicación de los datos también hizo que los atacantes de *Hacking Team* pasaran a estar en la mira de una gran operación de investigación policial que ofrecía una **recompensa interesante.**

Lo que los incidentes de *Hacking Team* y de *Ashley Madison* tienen en común es que la brecha de seguridad condujo a la divulgación de secretos que dañaron la reputación y el modelo de negocio de ambas organizaciones. En el caso de *Hacking Team*, los datos divulgados parecían demostrar que la empresa había estado vendiendo sus herramientas de vigilancia digital a regímenes represivos, pese a las declaraciones previas que hizo la empresa en sentido contrario. En el caso de *Ashley Madison*, los datos divulgados parecieron probar las afirmaciones de que la empresa en realidad no eliminaba a los clientes de su base de datos, a pesar de cobrarles dinero para hacerlo. Los datos expuestos también corroboraron la sospecha de que el sitio inventaba muchos perfiles femeninos, lo que socava seriamente la credibilidad de la empresa y su intento de remediar la situación.

En ambos casos, parece que las personas responsables de los ataques estaban descontentas con los modelos de negocio de

→ Una haxposición pertenece a una categoría diferente al robo de datos para su reventa .

las empresas atacadas. Esto me llevó a buscar algunos paralelismos con un webinario de agosto de 2015 sobre el ataque a Sony Pictures en 2014, donde se analizaron algunas **repercusiones en la seguridad corporativa.** Más allá de los verdaderos motivos tras el ataque a Sony Pictures, no cabe duda de que se divulgó cierta información confidencial que no daba una buena imagen de la empresa y sus ejecutivos. Como no parece haber un motivo político ni moral tras ninguno de los tres incidentes, me gustó la idea de considerarlos un nuevo nivel de hacktivismo.

Los primeros actos de hacktivismo solían ser simples alteraciones de los sitios web (por ejemplo, **la tienda de pieles Kriegsman Fur, hackeada en 1996** - advertencia: contiene lenguaje adulto). También surgió la práctica de ***doxing,*** es decir, la investigación, recopilación y difusión de información personal identificable acerca de un individuo específico. Sin embargo, por más desagradable que pueda ser, es cuantitativamente diferente y menos perjudicial que la *haxposición*.

El hacktivismo se hizo más agresivo hace unos 10 años. Las protestas del **Project Chanology** en 2008, en relación con Anonymous, utilizaron ataques de denegación de servicio distribuido (DDoS) y divulgaron comunicaciones internas de dicha organización.

Por supuesto, es razonable argumentar que el verdadero hacktivismo no incluye un pedido de rescate, algo que hicieron los atacantes en el caso de Ashley Madison y de Sony. Cuando los ladrones de datos piden el pago de un rescate a cambio de no publicar información interna de la empresa, agravan el robo con la extorsión y exceden el límite de ética para la mayoría de los credos activistas. Y cuando la amenaza implica la exposición de información personal identificable perteneciente a los empleados o a los clientes de la organización, se introduce un nuevo nivel de irresponsabilidad.

Las implicaciones de la haxposición

Independientemente de si los ataques a Hacking Team y a Ashley Madison califican como hacktivismo, la estrategia de haxposición representa una amenaza potencialmente más perjudicial para una organización que la de robar y vender sus datos a personas que los utilizan ilícitamente en secreto. El "daño potencial" es una función para medir la confidencialidad de los datos que estás tratando de proteger, donde *"seguro = mantener en secreto"*.

Consideremos un escenario en el que tienes una empresa de alimentos y unos cibercriminales roban tu receta secreta para cocinar las legumbres. Si la venden a uno de tus competidores o la publican en Internet, por más malo que sea, probablemente no hundirá tu empresa. A menos que la receta contenga un secreto peligroso. Supongamos que uno de los ingredientes secretos es un cancerígeno prohibido; la exposición de este tipo de dato puede dañar seriamente la reputación, los ingresos y la valoración de la empresa.

En los últimos años se combinaron varios factores que incrementan el riesgo que corren las empresas cuando guardan secretos peligrosos:

1. Acceso a cibercriminales:
Cualquiera puede contratar a un cibercriminal para realizar un ataque. Ya han

→
El verdadero hacktivismo no incluye un pedido de rescate, algo que hicieron los atacantes en el caso de Ashley Madison y de Sony.

quedado atrás los días en que solo eran unas pocas las personas técnicamente capacitadas para realizar actos de alteración digital, y cuando los únicos empleados descontentos capaces de venganza digital estaban en el departamento de TI. En la actualidad, los ataques informáticos son una opción para cualquier persona que esté seriamente descontenta con tu organización, independientemente de sus conocimientos técnicos y habilidades de *hacking*.

2. Acceso a la inteligencia de código abierto:
Cuando utilizas Internet para hacer publicidad de tu negocio, lo estás exponiendo al mundo, pero las repercusiones de esta realidad siguen eludiendo a algunas personas de negocios. Para ser más claro: no puedes utilizar la World Wide Web para promover productos y servicios controversiales para un grupo selecto de personas; así no es como funciona. Más allá de que estés vendiendo pieles, cuernos de rinoceronte en polvo o herramientas de vigilancia que pueden ser aprovechadas indebidamente por los regímenes represivos, tratar de hacerlo discretamente a través de la web no es posible. La historia y la lógica muestran claramente que cuando alguien lo intenta, el negocio termina siendo descubierto por los críticos, quienes lo analizan y posiblemente lo exponen.

3. Herramientas de publicación en abundancia:
Los sitios como Wikileaks y Pastebin permiten la divulgación anónima de información robada, lo que reduce los riesgos para quienes se dedican a la *haxposición*.

4. Apetito por la ira:
El alcance global de las redes sociales, que pueden actuar como un amplificador de la indignación (a veces en ausencia de datos que la justifiquen), puede ser un escenario atractivo para potenciar la cruzada de un cibercriminal, ya que aumenta la propagación y el impacto de los secretos publicados.

5. La complejidad es la enemiga de la seguridad y el secreto:
Está claro que guardar secretos es difícil cuando se mantienen en forma digital. Los sistemas complejos normalmente contienen múltiples vulnerabilidades sin corregir que son conocidas y pueden ser aprovechadas, además de cierta cantidad de exploits *o-day* desconocidos, para los cuales ni siquiera existe un parche. Por otra parte, los secretos digitales son mucho más fáciles de extraer: suelen ser un mero fragmento digital en el tráfico de red saliente, o una pequeña pieza de medios físicos.

¿Te acuerdas de cuando **acusaron a VW de robar información secreta de GM** en la década de 1990? La información supuestamente robada incluía 20 cajas extraídas en avión. Aunque negaron el carácter secreto de la información impresa en papel, todos esos datos en formato digital hoy podrían caber en una unidad flash más pequeña que un sello de correos, y mucho más fácil de robar.

¿Cuáles son las implicaciones de estos factores? Primero y principal, subrayan la necesidad de contar con la seguridad básica apropiada. Como mínimo, vas a necesitar:

- Un buen sistema de autenticación fuerte, antimalware y cifrado (estas medidas de seguridad podrían haber limitado los daños tanto para Hacking Team como para Ashley Madison).

→
¿Cuáles son las implicaciones de estos factores? Primero y principal, subrayan la necesidad de contar con la seguridad básica apropiada.

- Planes y capacidad de backup y de recuperación ante desastres.
- Un plan de respuesta ante incidentes (ausente al parecer en Sony Pictures y Avid Media).
- Monitoreo de amenazas internas (una persona de confianza con acceso privilegiado puede causar muchos más problemas que miles de atacantes externos; ver el caso de Snowden y la NSA, Agencia Nacional de Seguridad Estadounidense).

Más allá de estas técnicas básicas de seguridad, hay factores estratégicos que deben ajustarse para hacer frente a la amenaza de la *haxposición:*

- Evaluación de riesgos: ¿tus políticas y controles de seguridad reflejan una conciencia de la amenaza de *haxposición?*
- Conciencia operativa: ¿la organización es consciente de la posibilidad de estar fomentando un ataque de *haxposición* por la forma en que lleva a cabo sus operaciones?
- Transparencia en la organización: ¿es innecesariamente secreta en sus operaciones? ¿Las decisiones para mantener secretos se toman con plena conciencia de la posibilidad de fugas de datos y sus consecuencias asociadas?

Haxposición en 2016

¿Habrá más casos de haxposición en 2016? La respuesta depende de varios factores, como el grado de educación de las organizaciones sobre esta amenaza y las contramedidas que tomen. Si algunas empresas de alto perfil logran tener éxito en evitar este tipo de ataques y trabajan con la policía para llevar a los responsables ante la justicia, podría actuar como elemento de disuasión. Por desgracia, también es posible que los secretos empresariales arriesgados fomenten este tipo de ataques.

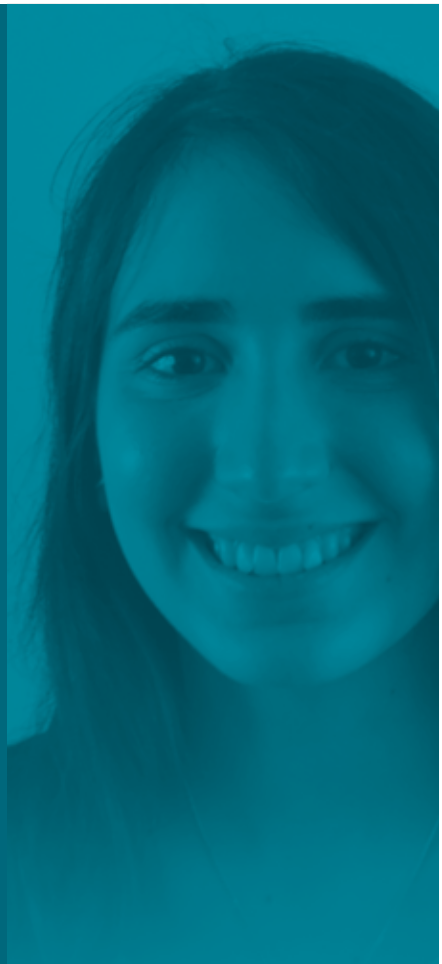
Pensemos en el escándalo de las **pruebas de emisiones diesel de Volkswagen** y en las serias **vulnerabilidades de seguridad de los sistemas informáticos de vehículos Chrysler, Jeep y Fiat.** Estos son ejemplos de algunas de las empresas más grandes del mundo y las marcas más conocidas que ponen en riesgo la salud y seguridad pública con acciones contraproducentes si se daban a conocer.

Los cibercriminales que creen tener la razón y el derecho de actuar como árbitros de la justicia pueden sentirse inclinados a buscar nuevos secretos y exponerlos públicamente, dañando a víctimas inocentes en el proceso.

> SI ALGUNAS EMPRESAS DE ALTO PERFIL LOGRAN TENER ÉXITO EN EVITAR ESTE TIPO DE ATAQUES Y TRABAJAN CON LA POLICÍA PARA LLEVAR A LOS RESPONSABLES ANTE LA JUSTICIA, PODRÍA ACTUAR COMO ELEMENTO DE DISUASIÓN.

7

Dispositivos móviles, amenazas y vulnerabilidades



- Un análisis panorámico de la seguridad móvil
- Los hitos de 2015
- ¿Cuáles son los próximos pasos de esta tendencia?
- Estrategias de defensa

Autor
Denise Giusto Bilic
Security Researcher

7 DISPOSITIVOS MÓVILES, AMENAZAS Y VULNERABILIDADES

Mientras los celulares y tabletas inteligentes concentran más y más servicios encargados de procesar información sensible, esta se vuelve más atractiva a los ojos de los cibercriminales. En este contexto, los principales escenarios de riesgo continúan siendo los mismos: extravío del equipo o instalación de aplicaciones maliciosas por descuido del usuario; sin embargo, las consecuencias de un ataque se vuelven exponencialmente más críticas.

Un análisis panorámico de la seguridad móvil

Para entender hacia dónde se dirige la sociedad en la utilización segura de las tecnologías móviles, se debe comenzar por revisar el estado de la protección de los dispositivos que utilizan esta tecnología, construyendo así, una mirada general de los hitos ocurridos en la seguridad móvil.

• Una revisión al pasado

2014 fue un año de mucha acción en materia de Seguridad Informática. Con el descubrimiento de vulnerabilidades trascendentales en diversas plataformas operativas de alto impacto -como fue el caso de ***Heartbleed, Shellshock*** o ***Poodle***-, quedó en evidencia la importancia de mantener actualizados sistemas operativos y aplicaciones.

En la misma línea, los sistemas móviles no resultaron exentos a esta tendencia: por ejemplo, se encontró la forma de **desactivar iCloud,** el sistema en la nube que bloquea los iPhone cuando son robados o extraviados. La falla, básicamente, permitía desbloquear al instante el teléfono de forma remota.

En Android se descubrió una vulnerabilidad que permitía **evadir el mecanismo de seguridad en navegadores.** El bug permitía al atacante acceder a los sitios que se encontraban abiertos en el dispositivo y tomar el control. En particular, investigadores descubrieron cómo podía utilizarse para **comprometer cuentas de Facebook.**

En cuanto a los códigos maliciosos, se vieron nuevas variantes de ransomware con dispositivos Android como objetivo, y es así que reapareció el **Virus de la Policía, pero esta vez dirigido a Android.** Esto cumplió el pronóstico que el Laboratorio de Investigación de ESET presentó en el **informe de Tendencias 2014,** en donde se vaticinó la intensificación del ransomware.

En esta línea, ESET analizó al ransomware *Android/Simplocker* que explora la tarjeta SD de un dispositivo Android en busca de ciertos tipos de archivos, los cifra y exige el pago de un rescate para descifrarlos. ***Simplocker*** **constituyó el primer malware de la familia** ***Filecoder*** destinado al sistema operativo de Google, buscando interceptar documentos con extensiones comunes, como JPEG, JPG, PNG, GIF, DOC, AVI y MP4.

El ransomware siguió haciéndose notar y fue así como se detectó ***Android Locker,*** un nuevo código malicioso que se hacía pasar por un antivirus. Además, solicitaba permiso para convertirse en administrador del dispositivo y tomar así el control del sistema, dificultando su desinstalación.

