LA SEGURIDAD COMO REHÉN

Tendencias 2017

ENJOY SAFER TECHNOLOGY™

índice

Introducción

Desde hace varios años, el equipo de Investigación de ESET realiza el informe de Tendencias, en el cual, a partir de una revisión de los acontecimientos recientes más preponderantes en materia de seguridad informática, presentamos los principales tópicos que tendrán relevancia para empresas y usuarios durante el próximo año.

Introducción

Al analizar el estado y la evolución de la tecnología en la actualidad hay un aspecto que resalta: cada vez existen más dispositivos, más tecnologías y, por lo tanto, un mayor número de desafíos para mantener la seguridad de la información, sea cual sea el ámbito de su implementación.

Este panorama nos lleva a la conclusión de que la seguridad debe considerarse a todo nivel y por esta razón es que nuestro documento de Tendencias 2017 abarca aspectos muy diversos.

En los últimos años, la infección con códigos maliciosos se ha vuelto más preocupante y evidente para los usuarios de la mano de una tendencia que se ha ido consolidando: el ransomware. **Este tipo de malware ha llamado la atención de usuarios de todo el mundo al encontrarse con su información o sus sistemas tomados de rehén por parte de ciberdelincuentes.** Pero más allá de esta prominente tendencia, creemos que es preciso hablar de la seguridad en términos más amplios, ya que el éxito del ransomware se combina (y no debe opacar) lo que sucede en diferentes ámbitos con respecto a la protección de la información.

Entre todos estos temas, decidimos hablar de cómo ha ido cambiando el panorama alrededor del reporte de vulnerabilidades. El hecho de que año a año el número de vulnerabilidades críticas reportadas no solo no decaiga, sino que permanezca constante (e incluso con una pequeña tendencia creciente), marca **la necesidad de que los fabricantes y desarrolladores se comprometan más con el desarrollo seguro de los productos y servicios informáticos.**

Por otra parte, los cada vez más frecuentes ataques a grandes infraestructuras y servicios en Internet nuevamente ponen sobre la mesa la discusión acerca de la importancia de considerar la seguridad en las infraestructuras críticas, un tema que tiene su capítulo especial dado lo sensible de este tema. Asimismo, elegimos darle un trato especial al resguardo de la información en el sector de la salud. A lo largo de dicha sección se plantean los retos que tiene este sector, que maneja datos muy sensibles y críticos, por lo que se ha convertido en un blanco para muchos atacantes.

Algo ligado a los puntos anteriores, y a muchos de los temas que desarrollamos en las secciones de este informe, tiene que ver con las legislaciones en materia de seguridad y tecnología. Este es un tema con varias implicancias y que se trata en un capítulo aparte, ya que sin lugar a dudas es fundamental y los gobiernos de cada país deben asumir su importancia. Pero a lo largo de dicho capítulo se podrá ver que no solo es necesario que los Estados lleven adelante esta tarea, sino que esto representa un especial desafío a la hora de tratar de llegar a acuerdos con el sector privado y con las personas, en su doble carácter de usuarios y ciudadanos.

Pero no solamente estos temas generales se plantean como un desafío para el próximo año, sino que también existen problemáticas ligadas a cuestiones más "cotidianas" como las amenazas en dispositivos móviles o en la Internet de las Cosas (IoT). Esto no es una novedad; de hecho es algo de lo que venimos hablando desde 2012, cuando empezó el crecimiento en la detección de nuevas familias para Android

La seguridad debe considerarse a todo nivel y por esta razón es que nuestro documento de Tendencias 2017 abarca aspectos muy diversos.

y, un año más tarde, aparecieron los primeros códigos maliciosos que afectaban a televisores Smart y otros dispositivos inteligentes. Sin embargo, este año, y dado el crecimiento del ransomware, descubrimos una tendencia que aparece en el horizonte: el Ransomware of Things (RoT), es decir, la posibilidad que se abre para que los cibercriminales **secuestren un dispositivo y luego exijan el pago de un rescate para devolverle el control al usuario.**

Con respecto a la evolución de las amenazas en dispositivos móviles, los desafíos de seguridad para el próximo año son varios y a lo largo de la sección correspondiente los repasaremos. ¿Es el modelo de distribución de aplicaciones realmente el más adecuado? **¿Cómo se puede lograr el desarrollo seguro de aplicaciones en el contexto de incorporación de otras tecnologías como la realidad aumentada y la realidad virtual a estos dispositivos cada vez más poderosos?** ¿Por qué los controles de seguridad no avanzan con la misma velocidad?

Por otra parte, si bien podría considerarse dentro de la categoría de IoT, las consolas de videojuegos merecen un capítulo aparte. Esta industria ha ido adquiriendo cada vez mayor relevancia y contiene una amplia variedad de usuarios de equipos con grandes capacidades de procesamiento a su disposición, **lo que los convierte en un objetivo muy atractivo para los cibercriminales.** Y si a lo anterior sumamos la tendencia a la integración de consolas con el entorno de equipos de escritorio, se pone de manifiesto la necesidad de hablar sobre seguridad con este público, ya que supone nuevos vectores de ataque.

Pero las tendencias que presentamos en este informe no solo tienen que ver con riesgos y amenazas, sino que también es preciso remarcar algo que viene sucediendo en la industria de la seguridad. Se trata de una nueva generación de herramientas de protección **que basan su estrategia comercial en desconocer el desarrollo y evolución de las herramientas de seguridad en general.** Dada la importancia que tiene este tema, y para evitar confusiones, nos propusimos desmitificar y aclarar lo que se ha venido constituyendo como soluciones de seguridad de "próxima generación" o "next-gen".

Existe un punto en común entre todas estas secciones y, en líneas generales, en casi todos los temas relacionados a la seguridad de la información: se trata ni más ni menos que de la educación y concientización de los usuarios. La velocidad con la que aparecen nuevas tecnologías, reportes de ataques, familias de malware o fallas de seguridad de impacto global **hacen de la seguridad un desafío cada vez más importante para las empresas, los gobiernos y los usuarios alrededor del mundo.** A la vez, se hace cada vez más evidente la importancia de la educación y concientización en materia de seguridad para impedir que las amenazas sigan avanzando. A lo largo de la sección correspondiente, repasaremos las diferentes problemáticas asociadas a este tema y veremos que la educación de los usuarios no está acompañando la velocidad con la que aparecen las nuevas tecnologías y las amenazas asociadas a ellas.

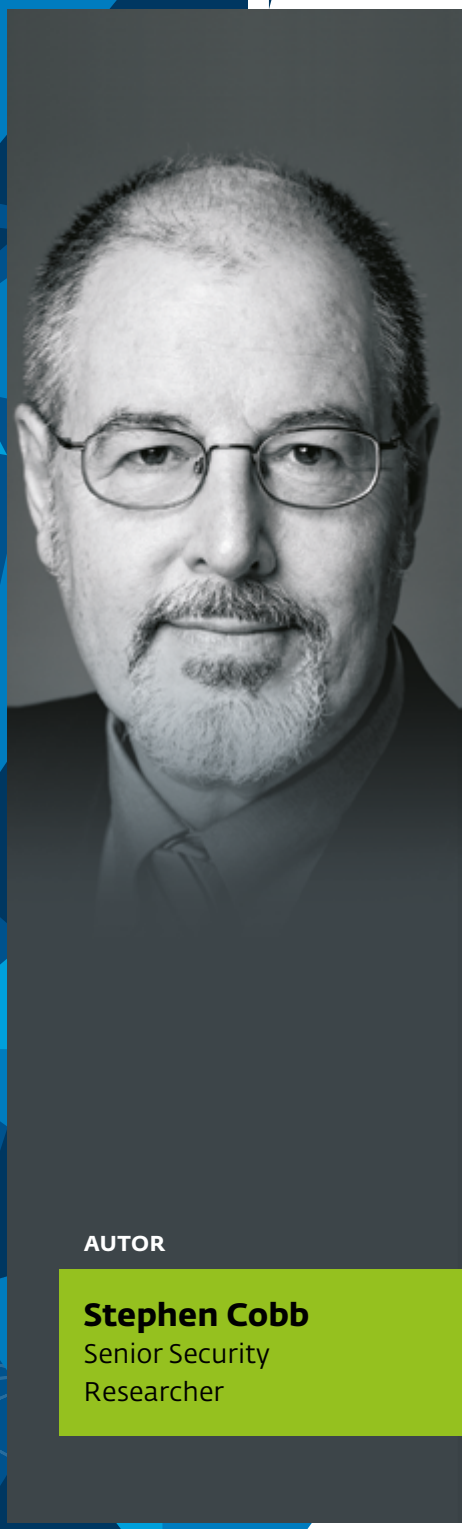
Es un placer para nosotros presentarles el documento que preparamos desde los Laboratorios de ESET a nivel global para plantear los desafíos en materia de seguridad que se deberán enfrentar en 2017. Nuestra idea es que puedan disfrutar de todo el documento, o bien que puedan leer sobre aquellas temáticas que más les interesen o con las que se identifiquen.

En definitiva, **a lo que apuntamos es a que los usuarios puedan conocer qué es lo que les espera en materia de seguridad, con el objetivo de poder estar mejor preparados para encarar los desafíos asociados** y, así, poder estar más protegidos.

Existe un punto en común entre todas estas secciones: la educación y concientización de los usuarios.

RoT:
el Ransomware de las Cosas

- Amenazas pasadas y futuras
- Cómo detener el RoT



AUTOR

Stephen Cobb
Senior Security Researcher

1

RoT: el Ransomware de las Cosas

De todas las tendencias de 2016, lo que más me preocupa es la disposición de algunas personas a participar de las siguientes tres actividades a escala: secuestrar sistemas informáticos y archivos de datos (mediante ataques de ransomware); denegar el acceso a datos y sistemas (con ataques de Denegación de Servicio Distribuido o DDoS); e infectar dispositivos que forman parte de la Internet de las Cosas (IoT, del inglés).

Lamentablemente, creo que estas tendencias continuarán en 2017 y es posible que incluso se vayan combinando a medida que evolucionen. Algunos ejemplos podrían ser utilizar los dispositivos IoT infectados para extorsionar sitios web comerciales con la amenaza de lanzar un ataque de DDoS, o bloquear los dispositivos IoT para pedir el pago de un rescate, a lo que yo llamo "jackware".

Amenazas pasadas y futuras

El uso indebido de los sistemas informáticos para extorsionar a los usuarios y sacarles dinero es casi tan antiguo como la computación misma. En 1985, un empleado de TI de una empresa de seguros de los Estados Unidos programó una bomba lógica para borrar registros vitales si alguna vez lo despedían. Dos años más tarde efectivamente lo despidieron y borró los registros, lo que condujo a la primera condena por este tipo de delitos informáticos. En 1989, se observó un tipo de malware que usaba el cifrado para secuestrar archivos y pedir rescate, como cuenta David Harley. Para el año 2011, la actividad de bloquear las computadoras para pedir rescate ya había comenzado a tomar nuevas formas cada vez más despreciables, tal como explica mi colega Cameron Camp.

Entonces, **¿de qué forma estos elementos evolucionarán o se fusionarán en el transcurso de 2017?** Algunas personas se han estado refiriendo al año 2016 como "El año del Ransomware", pero me preocupa que dentro de poco los titulares pasen a ser: "El año del Jackware". **El jackware es el software malicioso que intenta tomar el control de un dispositivo, cuyo objetivo principal no es el procesamiento de datos ni la comunicación digital.**

Un buen ejemplo son los "automóviles conectados", como vienen muchos de los modelos más recientes en la actualidad. Estos vehículos realizan una gran cantidad de procesamiento de datos y de comunicaciones; sin embargo, esa no es su función principal: su objetivo primordial es llevarte desde el punto A hasta el punto B. Entonces, **piensa en el jackware como una forma especializada de ransomware.** Con el ransomware tradicional, como Locky y Cryptolocker, el código malicioso cifra los documentos del equipo y exige el pago de un rescate para desbloquearlos. En cambio, **el objetivo del jackware es mantener bloqueado un automóvil u otro dispositivo hasta que pagues el rescate.**

El escenario de una víctima de jackware puede ser el siguiente: en una helada mañana de invierno abro la aplicación de mi automóvil instalada en el teléfono para arrancarlo y calentar el motor desde la comodidad de mi cocina, pero el coche no enciende. En cambio, aparece un mensaje en mi teléfono diciéndome que tengo que entregar X cantidad de moneda digital para

Algunos se refieren a 2016 como "El año del Ransomware". Me preocupa que dentro de poco los titulares sean "El año del Jackware".

reactivar mi vehículo. Afortunadamente (y pongo énfasis en esto): **el jackware, hasta donde yo sé, todavía solo existe en teoría.** Aún no ocurre en el mundo real o como se dice en la industria de la seguridad de la información, "in the wild".

Pero si nos basamos en las experiencias pasadas, debo admitir que **no tengo mucha fe en que el mundo sea capaz de detener el desarrollo y despliegue del jackware.** Ya hemos visto que una empresa automotriz puede vender más de un millón de vehículos con vulnerabilidades que podrían haber sido aprovechadas por el jackware: por ejemplo, el caso del Jeep Fiat Chrysler que salió en todas las noticias del año pasado.

Otro problema de gravedad similar fue la aparente falta de planificación por parte de la empresa para corregir dichas vulnerabilidades en el proceso de diseño del vehículo. Una cosa es vender un producto digital en el que más tarde se descubren errores (de hecho, esto es prácticamente inevitable), **pero otra muy distinta y mucho más peligrosa es vender productos digitales sin un medio rápido y seguro de corregir las posibles fallas.**

Aunque la mayoría de las investigaciones y los debates sobre el hacking de automóviles se centran en los problemas técnicos de los vehículos, es importante darse cuenta de que **una gran cantidad de dispositivos con tecnología IoT requieren un sistema de soporte que va mucho más allá del propio dispositivo.** Ya encontramos este problema en el año 2015 con VTech, un dispositivo de juegos perteneciente a la Internet de las Cosas para Niños (IoCT, del inglés). La poca seguridad en el sitio web de la empresa expuso los datos personales de los niños, recordándonos a todos la gran cantidad de superficies de ataque que crea la IoT.

También vimos este problema de infraestructura en 2016, cuando algunas cuentas de Fitbit tuvieron problemas (para ser claros, los dispositivos de Fitbit en sí no fueron vulnerados, y Fitbit parece tomarse en serio la privacidad). Este año también se descubrieron errores en la aplicación Web online para ConnectedDrive de BMW, que conecta los vehículos BMW a la IoT. Por ejemplo, puedes utilizarla para regular la calefacción, las luces y el sistema de alarma de tu casa desde el interior de tu vehículo.

La posibilidad de que las funcionalidades y la configuración de un sistema propio de un vehículo se puedan administrar de forma remota **a través de un portal que podría ser vulnerado es, como mínimo, inquietante.** Y siguen apareciendo nuevas quejas por la inseguridad vehicular, como este Mitsubishi con Wi-Fi, o la posibilidad de atacar radios para robar automóviles BMW, Audi y Toyota.

Aunque inicialmente pensé en el jackware como una evolución del código malicioso orientado específicamente a vehículos, pronto quedó claro que esta tendencia podría manifestarse en un ámbito mucho más amplio: pensemos en el **Ransomware de las Cosas** (RoT por Ransomware of Things en inglés). Una historia escalofriante de una ciudad de Finlandia muestra una de las posibles direcciones que puede llegar a tomar esta amenaza, ya que un ataque de DDoS dejó fuera de servicio el sistema de calefacción en pleno invierno. Si bien no hay indicios de pedidos de rescate, **no requiere mucha imaginación saber que ése será el siguiente paso.** "¿Quieres que el sistema de calefacción vuelva a funcionar? ¡Entonces paga!".

La tendencia del jackware podría manifestarse en un ámbito mucho más amplio: el Ransomware de las Cosas.

Cómo detener el RoT

Para que los dispositivos de la IoT no se conviertan en víctimas del RoT, deben ocurrir varias cosas en dos ámbitos diferentes de la actividad humana. **El primero de ellos es el técnico,** donde implementar la seguridad en una plataforma vehicular constituye un reto considerable. Las técnicas tra-

dicionales de seguridad, como el filtrado, el cifrado y la autenticación pueden llegar a consumir una enorme capacidad de procesamiento y ancho de banda, lo que puede sobrecargar los sistemas, algunos de los cuales operan con una latencia muy baja.

Las técnicas de seguridad como las barreras de aire y la redundancia tienen la tendencia de incrementar considerablemente el costo de los vehículos. Y sabemos que el control de costos siempre fue un requisito fundamental para los fabricantes de automóviles, hasta el último centavo.

El segundo ámbito en el que es necesario actuar para detener el RoT es **en la creación de medidas y en la política.** Las perspectivas aquí no son nada buenas, ya que hasta ahora el mundo ha fracasado estrepitosamente cuando se trata de disuadir los delitos cibernéticos.

Estamos presenciando un fracaso colectivo internacional para prevenir la evolución de una infraestructura criminal próspera en el ciberespacio, que ahora ya está amenazando todos los tipos de innovaciones en tecnología digital, desde la telemedicina hasta los drones, los grandes grupos de datos y los vehículos que se manejan en forma automática. Por ejemplo, como se menciona en la sección "Desafíos e implicaciones de legislaciones sobre ciberseguridad" de este documento, los políticos involucrados no aprobaron la legislación en 2016 que ayudaría a proteger la red inteligente, a pesar del apoyo bipartidista. Para que quede claro, **los términos como el RoT y el jackware no están pensados para provocar alarma. Simbolizan las cosas que pueden llegar a pasar si no hacemos lo suficiente durante 2017 para evitar que se conviertan en una realidad.**

Pero me gustaría terminar con **algunas noticias positivas sobre este tema.** En primer lugar, una variedad de agencias gubernamentales están intensificando sus esfuerzos para hacer que la IoT sea más segura.

En 2016, se publicaron los documentos Principios estratégicos para proteger la Internet de las cosas (en PDF) del Departamento de Seguridad Nacional de los Estados Unidos, y Publicación especial 800-160 del NIST (en PDF). El título completo de este último es *"Consideraciones de Ingeniería de Seguridad Informática para un Enfoque Multidisciplinario en la Ingeniería de Sistemas Seguros Confiables"*. El NIST es el Instituto Nacional de Estándares y Tecnología del Departamento de Comercio de los Estados Unidos. A lo largo de los años, esta agencia ha ejercido una influencia positiva en muchos aspectos de la ciberseguridad.

Esperamos que estos esfuerzos, junto a muchos otros en todo el mundo, **nos ayuden en 2017 a avanzar hacia la protección de nuestra vida digital contra aquellos que optan por utilizar indebidamente la tecnología para extorsionarnos.**

Por último, la evidencia de que podríamos estar progresando, al menos en términos de la mayor toma de conciencia pública sobre el potencial de la IoT para ocasionar problemas (así como sus beneficios y mejoras en la productividad), proviene de un tipo diferente de publicación: los resultados de una encuesta a consumidores de ESET. La encuesta titulada "Nuestras vidas digitales cada vez más conectadas" reveló que más del 40 por ciento de los adultos estadounidenses no confiaban en que los dispositivos IoT fueran seguros y estuvieran protegidos. Además, más de la mitad de los encuestados indicó que desistieron de comprar un dispositivo de la IoT porque les preocupa la privacidad y la seguridad.

¿La combinación del **sentimiento del consumidor y la guía gubernamental** será suficiente para obligar a las empresas a hacer sus **productos de la IoT más resistentes** al abuso? **Lo descubriremos en 2017.**

Estamos presenciando un fracaso colectivo internacional para prevenir la evolución de una infraestructura criminal próspera en el ciberespacio.

La educación en seguridad, una responsabilidad a nivel social

- Cambian las amenazas, pero la propagación se mantiene
- Cibercrimen: una actividad despiadada y eficiente
- La educación no es solo cuestión de edad
- La paradoja actual: más información, menos sensación de seguridad
- Pequeños cambios hacen grandes diferencias
- La educación hace la diferencia

AUTOR

Camilo Gutiérrez
Head of Awareness & Research

La educación en seguridad, una responsabilidad a nivel social

Hay una amenaza que lleva muchos años entre nosotros y que durante 2016 cumplió 25 años de haberse masificado a través de correos electrónicos.

Millones de usuarios en la red se habrán encontrado con ella pero a pesar de que muchos la puedan identificar, la realidad es que todavía hay personas que pueden verse envueltas por su engaño, unas por inocentes y desconocedoras, otras porque por simple curiosidad contestan para ver qué va a pasar y al final quedan atrapadas.

Si aún no saben de qué hablo, vamos a develar el misterio: **se trata de la famosa "Estafa Nigeriana" o "Estafa 419".** El origen de este tipo de engaño se remonta al siglo XIX y probablemente desde antes, con cartas ofreciendo repartir un jugoso tesoro. Pero esta estafa centenaria, lejos de desaparecer, **tomó fuerza con la evolución de la tecnología** y con el tiempo aparecieron múltiples variantes que migraron al correo electrónico.

Después de tanto tiempo, aún se siguen viendo mensajes en redes sociales y páginas web con el mismo tipo de engaños: que eres el visitante número 1.000.000, que te ganaste una lotería, que fuiste elegido para un viaje soñado son solo algunas de las excusas. Pero si las amenazas informáticas han venido evolucionando en los últimos años y ya hasta hablamos de ataques dirigidos, ciberguerra y APT, **¿cuál es la razón de que se siga viendo este tipo de engaños?**

Cambian las amenazas, pero la propagación se mantiene

Hace apenas cinco años, en nuestro informe de Tendencias 2012, hablamos de la creciente tendencia del malware en dispositivos móviles, donde amenazas como las botnets estaban a la cabeza. En los últimos años, los riesgos han ido evolucionando: empezamos a hablar de ciberespionaje y ataques dirigidos, de amenazas a la privacidad y los retos de seguridad en los nuevos dispositivos IoT y **para 2017, creemos que el ransomware seguirá aumentando su cantidad de víctimas.**

Sin embargo, todos estos tipos de amenazas que han ido cambiando con el tiempo **tienen un factor en común: el usuario como punto de entrada.** Sea un correo electrónico, un dispositivo USB abandonado adrede en un garaje o un mensaje en una red social o una contraseña débil, **los atacantes siguen encontrando en el comportamiento inocente y en muchos casos irresponsable de los usuarios** la posibilidad de comprometer la seguridad de un sistema.

Lamentablemente, esta realidad seguirá siendo la que aprovechen los atacantes durante 2017 y en años posteriores. La realidad es que a pesar de que puedan existir vulnerabilidades en dispositivos o aplicaciones que le permitan a un atacante tomar el control de un sistema, **la forma más sencilla de hacerlo será a través del engaño a los usuarios.** ¿Por qué habría de invertir horas en desarrollar un exploit, cuando con un simple correo electrónico puede lograr el mismo tipo de acceso a los sistemas? O desde otro punto de vista: ¿por qué un ladrón se tomaría el esfuerzo de cavar un túnel para entrar a una casa si solo tiene que llamar a la puerta?