Fue hacia el final del año que se presentó una **nueva muestra de ransomware** que utilizaba el navegador para mostrar

→ Mientras los celulares y tabletas inteligentes concentran más y más servicios encargados de procesar información sensible, esta se vuelve más atractiva a los ojos de los cibercriminales.

imágenes de pornografía infantil y luego bloquear el equipo en nombre del FBI. Una vez instalada, "Porn Droid" pedía permisos para convertirse en administrador del sistema y así poder bloquear la pantalla del dispositivo.

Además, se observó una complejización de los **troyanos apuntados a la plataforma Android,** expandiéndose a través de mercados no oficiales y redes sociales. Este fue el caso de **iBanking,** una aplicación maliciosa capaz de espiar las comunicaciones desarrolladas en el equipo, y que se enfocaba en sobrepasar el método de doble factor de autenticación de dispositivos móviles implantados por algunas instituciones bancarias.

En relación con iOS, es posible mencionar el caso de **WireLurker,** un código malicioso dirigido a equipos Mac y iPhones, siendo el primero en poder infectar incluso equipos sin *jailbreak*. Acorde a la **BBC,** alrededor de 400 aplicaciones fueron infectadas con este malware y se descargaron cerca de 350 mil veces.

- Viejas tendencias que cobran fuerza

Con el advenir del año 2015 se hizo notable cómo estas tendencias, que fueron cobrando fuerza a lo largo de 2014, terminaron arraigándose en el terreno móvil para convertirse en la nueva regla.

En este sentido, los cibercriminales iniciaron una etapa de diversificación y complejización de sus amenazas, por lo que ahora es posible apreciar campañas de difusión de malware móvil más organizadas, que abarcan nuevos vectores de infección y buscan dificultar la remoción de las amenazas.

A lo largo del año se encontraron una gran cantidad de vulnerabilidades, y la explotación de las mismas se convirtió en un mecanismo cada vez más vigente entre los atacantes para ganar el control de los dispositivos. Este último punto plantea nuevas presiones para la rápida actualización de plataformas, lo que puede devenir en una importante falencia para sistemas operativos como Android, donde existe tal cantidad de proveedores de equipos que las actualizaciones pueden tardar demasiado en ser desplegadas a los usuarios finales.

Como consecuencia de estos ataques mejor orquestados, los códigos maliciosos comenzaron a colarse en cientos en las plataformas oficiales para la distribución de aplicaciones legítimas. Esto plantea nuevos retos de cara al futuro, instando a las empresas de sistemas operativos móviles a desarrollar mejores métodos de detección de actividad maliciosa.

El ransomware, una de las **actividades más rentables del mundo del cibercrimen,** se consolidó en plataformas móviles con nuevas técnicas para bloqueo de los equipos, evidenciando una ramificación en las técnicas utilizadas para comprometer los distintos dispositivos. Finalmente, cabe destacar la utilización de aplicaciones populares en plataformas móviles como WhatsApp o Facebook para aumentar el alcance de campañas de malware multiplataforma haciendo uso de viejas técnicas de Ingeniería Social.

- ¿Cómo impactan estos antecedentes a los usuarios?

Existen dos factores determinantes parar que un cibercriminal se sienta atraído a

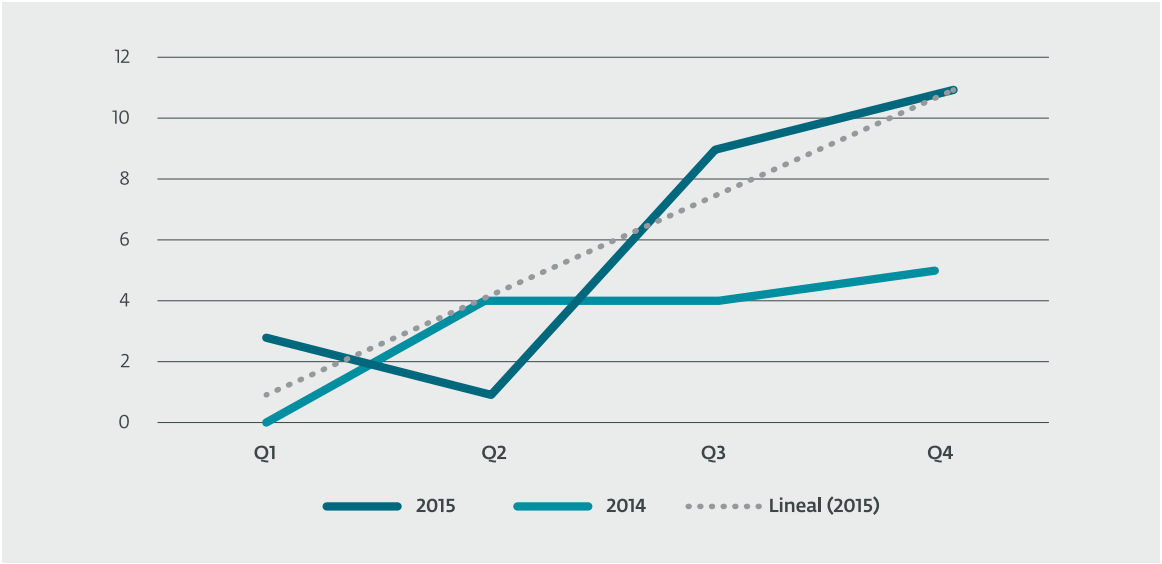
→
El ransomware, una de las actividades más rentables del mundo del cibercrimen, se consolidó en plataformas móviles con nuevas técnicas para bloqueo de los equipos.

desarrollar amenazas para una determinada plataforma: su masividad y la cantidad de vulnerabilidades que puedan ser explotadas. A medida que los sistemas operativos son más y más utilizados por el usuario tecnológico promedio, aumenta la cantidad de potenciales víctimas susceptibles a una única campaña de malware. Entonces, queda claro que no existen sistemas operativos invulnerables y que la cantidad de amenazas que se encuentran orientadas a una determinada plataforma es una medida proporcional a la cantidad de usuarios que posee. Con esto en mente, una manera de identificar a los sistemas más expuestos y transpolar el impacto en la proliferación de amenazas móviles en cada una de las plataformas, resulta de hacer una comparación entre las porciones de mercado que ocupan.

Según **Gartner,** Android cerró el segundo cuatrimestre de 2015 con un 82,2% de mercado, frente a un 14,6% de iOS y, muy por detrás, un 2,5% para Windows Phone y 0,3% para BlackBerry. Es decir que Android -aunque con un pequeño decrecimiento respecto al mismo período de 2014-, continúa liderando el mercado, mientras Apple incrementa de a poco su participación. Esto significa que, con cada nueva contingencia en materia de seguridad de Android que se torna realidad, millones de usuarios a nivel global quedan desprotegidos.

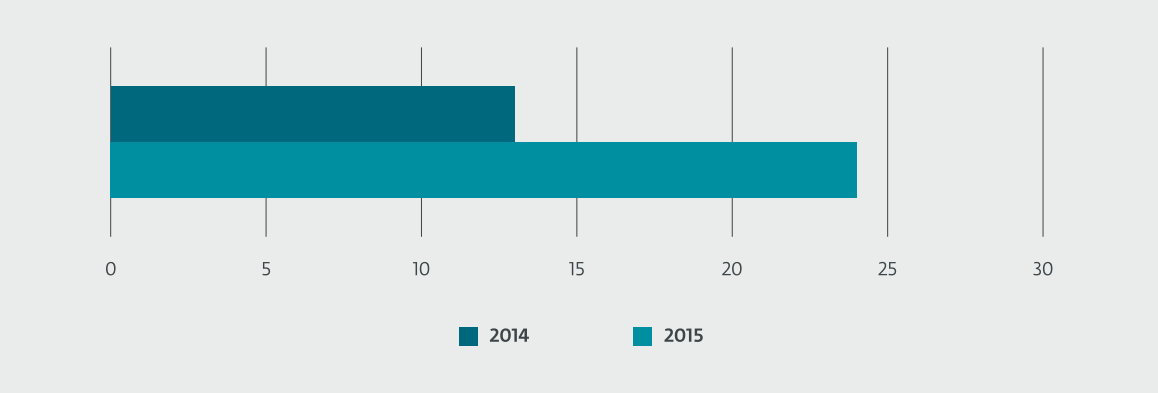
Paralelamente, surge una pregunta: ¿hay más amenazas para iPhones e iPads ahora? La respuesta es que sí. En lo que respecta a iOS, si comparamos la cantidad de nuevas amenazas detectadas por los productos de ESET desde comienzo de 2015 con la cantidad de nuevas amenazas detectadas en el mismo período del año 2014, los números actuales duplican las estadísticas pasadas. (Gráficos 7 y 8)

Gráfico 7 Nuevas variantes de malware en iOS



Nota: las cifras del cuarto trimestre de 2015 incluyen solo estadísticas hasta noviembre de dicho año inclusive, con lo que se estima que el porcentaje final para este trimestre será aún mayor una vez concluido el año.

Gráfico 8 Nuevas variantes de malware en iOS



Gran porcentaje de estas familias de códigos maliciosos buscan vulnerar estos sistemas a través del engaño, instando a los usuarios a que intencional y ciegamente cedan su información a través de técnicas de Ingeniería Social. Además, la gran cantidad de vulnerabilidades descubiertas sobre estos sistemas en el último tiempo deja desprotegidos a los usuarios que no estén pendientes de actualizar sus sistemas operativos y aplicaciones siempre que esté disponible una nueva versión.

En el mismo sentido, aquellos dispositivos que han atravesado un proceso de ***jailbreak*** -o dispositivos ***rooteados,*** en el caso de Android- pueden terminar alojando malware como troyanos, gusanos, *backdoors*, entre otros. Esto es porque resulta mucho más sencillo para los códigos maliciosos llegar a ejecutar comandos con permisos de administrador sin la expresa -y descuidada- autorización del usuario. Además, estos procesos rompen el mecanismo de despliegue de actualizaciones soportado nativamente por la plataforma, de modo que pueden impedir al usuario de obtener las últimas versiones del sistema o parches de seguridad, dejando al equipo vulnerable.

Los hitos de 2015

- Vulnerabilidades a la orden del día

La aparición de vulnerabilidades en aplicaciones usadas por millones de personas siempre suele causar revuelo, especialmente si afectan la privacidad o impiden el uso de los equipos. Iniciando el año, una **vulnerabilidad en la aplicación de gestión de correos electrónicos en Android** causó un alboroto al hacer que el dispositivo colapse y dejara de responder tan solo con recibir un mensaje especialmente diseñado para este fin.

Otras vulnerabilidades afectaron en 2015 al sistema Android, como aquella conocida como ***CVE-2015-3860*** mediante la cual atacantes podrían haber **burlado la seguridad del bloqueo de pantalla en Android** y tomar el control del smartphone. Aunque se demostró que el ataque era posible, la falla fue rápidamente solucionada.

Mientras tanto, **Samsung también descubrió un importante fallo de seguridad** con actualizaciones a su aplicación de teclado ***SwiftKey,*** lo que potencialmente permitía que archivos maliciosos se pudieran enviar al dispositivo, a través de un

ataque *Man-In-The-Middle*. 600 millones de teléfonos Samsung Galaxy podrían haberse visto vulnerados.

Sin lugar a dudas, la falla más notoria en esta plataforma fue la denominada ***Stagefright,*** que podía permitirle a los atacantes robar información de dispositivos a través de código ejecutado de manera remota con tan solo enviar un SMS preparado para tal fin. Con 950 millones de usuarios de Android potencialmente afectados y las tentativas consecuencias de su explotación, ciertamente la severidad de esta vulnerabilidad superó por lejos a otras vulnerabilidades acontecidas en el año.

Por su parte, iOS también se vio comprometido a través de numerosas falencias. Hacia mediados de año, un **artículo académico** reveló una serie de fallas que, combinadas, podrían explotar apps maliciosas para obtener acceso no autorizado a los datos almacenados por otras aplicaciones (contraseñas de iCloud, tokens de autenticación o credenciales web almacenadas en Google Chrome).

Otra **vulnerabilidad en Airdrop de iOS** permitió instalar apps maliciosas aparentemente legítimas con gran sigilo. ***Airdrop*** es una característica que se introdujo en iOS 7 y que permite compartir ficheros entre usuarios de otros dispositivos cercanos. Así, la vulnerabilidad conseguía hacer un envío de archivos incluso aunque el usuario no los aceptara.

Este año, **Apple también cambió los mecanismos de privacidad de datos** para sus aplicaciones: diseñó una nueva actualización de privacidad para iPhone para evitar que las apps de iOS vean qué otras apps han sido descargadas al dispositivo. De esta forma, los anunciantes no tendrán acceso a los datos de las aplicaciones.

Pero, ¿qué pasó con el malware móvil? El año 2015 representó un gran crecimiento en la cantidad de variantes maliciosas para plataformas móviles. Aún más, lo que capturó más la atención de los usuarios fue la revelación de encontrar cientos de aplicaciones maliciosas siendo distribuidas a través de tiendas oficiales. Esto remarca la importancia de la educación entre los usuarios y la importancia de que puedan discriminar en qué desarrolladores confiarán y los permisos que otorgarán a cada aplicación.

Por parte de Android, se hallaron **más de 30 aplicaciones de tipo scareware disponibles para descarga desde la tienda oficial Google Play Store.** Más de 600 mil usuarios de Android descargaron estas aplicaciones maliciosas, que se hacían pasar por trucos para el popular juego **Minecraft** mientras estaban activas.

También, más de 500 mil usuarios de Android resultaron víctimas de ataques de **falsas apps de Google Play** con funcionalidades de phishing que extraían credenciales de Facebook. ESET detecta estos troyanos como ***Android/Spy.Feabme.A.***

Desde los laboratorios de ESET, se detectaron más de **50 troyanos clicker de sitios pornográficos** que estaban disponibles para su descarga. Cuatro de ellos tenían más de 10 mil instalaciones y uno tenía más de 50 mil.

Por su parte, dentro de las muestras encontradas en la Play Store estaba ***Android/Mapin:*** un troyano backdoor que tomaba el control del dispositivo y lo convertía en

→

Lo más llamativo fue encontrar cientos de apps maliciosas siendo distribuidas en tiendas oficiales.

parte de una botnet, al mando del atacante. En algunas variantes de esta infiltración, por lo menos debían transcurrir tres días para que el malware alcanzara la funcionalidad completa de un troyano. Probablemente sea este retraso lo que le permitió al código pasar tanto tiempo sin ser detectado por el sistema de prevención de malware de Google. Según **MIXRANK,** una de sus variantes enmascarada como el famoso juego **Plants vs Zombies 2** fue descargada más de 10 mil veces antes de eliminarse de la Play Store.