¿Por qué un ladrón se tomaría el esfuerzo de cavar un túnel para entrar a una casa si solo tiene que llamar a la puerta?

Cibercrimen: una actividad despiadada y eficiente

Es difícil negar que durante 2017 se seguirán observando evoluciones de las familias de códigos maliciosos, que **el ransomware seguirá su infame reinado como la amenaza con mayor crecimiento y que de a poco veremos más amenazas para dispositivos IoT.**

El cibercrimen se ha llegado a catalogar como una actividad despiadada, donde hasta sectores como el de la salud se ven amenazados e infraestructuras como las de los cajeros automáticos están en un riesgo latente a nivel mundial.

Además, durante 2016 quedó claro cómo los cibercriminales de la actualidad vienen armados no solo con diferentes tipos de software malicioso y técnicas de Ingeniería Social, sino también con "planes de negocio" **para extorsionar a sus víctimas y obtener algún tipo de ganancia económica.**

Estamos frente a la necesidad de dejar de hablar genéricamente sobre los riesgos de seguridad. **Es necesario que los usuarios, ya sea en la empresa o a modo personal, reconozcan los ataques que pueden afectarlos**. Desde un fraude por correo electrónico hasta un secuestro de información, todos deben ser concebidos como factibles y es necesario tomar las medidas de concientización y tecnológicas para evitarlos.

La educación no es solo cuestión de edad

El mundo digital está habitado por dos tipos de actores: **los nativos y los inmigrantes digitales**. Los primeros tienen incorporado el uso de la tecnología en la mayoría de los aspectos de su vida diaria desde temprana edad; en cambio, los segundos la usan para resolver muchas de sus actividades diarias a pesar de que tuvieron que adaptarse y acostumbrarse a hacerlo.

Sería lógico de esperar que los nativos digitales sean menos susceptibles a este tipo de engaños. Sin embargo, este año, un estudio del BBB Institute dejó en evidencia que **los jóvenes de entre 25 y 34 años son más susceptibles a scams,** mientras que otros estudios demuestran que los más jóvenes son los que tienen los comportamientos más riesgosos al momento de navegar en Internet, tales como conectarse a redes Wi-Fi poco seguras, conectar dispositivos USB que les dan terceros sin mayores cuidados y la poca utilización de soluciones de seguridad.

Por otra parte, si bien los inmigrantes digitales pueden ser más cautelosos al momento de utilizar la tecnología, nos encontramos con que muchas veces pueden ser víctimas de ataques o tener comportamientos poco seguros. Generalmente, **se debe al desconocimiento de las características de seguridad que pueden tener los diferentes dispositivos** o a la falta de información sobre el alcance de las amenazas informáticas y el cuidado que se debería tener.

En definitiva, no importa la edad. **La necesidad de que todos los usuarios conozcan sobre las amenazas, la forma en que actúan y las mejores alternativas para proteger sus dispositivos** son puntos en los cuales los usuarios deben enfocarse para protegerse.

La paradoja actual: más información, menos sensación de seguridad

Sin lugar a dudas, hace ya casi cuatro años, después de las revelaciones de Snowden, **la sensación de seguridad en relación a la información es cada vez menor**. Lo paradójico es que **en la actualidad hay más información acerca de lo que pasa con ella.**

Sentirse vigilados es una preocupación para muchos usuarios y precisamente

Es necesario que los usuarios, ya sea en la empresa o a modo personal, reconozcan los ataques que pueden afectarlos.

una de las lecciones más importantes aprendidas a partir de las revelaciones de Snowden: si se autoriza a alguien a actuar en secreto y se le adjudica un presupuesto considerable, no se puede suponer que, por más que sea buena persona, **va a hacer lo correcto, de la forma correcta y sin consecuencias perjudiciales.**

Sin embargo, **no se trata de volverse paranoico o pensar en no tener ningún tipo de conexión en Internet.** Un reto importante a enfrentar es **la necesidad de educarse acerca de cómo protegerse en la red,** qué tipo de información publicar y cuáles son las medidas de protección que van a permitir garantizar la seguridad y privacidad de la información.

Pequeños cambios hacen grandes diferencias

Desde ESET creemos firmemente que la seguridad no se trata solamente de una solución tecnológica, ya que también **hay un componente humano que es necesario proteger.** Si bien los esfuerzos de concientización en seguridad informática ya son una realidad en muchos ámbitos de la vida actual, hay muchos usuarios que aún no tienen una formación adecuada en estos temas. Y aunque muchos reconocen las amenazas para computadoras, **aún no lo hacen en dispositivos móviles y mucho menos en dispostivos IoT.**

De acuerdo a encuestas realizadas por ESET, **solamente el 30% de los usuarios utiliza una solución de seguridad en sus dispositivos móviles[1],** a pesar de que más del **80% reconoce que los usuarios son los que tienen la mayor cuota de responsabilidad** al momento de caer en engaños por no tomar consciencia ni educarse sobre las diferentes estafas.

Durante estos próximos años veremos cómo las amenazas se empiezan a propagar hacia todo tipo de dispositivos conectados a Internet y que manejen información sensible. Así que **es necesario que se piense la seguridad en todo momento y contexto,** desde un dispositivo de uso personal con conexión Wi-Fi hasta infraestructuras críticas conectadas y manipuladas de forma remota a través de Internet.

Es una realidad que todas las tecnologías cambian rápidamente y cada vez hay más modos de infección, que pueden ser fácilmente aprovechados por los atacantes si los usuarios no están educados en estos temas. Por ello, no se puede permitir que el avance de la tecnología se vuelva en contra del usuario.

Para 2017, las tendencias en materia de protección deberán acompañar la realidad de los incidentes de seguridad que se están viendo, y por esta razón es primordial la educación. Si los usuarios reconocen que el uso de una contraseña como medida única puede representar un riesgo de fuga de información, sabrán que adoptar un mecanismo de doble autenticación, que añade una capa adicional de seguridad, va a marcar una diferencia a su favor. Así que **el desafío es, además de reconocer las amenazas, capacitarse en el uso de las herramientas de seguridad que van a permitirles mantener a salvo su información.** De lo contrario, el crecimiento de amenazas y ataques seguirá siendo una constante.

De igual manera, el mejor modo de garantizar la confidencialidad de la información es haciendo uso de tecnologías de cifrado en todas las formas de comunicación. A la vez, cuando se habla de ransomware, la mejor manera de asegurarse contra la pérdida definitiva de la información es teniendo un adecuado backup de los datos más sensibles.

> No se puede permitir que el avance de la tecnología se vuelva en contra del usuario.

1- Encuesta realizada por ESET Latinoamérica a su comunidad online durante agosto de 2016.

Pero la adopción de estas tecnologías durante el próximo año parte del reconocimiento de las amenazas, y la base fundamental para esto es tener usuarios educados y que puedan decidir acerca de cuál es la mejor manera de protegerse.

La educación hace la diferencia

Para todos aquellos que estamos en el mundo de la seguridad informática no hay una máxima mejor aprendida que aquella que dice que **el eslabón más débil en la cadena es el usuario final.**

Dado que ya desde 2015 se advirtió que cada vez hay más y más tecnología de la información para defender, pero la cantidad de gente capacitada para asegurarla es peligrosamente baja, **es necesario tomar la educación como el factor fundamental para marcar la diferencia.** Si bien todo el proceso de formación de nuevos profesionales que trabajen en seguridad no va a ser algo inmediato, **en los próximos años el foco debe dirigirse a la concientización de usuarios** sobre cuidados básicos en Internet, pues **ahí es donde está la masa crítica que aprovechan los atacantes para obtener sus ganancias.** Así que el gran reto para quienes nos encargamos de la seguridad es convertirnos en la primera línea de defensa de la información: la educación como herramienta para enseñarles a los usuarios sobre las amenazas actuales y cómo se propagan es lo que puede marcar la diferencia en el futuro para disminuir el impacto del cibercrimen.

No se debe olvidar que la seguridad es algo transversal y ya no es exclusiva de aquellos que trabajamos en tecnología: hoy en día es igual de crítica la información que maneja un periodista o un ejecutivo, e incluso se vuelve más sensible cuando hablamos de profesionales de la salud y los registros médicos de pacientes que manejan a diario.

Para lograr esto es necesaria una participación activa de los gobiernos y las empresas. Estamos en el punto en el que se necesita que en la educación se traten los temas de seguridad de manera formal y que las empresas no dejen estos temas solo como una inducción al momento de iniciar la relación laboral, sino **que sea algo continuo y constante en el tiempo.** El usuario final debe sentirse como **una parte de toda la cadena de seguridad** y debe entender en primera instancia que las amenazas existen, pero que existen también los mecanismos necesarios para disfrutar de la tecnología de forma segura.

No se debe olvidar que la seguridad es algo transversal y ya no es exclusiva de aquellos que trabajan en tecnología.

Mobile: el malware y su realidad... ¿aumentada?

- Traspasando los límites de la percepción
- Apps vulnerables con API no tan seguras
- Android... ¿un sistema inseguro?
- Apps maliciosas en mercados oficiales
- Facilidad de actualización
- Plataformas móviles bajo ataque

AUTOR

Denise Giusto Bilic
Security Researcher

Mobile: el malware y su realidad... ¿aumentada?

En un principio, se esperaba de los dispositivos móviles que evolucionasen hasta convertirse en computadoras de bolsillo tan capaces como cualquier equipo de escritorio. Es claro que hoy nuestros teléfonos y tabletas inteligentes han trascendido este propósito, generando nuevas maneras de interacción tecnológica antes impensadas.

En este contexto de revolución socio-tecnológica, **el auge de las tecnologías de realidad virtual incorpora nuevos riesgos de seguridad que atañen no solo a la información digital, sino al bienestar físico del usuario.** Mientras estas aplicaciones concentran datos cada vez más sensibles, **el malware móvil no deja de crecer y complejizarse,** reforzando la importancia del desarrollo seguro. Ante la gran cantidad de potenciales víctimas, **los mercados oficiales de aplicaciones sucumben frente a las nuevas campañas de códigos maliciosos** que se cuelan en sus trincheras.

¿Es este el escenario que nos aguarda en tendencias de seguridad móvil? A lo largo de esta sección analizaremos cómo se proyectarán estos riesgos sobre el futuro próximo.

Traspasando los límites de la percepción

Previo al surgimiento de **Pokémon GO,** nunca antes la realidad aumentada había sido experimentada por tantas personas fuera de la comunidad de aficionados, lo que ha situado a esta tecnología al frente en lo que a tendencias móviles refiere. Simultáneamente, **cada vez resulta más común ver a personas utilizando dispositivos de realidad virtual** gracias a proyectos como Google Cardboard, que sirvieron para propagar el concepto entre el público al volverlo más accesible. El éxito masivo de aplicaciones como Pokémon GO se convierte inexorablemente en un atractivo para cibercriminales que buscarán inyectar códigos maliciosos en futuras aplicaciones de realidad aumentada, distribuyendo sus creaciones a través de servidores maliciosos, sitios comprometidos, tiendas no oficiales e, incluso, mercados oficiales de aplicaciones.

Al momento de escritura de este artículo, ya podemos ver el primer disfrute público de Father.IO: una aplicación móvil que combina realidad aumentada y virtual en un juego de guerra colaborativo y que parecerá ser todo un éxito durante el próximo año. **Los usuarios deberán tener mucho cuidado para evitar malware que intente hacerse pasar por la app genuina,** software de instalación o manuales de uso.