El ransomware continuó avanzando en sistemas Android. En esta categoría, desde ESET se descubrió una agresiva **amenaza para Android capaz de cambiar el código PIN del equipo** e inutilizarlo. Este es el primer código en su tipo para este sistema operativo y fue catalogado como *Android/Lockerpin*.

Este troyano obtiene los derechos de administrador de dispositivos haciéndose pasar por la "instalación de un parche de actualización". No mucho después, pedirá al usuario que pague un rescate de 500 dólares supuestamente por ver y guardar material pornográfico prohibido.

Ni el propietario ni el atacante pueden desbloquear el dispositivo, debido a que el PIN se genera al azar y no se envía al atacante. La única forma práctica de desbloquearlo es restableciendo los valores de fábrica.

Respecto a iOS, Apple debió remover de su App Store más de 300 aplicaciones para iOS infectadas con malware, luego de que se confirmara un problema en su seguridad. Este ataque, denominado **XCodeGhost,** fue un ingenioso y efectivo asalto que consiguió hacer pasar por seguras varias decenas de aplicaciones infectadas.

¿Cómo lograron estas aplicaciones implantarse en la tienda oficial? Los ciberdelincuentes optaron por infectar el compilador (XCode) que se utiliza para crear las aplicaciones en iOS. De esta forma, los desarrolladores incluían código malicioso en sus aplicaciones sin saberlo y, al estar firmadas por el desarrollador legítimo, se subían a la App Store sin objeciones.

Para Apple, este hecho marcó un hito a partir del cual deberán diseñarse e implementarse los recaudos necesarios para perfeccionar los sistemas de verificación de códigos maliciosos en las aplicaciones que serán examinadas para, luego, subirse a la tienda en línea.

Poco después del hecho, investigadores encontraron otras **256 aplicaciones que violaban la política de privacidad de la App Store,** la cual prohíbe la recolección de direcciones de correo electrónico, aplicaciones instaladas, números de serie y demás información de identificación personal que se pueda utilizar para rastrear usuarios. Estas aplicaciones representaron una invasión a la privacidad de los usuarios que las descargaron, estimados en un millón.

También se debe mencionar a ***YiSpecter:*** un nuevo malware para iOS que se aprovecha de API privadas en el sistema operativo para implementar funcionalidades maliciosas. Lo alarmante del caso es que afecta a dispositivos iPhone ya sea que tengan hecho el *jailbreak* o no. Este malware puede descargar, instalar y poner en marcha aplicaciones para iOS arbitrarias, incluso sustituyendo las verídicas ya instaladas en el dispositivo.

→
¿Cómo lograron estas aplicaciones implantarse en la tienda oficial? Los ciberdelincuentes optaron por infectar el compilador (XCode) que se utiliza para crear las aplicaciones en iOS.

- Estafas multiplataforma

Este año se observaron **grandes campañas de fraudes difundidas a través de aplicaciones móviles** que afectaron a marcas de diversas tiendas muy populares como Zara, Starbucks y McDonald's, entre otras, robando datos personales de las víctimas.

La Ingeniería Social, es decir, el arte de disuadir a las personas con algún fin, es uno de los puntos fuertes en este tipo de fraudes. En estos casos, nuevamente se demuestra por qué la educación es la primera barrera de protección; en ese sentido, es necesario reflexionar y alertar sobre estas nuevas tendencias que utilizan antiguas técnicas en canales como WhatsApp.

Otro punto a resaltar es que los servidores maliciosos utilizaban técnicas de geolocalización para potenciar la propagación convirtiendo a un usuario no solo en víctima, sino también en vector de difusión. Así, redirigían el tráfico a una u otra página fraudulenta según el país y el tipo de dispositivo del que proviniese. Esto demuestra cómo poco a poco se está ingresando en una etapa de amenazas multiplataforma, con campañas diseñadas para comprometer a los usuarios a través de sus diferentes equipos tecnológicos.

¿Cuáles son los próximos pasos de esta tendencia?

Hasta el momento, algunas organizaciones e individuos han restado importancia a la seguridad de sus dispositivos móviles; no obstante, esto es un error y simplemente no debe continuar de la misma manera. Es crítico comprender que la movilidad no existe en el vacío, muy por el contrario, posee un impacto real en la sinergia de los diversos componentes de seguridad presentes en los diversos sistemas con los que interactuamos cotidianamente. En este sentido, la implementación de estrategias de seguridad que incluyan equipos móviles personales como potenciales vectores de compromiso es imperativa.

Asimismo, es necesario considerar la relación entre Internet de las Cosas y los sistemas operativos móviles, ya que serán estas últimas las plataformas que soportarán la estructura de datos en los nuevos *gadgets* electrónicos porvenir. **Android Auto** es un interesante ejemplo de ello. Hoy el ransomware secuestra laptops y smartphones; pronto quizás lo haga con el encendido de automóviles, como se debatió en las diferentes secciones del presente informe.

Respecto a estos códigos que secuestran la información o el uso de los dispositivos, es de esperarse un incremento en su producción, mientras los cibercriminales descubren las virtudes que guardan los equipos móviles. Como toda actividad económica que muestra altas tasas de rentabilidad, su crecimiento en el tiempo parece inevitable. Dada la utilización de la nube como almacén de perfiles de usuario disponibles a lo largo de diversas plataformas, la utilización de estos equipos como vector de ataque para denegar acceso a estos datos podría tener gran repercusión, expandiendo el abanico de ataques posibles contra la información personal.

Es posible también, que aparezcan nuevas campañas de malware multiplataforma, ya sea a nivel de distribución (servidores maliciosos que entreguen contenido especializado según la plataforma que realiza la petición) como de ejecución (la

→ **La implementación de estrategias de seguridad que incluyan equipos móviles personales como potenciales vectores de compromiso es imperativa.**

utilización de plataformas y lenguajes para la generación de ejecutables que soporten múltiples entornos).

A medida que se intensifica la búsqueda de mejores barreras de protección, los creadores de malware para plataformas móviles desarrollarán **nuevas maneras de complicar el análisis** de sus producciones. Resulta inevitable pensar que, con el correr del tiempo, será cada vez más difícil analizar estas muestras maliciosas.

A lo largo de 2015, los Laboratorios de Investigación de ESET vieron cómo la tasa de creación de amenazas se ha mantenido relativamente constante en lo que a Android refiere, promediando unas 200 nuevas muestras maliciosas por mes.

De ellas, casi la totalidad son códigos maliciosos del tipo troyano, como se puede apreciar en el siguiente gráfico. Por lo anterior, no resulta descabellado proyectar sobre el próximo año una mayor complejidad en las técnicas de compromiso utilizadas por estos códigos. (Gráfico 9)

De esas nuevas amenazas surgidas a lo largo del presente año, algunas presentaron mayor crecimiento que otras, lo que se ilustra en el gráfico a continuación. Como es posible observar, los troyanos SMS tuvieron un gran crecimiento en 2015. (Gráfico 10)

Del mismo modo, se detectó una gran cantidad de nuevos espías móviles que intentaron robar credenciales bancarias, crediticias, e interceptar datos privados de los usuarios de los terminales, como mensajes enviados o lista de contactos.

También se percibió un incremento notorio en los códigos maliciosos móviles que intentan impedir que el usuario utilice su propio equipo, generalmente para luego solicitar un rescate. Particularmente son las familias *Android/Locker* y *Android/LockScreen*, que juntas lograron un crecimiento del 600% respecto al año pasado en cuanto a la cantidad de variantes existentes. Esto último sin considerar nuevas muestras como *Android/Lockerpin*, mencionada anteriormente.

Gráfico 9 Troyanos en Android durante 2015

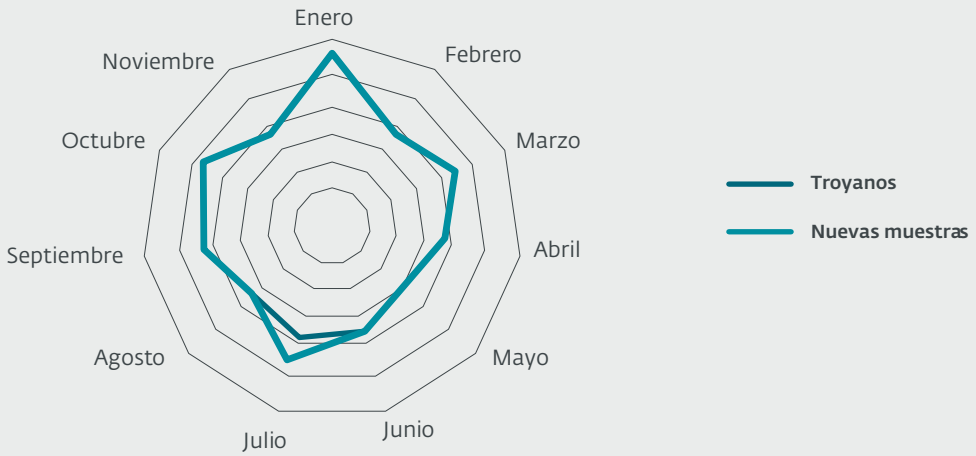
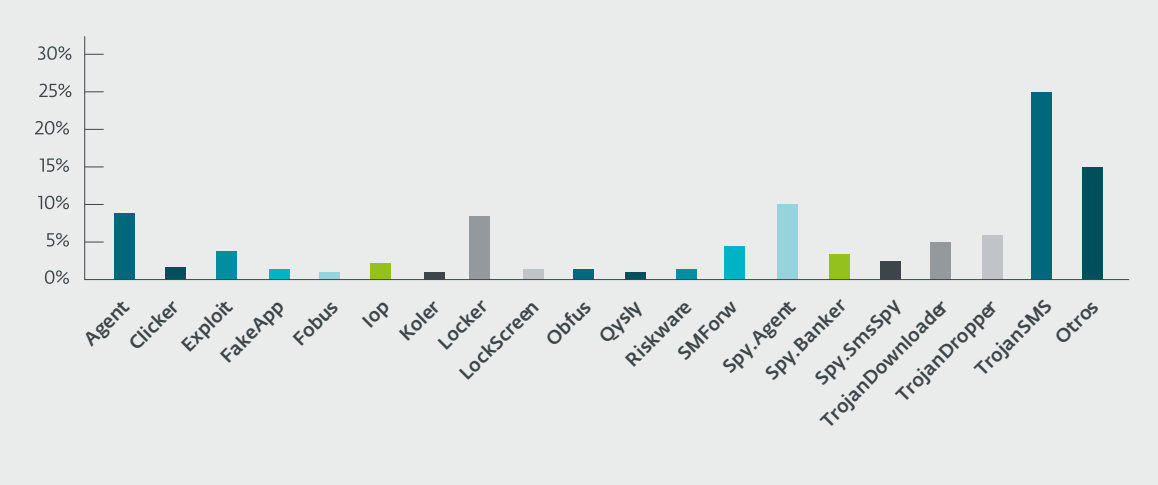


Gráfico 10 Familias de malware para Android que más crecieron en 2015

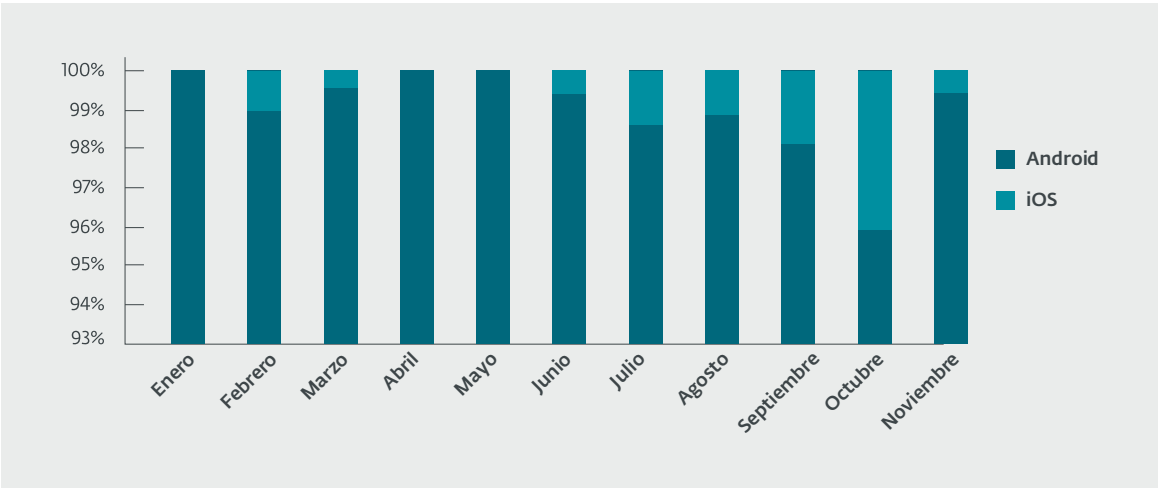


Estas tendencias podrían acentuarse a lo largo de 2016, de modo que se estaría frente a casos de ransomware más diversos y RATs más complejos que intentarán ganar el control de los equipos para robar la información sensible de sus usuarios.

Aunque la cantidad de malware conocido para iOS continúa representando porcentajes significantemente menores cuando es contrastada con la existente para Android– lo que se puede ver en el gráfico que sigue-, esta nueva oleada de códigos maliciosos móviles difícilmente dejará de lado a iOS. Si se analiza el aumento en la cantidad de familias maliciosas para esta plataforma durante 2015, se puede ver cómo este valor crece exponencialmente hacia fines de este año.(Gráfico 11)

Dentro de estas nuevas amenazas, las variantes que se muestran en el gráfico a continuación tuvieron un mayor crecimiento durante este año. Acompañando una mayor cantidad del *malware* para iOS,

Gráfico 11 Nuevas variantes de malware en 2015



es posible esperar nuevas variantes de spyware que exploten teléfonos inteligentes, incluso con las protecciones de fábrica intactas, es decir, sin *jailbreak*. (Gráfico 12)

Finalmente, el desarrollo seguro para prevenir vulnerabilidades será crucial para la creación de aplicaciones robustas. La seguridad no puede ser un agregado al proceso de diseño; por el contrario, debe plantearse desde los mismos comienzos. Del mismo modo, la puesta en marcha de sistemas para la evaluación estática y dinámica de sistemas será necesaria para la identificación temprana de potenciales vulnerabilidades.