Estas nuevas tecnologías combinadas con aplicaciones de uso cotidiano plantean riesgos de seguridad antes no contemplados, en adhesión a otros peligros móviles que ya mencionamos en nuestro informe de Tendencias 2016, como la propagación de malware y compromiso por vulnerabilidades. A medida que la persona como entidad física se transforma en una variable de juego, **ya no solo deberemos preocuparnos por la protección de los datos en los dispositivos, sino también por la integridad del jugador.** La sensatez –o falta de ella–

Mientras estas aplicaciones concentran datos cada vez más sensibles, el malware móvil no deja de crecer y complejizarse, reforzando la importancia del desarrollo seguro.

jugará un rol crucial en la seguridad física. Hemos atestiguado casos de personas intentando cazar pokémones mientras manejan, en lugares de propiedad privada, en zonas altamente inseguras, o tan absortos en la realidad aumentada que olvidan mirar si algún vehículo se aproxima al cruzar la calle.

La confluencia de desconocidos en el mismo lugar también planteará riesgos al no conocer frente a quién nos exponemos. Este quizás haya sido uno de los aspectos más controversiales alrededor del surgimiento de Pokémon GO, ya que varias personas resultaron heridas en altercados en gimnasios Pokémon o al intentar comenzar batallas con desconocidos.

Al tratarse de *apps* que pueden poner en riesgo la vida de sus usuarios, **el diseñar un modelo de seguridad de manera inherente al proceso de desarrollo será un factor ineludible en la creación de nuevas aplicaciones.** Después de todo, si no se consideran los aspectos físicos de la usabilidad, **¿qué puede esperarse de fallos de seguridad más técnicos y quizás menos visibles para usuarios y diseñadores?**

Apps vulnerables con API no tan seguras

Si algo ha marcado el desarrollo de software hasta la fecha es **el modo en que las consideraciones de seguridad son aplazadas hasta etapas tardías del proyecto, si es que son contempladas en lo absoluto.** Dejando de lado algunas pocas aplicaciones que deben cumplimentar estándares de seguridad, **pocos desarrolladores se preocupan por realizar exhaustivos controles de *pentesting*** sobre sus productos antes de liberarlos al público.

A medida que los móviles se plantean como constructores de relaciones humanas que exceden el espacio digital, ya sea para jugar, practicar deportes o encontrar el amor; **la seguridad se vuelve un factor crítico** en el proceso de desarrollo para evitar diseños inseguros.

Por ejemplo, recientemente investigadores descubrieron que la API de Tinder entregaba –al momento de la escritura de este artículo– la geolocalización exacta de la persona cada vez que se producía un *match*. Otro ejemplo rotundo fue el caso de Nissan Leaf, cuando se descubrió que podrían accederse algunos controles no críticos del vehículo a través de vulnerabilidades en la API provista por la compañía para desarrollos móviles.

Las librerías de anuncios publicitarios también tendrán un rol importante en la seguridad. Estas librerías son muy utilizadas por los desarrolladores en plataformas donde los usuarios no suelen estar dispuestos a pagar por conseguir la funcionalidad que sus creaciones proveen. Usualmente encontramos al menos una de ellas por aplicación y muchas veces contienen API inseguras que podrían ser explotadas para la instalación de *malware* o el robo de información.

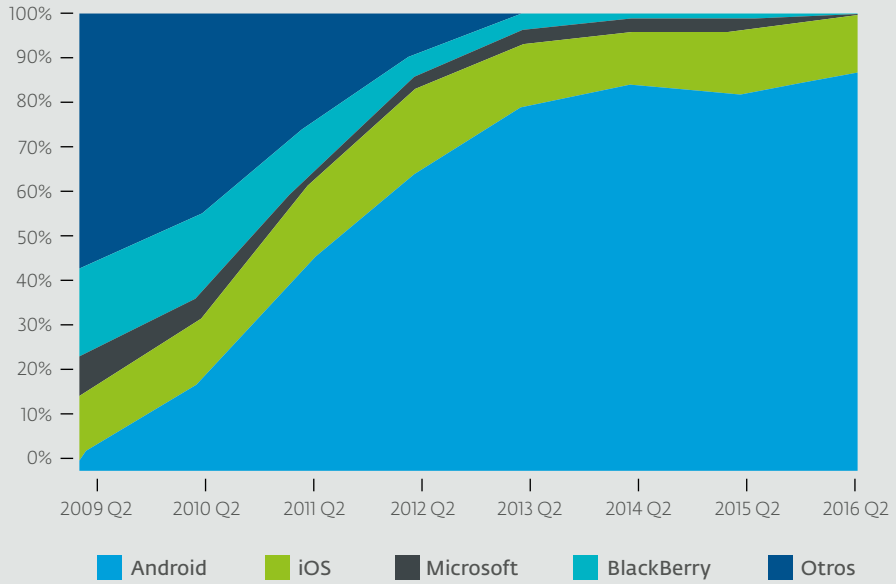
En adhesión a estos errores involuntarios en el proceso de desarrollo, **también están aquellas creaciones maliciosas cuya propagación en ocasiones es favorecida por las políticas poco restrictivas** en ciertos repositorios de aplicaciones que envisten involuntariamente a los cibercriminales bajo la fiabilidad de los mercados oficiales.

Android... ¿un sistema inseguro?

En 2007, el **surgimiento de iOS revolucionó la industria móvil al forzar a los consumidores a repensar la función de los dispositivos tecnológicos** en nuestro día a día. Por aquellos tiempos poco se debatía sobre el rol de la seguridad de la información en las innovaciones tecnológicas y sus posibles consecuencias en la protección de los datos.

Si no se consideran los aspectos físicos de la usabilidad, ¿qué puede esperarse de fallos de seguridad más técnicos y quizás menos visibles para usuarios y diseñadores?

Market Share de los diferentes OS



Fuente: Statista

La expansión de Android a otros dispositivos lo convierte en un potencial vector de ataque multiplataforma.

Aproximadamente un año luego de la presentación de iOS, un nuevo sistema operativo apareció como plausible oponente: **Android, de la mano de Google.** Con un sistema de código abierto, un mercado de apps menos restrictivo, la posibilidad de adaptarse a diferentes OEM y gran flexibilidad en cuanto a personalización, Android rápidamente aumentó su participación en el mercado.

Hacia fines de 2009 los usuarios móviles comenzaron a disgregarse en bandos antagónicos según su predilección por cada sistema, apostando a uno u otro. Fue entonces cuando emergieron los **primeros cuestionamientos sobre si estas características tan apreciadas en Android podrían jugar un papel negativo al momento de replantear su seguridad.** Hoy quizás estemos viendo los resultados de dicha apuesta. Para el segundo trimestre de 2016, este sistema abarcaba el 86,2% de los equipos en uso. **La masividad de usuarios a los que alcanza lo vuelve un blanco preferente para atacantes.** Su expansión a otros dispositivos como tabletas inteligentes, televisores, *wearables* y autos, lo convierte en **un potencial vector de ataque multiplataforma** en un escenario que se complica mientras cobran vida nuevos sistemas de domótica.

Existe una pluralidad de causantes que propiciarían ataques multiplataforma. En primer lugar, la interconexión entre dispositivos que permite la fácil propagación de amenazas y de estafas mediante Ingeniería Social. Además, componentes comunes a lo largo de la estructura del sistema operativo que pueden no ser actualizados frecuentemente por los diferentes OEM. Finalmente, cada vez son más comunes los *frameworks* de desarrollo que permiten rápidamente exportar ejecutables para diferentes equipos, los cuales podrían propagar fallos de seguridad entre distintos terminales. **En la Internet de las Cosas (IoT) no cuesta imaginar más de estos ataques a futuro.**

Apps maliciosas en mercados oficiales

Una moneda corriente de los últimos tiempos ha sido **la aparición de apps maliciosas en los repositorios oficiales de iOS y**

Android, una tendencia que al principio parecía extraordinaria pero que lamentablemente se ha ido consolidando con el tiempo. Esta tendencia golpeó inclusive a la App Store de Apple, teóricamente más restrictiva que la Play Store de Android.

En cuanto a la publicación de aplicaciones, **existen numerosos factores que favorecen la existencia de códigos maliciosos en la tienda de apps de Google.** No solo la mayor cantidad de potenciales víctimas hacen de Android un blanco predilecto para los cibercriminales, sino que **la rapidez de publicación de la Play Store es otro condimento que la convierte en un entorno preferido por muchos atacantes** para intentar propagar sus amenazas.

En Android cualquier desarrollador puede crear una cuenta con **un único pago de U$D 25, subir una aplicación y tenerla publicada dentro de las 24 horas.** En contraposición, **en iOS el costo de la membresía es superior a U$D 99 anuales y el período de espera hasta la publicación puede extenderse por semanas.** Por ello, aunque se realicen mejoras a Bouncer (el módulo de Google para análisis automático y detección de malware) y se refuerce el análisis manual de código, la enorme cantidad de nuevas apps que diariamente se crean y la premura con que estas son incorporadas al mercado complican el correcto análisis de cada una de ellas.

Podemos pensar entonces que, para reducir a futuro los casos de *malware* en la tienda oficial, **Google deberá modificar alguna de estas variables** –o ambas– para así destinar más recursos al análisis intensivo de una cantidad reducida de aplicativos o extender el tiempo de análisis, menoscabando la rapidez de publicación. Una de las variadas estrategias que Google podría utilizar para reducir el número de aplicaciones candidatas a publicación podría ser **aumentar el precio de la membresía para desarrolladores.**

Lo cierto es que mientras el marco de políticas de publicación en la Play Store continúe igual y ninguna de estas acciones correctivas tenga lugar, **podremos esperar una mayor cantidad de malware en tiendas oficiales para 2017** a medida que los atacantes consolidan este nuevo modus operandi y descubren nuevas mecanismos para evadir la detección.

Con respecto a este último punto, es preciso decir que **existen muchas técnicas que complican la detección de códigos maliciosos móviles:** bombas de tiempo, código dinámico ejecutado a través de reflexión, empaquetadores, cifrado, strings ofuscadas, scripts en otros lenguajes de programación para la descarga remota del código malicioso, nuevas formas de C&C, antiemulación, rootkits... Pero, por sobre todo, los ciberatacantes apuestan y seguirán apostando a la Ingeniería Social, esperando atentamente el lanzamiento oficial de apps populares para distribuir versiones falsas de estas, como ocurrió recientemente con Pokémon GO, Prisma o Dubsmash.

La inmediatez con que estas aplicaciones maliciosas consiguen cientos y hasta miles de descargas es un motivo de preocupación entre usuarios de esta plataforma. **¿Qué ocurrirá entonces cuando los cibercriminales decidan masificar la complejidad de sus creaciones?**

La diferencia en la cultura que los usuarios del sistema tienen respecto a la instalación de aplicaciones también juega un rol contraproducente cuando de Android se trata. **La facilidad con la que alguien puede modificar un APK** obtenido del mercado oficial para inyectar código malicioso y distribuirlo a través de sitios o mercados fraudulentos, **sumado a la facilidad que tienen los usuarios para instalar archivos de fuentes no desconocidas, resulta en una mayor tasa de detecciones** (y en el peor de los casos, de infecciones) en comparación con otros sistemas móviles.

Mientras el marco de políticas de publicación en la Play Store continúe igual, podremos esperar una mayor cantidad de malware para 2017.