Estrategias de defensa

El malware móvil es una amenaza real y por esto es necesario permanecer alerta para evadir sus intentos de infección. Llegó la hora de preguntarse qué pueden hacer los usuarios ante esta diversidad de amenazas móviles.

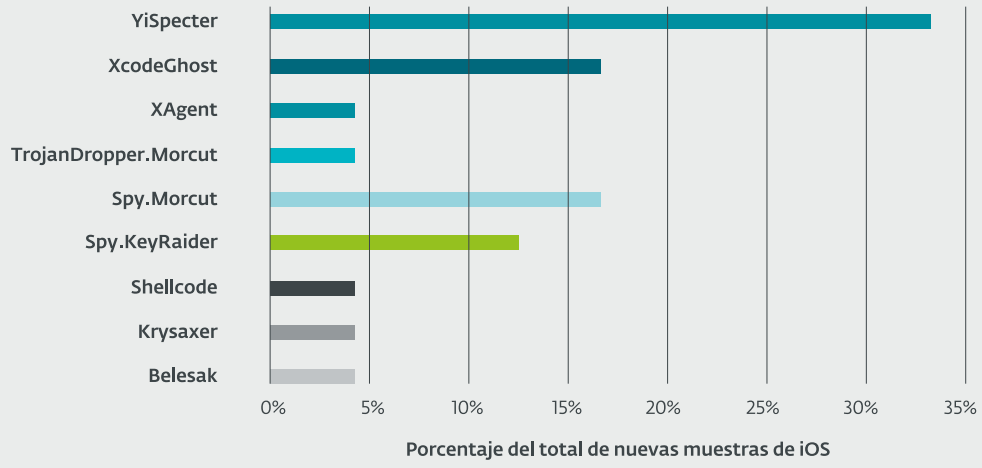
- **Usuarios hogareños**

Además de la instalación de una solución de seguridad móvil, es necesario ser sumamente cuidadosos al momento de instalar aplicaciones desde tiendas no oficiales. De hecho, la mejor práctica será evitar completamente este tipo de instalaciones; prohibir la instalación desde orígenes desconocidos y saber cómo determinar si una aplicación es legítima.

Al navegar por la web, es importante no hacer caso de aquellos sitios que insten sospechosamente la descarga de archivos APK desde páginas de reputación dudosa. Más aun, tampoco se puede confiar en mensajes SMS con enlaces extraños que se reciban, incluso, desde los propios contactos.

Hemos visto que los casos de malware propagándose a través de plataformas oficiales no dejan de aumentar, tanto en Android como Apple. Con vista en nuevos

Gráfico 12 Familias de malware para iOS que más crecieron en 2015



casos que puedan darse a conocer, la precaución también en estos sitios debe ser la regla: investigar quién es el desarrollador, qué otras aplicaciones ha realizado y si acaso alguien lo ha acusado de ser un fraude. Asimismo, las compañías deberán reforzar aún más sus procesos de revisión en sus repositorios, para minimizar este tipo de casos.

Realizar procesos de *rooting* o de *jailbreaking* dentro de los dispositivos rompe el esquema de seguridad que los sistemas operativos son capaces de brindar, lo que facilita la instalación de amenazas. Por ello es recomendable evitar este tipo de prácticas.

Como se ha visto a lo largo de esta sección, existen muchas vulnerabilidades que pueden ser explotadas para ejecutar códigos maliciosos. Se torna necesario, entonces, mantener actualizados los sistemas operativos y aplicaciones que se utilicen, instalando siempre los últimos parches de seguridad.

Particularmente en Android, con la gran variedad de modelos de equipos disponibles, los usuarios tienen poco control respecto a cuándo las actualizaciones son finalmente desplegadas a sus equipos por los fabricantes. En vistas a la no existencia de una solución contundente para esta problemática, es aconsejable tomar este factor como un determinante al momento de decidir qué dispositivo adquirir. Los dispositivos de Google –Google Nexus– siempre llevarán la delantera en este sentido, reduciendo el periodo de exposición a vulnerabilidades.

Para proteger la confidencialidad de los datos ante la pérdida del terminal, es aconsejable mantener el equipo cifrado e instalar una solución de seguridad que permita la gestión remota del dispositivo para bloquearlo o rastrearlo.

De cara al abrupto y continuo crecimiento que presenta el ransomware móvil, es sumamente importante que los usuarios realicen copias de respaldo de la información crítica en otros medios confiables, para así no verse obligados a pagar un rescate por recuperarla.

Finalmente, realizar un análisis de los gastos que son acreditados a los equipos será de utilidad para identificar de manera temprana cualquier infección que haya podido saltearse las precauciones anteriormente mencionadas.

• ¿Y en entornos corporativos?

Las tendencias en malware que afectan a los usuarios particulares indudablemente deberán ser tratadas también a nivel organizacional. Después de todo, una infección masiva de troyanos SMS que produzcan gastos telefónicos a través de cuentas corporativas, la fuga de información causada por códigos espías o la pérdida de datos ligada a un caso de ransomware móvil impactarán directamente el corazón económico de la empresa.

Resulta clave comprender que los móviles de usuarios corporativos pueden ser utilizados para apalancar ataques sobre las redes de la organización. El apuntalamiento de la defensa comienza con asimilar el riesgo que estos dispositivos presentan en la era de la interconexión multiplataforma. Una modalidad puede ser invertir en equipos para uso exclusivamente corporativo, que posean herramientas configuradas para la gestión

→
Realizar procesos de *rooting* o de *jailbreaking* dentro de los dispositivos rompe el esquema de seguridad que los sistemas operativos son capaces de brindar.

remota de los mismos, estén debidamente cifrados y conectados a la intranet empresarial sobre el uso de una VPN. Además, la separación del tráfico móvil de las redes empresariales transaccionales y la utilización de soluciones de seguridad en los terminales resultan imprescindibles en el marco de un enfoque preventivo.

Estas medidas deben ser acompañadas por el fortalecimiento de sistemas de *Data Loss Prevention* (DLP) y *Content Monitoring and Filtering* (CMF), y la creación de políticas que delineen la administración de aplicaciones móviles y la configuración de plataformas seguras.

Medidas comúnmente utilizadas en políticas de seguridad para equipos de escritorio son igualmente válidas, como definir contraseñas seguras con restricciones de longitud, durabilidad y tiempo de expiración.

Dentro de la política debiese establecerse qué plataformas, versiones y fabricantes serán permitidos y cuáles no. El tratamiento de aplicaciones cuando estas están debidamente firmadas debe ser obligatorio, como también desaprobar procedimientos para ganar privilegios de administrador sobre el sistema.

Acompañando estas soluciones tecnológicas es necesario crear planes de capacitación en seguridad que alerten a los usuarios finales para que de esta manera estén prevenidos contra la creciente variedad de códigos maliciosos a los que estarán expuestos durante el próximo año.

> MEDIDAS COMÚNMENTE UTILIZADAS EN POLÍTICAS DE SEGURIDAD PARA EQUIPOS DE ESCRITORIO SON IGUALMENTE VÁLIDAS.

8

Windows 10:
funcionalidades de seguridad y privacidad del usuario

- Características de seguridad
- Privacidad y aceptación del usuario

Autor
Aryeh Goretsky
Distinguished Researcher

8 WINDOWS 10: FUNCIONALIDADES DE SEGURIDAD Y PRIVACIDAD DEL USUARIO

Microsoft Windows 10 llegó a mediados de 2015 y constituyó el primer lanzamiento de una versión de Windows bajo el nuevo CEO, Satya Nadella. Con Windows 10, Microsoft está empezando a cumplir con su proyecto de reinvención mediante el cual pasará de ser una empresa de software a una enfocada en dispositivos y servicios, y pretende alcanzar la ambiciosa meta de los mil millones de dispositivos que usen su nueva versión de Windows en tres años. Sin embargo, para lograrlo, Windows 10 no solo debe mejorar la seguridad, sino que también necesita ganarse la confianza tanto de consumidores como empresas.

Características de seguridad

Con Windows 10, Microsoft hizo una gran inversión en materia de seguridad, que abarca mejoras para *Windows Defender*, tales como la posibilidad de detectar en memoria los códigos maliciosos que no crean archivos y ajustar la sensibilidad de los archivos de exploración dependiendo de su ubicación o desde dónde se descargaron: una incorporación que puede llegar a mejorar la detección de nuevos códigos maliciosos, pero que a su vez también puede aumentar el índice de falsos positivos. Asimismo, se mejoró la gestión y la exploración offline de modo que a los administradores de sistemas les resulte más fácil usar el software.

Con la creciente tendencia de políticas BYOD y la gran cantidad de trabajadores remotos, mantener los equipos infectados fuera de las redes corporativas es un desafío cada vez mayor. La solución que ofrece Microsoft es la funcionalidad *Conditional Access*, que sustituye la tecnología anterior de Microsoft, *Network Access Control o NAC*, por una solución más escalable y en la nube; su objetivo no solo es comprobar la salud de las PC conectadas a la red, sino también evaluar la integridad del sistema, lo que no era posible con la tecnología anterior.

Otra de las novedades de Windows 10 es la funcionalidad *Device Guard*, una combinación del sistema operativo Windows 10 con funciones de administración y características de hardware que les permiten a los administradores de sistemas bloquear los equipos en forma segura. Aunque el concepto es similar al de AppLocker (y en parte está basado en él), *Device Guard* se aplica a través de Secure Boot y no está destinado a las PC de uso general. A su vez, Secure Boot también tiene como requisito previo que los equipos que lo ejecutan cuenten con una interfaz UEFI y un chip TPM.

En su actualización actual, Device Guard está diseñado para sistemas de un solo uso rigurosamente administrados, tales como cajeros automáticos, pequeños comercios, puntos de venta y otros sistemas

> CON LA CRECIENTE TENDENCIA DE POLÍTICAS BYOD Y LA GRAN CANTIDAD DE TRABAJADORES REMOTOS, MANTENER LOS EQUIPOS INFECTADOS FUERA DE LAS REDES CORPORATIVAS ES UN DESAFÍO CADA VEZ MAYOR.

integrados donde solo se usa una única cuenta estándar (de utilizarse alguna).

Las mejoras de seguridad también se implementaron en el sistema operativo Windows 10. *Virtualization Based Security* (hasta hace poco conocido en Windows 10 como *Virtual Secure Mode*) traslada el sector central del sistema operativo (su núcleo) al hipervisor, junto con otros servicios de Windows que suelen ser el objeto de amenazas, como el Local Security Authority Subsystem Service (LSASS), el servicio que administra la seguridad del sistema operativo.

Microsoft Edge es el nuevo navegador web de Windows. Se diseñó desde su base para reemplazar Internet Explorer con el objetivo de proporcionar una experiencia de navegación moderna y segura. Su código base simplificado implica menos vulnerabilidades que los atacantes pueden llegar a aprovechar. Y aunque es una aplicación de escritorio, Edge se implementa como aplicación universal, es decir que se ejecuta en forma aislada, como si fuera en modo *sandbox*. Estas técnicas, junto con el cese del soporte para extensiones binarias como ActiveX y las mejoras en SmartScreen, convierten a Edge en un navegador Web más seguro que su predecesor, Internet Explorer. Aunque Internet Explorer sigue presente en Windows 10 para los sitios que lo requieran, Microsoft recomienda firmemente el uso de Edge.

Privacidad y aceptación del usuario

No sirve de nada que Microsoft cree la versión de Windows más segura de la historia si no logra que los usuarios confíen en él. Windows 10 introdujo un cambio en el tipo y la cantidad de información que Microsoft recopila sobre sus clientes, por lo que aún muchos dudan si actualizarán sus sistemas a la última versión del sistema operativo de escritorio insignia de Microsoft. De todas formas, la recopilación de datos y de telemetría realizada por Microsoft no es una novedad: la compañía inicialmente comenzó a recoger los informes de fallos y telemetría durante la era de Windows XP, y ahora solo vemos la continuidad de dichos esfuerzos.

Si bien el alcance de la recopilación puede ser algo nuevo para Microsoft, desde hace tiempo este nivel de recopilación viene siendo normal en sistemas operativos de empresas como Apple y Google, y Microsoft tan solo se está poniendo al día con esta práctica. Sin embargo, es la primera vez que se hace en sistemas Windows para equipos de escritorio, por lo que algunos usuarios y defensores de la privacidad están comprensiblemente preocupados por las intenciones de Microsoft.

Otro tema de preocupación son los nuevos procedimientos de actualización de Microsoft para Windows 10. Las actualizaciones de Windows 10 Home (la versión de Windows 10 que Microsoft ofrece para los equipos de consumidores finales) no solo se instalarán automáticamente, sino que serán obligatorias. Windows 10 Pro cuenta con una opción para posponer estas mejoras; sin embargo es algo temporal y la opción no está disponible cuando las mejoras en cuestión son para resolver vulnerabilidades de seguridad.

Las **empresas tendrán un nivel adicional de control** que les permitirá aceptar actualizaciones y decidir el momento de su instalación, pero aún así deberán aplicar todas las actualizaciones a la mayoría

→

No sirve de nada que Microsoft cree la versión de Windows más segura de la historia si no logra que los usuarios confíen en él.

de los equipos con Windows 10, excepto para ciertas licencias y casos de uso de Windows 10 Enterprise.

Esto marca un cambio importante, dado que los administradores de sistemas y los usuarios domésticos están acostumbrados a tener un control granular de las actualizaciones que desean aplicar y las que prefieren posponer, y, al combinarse con la decisión de Microsoft de no seguir publicando detalles sobre lo que soluciona cada actualización del sistema operativo, provocó la ansiedad en muchas personas que preferirían saber cuáles son los errores que se están reparando y qué impacto pueden tener dichas actualizaciones en sus equipos.

No cabe duda de que Windows 10 ha logrado grandes avances en materia de seguridad, pero las preocupaciones sobre la **privacidad y la transparencia** sobre lo que las actualizaciones pueden resolver se están acumulando, por lo que Microsoft tendrá que abordar estas inquietudes de los usuarios si piensa alcanzar sin inconvenientes su meta de mil millones de dispositivos que usen Windows 10 en tres años.

> NO CABE DUDA DE QUE WINDOWS 10 HA LOGRADO GRANDES AVANCES EN MATERIA DE SEGURIDAD, PERO LAS PREOCUPACIONES SOBRE LA PRIVACIDAD Y LA TRANSPARENCIA SOBRE LO QUE LAS ACTUALIZACIONES PUEDEN RESOLVER SE ESTÁN ACUMULANDO

9

Infraestructuras críticas: momento de preocuparse por la seguridad

- Sistemas críticos expuestos
- La gestión de los activos de información como factor clave
- Amenazas comunes atacando industrias indiscriminadamente
- El sector de la salud, uno de los más expuestos
- Dispositivos médicos con grandes vulnerabilidades
- Robo de registros: más que simples datos expuestos
- Conclusión: pensar en seguridad para evitar intrusiones

Autor
Camilo Gutiérrez Amaya
Sr. Security Researcher

9 INFRAESTRUCTURAS CRÍTICAS: MOMENTO DE PREOCUPARSE POR LA SEGURIDAD

Desde hace años la seguridad de los sistemas industriales se convirtió en tema de análisis y discusión; fundamentalmente, luego de la aparición de amenazas como **Stuxnet en 2010** y de que se comprobara la vulnerabilidad de estos sistemas ante ataques externos.

Cinco años después de este hecho y en los que surgieron otras amenazas- como **Flame** o **Duqu-,** es posible afirmar que los equipos de Seguridad Informática de las organizaciones se encuentran ante muchos desafíos para salvaguardar sus datos críticos de amenazas, que ya no discriminan el tipo de industria al que quieren atacar.

La pregunta entonces se hace muy clara: **¿están todas estas empresas e industrias preparadas para afrontar los desafíos venideros?**

Sistemas críticos expuestos

Como se dijo anteriormente, hace años que se empezó a considerar la importancia de garantizar la Seguridad de la Información en infraestructuras críticas, sin embargo, aún es posible encontrar casos que evidencian que todavía hace falta seguir mejorando en esta materia.

En gran medida, las principales falencias de seguridad se deben a que los sistemas operativos (SO) utilizados en estas plataformas son obsoletos. Además, los sistemas de control -ya sean PLC *(Programmable Logic Controllers)*, HMI *(Human Machine Interfaces)* o los sistemas **SCADA *(Supervisory Control And Data Acquisition)***- están diseñados para funcionar con SO como Windows XP, Windows 2000, Windows 98 e, incluso, Windows 3.11.

En esta línea, tampoco existe una política clara de actualización de los sistemas que controlan estas infraestructuras; cabe destacar que este punto excede a las industrias y llega hasta los fabricantes del hardware, quienes tienen una postura estricta- incluso bastante riesgosa- sobre el cambio o actualización de los SO que controlan su hardware. Muchos de los fabricantes prohíben el cambio o actualización de los sistemas que controlan el hardware, para garantizar su correcto funcionamiento.

En conclusión, las empresas se encuentran gestionando infraestructuras críticas con SO obsoletos, vulnerables y conectados a Internet, lo cual aumenta las posibilidades de un incidente. Así, entre los fabricantes y las industrias, es necesario que unan esfuerzos para actualizar sus infraestructuras y mitigar las brechas de seguridad que abren las puertas a posibles ataques.

La gestión de los activos de información como factor clave

Más allá del hecho de que en muchas industrias aún cuenten con sistemas operativos vulnerables, algo que también llama sumamente la atención es que los dispositivos de control, por la propia naturaleza de sus funciones, suelen estar conectados directamente a Internet para poder realizar tareas de mantenimiento y gestión. Esto presenta un importante riesgo de seguridad, ya que dicho acceso

→

Las empresas se encuentran gestionando infraestructuras críticas con SO obsoletos, vulnerables y conectados a Internet, lo cual aumenta las posibilidades de un incidente.

se encuentra disponible a toda hora, y si no se siguen unas medidas de gestión apropiadas, podría permitir el ingreso de personal no autorizado. Es así como la política de gestión debería contemplar la posibilidad de que el acceso se otorgue solo cuando se requiera realizar soporte, o que la comunicación se realice por medio de una conexión segura, como una VPN.

Adicionalmente a estas políticas, es necesario considerar la funcionalidad de mecanismos de control y protección, como los *firewalls*. Muchas empresas basan las configuraciones de estos dispositivos en reglas que controlan cuándo dos equipos pueden, o no, entablar una comunicación por un canal determinado. No obstante, no hay un análisis del tráfico de esa conexión porque cada sistema de control cuenta con protocolos específicos y son desconocidos para los *firewalls*. Por lo tanto estamos frente a protocolos de comunicación que son sencillos de interpretar y por lo tanto deberían configurar tareas de análisis en los *firewalls* actuales, para aumentar así la capacidad de control e identificación de protocolos propietarios propios de los sistemas industriales. Si bien ya existen algunos desarrolladores de *firewalls* industriales que están comenzando a implementar dispositivos con estas capacidades, el cambio de este hardware en las industrias es muy lento y aún queda mucho trabajo por hacer.

Sumado a los puntos anteriores, hay un problema estrechamente relacionado con la gestión del negocio y la parte de seguridad, y es que suelen manejarse como dos entidades distintas. Esto genera grandes inconvenientes en la comunicación y puede generar problemas de seguridad considerables para una empresa, dado que si desde la gestión del negocio se entiende a la seguridad como un "obstáculo" y no como algo integrado y esencial para el crecimiento de la compañía, la posibilidad de ocurrencia de incidentes de seguridad crece, originando en última instancia problemas para la organización y su negocio. La disponibilidad de determinados servicios industriales críticos, ya sean de la infraestructura nacional o corporativa, usualmente suele priorizar ante la correcta configuración e seguridad abriendo las puertas a posibles ataques remotos de los sistemas industriales expuestos en Internet.

Por último, en algunos casos, y para cumplir con los objetivos del negocio, se suele seguir una postura muy cuestionable desde el punto de vista de la seguridad, la tradicional frase "si funciona, no lo toques", lo que significa que en ocasiones, por temor a realizar un desajuste en algo que supuestamente funciona correctamente, los equipos de seguridad no hacen las tareas de mantenimiento correspondientes. Esto presenta varios problemas de seguridad, ya que la falta de actualización y revisión de estos sistemas podría generar una falla de los mismos o incluso un acceso indebido por parte de un atacante.

→ **La tradicional frase "si funciona, no lo toques", significa que los equipos de seguridad no hacen las tareas de mantenimiento correspondientes.**

Amenazas comunes atacando industrias indiscriminadamente

Cuando se piensa en los ataques que pueden sufrir diferentes tipos de industrias como energía, petróleo, minería y diferentes sistemas industriales, no solo se trata de amenazas avanzadas y complejas como **Stuxnet, Duqu** o **Flame.**

Durante 2015 se **reportaron casos** de compañías de energía atacadas por un

código malicioso llamado **Laziok,** usado para recolectar información de sistemas infectados, incluyendo el nombre de la computadora, el tamaño de la memoria RAM y del disco rígido, el tipo de CPU y el software antivirus.

Con esta información los cibercriminales podrían determinar si las computadoras son blancos viables para ataques posteriores. Lo curioso de estos casos es que la amenaza se propagaba a través de correos electrónicos con archivos adjuntos que trataban de explotar una vulnerabilidad en *Microsoft Office*. Algo más problemático aún, es que a pesar de que existe una solución a esta falla desde abril de 2012, muchas industrias todavía no la habían aplicado.

El sector de la salud, uno de los más expuestos

Además del sector industrial, en el último año la seguridad en la industria de la salud se ha puesto en el centro del debate. Durante 2015 y como parte del **Reporte de Investigaciones de Fuga de Información de Verizon,** se identificaron alrededor de 80 mil incidentes de seguridad- de los cuales **234 estuvieron relacionados a la salud**- y 2.100 fugas de información- 141 de ellas también de dicha industria.

Una gran cantidad de cuestiones de seguridad se han vuelto más evidentes, incluyendo principalmente la mala utilización o malas prácticas por parte de empleados, que representaron el 15% de los incidentes de la industria de salud en 2014 y que durante 2015 crecieron hasta convertirse en un 20%, de acuerdo al informe de Verizon antes citado.

Otra cuestión en la que las organizaciones de salud se han vuelto más vulnerables son los ataques a aplicaciones web y ataques de denegación de servicio (DDoS), dejando a esta industria un 4% por encima del promedio de todas las demás.

A lo anterior hay que sumar los resultados expuestos por el reporte del **Instituto Ponemon,** que reveló que la causa de las brechas de seguridad en instituciones relacionadas a la salud cambió de cuestiones accidentales a otras de índole intencional. Esto se explica en un aumento del 125% en los ataques cibercriminales con respecto a cinco años atrás, reemplazando a las laptops perdidas como la principal causa de la fuga de datos.

Además, el estudio de 2015 titulado **Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data** concluyó que *"la mayoría de las organizaciones no está preparada para responder a nuevas amenazas y no cuenta con los recursos adecuados para proteger la información de los pacientes"*. El 45% de las organizaciones confirmó que los ataques informáticos fueron la causa fundamental de las brechas, por encima del 40% de 2013.

Dispositivos médicos con grandes vulnerabilidades

Sumado a los problemas anteriores asociados con la gestión de la seguridad, también se encuentran aquellos que están los relacionados con las características de los nuevos equipamientos médicos. Todas estas mejoras están vinculadas, en gran medida, con nuevas funcionalidades que brindan conexión a Internet. Por ejemplo, en el caso de los dispositivos implantados (IMD) que permiten solucionar afeccio-

→

El reporte del Instituto Ponemon, que reveló que la causa de las brechas de seguridad en instituciones relacionadas a la salud cambió de cuestiones accidentales a otras de índole intencional.

nes de variada índole, no siempre se tienen en cuenta consideraciones en materia de seguridad y, por el contrario, están siendo subestimadas.

Las amenazas a estos dispositivos médicos son muy reales y existen muchos ejemplos de equipos médicos infectados por códigos maliciosos, en la mayor parte de los casos de manera inadvertida. De hecho, **durante 2014 fue reportada una vulnerabilidad en más de 300 dispositivos quirúrgicos** que podría permitir cambiar su configuración. Tal como pasa con la seguridad industrial, la conectividad es un aspecto crítico. A través de este punto es posible encontrar que la seguridad en las conexiones inalámbricas que realizan es a menudo muy pobre, y que la industria de equipamiento médico continúa relegando la inclusión de mecanismos de seguridad en sus dispositivos.

Por estos motivos, los dispositivos médicos son considerados un blanco fácil ya que presentan aplicaciones antiguas con un inadecuado nivel de seguridad. La gran mayoría de los dispositivos biomédicos no permiten modificaciones y no tienen la capacidad para correr agentes de autenticación de terceros dejando vulnerable el ingreso desde navegadores web.

En 2015 investigadores de seguridad descubrieron vulnerabilidades de sistemas médicos críticos, lo que las pone en riesgo de ser explotadas por atacantes. Dentro **del informe que presenta su investigación,** demostraron como a través de Shodan, que permite buscar ordenadores en Internet, pudieron encontrar **hasta 68 mil sistemas y equipos médicos vulnerables** de una misma entidad de salud en Estados Unidos que estaban expuestos a ataques.

Es por esta razón que el sector salud debe que tener mayor determinación al momento de planificar sus defensas; debe ser más rápido al realizar las evaluaciones de riesgo para asegurarse de que el dinero está bien invertido, y de que los recursos y activos se encuentran bien protegidos. Lo ideal es que las evaluaciones de riesgos se realicen en forma continua y no periódica. Esto ayuda a asegurar que los nuevos activos, las estrategias y las defensas tanto físicas como digitales se incluyan en los planes de negocio y respuesta a incidentes lo antes posible.

Robo de registros: más que simples datos expuestos

Es claro que los ataques y fallas descritos hasta ahora abren la posibilidad a que un ciberdelincuente recopile una gran cantidad de información particularmente de la industria de la salud, como por ejemplo nombres de pacientes, números de obras sociales, teléfonos, direcciones, direcciones de correo electrónico y otros datos personales. Sin embargo, también se podrían filtrar datos aún más críticos, como un registro médico que puede contener detalles sobre diagnósticos, medicaciones, etc. Esta información tiene mucho valor para los atacantes y de robarse, puede comercializarse, al igual que el resto de los datos personales anteriormente comentados, en un mercado negro mucho más específico.

Independientemente de dónde se obtenga la información, ya sean datos que pueden estar públicos online o muy específicos que fueron robados de informes médicos, si una persona llega a recopilar una gran cantidad de ellos podría comercializarla y hasta realizar dife-

→
Los dispositivos médicos son considerados un blanco fácil ya que presentan aplicaciones antiguas con un inadecuado nivel de seguridad.

rentes tipos de robo de identidad; entre ellos: crear identificaciones falsas, abrir cuentas bancarias y obtener tarjetas de crédito, cometer fraudes impositivos e incluso usarlos para contestar las preguntas de seguridad de acceso a cuentas online, desplazando así el ataque a nuevos horizontes digitales.

Está claro que las bondades de Internet y las redes inalámbricas son muy interesantes para este tipo de industria. Principalmente, permiten contar con un acceso instantáneo a una gran cantidad de información sobre datos médicos de los pacientes desde cualquier lugar con una conexión. No obstante, estos datos son muy sensibles y es indispensable no solo tener una protección realmente inteligente para los equipos que la alojan, sino también agregar barreras adicionales, como el cifrado y la doble autenticación, así como una segmentación saludable de la red y estrategias confiables de recuperación ante posibles incidentes.

Conclusión: pensar en seguridad para evitar intrusiones

Luego de analizar estos casos, es evidente que aún falta mucha concientización y educación en materia de Seguridad de la Información en empresas y administraciones públicas. Los atacantes siempre buscan la manera de acceder a un sistema por cualquier tipo de brecha que tengan disponible, y una vez que lograron vulnerar los perímetros pueden no solo robar información o infectar equipos para incorporarlos a una red maliciosa y usarlos a su merced, sino también alterar el correcto funcionamiento del equipamiento industrial.

Una muestra de la preocupación de proteger las infraestructuras críticas son las iniciativas de la Fundación Nacional para la Ciencia (*National Science Foundation*, en inglés) de los Estados Unidos, que entregó a la Universidad Cristiana de Texas (TCU) **aproximadamente 250 mil dólares para ayudarla a crear medidas efectivas** que protejan los dispositivos médicos de ciberataques. En esta misma línea, se encuentra la **Agencia Europea de Seguridad de la Información y las Redes (ENISA, por la sigla de *European Union Agency for Network and Information Security* en inglés)** que afirmó que durante 2016 enfocará su atención en el desarrollo de buenas prácticas en lo que refiere a "infraestructuras críticas inteligentes emergentes".