Facilidad de actualización

Fueron varias las investigaciones que argumentaron a lo largo de los años que la característica Open Source de Android irremediablemente implicaría un mayor número de vulnerabilidades al descubierto y, consecuentemente, un aumento en la frecuencia de ataques. **No obstante, 2016 ha sido el primer año en que Android pareciera terminar con un mayor número de vulnerabilidades publicadas que iOS.**

No obstante, **la forma en que los parches de seguridad son desplegados continúa dejando inseguros a los usuarios de Android,** creando una amplia ventana de tiempo entre el momento en que la vulnerabilidad es conocida y aquel en que los diferentes OEM y operadores telefónicos emiten la mejora de seguridad para las diferentes versiones del sistema, si es que deciden hacerlo.

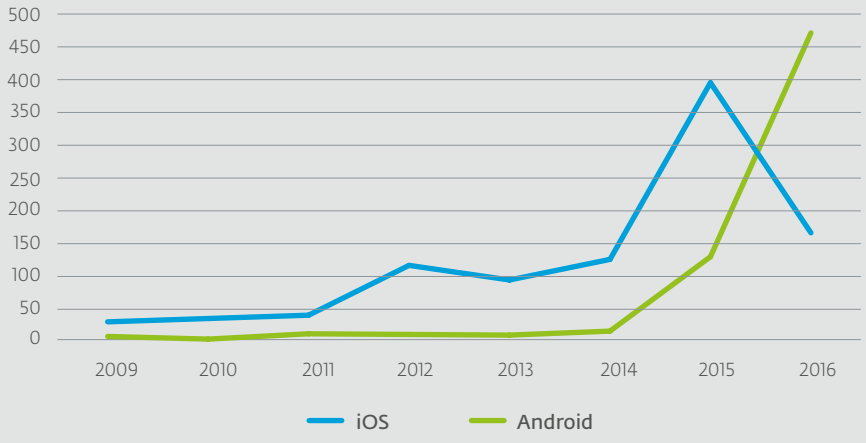
Para lo que resta de este 2016 y próximo 2017, el plan de actualizaciones propuesto por Google para Android 7.0 Nougat en dispositivos Nexus incluye parches de seguridad mensuales, más las actualizaciones trimestrales de funcionalidad y correcciones de *bugs*. Entretanto, **poco se ha progresado durante este año hacia el logro de un consenso para la rápida liberación de parches.** Por el contrario, las batallas de poder por la dominancia del mercado móvil han aletargado la resolución del conflicto. Por su parte, Samsung, el principal fabricante de dispositivos con Android se niega a ceder el control del SO de sus equipos a Google. Mientras, Google acude a fabricantes más dóciles que desplacen a Samsung y disminuyan su cuota de mercado.Existen algunos indicadores de que Google ha ideado un nuevo plan para solucionar este problema. Hasta entonces, una de las opciones que se presenta para aquellos usuarios móviles de Android preocupados por contar con los últimos parches de seguridad, **será adquirir equipos Nexus** –rebautizados Pixel por Google–, **para así cerciorarse de obtener las actualizaciones lo antes posible de la mano de la propia madre nodriza.**

La forma en que los parches de seguridad son desplegados continúa dejando inseguros a los usuarios de Android.

Plataformas móviles bajo ataque

Desde 2012, **la cantidad de detecciones de amenazas para el mundo móvil no deja de aumentar, crecimiento que podemos proyectar para el próximo año.** Esto es una reflexión estadística de la mayor im-

Cantidad anual de vulnerabilidades en Android e iOS desde 2009



Observación: Las vulnerabilidades de 2016 contabilizan hasta el 14 de noviembre de 2016.

Fuente: www.cvedetails.com

portancia que los cibercriminales otorgan a estos equipos a medida que se vuelven cada vez más personales.

Más allá de lo planteado a lo largo de esta sección, **es importante remarcar que los usuarios de Apple tampoco deben caer en una falsa sensación de seguridad.** Según los datos obtenidos de nuestros productos, **las detecciones por iOS continúan representando menos del 1% de las detecciones por Android a nivel mundial.** No obstante, las detecciones para este OS no hacen más que acrecentarse de manera exponencial: **En lo que va de 2016, ya se han detectado más de cinco veces la cantidad de detecciones para iOS correspondientes a todo el 2015** y podemos esperar que esta mayor exposición continúe durante 2017. Sumado a esto, graves vulnerabilidades continúan al acecho. Poco tiempo atrás, Apple liberó parches de seguridad para un conjunto de vulnerabilidades zero-day que otorgaban a los cibercriminales el control completo sobre el equipo y eran utilizadas para el espionaje de individuos.

El crecimiento del malware móvil es una realidad innegable, una que veníamos vaticinando desde hace ya algunos años y actualmente se consolida ante nuestros ojos. **Durante 2015 la cantidad de nuevas variantes de códigos maliciosos creados para Android promediaba las 200 variantes mensuales; durante 2016 este número ascendió a 300 nuevas variantes mensuales (en iOS el número es de 2 mensuales).** No debería sorprendernos que este incremento continúe durante el próximo año, **promediando las 400 nuevas variantes mensuales de malware móvil para Android al concluir el 2017.** Esto nos brinda una medida no solo de la cantidad de códigos maliciosos, sino también de la rapidez con la que estas campañas maliciosas evolucionan. **Durante el año venidero podremos observar más ransomware, más apps falsas, códigos maliciosos más rebuscados y muchas más estafas móviles a través de WhatsApp y aplicaciones de redes sociales.** A medida que los usuarios comprenden el peligro de instalar aplicaciones desde fuentes no confiables, los cibercriminales apostarán a nuevas campañas de Ingeniería Social a través de mercados oficiales y podemos esperar ver muchos más casos así con el correr de los meses. Qué curso de acción tomarán Google y Apple para contener esta situación será lo que restará por ver durante el próximo año.

Acompañando el aumento en la cantidad de nuevas variantes de códigos maliciosos, **una gran preocupación para los usuarios móviles serán las vulnerabilidades no solo del sistema operativo sino también de las aplicaciones que utilizan.** A medida que estas apps concentran datos que pueden poner en peligro la integridad física de sus usuarios, será un desafío para sus creadores el adoptar prontamente procesos de desarrollo seguro que garanticen la minimización del riesgo de exposición, por ejemplo, mediante API incorrectamente diseñadas.

Por lo pronto, **la reciente liberación de iOS 10 y Android 7.0 Nougat plantea algunas remarcables mejoras en el estado de la seguridad móvil,** especialmente para este último sistema. Por parte de Google, comienzan a vislumbrarse esfuerzos por unificar algunos aspectos de seguridad a través de los distintos modelos de teléfonos y tabletas disponibles en el mercado. Además, la firma continuará depositando esperanzas en su agresivo programa de bug hunting como medio para el descubrimiento de vulnerabilidades. Otra característica remarcable de Android 7.0 Nougat es que ha introducido diferentes mejoras en el manejo de permisos y aplicaciones que dificultarán la instalación de malware dentro del equipo y limitarán el control que estas aplicaciones logren, **en un claro intento por derrotar el aumento del ransomware móvil, uno de los principales desafíos que hay en lo relativo a la seguridad mobile.**

Durante 2016 la cantidad de nuevas variantes de códigos maliciosos creados para Android fue de 300 nuevas variantes mensuales.

Por parte de Google, comienzan a vislumbrarse esfuerzos por unificar algunos aspectos de seguridad.

Vulnerabilidades: los reportes bajan, pero ¿estamos más seguros?

- Baja la cantidad de reportes, pero ¿baja el riesgo?
- Desarrollo seguro de software
- El protagonismo de múltiples vulnerabilidades y su rol en la concientización
- En ocasiones, un buen ataque es la mejor defensa
- Conclusión

AUTOR

Lucas Paus
Security Researcher

4

Vulnerabilidades: los reportes bajan, pero ¿estamos más seguros?

La globalización tecnológica y los múltiples dispositivos que hoy se utilizan interconectados de manera natural han incrementado en gran parte los vectores de ataque disponibles para los ciberdelincuentes. Es por ello que la explotación de vulnerabilidades sigue siendo una de las principales preocupaciones en cuanto a incidentes de seguridad en las empresas a nivel mundial.

Atravesando las barreras de seguridad sobre distintas plataformas, es posible para los atacantes encontrar y explotar fallas de programación que permitirán distintas acciones, que van desde el robo de información o propagación de malware sin la necesidad de una mayor intervención por parte del usuario, hasta la caída del sistema o servicio.

En este contexto de auge tecnológico y vulnerabilidades, se incorporan nuevos desafíos de seguridad que atañen no solo a la información digital, sino también al acceso a infraestructuras críticas, autos inteligentes, IoT, industrias 4.0 e inclusive el manejo ciudades inteligentes. Mientras aplicaciones y sistemas operativos se concentran en ser más funcionales y competitivos en el mercado, **surge la necesidad de reforzar la importancia del desarrollo seguro** en conjunto con la periodicidad en auditorías de seguridad. Durante 2016 vimos alianzas estratégicas entre Microsoft y Canonical, con el objetivo de integrar herramientas de Ubuntu (Linux) a Windows 10, las cuales podrían convertirse en un nuevo vector de ataque multiplataforma como lo son, en muchos casos, las vulnerabilidades en Java o en navegadores web. **¿Serán estos nuevos escenarios los que agudizarán la importancia de encontrar y mitigar de manera inmediata las vulnerabilidades? ¿Se ha reducido el número de vulnerabilidades encontradas? ¿De qué manera podremos asegurar con mayor certeza la seguridad de la información tanto a nivel hogareño como en empresas?** A lo largo de esta sección se responderán estas cuestiones y, además, se observará el contexto futuro que nos aguarda en torno a las vulnerabilidades.

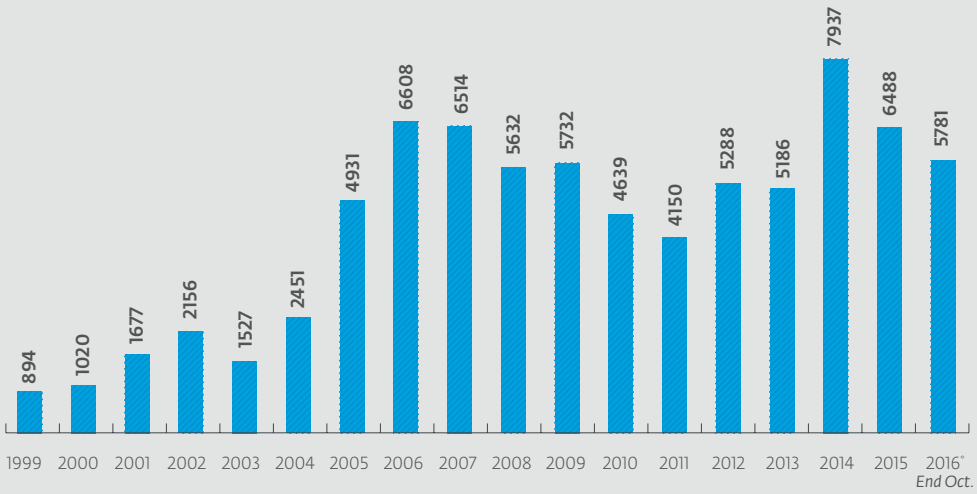
Baja la cantidad de reportes, pero ¿baja el riesgo?