Las industrias que utilizan estos sistemas con grandes falencias de seguridad se encargan de brindar servicios esenciales para la población. Entre ellas se encuentran desde plantas potabilizadoras de agua, las que generan y distribuyen la electricidad, las que se encargan de la distribución del gas natural o incluso aquellas que manejan información médica. Se trata de sistemas que manejan información realmente sensible y de ahí la criticidad de los riesgos asociados y el impacto si alguno de ellos llegara a fallar o fuera vulnerado.

Si bien se han realizado algunos cambios en muchas de las industrias buscando mejorar la seguridad, aún falta mucho trabajo por realizar en los diferentes sectores. Para 2016 los ataques a este tipo de infraestructuras podrían incrementarse si no se sigue avanzando de forma rápida en su adecuada protección, por lo tanto todas las actividades vinculadas con la Seguridad Informática en este tipo de ambientes seguirá ganando terreno como un factor clave en la gestión.

→
Se trata de sistemas que manejan información realmente sensible y de ahí la criticidad de los riesgos asociados .

10

Leyes y Regulaciones: un esfuerzo en conjunto

- Cumplimiento de estándares y mejores prácticas de seguridad
- Leyes de protección de datos personales en el mundo
- Seguridad de la información: un esfuerzo compartido entre gobiernos, empresas y usuarios

Autor
Miguel Ángel Mendoza
Security Researcher

10 LEYES Y REGULACIONES: UN ESFUERZO EN CONJUNTO

El cumplimiento *(compliance)* es un elemento considerado esencial para el logro de los objetivos en las organizaciones dentro la gestión de seguridad de la información. Está relacionado a la conformidad con requisitos previamente establecidos y que son aplicables a las empresas de acuerdo a sus funciones y características, por lo que resulta mandatario satisfacer estas condiciones. Entre el conjunto de requisitos que las organizaciones buscan cubrir se pueden enlistar especificaciones consideradas en políticas, estándares, leyes o reglamentos.

En el ámbito de la seguridad de la información, algunos requisitos deben ser cumplidos de manera obligatoria, por ejemplo, las legislaciones enfocadas en proteger los datos personales de los usuarios o clientes de las empresas (generalmente aplicables al ámbito privado, aunque tampoco deben descartarse a las instituciones públicas). En el mismo sentido, las organizaciones comprometidas con la protección de la información propia o de terceros, cumplen con estándares o normas de seguridad que han sido adoptados de manera voluntaria.

Por lo tanto, sin importar si se trata de organizaciones públicas o privadas, grandes o pequeñas, lucrativas o no, la información sensible que procesan, almacenan o transmiten requiere de medidas de protección que pueden ser establecidas por iniciativa propia o bien, por alguna parte interesada como proveedores, socios, clientes o gobiernos. Tal como se ha visto en los últimos años, con fugas de información enormes como la de Sony, Ashley Madison o Target, la información personal de los usuarios y el compromiso de las empresas en el manejo y protección de esos datos son un tema más que importante y con una total vigencia en la actualidad y en lo venidero.

En este contexto, los requisitos establecidos por las normativas deben ser cumplidos para satisfacer las necesidades de seguridad, las cuales se establecen de acuerdo al valor de la información. Entre estos requisitos, los puntos que han tenido mayor relevancia en los últimos años están relacionados con las leyes de protección de datos y la adopción de estándares de seguridad.

Cumplimiento de estándares y mejores prácticas de seguridad

Las organizaciones pueden adoptar normativas por iniciativa del propio personal interesado en la protección de la información, o bien por cumplimiento con algún requisito contractual o regulatorio. En este sentido, se cuenta con marcos de referencia o estándares que avalan y certifican las medidas de seguridad adoptadas y adaptadas en las empresas.

Una referencia en temas de seguridad continúa siendo **ISO/IEC 27001,** un estándar internacionalmente utilizado para gestionar la seguridad de la información, que representa la experiencia acumulada de expertos en el tema. Se trata de un documento abierto, por lo que su implementación debe realizarse en función de las características, necesidades y condiciones de cada organización, sin importar su tipo o sus actividades.

La estructura del estándar se reduce a dos elementos básicos: las cláusulas de requi-

→

Las organizaciones pueden adoptar normativas por iniciativa del propio personal interesado en la protección de la información, o bien por cumplimiento con algún requisito contractual o regulatorio.

sitos para que una organización funcione alineada con un sistema de gestión de seguridad de la información (SGSI) y un conjunto de objetivos de control y controles de seguridad, que consideran distintos enfoques para la protección. A partir de ello, se busca que las organizaciones puedan gestionar los riesgos asociados a la información.

Bajo este principio las organizaciones han comenzado a alinearse a las directrices y buenas prácticas definidas en ISO/IEC 27001. Desde la publicación de la versión de 2005 y después con su actualización a la versión de 2013, el número de certificados emitidos ha crecido año a año. (Gráfico 13)

De acuerdo con un estudio de la Organización Internacional de Normalización (ISO), **durante 2014 se emitieron 23.972 certificados de ISO/IEC 27001** en todo el mundo, lo que representa un incremento de 7% respecto al año anterior. Comparado con años anteriores, ISO/IEC 27001 experimentó una leve desaceleración, con un crecimiento modesto, contrario a los pronósticos que consideraban periodos previos.

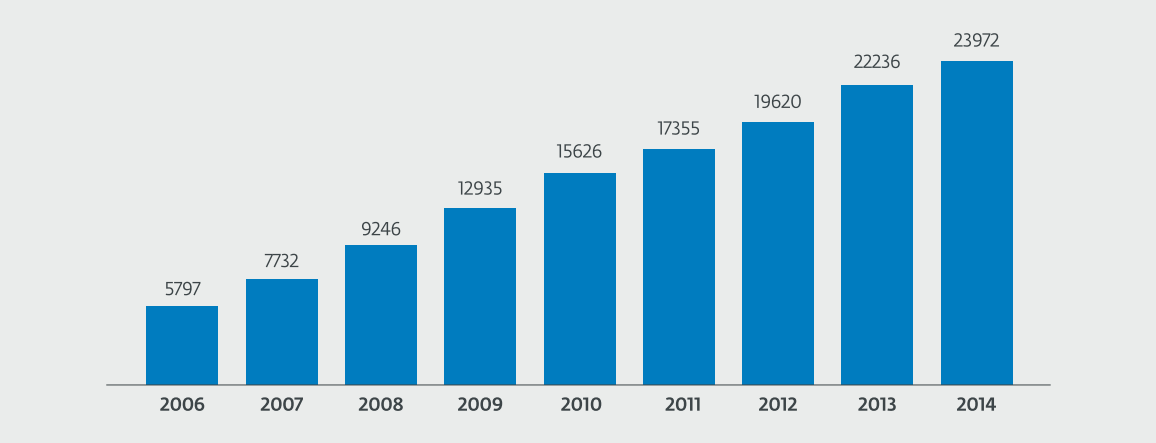
Japón encabeza la lista del sector de la seguridad de la información con 7.181 certificados, aunque el Reino Unido también ocupa un lugar destacado con el crecimiento más importante en términos absolutos, con 2.261 certificados obtenidos en 2014; en tercer puesto se ubica India con 2.170.

A partir de estos resultados, es evidente que se tiene una tendencia hacia el aumento de certificaciones en los últimos años a nivel mundial, pero también es cierto que se necesitan más esfuerzos en la materia dado que, por ejemplo, existen grandes brechas entre los países.

El siguiente mapa muestra la cantidad de certificados obtenidos por país, donde claramente se destacan Japón, Reino Unido, India y China, como los países de encabezan el número de organizaciones que han obtenido un mayor número de certificados ISO/IEC 27001. (Gráfico 14)

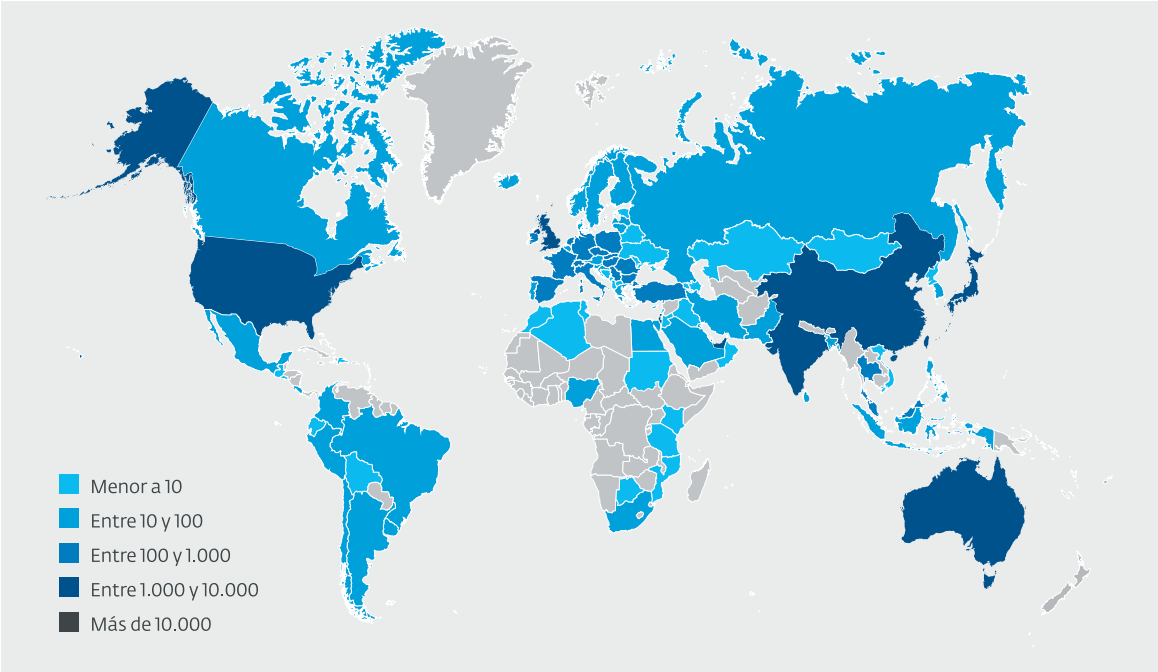
Aunque por sí misma una certificación no garantiza que las organizaciones puedan ser inmunes a las amenazas informáticas, el documento es una muestra

Gráfico 13 Certificaciones ISO / IEC 27001 a nivel mundial



Fuente: ISO

Gráfico 14 Certificaciones ISO / IEC 27001 a nivel mundial



Fuente: http://www.iso.org/iso/home/standards/certification/iso-survey.htm

de que se llevan a cabo acciones orientadas a la protección de la información, gestionan los riesgos y que la seguridad está considerada desde la alta dirección, cumpliendo tres aspectos fundamentales como son el gobierno corporativo, la gestión de riesgos y el cumplimiento (o GRC por sus siglas en inglés).

Leyes de protección de datos personales en el mundo

Por otro lado, otro tema de cumplimiento está relacionado con las leyes de protección de datos personales. En este sentido la privacidad adquiere mayor relevancia con el paso de los años, desde la aparición del derecho a la privacidad como parte de la Declaración de los Derechos Humanos, que establece que ninguna persona debe ser objeto de injerencias arbitrarias a su condición íntima.

Con el avance y acceso a nuevas tecnologías de información, cada vez más datos se encuentran en formato digital, lo que representa nuevos retos que exigen un balance entre el derecho a la intimidad de los individuos y la manipulación de su información por parte de terceros, como resultado del uso de la tecnología.

Este tipo de datos están referidos a cualquier tipo de información concerniente y asociada a una persona que permite identificarla, caracterizarla y determinar sus actividades, tanto públicas como privadas. Cada individuo es dueño de su información personal y es quien decide si la comparte o no, así como la forma en la cual debe ser tratada por las entidades que acceden a ella.

Entre los datos personales se encuentran aquéllos que identifican a la persona o permiten tener comunicación con su ti-

tular; datos relacionados con el empleo, sobre características físicas como la fisonomía, anatomía o rasgos de la persona. También considera información relacionada con la formación y actividades profesionales, datos relativos a sus bienes, o bien, información biométrica.

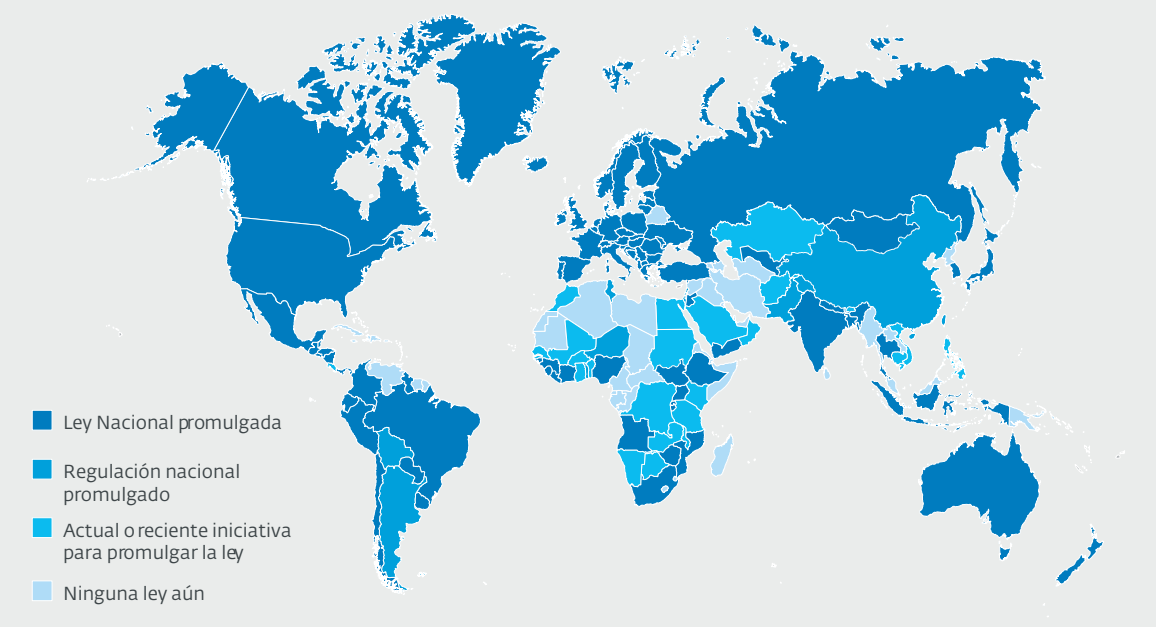
Además, otro tipo de información puede resultar sensible como los datos que involucran el ámbito privado de su titular cuyo uso indebido podría derivar en alguna afectación negativa, como la discriminación. Aquí se incluyen aspectos como el origen étnico, estado de salud, creencias religiosas, preferencia sexual, afiliación u opiniones políticas.

Por ello, organismos internacionales instan a los países a legislar en la materia. De acuerdo con un **estudio realizado a finales de 2014,** más de 100 países habían adoptado leyes de privacidad y protección de datos en posesión de gobiernos y empresas privadas. El estudio realizado por la organización Artículo 19, muestra los países que cuentan con este tipo de leyes o que cuentan con iniciativas pendientes para su adopción.(Gráfico 15)

Diferentes iniciativas de protección han generado una tendencia a la incorporación del derecho a la protección de datos personales a través de leyes y reglamentos desarrollados en distintas partes del mundo, puesto que se trata de un derecho universal que brinda la facultad para controlar a voluntad los datos personales de cada individuo.

Otro elemento impulsor de las leyes de protección de datos son los negocios. La privacidad se ha convertido en una condición necesaria para el comercio entre países, por lo que el incumplimiento de las normas de protección puede significar la pérdida de oportunidades de negocio. Los acuerdos internacionales de

Gráfico 15 Leyes de privacidad y protección de datos en el mundo



Fuente: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416

comercio que consideran la protección de datos personales, instan a los países a legislar en la materia.

Un ejemplo se encuentra en los **principios de privacidad de *safe harbor*** emitido en el año 2000, el cual desarrolla un framework para la recopilación, uso y retención de información personal transferidos de los países miembros de la Unión Europea a empresas de Estados Unidos, como parte del cumplimiento con la directiva en materia de protección de datos de la UE.

Sin embargo, el pasado 6 de octubre los acuerdos de *safe harbor* fueron declarados inválidos por una corte europea, ya que el Tribunal Europeo de Justicia consideró que el acuerdo contiene desperfectos debido a que permitió a las autoridades gubernamentales estadounidenses obtener acceso a la información de ciudadanos europeos.

El tribunal tomó la decisión a partir de las declaraciones de Edward Snowden, por las cuales considera que las agencias de inteligencia estadounidenses pudieron acceder de manera casi ilimitada a los datos, infringiendo el derecho a la privacidad considerados en los países miembros de UE.

> SIN DUDA, EL CUMPLIMIENTO DE NORMATIVAS ES UNA ACTIVIDAD NECESARIA PARA QUE LAS ORGANIZACIONES LOGREN SUS OBJETIVOS Y ALCANCEN SU MISIÓN.

Seguridad de la información: un esfuerzo compartido entre gobiernos, empresas y usuarios

Sin duda, el cumplimiento de normativas es una actividad necesaria para que las organizaciones logren sus objetivos y alcancen su misión, alineadas a requisitos que son impuestos de manera voluntaria o por alguna parte interesada.

Es posible pronosticar que la adopción de medidas de protección de los datos como una forma de autorregulación continuará vigente, sobre todo si consideramos que el desarrollo permanente de amenazas informáticas y la identificación continua de vulnerabilidades determina el dinamismo de los riesgos asociados a la información. Estos últimos factores, que podrían ser considerados como "externos" a los intereses de las organizaciones, son los que podrían inclinar la balanza hacia la decisión de adoptar y cumplir con normativas dada la importancia que los datos personales tienen hoy en día.

Además, la privacidad continuará siendo un tema a tratar en los próximos años si consideramos que la **filtración de información de inteligencia realizada en 2013 por Snowden,** relacionada con el control ejercido por el gobierno estadounidense sobre la privacidad de los datos de los ciudadanos y el mundo en general, continúa repercutiendo en las relaciones internacionales. Aquí nos encontramos con otro factor que podría continuar empujando a las organizaciones públicas y privadas, hacia la adopción y el cumplimiento de normativas: la presión que puedan ejercer los usuarios en pos de que sus datos personales sean protegidos.

→

Es posible pronosticar que la adopción de medidas de protección de los datos como una forma de autorregulación continuará vigente, sobre todo si consideramos que el desarrollo permanente de amenazas informáticas

El apego a las leyes o estándares nos muestra la relevancia que continúa adquiriendo la seguridad de la información, si se asocia con la protección de los datos y la privacidad. Para lograr los objetivos en la materia, se requiere la participación de los gobiernos interesados en legislar temas de seguridad y fomentar la creación de instituciones encargadas de hacer cumplir las leyes.

Por otro lado, las empresas que procesan la información de los usuarios en el marco de las normas, estándares, legislaciones o reglamentos; la participación de los usuarios a través de la aplicación de buenas prácticas de seguridad, y finalmente las empresas y organizaciones que tienen como principal propósito preservar la confidencialidad, integridad y disponibilidad de la información.

LA SEGURIDAD DE LA INFORMACIÓN, ASOCIADA A LA PROTECCIÓN DE DATOS Y A LA PRIVACIDAD, REQUIERE DE LOS ESFUERZOS DE LOS GOBIERNOS, EMPRESAS Y USUARIOS

11

Amenazas a los menores en la web

- Privacidad y sexting
- Grooming
- Ciberbullyng
- La legislación y el contrato social como prevención

Autor
Sebastián Bortnik
Research & Technology Manager

11 AMENAZAS A LOS MENORES EN LA WEB

La relación entre los menores de edad y las computadoras se ha convertido en los últimos años en una dependencia constante y sin horarios. **Ya no hay momentos de "conexión a Internet", como podía suceder hace algunos años, sino que en la actualidad los niños "viven conectados".** En el mundo de los nativos digitales, jóvenes que utilizan dispositivos informáticos desde muy pequeños; los smartphones, las tablets y las computadoras son herramientas de uso diario que los mantienen ya no solo conectados, sino "viviendo" en Internet. Su vida social se reparte entre lo que realizan en su mundo físico y su intensa vida en el mundo digital. **El 95% de los adolescentes poseen redes sociales** y allí dialogan, comparten e interactúan con sus amigos y, quizás, también con sus no-tan-amigos.

Sumado a las redes sociales, herramientas como WhatsApp, los juegos en línea y otros portales, potencian el uso comunicacional de Internet que hacen los menores y el tipo de datos que consumen y comparten allí. Asimismo, la comunidad de portales para menores de edad ha crecido y muchas de estas poseen servicios y funcionalidades pagas, por lo que **la variable de riesgo financiera asociada al uso de tarjetas de crédito también existe entre los niños y jóvenes.**

¿Cuán preparados están los adultos para acompañar esta situación? En los últimos años se ha acentuado la brecha digital entre padres e hijos. Encuestas afirman que el **50% de los padres no saben lo que hacen sus hijos en Internet** y uno de cada diez chicos indica que sus padres no conocen las tecnologías que ellos utilizan.

De esta manera, los ataques informáticos a los menores de edad en Internet se confirman como una tendencia cada vez más masiva, y en este contexto, **los ataques a la privacidad de los menores en Internet emergen como riesgo** basados en tres pilares: los datos personales, los datos financieros y la sexualidad.

Privacidad y sexting

La privacidad en Internet es el control que ejerce un usuario sobre su información para limitar la cantidad de personas autorizadas a obtenerla. Esto incluye datos personales, fotografías, archivos, etc. Cuando se trata de los menores de edad, la acción de control requiere habilidades que muchas veces los niños aún no poseen, tales como distinciones sociales sobre el riesgo asociado a compartir o no determinados datos, que se desarrollan durante la adolescencia o adultez.

Tanto las redes sociales como los juegos con funcionalidades sociales (chats, interacción, amigos, etc.) que están segmentados para el público infantil, son lugares factibles para que adultos puedan engañar a estos menores y acceder así a datos o información a través de la manipulación.

Por otro lado, los propios chicos muchas veces comparten información por demás sin ser conscientes de los alcances que esto podría tener. Un claro ejemplo de esto último es el **sexting,** término para referirse al envío de contenidos eróticos de forma voluntaria por medio de canales digitales.

Es una práctica común entre jóvenes y observa de forma numerosa entre grupos de adolescentes. Diversas encuestas ubican al menos un 25% de las menores entrevistadas como que alguna vez enviaron o

→
¿Cuán preparados están los adultos para acompañar esta situación? En los últimos años se ha acentuado la brecha digital entre padres e hijos.

publicaron electrónicamente fotos desnudas o semi desnudas. Por el otro lado, más de la mitad de los jóvenes afirma haber visto imágenes privadas que no estaban destinadas para ellos.

Muchas veces estos materiales que originalmente eran contenido erótico para una pareja, son compartidos a un grupo limitado de personas, sin tomar consciencia de la viralización que tiene este tipo de materiales. Los principales medios involucrados son aplicaciones de smartphones como por ejemplo WhatsApp, Kik, Snapchat o Twitter.

La Alianza por la Seguridad en Internet (ASI) estima que en México, uno de cada diez de los jóvenes de escuela secundaria envió imágenes propias, desnudas o semidesnudo, a conocidos o extraños a través de un teléfono móvil o una computadora. La empresa mexicana **Mattica coloca a México en primer lugar de envíos de sexting en América Latina.**

Grooming

El Grooming es uno de los delitos con mayor impacto sobre niños en la web en los últimos años. Se trata de la labor deliberada de un adulto hacia un menor a través de Internet para lograr que éste realice acciones de índole sexual; como enviar fotos eróticas o realizar acciones sexuales frente a una cámara web. En otros casos, esta acción es previa para poder coordinar un encuentro físico con el menor.

El adulto generalmente realiza contacto con el menor simulando ser de una edad similar, con el objetivo de ganarse la amistad de la víctima, creando así una conexión emocional con esta. Es decir, generar suficiente empatía con el fin de disminuir las inhibiciones del niño.

En muchos casos, una vez obtenido cierto material, comienza una extorsión hacia los menores amenazando con compartir el contenido erótico entre sus amigos y familiares si no siguen cumpliendo con los requerimientos del *groomer* (el individuo que realiza esta acción).

Este tipo de problemáticas, si bien no son nuevas, comienzan a emerger también en el mundo digital, dada la facilidad para los atacantes para poder explotar el anonimato, simular su identidad y generar acciones simultáneas con muchas potenciales víctimas. En la mayoría de los casos, la comunicación inicia en las redes sociales para luego extenderse en algunos de estos al mundo físico; llegando en casos extremos a situaciones ligadas a pedofilia o violaciones de niños.

Con respecto, a los *groomers*, pueden ser hombres o mujeres de cualquier edad y de cualquier estrato económico o social. Suele comenzar de manera online y en muchas ocasiones, el atacante invierte tiempo considerable durante este ciclo de elaboración de la problemática con el fin de ganarse la confianza de los menores; en diversas ocasiones cambiando su identidad, dando contención, obsequiando regalos, o simplemente pasando tiempo con ellos en alguna comunidad virtual o juegos en línea.

Para el 68,3% de los adultos encuestados por ESET Latinoamérica, el grooming es una amenaza muy frecuente: 1 de cada 4 encuestados confirmó conocer un niño que ha sido víctima de esta problemática. De estos menores, un 52,9% tiene entre 11 y 15 años, y un 33,7% entre 7 y 10.

Ciberbullyng

La misma falta de control que pueden tener los menores en Internet para identificar a algún adulto peligroso, se potencia para el criterio al momento de publicar contenidos, ya no solo en torno a la privacidad, sino también a los contenidos violentos o agresivos.

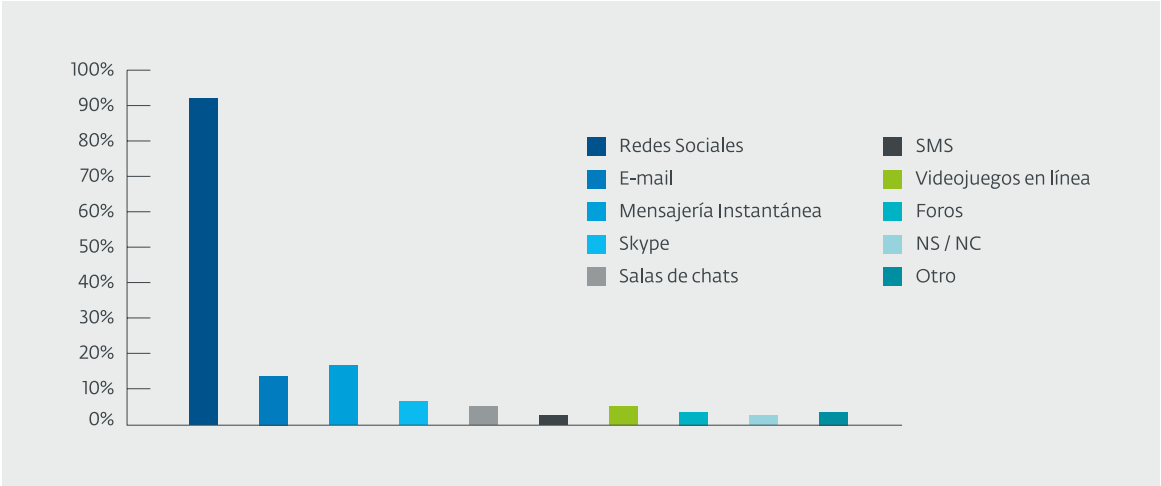
Se conoce como *ciberbullying* al hostigamiento a través de medios informáticos como redes sociales, chat, correo electrónico o sitios web. Consiste en molestar, amenazar, humillar o acosar a una persona utilizando dichos medios. Las formas más comunes son la difusión de falsos rumores, videos o fotos humillantes, y la creación de perfiles o sitios para agredir a la víctima. También puede ocurrir que el agresor se haga pasar por otra persona para decir cosas desagradables o amenace a la víctima con publicar su información personal. Generalmente, los afectados son personas vulnerables que son vistas como "diferentes" por quien las molesta. El *ciberbullying* se expande viralmente por la Web y es difícil de detener. Por tal motivo, resulta invasivo y dañino.

Muchos años atrás, el hostigamiento solo se realizaba de forma presencial en el colegio o en el club, pero desde la aparición del *ciberbullying*, este acoso es más constante y traumático para los chicos porque incluso se podría mantener y expandir a través de Internet y las Redes Sociales durante todo el día.