Paradójicamente, a pesar de la llegada de nuevas tecnologías, **la cantidad total de vulnerabilidades de todo tipo reportadas anualmente ha ido disminuyendo en los últimos años.** Se puede observar que, a pesar de la cantidad de nuevos vectores que han entrado en juego, **la cantidad de CVE reportados va en descenso en los últimos dos años, después de un máximo histórico en 2014.**

De hecho, **para finales del tercer trimestre de 2014 se habían publicado 5405 vulnerabilidades, mientras que en el mismo periodo de 2015 la cifra bajó a 4864** (Fig 2). **Finalizando el mes de octubre de 2016, la cifra llegó a 5781 (Fig 1),** casi la misma cantidad que el año pasado. Esto significa que **no hay un incremento abrupto en el total de vulnerabilidades publicadas.** Siguiendo esta línea y ligado al hecho de que el desarrollo seguro sigue ganando terreno, **para 2017 no se esperaría un crecimiento abrupto en la cantidad de vulnerabilidades reportadas.**

Paradójicamente, a pesar de la llegada de nuevas tecnologías, la cantidad total de vulnerabilidades de todo tipo reportadas anualmente ha ido disminuyendo en los últimos años.

FIG. 1 | Vulnerabilidades publicadas por año



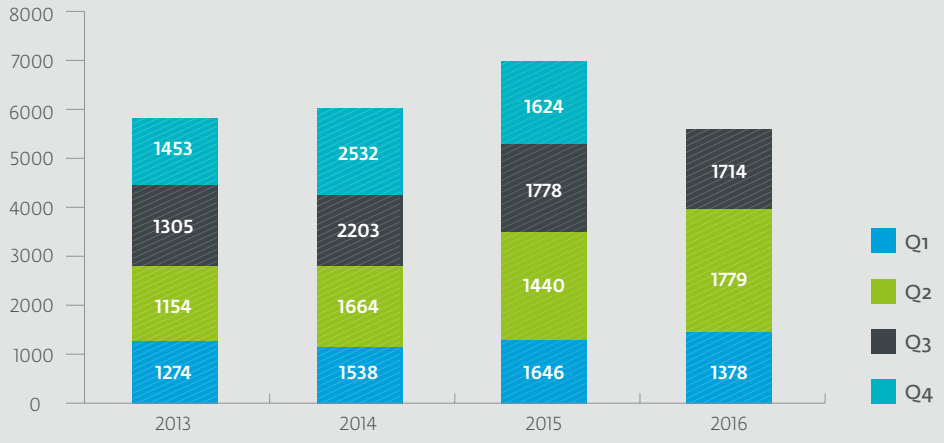
Fuente: National Vulnerability Database

El decrecimiento general en la cantidad de fallas reportadas no es una señal de tranquilidad, pues los reportes de vulnerabilidades críticas en los últimos años han crecido.

Sin embargo, más allá del optimismo que puede generar este decrecimiento en la cantidad de vulnerabilidades publicadas, **este dato cobra otro significado cuando se observa cuántas de esas vulnerabilidades son de las consideradas "críticas" (Fig 3)**, es decir, aquellas que poseen un mayor impacto sobre la seguridad del usuario.

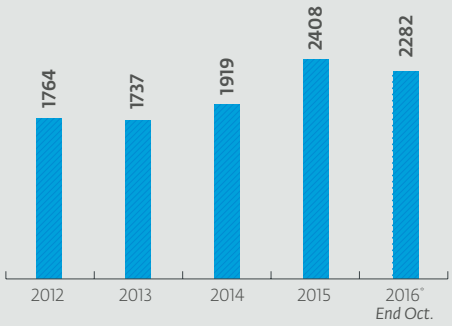
Finalizando el tercer trimestre de 2016, la cantidad de vulnerabilidades críticas reportadas corresponde a un 40% del total, un porcentaje mayor a lo que se había visto en años anteriores. Por lo tanto, el decrecimiento general en la cantidad de fallas reportadas no es una señal de tranquilidad, pues los reportes de vulnerabilidades críticas en los últimos años han crecido. Pero más allá de las cantidades de vulnerabilidades encontradas, no se puede dejar de lado que su explotación no es directamente proporcional a la cantidad de CVE reportados. **El riesgo que tiene una vulnerabilidad de ser explotada está ligado a cuestiones como la masividad del uso de la aplicación o protocolos vulnerables, la dificultad de su explotación y la criticidad de la información almacenada.**

FIG. 2 | Vulnerabilidades publicadas por trimestre



Fuente: National Vulnerability Database

FIG. 3 | Número de vulnerabilidades críticas reportadas por año



Fuente: National Vulnerability Database

Por ejemplo, CVE-2016-2060 es una vulnerabilidad crítica que afecta a **millones de dispositivos con Android,** permitiendo que ciertas aplicaciones ganen privilegios y puedan obtener acceso a información privada del usuario. En cuanto a protocolos, en el caso de OpenSSL encontramos a DROWN, una vulnerabilidad crítica publicada en 2016 y cuyo impacto se estimó que puede llegar a afectar al **25% de los dominios más visitados de Internet** y hasta una tercera parte de todos los servidores de la Web. Lo anterior deja en evidencia cómo dos CVE pueden tener un gran impacto, que va desde usuarios hogareños a empresas.

Desarrollo seguro de software

Cuando vemos la disminución en la cantidad de vulnerabilidades reportadas, parte de ese logro puede estar asociado a los nuevos paradigmas en el desarrollo de sistemas. De hecho, uno de los grandes desafíos que se plantean año a año desde la seguridad informática es el modo en que se aplica la seguridad a los nuevos proyectos. **Con anterioridad, hemos visto muchas veces la priorización de la innovación por sobre la seguridad de la información.** Más allá del impulso o la obligación que genera la constante necesidad de novedades dentro del mercado tecnológico, relegar la seguridad de la información de los desarrollos es una práctica riesgosa, no solo desde el punto de vista de la protección de datos, sino también para la continuidad del negocio. A fin de cuentas, **un incidente a gran escala podría tener un enorme impacto en la imagen corporativa.**

Sin embargo, este es un paradigma que se está intentando cambiar; **la nueva tendencia hace creer que poco a poco los desarrolladores están siendo acompañados por especialistas en seguridad y criptografía desde las fases primarias.** Por lo tanto, en la medida en que se sigan mejorando estas buenas prácticas en el ciclo de vida del software (Systems Development Life Cycle o SDLF), esperaremos que la cantidad de CVE no tenga un gran incremento, lo cual reducirá la posibilidad de explotación de vulnerabilidades sobre los distintos sistemas desarrollados.

Todas estas mejoras en el SDLF se hacen aún más necesarias si contemplamos escenarios conocidos y que vienen creciendo en los últimos años, como la cantidad de aplicaciones y servicios basados en la nube o su futura migración, el isomorfismo, las aplicaciones de Big Data o las interfaces de Desarrollo de Aplicaciones (API). Todas ellas deberán contar con las debidas validaciones de entrada, garantizar las codificaciones de salida mediante prácticas criptográficas y contar con correcto manejo de logs, memoria, errores y archivos.

Para fortalecer la mejora en todo el ciclo, **el reto para 2017 se va a centrar en mejorar la gestión de vulnerabilidades que se vayan encontrando.** Así que tanto para los fabricantes y desarrolladores como para los usuarios, el desafío será contar con las medidas de control para evitar la explotación de las vulnerabilidades y, al mismo tiempo, reportarlas y gestionarlas en forma satisfactoria.De este modo, se prevé que la instauración de un ciclo de desarrollo seguro, a partir de la consolidación de un modelo de diseño orientado a la seguridad, comen-

Tanto para los fabricantes y desarrolladores como para los usuarios, el desafío será contar con las medidas de control para evitar la explotación de las vulnerabilidades y, al mismo tiempo, reportarlas y gestionarlas en forma satisfactoria.

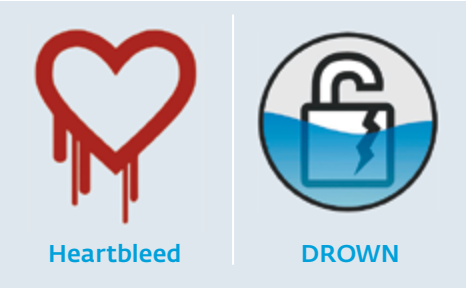
zará a generar sinergia entre áreas de seguridad y desarrollo, **lo cual nos acercará hacia el despliegue de sistemas más robustos, eficaces y más rentables.**

El protagonismo de múltiples vulnerabilidades y su rol en la concientización

Del lado de los usuarios, **en el último tiempo, algunas de las vulnerabilidades críticas no han pasado desapercibidas.** Durante más de tres décadas, las empresas de antivirus y los investigadores de seguridad han ido denominando con nombres a diversos códigos maliciosos que han tenido gran impacto. Podemos resaltar ejemplos como los antiguos gusanos Morris o Sasser, el virus Melissa y algunos más actuales, como los ransomware CTB-Locker y Locky.

Esta práctica ha ido un paso más allá y **desde 2014 también se ha comenzado a bautizar a determinadas vulnerabilidades críticas.** Un claro ejemplo fue CVE-2014-0160, mucho más conocida como Heartbleed, una infame vulnerabilidad que no solo se hizo de un nombre, sino también de un logotipo. Naturalmente, **los nombres buscan generar una caracterización de las amenazas, intentando acercarse a un punto de referencia o entendimiento acerca de su funcionamiento.** Además, **esta clase de bautismo de vulnerabilidades tiene una mayor eficacia en la concientización de los distintos departamentos de TI, buscando que a partir de la identificación de una vulnerabilidad se tomen las medidas necesarias para mitigarla.**

Durante 2015 resaltaron nombres como FREAK (CVE-2015-0204) y Logjam (CVE-2015-4000). En 2016 nos encontramos con otras tres notables: Badlock (CVE-2016-2118), que afectó a Samba; HTTPoxy (CVE-2016-5387), aunque había sido detectada por primera vez hace 15 años; y DROWN, que afectó a protocolos TLS/SSL. Seguramente el próximo año continuará este "bautismo" de vulnerabilidades y **se espera que más allá de los efectos de marketing o promoción, dichas denominaciones logren incrementar los esfuerzos en la concientización de los usuarios.** Así, tomarán las acciones necesarias para mitigar el impacto que dichas vulnerabilidades podrían tener en sus sistemas.



En ocasiones, un buen ataque es la mejor defensa

La cuestión de las vulnerabilidades también ha sido una preocupación para los principales servicios y empresas del mundo tecnológico. **Años atrás, las compañías habían tomado una posición bastante ofensiva respecto a la gestión de seguridad y vulnerabilidades,** principalmente generando políticas y controles a fin de respaldarla. **Los últimos tiempos fueron beneficiosos para auditorías y pentesting,** que han ganado gran terreno principalmente en entornos corporativos, donde en muchos casos, por normativas regulatorias y de concientización, se deben realizar de forma periódica.

Sin embargo, grandes empresas y entidades gubernamentales están apoyándose en una tendencia que se acerca a lo que podría ser un ataque real. **Consiste en contratar especialistas en seguridad particulares para realizar pruebas de penetración con una remuneración acorde a los resultados obtenidos,** lo que se ha denominado como **Vulnerability Reward Program** o **Bug Bounty Program.** Empresas líderes

La cuestión de las vulnerabilidades también ha sido una preocupación para los principales servicios y empresas del mundo tecnológico.

como Facebook, Google o Yahoo!, entre muchas otras, ya formalizan enérgicamente este tipo de actividades; entidades gubernamentales no se quedan atrás, como es el caso del Departamento de Defensa de los Estados Unidos, que lo propuso para el Pentágono y para el ejército.

Para los desarrolladores de aplicaciones y fabricantes de dispositivos IoT, **este tipo de programas pueden traer mejoras en sus productos más rápidamente,** ya que normalmente las pruebas son realizadas por una cantidad mayor de investigadores, las vulnerabilidades son reportadas de inmediato y, dado que los tiempos pueden ser significativamente más extensos, se pueden hacer exploraciones más profundas. De este modo, estas causas y otras referidas a presupuesto y motivación de los especialistas involucrados seguirán afianzando la tendencia en el futuro.

Conclusión

Las empresas hoy en día están más preocupadas por incidentes de seguridad como la fuga de información o el acceso indebido a datos sensibles; sin embargo, **no han mejorado sustancialmente sus prácticas de gestión de seguridad,** tal como se evidenció en el ESET Security Report 2016. Por lo tanto, **los principales retos para el ámbito corporativo en 2017 van a estar ligados a enfocar los esfuerzos en la gestión de la tecnología,** complementándolos con una necesaria concientización de los colaboradores sobre los riesgos, para además poder cumplir con las normativas impuestas por entes reguladores del negocio.

A todo esto se suma la necesidad de profundizar en la cultura de resiliencia, lo que deja a los especialistas de seguridad en el papel protagónico para actuar como facilitadores a las áreas de IT en la corrección de errores de código y la mitigación de impactos. De esta manera, **la gestión debe enfocarse en la adecuada implementación de políticas de seguridad y en los planes que permitan la continuidad del negocio,** incluyendo una adecuada comunicación de los incidentes para mantener informados a los usuarios. **Del lado de los desarrolladores, se espera que se continúe afianzando el paradigma de desarrollo seguro.** A partir de una mayor concientización de los usuarios sobre los riesgos de las vulnerabilidades, no sería extraño que exista una mayor demanda de mejor protección de la información personal que las empresas manejan. En caso de que esto ocurra, el desarrollo seguro podrá ser un diferencial competitivo dentro de la industria tecnológica y, en un futuro, se convertirá en un incentivo para los desarrolladores.

Por otra parte, nuevos códigos maliciosos han comenzado a utilizar las vulnerabilidades para su propagación, ya que simplemente visitando un enlace, una víctima desprotegida puede ver cómo la información de sus dispositivos es cifrada; esto sucede con algunas variantes del ransomware CryptoWall 3.0. De manera similar, **los exploit kits seguirán siendo utilizados en mayor medida para la propagación de malware e inclusive en ataques más dirigidos como los APT,** instaurándose sobre sitios vulnerados o generados especialmente para tal fin.

Las vulnerabilidades de software en muchos casos son difíciles de predecir y la utilización de los famosos 0-days sigue dejando a los sistemas expuestos; sin embargo, la industria antivirus también ha tomado nota de esta tendencia y por eso existen soluciones de seguridad con heurística avanzada, que poseen tecnología capaz de detectar este tipo de exploits y bloquearlos. De este modo, tanto las soluciones de seguridad como la gestión de actualizaciones y de vulnerabilidades seguirán ganando protagonismo para la mitigación de este tipo de problemática, con el objetivo de minimizar o eliminar la brecha de exposición y fuga

Los principales retos para el ámbito corporativo en 2017 van a estar ligados a enfocar los esfuerzos en la gestión de la tecnología, complementándolos con una necesaria concientización de los colaboradores.

Software de seguridad "next-gen": mitos y marketing

- La era de los dinosaurios
- La teoría de la evolución
- La selección natural y no natural
- Evaluación del producto completo
- En el Cenozoico

AUTOR

David Harley
Senior Research Fellow

5

Software de seguridad "next-gen": mitos y marketing

La era de los dinosaurios

Hay una concepción del mercado actual de la seguridad informática que últimamente está apareciendo con demasiada frecuencia en los medios de comunicación. Diferencia dos tipos de tecnología de detección de malware: **una de "primera generación" o "tradicional"** (a veces incluso la llaman tecnología "fosilizada" o "de la época de los dinosaurios") que, según dicen, se basa invariablemente en la detección mediante el uso de firmas de virus; **y otras tecnologías (supuestamente) superiores de la "siguiente o última generación" ("next-gen"),** que utilizan métodos de detección sin firmas. **Por supuesto, esta concepción se ve muy favorecida por las empresas que comercializan "soluciones next-gen"; sin embargo, no refleja la realidad.**

La teoría de la evolución

En primer lugar, quisiera discrepar con el término "de primera generación". No se puede meter en la misma bolsa a una suite de seguridad moderna convencional y a las primeras tecnologías "de una sola capa" (como los motores de firmas estáticas, la detección de cambios y las vacunas antivirus), al igual que tampoco hay punto de comparación entre Microsoft Word y *ed* o *edlin.*

Por más que tengan los mismos propósitos fundamentales que las aplicaciones hace rato obsoletas (ya sean la creación de texto y su procesamiento o, en nuestro caso, la detección y/o el bloqueo de software malicioso), tienen una gama mucho más amplia de funcionalidades. Un procesador de textos moderno incorpora elementos de otros ámbitos, que décadas atrás se habrían considerado puramente del dominio de procesadores de texto, hojas de cálculo y bases de datos.

El origen del engaño

Una suite de seguridad moderna enfocada en combatir malware no incluye una variedad tan amplia de elementos programáticos. No obstante, tiene capas de protección genérica que van más allá de las firmas (incluso de las firmas genéricas). Han ido evolucionado para convertirse en generaciones muy diferentes de productos y han incorporado tecnologías que aún no existían cuando se lanzaron al mercado los primeros productos de seguridad.

Hablar de los productos que recién llegan al mercado como si solo por eso fueran "la siguiente generación" que supera a la tecnología primitiva basada en firmas es un concepto erróneo y totalmente engañoso.

¿Firmas? ¿Qué firmas?

Hoy en día, incluso los motores antimalware comerciales modernos de una sola capa **van mucho más allá de la mera búsqueda de muestras específicas y de simples firmas estáticas.** Amplían su capacidad de detección de familias de malware conocidas y con valores de hash específicos, mediante la inclusión de otros elementos como las listas blancas, el análisis de la conducta, el bloqueo del comportamiento y la detección de cambios, entre otros, que antes solo se consideraban parte de las tecnologías puramente "genéricas".

Con esto no quiero decir que hay que confiar totalmente en un producto de una sola

Hablar de productos recién llegados al mercado como si solo por eso fueran "la siguiente generación" es un concepto erróneo y totalmente engañoso.

capa como los que suelen ofrecer muchas empresas convencionales en forma gratuita. **También es necesario utilizar otras "capas" de protección,** ya sea mediante el uso de una suite de seguridad de categoría comercial o replicando las funcionalidades en múltiples capas de este tipo de soluciones con componentes extraídos de diversas fuentes, incluyendo un producto antimalware de una sola capa.

Sin embargo, este último enfoque requiere un nivel de comprensión de las amenazas y las tecnologías de seguridad que la mayoría de las personas no tiene. De hecho, no todas las organizaciones tienen acceso a personal interno con tantos conocimientos, lo que muchas veces las deja a merced del marketing que se hace pasar por servicios de asesoramiento técnico.

Vuelta a la base

Aunque algunos productos "next-gen" son tan reservados acerca del funcionamiento de su tecnología que hacen que los productos antimalware convencionales parezcan de código abierto, **está claro que las distinciones entre los productos "fosilizados" y los "de la siguiente generación" suelen ser más terminológicas que tecnológicas.** No creo que los productos "next-gen" hayan ido mucho más allá de estos enfoques básicos para combatir el malware empleados por las soluciones "tradicionales" y definidos hace mucho tiempo por Fred Cohen (cuya introducción y definición del término virus informático prácticamente dio inicio a la industria antimalware en 1984). A saber:

- La identificación y el bloqueo de comportamiento malicioso.
- La detección de cambios inesperados e inapropiados.
- La detección de patrones que indiquen la presencia de malware conocido o desconocido.

Las maneras de implementar esos enfoques sin duda son mucho más avanzadas, pero esto no quiere decir que dicha progresión sea propiedad exclusiva de los productos lanzados recientemente. Por ejemplo, lo que generalmente vemos descrito como "indicadores de sistemas comprometidos" también podrían describirse como firmas (más bien débiles).

Más de un fabricante no ha logrado diferenciar en forma convincente entre el uso del análisis y el bloqueo de la conducta por parte de los productos antimalware convencionales. Es decir, no encuentran una diferencia entre el uso en sus propios productos de las funcionalidades de (por ejemplo) análisis/monitoreo/bloqueo del comportamiento, análisis de tráfico, etc.; y el uso de estas mismas tecnologías por parte de los productos antimalware convencionales. En su lugar, **eligieron promover una visión engañosa de la "tecnología fosilizada" y la cubrieron con palabras tecnológicas de moda para su comercialización.**

Bienvenido a la máquina

Consideremos, por ejemplo, las menciones frecuentes del "análisis de la conducta" y de las técnicas de aprendizaje automático (machine learning) "puro" como tecnologías que diferencian la siguiente generación de la primera. En el mundo real, el aprendizaje automático no se aplica únicamente a este sector del mercado. El progreso en áreas como las redes neuronales y el procesamiento en paralelo es tan útil para la seguridad en general como para otras áreas de la informática: por ejemplo, sin un cierto grado de automatización en el proceso de clasificación de muestras, no podríamos empezar a lidiar con la avalancha diaria de cientos de miles de muestras de amenazas que se deben examinar para lograr una detección precisa.

Sin embargo, el uso de términos como "pure machine learning" en el marketing de "next-gen" es un recurso de oratoria y no tecnológico. **Hablar de aprendizaje automático puro no solo implica que el**

Está claro que las distinciones entre los productos "fosilizados" y los "de la siguiente generación" suelen ser más terminológicas que tecnológicas.

aprendizaje automático en sí mismo de alguna manera ofrece una mejor detección que cualquier otra tecnología, sino también que es tan eficaz que no hay necesidad de supervisión humana. De hecho, **si bien la industria antimalware convencional ya ha utilizado el aprendizaje automático durante mucho tiempo, tiene sus ventajas y desventajas como cualquier otro enfoque.** No menos importante es el hecho de que **los creadores de malware suelen estar al día de los avances en machine learning** (al igual que los proveedores de seguridad que detectan su malware) y dedican mucho esfuerzo para encontrar formas de evadirlo, como ocurre con otras tecnologías antimalware.

El análisis del comportamiento

Del mismo modo, **cuando los fabricantes de productos "next-gen" hablan del análisis de comportamiento como si ellos fueran quienes lo inventaron, en el mejor de los casos estarán mal informados:** el concepto de análisis de la conducta y las tecnologías que utiliza este enfoque se han estado usado en las soluciones antimalware convencionales durante décadas. **De hecho, casi cualquier método de detección que vaya más allá de las firmas estáticas se puede definir como análisis del comportamiento.**

La selección natural y no natural

El periodista Kevin Townsend hace poco me preguntó:

> *¿Hay alguna manera de que la industria pueda ayudar al usuario a comparar y elegir entre productos de la primera [...] y la segunda generación [...] para la detección de software malicioso?*

Dejando de lado la terminología totalmente errónea de la primera y segunda generación, la respuesta es sí, por supuesto que la hay. De hecho, algunas de las empresas que promueven sus productos como "de segunda generación" y alegan que su tecnología es demasiado avanzada para estas pruebas comparativas **en realidad han dado la razón sin darse cuenta cuando comenzaron a comparar la eficacia de sus propios productos con los de fabricantes de la "primera generación".** Por ejemplo, al menos un fabricante de "next-gen" usó muestras de malware en sus propias demostraciones públicas: si no es posible comparar las diferentes generaciones de productos en un mismo entorno de prueba independiente, ¿cómo se puede reclamar que estos tipos de demostraciones públicas son válidas?