Aunque no es un hecho exclusivo de los menores, el *ciberbullying* es más difícil de controlar en este segmento. Además, puede que las agresiones permanezcan en el ciberespacio durante mucho tiempo, por lo que afectan a largo plazo a quien las sufre.

Según la encuesta antes mencionada, las redes sociales son el lugar más propenso a encontrar este tipo de incidentes, estando en segundo lugar la mensajería instantánea, especialmente a través de dispositivos móviles.

Gráfico 16 Sitios donde se han visto actos de cyberbullying

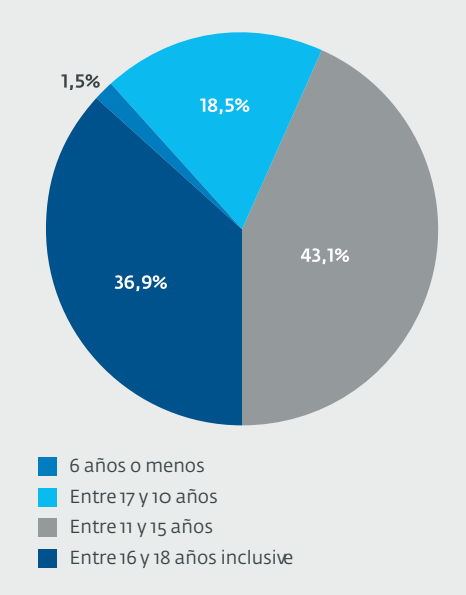


Fuente: ESET Latinoamérica

Según esta encuesta, el 42% de la gente encuestada conoce a alguien que recibió este tipo de amenazas por Internet, y el 80% de los afectados estaba en el rango de 11 a 18 años de edad, lo cual resulta curioso ya que por ejemplo, Facebook solo permite crear cuentas a personas mayores de 14 años.

Gráfico 17

Rangos de edades de víctimas de cyberbullying



Fuente: ESET Latinoamérica

Sin ser específicamente una amenaza informática, el *ciberbullyng* ya está formando parte de la agenda de riesgos de los menores en Internet y esta tendencia se profundizará los próximos años.

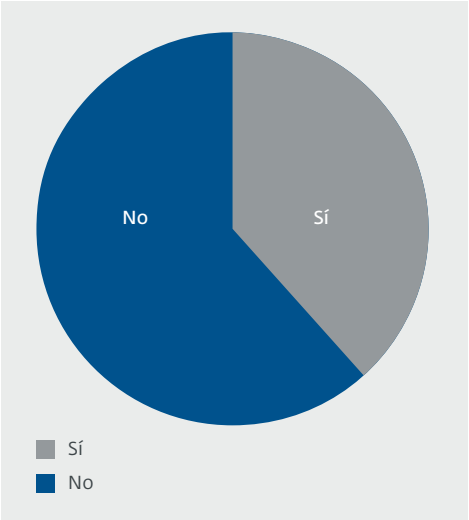
La legislación y el contrato social como prevención

El gran problema al que se enfrentan los adultos, es la capacidad para detectar este tipo de incidentes cuando ocurren entre los chicos por lo que los especialistas recomiendan prestar atención a sus **cambios de conducta o humor.** Si un menor presenta repentina tristeza, descenso en el rendimiento escolar o necesidad de soledad, es necesario charlar en confianza para entender qué le ocurre, ya que podría estar siendo víctima de alguna de las situaciones nombradas. En ese contexto, incluir su vida social digital en estos diálogos es fundamental para una correcta detección de cualquier inconveniente que pudiera estar ocurriendo.

Asimismo, las **aplicaciones de control parental** (tanto para **entornos de escritorio** como **móviles)** están comenzando a ser una herramienta indispensable para los adultos ante el creciente uso de las tecnologías por parte de los chicos. Lamentablemente la tendencia tiende a un incremento en las problemáticas ya explicadas. Según el 75% de los encuestados por ESET Latinoamérica, este tipo de problemáticas se da de forma frecuente,

Gráfico 18

¿Conoces alguna ley de tu país que penalice estos actos?



Fuente: ESET Latinoamérica

pero sin embargo sólo algo más que la mitad conoce sobre leyes que castiguen estos tipos de actos.

En este contexto, es fundamental seguir trabajando no solo en la creación, sino también en la promoción y divulgación de las leyes que den soporte y protección a los menores cuando estos incidentes ocurren en la red.

Esta legislación debe ser acompañada por las "normas del hogar", o sea, los estándares sociales. Padres y madres en sus hogares; y docentes y directivos en las instituciones educativas; son quienes deben agregar el uso de Internet dentro de un contexto de orden, con pautas y reglas claras.

Por ejemplo, la organización sin fines de lucro **Argentina Cibersegura propone el uso de un Contrato de Internet,** para que los padres dialoguen con sus hijos sobre estos temas y hagan acuerdos básicos para el uso de la computadora, el teléfono móvil, Internet, y las tecnologías en general.

Una de las mayores preocupaciones entre los adultos referida a este tema está vinculada a la forma de monitorear a los menores en redes sociales y juegos en línea. La comunicación y la concientización, forman la primera barrera de defensa para lidiar con este tipo de incidentes, y por eso es de vital importancia reforzarlos periódicamente entre niños y adultos, con la aspiración de acortar la brecha generacional y para que ante cualquier duda o sospecha, los menores puedan alertar a sus padres.

Es muy importante remarcar a los menores que los "desconocidos" con los que chatean, continúan siendo desconocidos. Es indispensable ocuparse de promulgar la noción de anonimato y falsa identidad en la web, explicándoles lo fácil que es generar un perfil con datos falsos.

En definitiva, la concientización en conjunto hacia adultos y menores, será fundamental para disminuir la negligencia con la que se abordan en muchos casos estas situaciones que son tendencia; y que seguramente lo seguirán siendo.

> EN DEFINITIVA, LA CONCIENTIZACIÓN EN CONJUNTO HACIA ADULTOS Y MENORES, SERÁ FUNDAMENTAL PARA DISMINUIR LA NEGLIGENCIA CON LA QUE SE ABORDAN EN MUCHOS CASOS ESTAS SITUACIONES QUE SON TENDENCIA.

12

Conclusión:
2016, el desafío de la seguridad

12 CONCLUSIÓN: 2016, EL DESAFÍO DE LA SEGURIDAD

A lo largo de las secciones que conforman este informe de tendencias del Laboratorio de ESET, repasamos y debatimos acerca de las problemáticas, los sucesos y desafíos que la seguridad deberá enfrentar en 2016 y también en los años venideros. Ante un panorama cada vez más desafiante y cambiante, será una constante la mayor preparación que necesitarán los equipos de seguridad de las empresas y también los usuarios hogareños para proteger su información de forma adecuada.

→ Desde ESET creemos que la respuesta debería ser que la seguridad esté en todos lados

Es cierto que los ataques se van complejizando cada vez más, que proteger toda la información de una empresa parece ser una tarea ardua y compleja y que encontrar personal capacitado y dispuesto a combatir los ataques es cada vez más difícil de hallar. Sin embargo, aunque **el panorama pueda parecer cuesta arriba,** desde los Laboratorios de ESET creemos que **es posible proteger a los usuarios y a las empresas, y que la combinación de la tecnología, la gestión y la educación son factores cada vez más importantes para estar protegidos.**

Tal como hemos planteado: el avance tecnológico brinda nuevas posibilidades a los usuarios y empresas, pero es un movimiento que no es ajeno a los cibercriminales. Si a esto se suma el factor de que varias de las esferas de la vida cotidiana se ven cruzadas por la tecnología, podemos llegar a la afirmación de que la inseguridad podría llegar a estar en "todos lados". Como consecuencia de este movimiento, desde ESET creemos que la respuesta debería ser que la seguridad esté en todos lados, y allí residen los desafíos para las empresas, gobiernos y usuarios.

Los desafíos que existen de cara al futuro no son imposibles: que, de acuerdo a **Gartner,** en 5 años nos encontremos con más de 25 mil millones de dispositivos conectados a Internet no significa que los usuarios deban entrar en una paranoia acerca de su privacidad y la seguridad de su información. Las empresas, además de **seguir invirtiendo en seguridad,** deberán evaluar las tecnologías que utilizan para **detectar y erradicar de sus redes las amenazas.** La implementación de diferentes capas de protección, o tecnologías que sean capaces de detectar un ataque en sus diferentes etapas, minimizan la exposición a ser víctimas de casos de fuga de información, secuestros de datos, acortando la brecha de exposición y los tiempos de respuesta de cara a incidente.

La habilidad de los empleados de una empresa para detectar un posible ataque, principalmente a través de campañas de *spear phishing* ayudan a reducir el tiempo de identificación de una ataque y esta tarea no es posible sin capacitación y educación en seguridad informática. Al mismo tiempo, **la capacitación en áreas de seguridad informática no se va a desarrollar en una empresa si la gerencia no lo ve importante y relacionado al negocio.** En otras palabras, si una empresa no se preocupa por la educación de sus usuarios y la correcta implementación de sus tecnologías de protección, será más propensa a ser víctima de un ataque informático.

En base a las predicciones de cara al futuro, es importante remarcar que **la seguridad de la información no es algo que depende de los avances que logren los cibercriminales en sus herramientas, sino de las medidas que usuarios, gobiernos y empresas adopten para proteger la información, los sistemas y la infraestructura.** Sí, se presentan desafíos que corresponden a diferentes

grupos, y cada uno tiene una responsabilidad en lo que respecta a la seguridad de la información que es necesario afrontar.

Desde la exigencia de los usuarios por **mayores niveles de seguridad y privacidad,** la importancia de proteger a los menores en Internet, las acciones que las fuerzas de seguridad deban llevar adelante para combatir al cibercrimen hasta la implementación de millones de nuevos dispositivos que interconecten la vida de los usuarios, empresas y gobiernos; son un desafío de cara a los años por venir. Y en el que las empresas de seguridad, las tecnologías de protección y la educación del usuario jugarán un rol clave en entender, analizar y proteger las más diversas tecnologías.

El rol del usuario está tomando cada vez más importancia en torno a la seguridad y esto es una tendencia que seguirá en aumento. Desde hace algunos años, los usuarios exigen una mayor seguridad a las empresas para resguardar sus datos, para proteger su información, pero más allá de estas exigencias, es aún más relevante que se eduquen sobre cómo estar seguros en Internet, entender qué es la seguridad y cómo protegerse. En otras palabras, los usuarios ya no pueden hacer la mirada a un lado en lo que respecta a su información ya que, en la actualidad, gran parte de ella se almacena en diferentes formatos digitales. **Tanto en 2016 como en los próximos años, los usuarios deberán tomar un rol más activo en su seguridad, capacitándose e informándose para poder proteger sus datos en compañía de empresas de seguridad y los servicios que utilicen.**

Además, por parte de las empresas se deberá trabajar los pilares de la tecnología, la gestión y la educación de su personal, aunque también hay que remarcar el rol de los Estados y las fuerzas de seguridad. Desde la promulgación de leyes que acompañen una evolución segura de las nuevas tecnologías, definiendo los estándares, las reglas y cómo respetar la privacidad de los usuarios, hasta asegurar los servicios e infraestructuras que acompañan el desarrollo de un país. Las **inversiones en investigación y desarrollo de nuevas tecnologías** deberán estar acompañadas de un plan de seguridad que evalúe y detalle las medidas de seguridad que deberán seguir para que sean seguros.

Es por ello, que ante una mayor superficie de ataques posibles, nuevas vulnerabilidades en tecnologías ampliamente utilizadas, el mayor desafío para 2016 estará enfocado a proteger las redes, los accesos a Internet y la manera en la que los dispositivos se intercomunican. Desde el *router* que brinda acceso a Internet en un hogar hasta la infraestructura de las ciudades más modernas, se deberán aplicar las mejores prácticas de seguridad para proteger los datos, la información y la privacidad. Este es un trabajo que necesita ser realizado en conjunto: con una participación más activa de los usuarios; una mirada más crítica de las empresas en cuanto a cómo protegerse y a tomar un rol proactivo en su seguridad; y en los gobiernos, de cara a acompañar el desarrollo económico garantizando las normas, para que tanto las empresas como los ciudadanos estén protegidos en caso de que se dé un incidente informático.

2016 será un año más que desafiante, pero no hay que afrontarlo con miedo, sino con una actitud proactiva, ocupándose de todas las aristas de la seguridad presentadas a lo largo de este informe, y poniendo foco todos los nuevos dispositivos que aparecerán en los próximos años.

→
2016 será un año más que desafiante, pero no hay que afrontarlo con miedo, sino con una actitud proactiva, ocupándose de todas las aristas de la seguridad presentadas a lo largo de este artículo.

Fundada en 1992, ESET es una compañía global de soluciones de software de seguridad que provee protección de última generación contra amenazas informáticas y que cuenta con oficinas centrales en Bratislava, Eslovaquia, y de Coordinación en San Diego, Estados Unidos; Buenos Aires, Argentina y Singapur. En 2012, la empresa celebró sus 20 años en la industria de la seguridad de la información. Además, actualmente ESET posee otras sedes en Londres (Reino Unido), Praga (República Checa), Cracovia (Polonia), Jena (Alemania) San Pablo (Brasil) y México DF (México).

Desde 2004, ESET opera para la región de América Latina en Buenos Aires, Argentina, donde dispone de un equipo de profesionales capacitados para responder a las demandas del mercado en forma concisa e inmediata y un Laboratorio de Investigación focalizado en el descubrimiento proactivo de variadas amenazas informáticas.

El interés y compromiso en fomentar la educación de los usuarios en seguridad informática, entendida como la mejor barrera de prevención ante el cada vez más sofisticado malware, es uno de los pilares de la identidad corporativa de ESET. En este sentido, ESET lleva adelante diversas actividades educativas, entre las que se destacan la Gira Antivirus que recorre las universidades de toda la región, el ciclo de eventos gratuitos ESET Security Day y ACADEMIA ESET, la plataforma de e-learning de seguridad de la información más grande en habla hispana.

Además, el Equipo de Investigación de ESET Latinoamérica contribuye a WeLiveSecurity en español, el portal de noticias de seguridad en Internet, opiniones y análisis, cubriendo alertas y ofreciendo tutoriales, videos y podcasts. El sitio busca satisfacer a todos los niveles de conocimiento, desde programadores aguerridos hasta personas buscando consejos básicos para asegurar su información en forma efectiva. Para más información visite: **www.welivesecurity.com/la-es**

www.eset-la.com

ENJOY SAFER TECHNOLOGY™