Otro argumento de marketing engañoso de los fabricantes de productos de "next-gen" es afirmar que "los productos de la primera generación no detectan el malware en memoria que no se basa en archivos" (lo cual hemos hecho durante décadas). Un ejemplo particularmente inepto es cuando se utilizaron los resultados de una encuesta mal confeccionada que se basaba en los derechos a la Libertad de Información para "probar" el "fracaso lamentable" del antimalware tradicional sin siquiera intentar distinguir entre los intentos de ataque y los ataques exitosos.

Pruebas y pseudo pruebas

Es muy común que los datos de VirusTotal (VT) se utilicen indebidamente por errores de interpretación, como si este y otros servicios similares fueran adecuados para usarse como "servicios de evaluación de múltiples motores antivirus", lo que no es el caso. Como explica VT:

> *No se debe utilizar VirusTotal para generar métricas comparativas entre diferentes productos antivirus. Los motores antivirus pueden ser herramientas sofisticadas con funcionalidades de detección adicionales que posiblemente no funcionen dentro del entorno de exploración de VirusTotal. En consecuencia, los resultados de los análisis de VirusTotal no están destinados a utilizarse para comparar la eficacia de los productos antivirus.*

El uso de términos como "pure machine learning" en el marketing de "next-gen" es un recurso de oratoria y no tecnológico.

Se puede decir que VT "prueba" un **archivo** mediante su exposición a un lote de motores de detección de malware. Sin embargo, no utiliza toda la gama de tecnologías de detección incorporadas en estos productos, por lo que no prueba ni representa con precisión la eficacia de los **productos.**

Un fabricante de productos de "next-gen" habló orgulloso sobre la detección de una muestra específica de ransomware por su producto un mes antes de que la muestra fuera enviada a VirusTotal. Sin embargo, al menos un fabricante convencional/tradicional ya había detectado ese hash un mes antes de que el fabricante de productos de "next-gen" anunciara dicha detección. Simplemente no se puede medir la eficacia de un producto a partir de los informes de VirusTotal, porque VT no es una entidad de evaluación y sus informes solo reflejan parte de la funcionalidad de los productos que utiliza.

De lo contrario, no habría necesidad de que existieran entidades evaluadoras de renombre como Virus Bulletin, SE Labs, AV-Comparatives y AV-Test, que se esfuerzan enormemente para que sus pruebas sean lo más precisas y representativas posible.

Hacia la cooperación

Uno de los giros radicales más dramáticos de 2016 tuvo lugar cuando VirusTotal cambió sus términos y condiciones de modo que **las empresas de "next-gen" que quieran beneficiarse del acceso a las muestras presentadas por las empresas "de la primera generación", ahora también deberán contribuir.** Para citar el blog de VirusTotal:

> *...Ahora se requiere que todas las empresas integren su motor de detección en la interfaz VT pública, con el fin de ser elegibles para recibir los resultados de antivirus como parte de los servicios de la API de VirusTotal. Además, los nuevos motores que se unan a la comunidad tendrán que pasar una certificación y/o revisiones independientes por los auditores de seguridad de acuerdo con las mejores prácticas de la organización Anti-Malware Testing Standards Organization (AMTSO).*

Mientras que muchos fabricantes de productos de "next-gen" inicialmente respondieron con frases como *"No es justo"*, *"Los dinosaurios conspiran contra nosotros"* y *"Como no utilizamos firmas, no necesitamos a VT ni nos importa lo que haga"*, al parecer, varias empresas importantes de la industria igualmente se prepararon para cumplir con los requisitos, unirse a la AMTSO y abrirse al mundo de las pruebas independientes (con esto quiero decir a las pruebas **reales,** no a las pseudo pruebas como usar datos de VirusTotal).

Dado que los fabricantes de soluciones de "next-gen" en el pasado solían protestar porque sus propios productos no se podían probar, sobre todo por las entidades evaluadoras "tendenciosas" representadas en la AMTSO, quizá esto sugiera la posibilidad alentadora de que **no todos los clientes se basan exclusivamente en el marketing al momento de tomar decisiones de compra.**

Compartir en partes iguales

¿Por qué los fabricantes de productos de "next-gen" ahora decidieron que **sí** necesitan trabajar con VirusTotal? **Resulta que VT comparte las muestras que recibe con los fabricantes y suministra una API que sirve para comprobar archivos automáticamente, mediante su verificación con todos los motores empleados por VT.** Esto no solo les permite a las empresas de seguridad acceder a una base común de muestras compartidas por los fabricantes convencionales, sino que **también les permite compararlas con muestras indeterminadas y con sus propias detecciones, de modo que pueden "entrenar" sus algoritmos de aprendizaje automático** (cuando sea pertinente).

¿Y por qué no? Eso no es muy diferente a la forma en que los fabricantes que llevan más tiempo establecidos utilizan Virus-

Simplemente no se puede medir la eficacia de un producto a partir de los informes de VirusTotal.

Total. La diferencia radica en el hecho de que **bajo los nuevos términos y condiciones, los beneficios son para tres partes: los fabricantes** (de cualquier generación de productos) se benefician con el acceso a los recursos de VirusTotal y a ese enorme conjunto de muestras. **VirusTotal se beneficia por ser un agregador de información,** así como en su papel de proveedor de servicios Premium. **Y finalmente, el resto del mundo se beneficia por la existencia de un servicio gratuito que les permite a los usuarios revisar archivos sospechosos** individuales usando una amplia gama de productos.

Aumentar esta gama de productos para incluir tecnologías menos tradicionales debería mejorar la precisión del servicio, mientras que los nuevos participantes, tal vez, serán más escrupulosos y no usarán indebidamente los informes de VT como pseudo pruebas y para marketing cuando ellos mismos están expuestos a ese tipo de manipulación.

Evaluación del producto completo

La forma en que los evaluadores alineados con la AMTSO se han ido desplazando hacia las "evaluaciones de productos completos" en los últimos años es exactamente la dirección que deben tomar si piensan evaluar aquellos productos menos" tradicionales" de manera justa (o, en todo caso, igual de justa que a los productos convencionales).

Sin embargo, se puede argumentar que las entidades evaluadoras **podrían** estar usando metodologías conservadoras. Hace no mucho tiempo, las pruebas estáticas estaban a la orden del día (y en cierta medida las siguen usando los evaluadores que no están alineados con la AMTSO, que ha desalentado su uso desde que se fundó la organización). AMTSO, a pesar de todos sus defectos, es mayor (y más desinteresada) que la suma de sus partes, ya que está integrada por una serie de investigadores que provienen tanto de los fabricantes como de las organizaciones evaluadoras, y, en cambio, el personal de marketing no se encuentra fuertemente representado. De este modo, **no es tan fácil para las empresas individuales ubicadas a ambos lados de esta línea divisoria ejercer una influencia indebida sobre la organización si solo buscan sus propios intereses.**

Si las empresas de "next-gen" son capaces de apretar los dientes y comprometerse con esta cultura, todos saldremos beneficiados. En el pasado, la AMTSO ha sufrido la presencia de organizaciones cuyo propósito parecía centrarse excesivamente en la manipulación o cosas peores; sin embargo, **el nuevo equilibrio entre los fabricantes "viejos y nuevos" y los evaluadores que forman parte de la organización presenta buenas posibilidades de sobrevivir a cualquier tipo de actividad dudosa de este estilo.**

En el Cenozoico

Hace varios años, cerré un artículo de Virus Bulletin con estas palabras:

> *¿Podemos imaginar un mundo sin antivirus, ya que al parecer se están leyendo sus últimas exequias fúnebres? Las mismas empresas que actualmente menosprecian los programas antivirus a la vez que financian sus investigaciones ¿serán capaces de igualar la experiencia de las personas que trabajan en los laboratorios antimalware?*

Creo que tal vez ya tenemos la respuesta… Pero **si la autodenominada "next-gen" acepta sus propias limitaciones, modera sus métodos agresivos de marketing y aprende sobre los beneficios de la cooperación entre empresas con diferentes fortalezas y capacidades, aún todos podremos beneficiarnos de esta distensión diplomática.**

No todos los clientes se basan exclusivamente en el marketing al momento de tomar decisiones de compra.

AMTSO, a pesar de todos sus defectos, es mayor (y más desinteresada) que la suma de sus partes.

IoT y ransomware en el sector de la salud: la punta del iceberg

- El ransomware es solo la punta del iceberg
- Dispositivos médicos y para monitorear la actividad física
- Protección de dispositivos médicos

AUTOR

Lysa Myers
Security Researcher

6

IoT y ransomware en el sector de la salud: la punta del iceberg

Las filtraciones de datos de Anthem y Premera del año pasado hicieron que el público general tomara más consciencia sobre la importancia de la seguridad en las organizaciones de la industria de la salud.

El año 2016 trajo un menor número de casos de brechas masivas en el sector, pero lamentablemente esto no significa que el problema esté resuelto. De hecho, este año hubo un exceso de ataques de ransomware exitosos a una gran variedad de industrias, entre las cuales **los centros de salud constituyeron un objetivo particularmente atractivo.** Si a estos eventos le sumamos la mayor cantidad de dispositivos médicos conectados a Internet y aquellos para monitorear la actividad física, **todo indicaría que el sector sanitario seguirá enfrentando desafíos de seguridad significativos en el futuro.**

El ransomware es solo la punta del iceberg

Se podría pensar en la creciente ola de ransomware como un problema en sí mismo. **Si bien está causando grandes dolores de cabeza y pérdidas monetarias, su éxito es síntoma de un problema aún mayor.** El ransomware es un tipo de amenaza que generalmente se puede mitigar si se siguen las prácticas mínimas de seguridad para endpoints y redes. De hecho, **cuando se descubrieron las primeras variantes, muchos expertos en seguridad no se tomaron el problema tan en serio, ya que consideran que estos ataques se pueden frustrar fácilmente,** incluso cuando el archivo de malware en sí no se llega a detectar antes de la ejecución: en este caso, **para evitar pagar el rescate, la víctima solo deberá restaurar el sistema desde sus backups.** Pero, **lamentablemente, cuando se trata de seguridad práctica, las medidas de protección a menudo no se aplican de la forma en que la comunidad de seguridad esperaría.** A muchos les puede parecer al principio que es más costoso restaurar el sistema desde los backups que pagando el pedido de rescate. **Algunas empresas directamente no hacen backups periódicos.** Los productos de seguridad diseñados para detectar correos electrónicos, archivos, tráfico o enlaces maliciosos pueden estar configurados incorrectamente. **A veces ni siquiera se usan productos de seguridad.** Las estrategias de creación de backups pueden estar mal implementadas, de modo que las copias de seguridad también son vulnerables a los ataques de ransomware u otros riesgos. Los usuarios pueden desactivar sus productos de seguridad o deshabilitar ciertas funciones si consideran que dichas medidas les impiden hacer su trabajo. **Más allá de la causa, el resultado final es que las empresas afectadas pueden sentir que deben pagarles a los criminales con la esperanza de recuperar sus datos.**

En las instituciones sanitarias, donde el acceso rápido a los datos puede ser una cuestión de vida o muerte, el costo de ser atacado por el ransomware crece considerablemente. Los delincuentes lo saben y están apuntando en forma deliberada a las organizaciones médicas. Revertir esta tendencia requiere algunas acciones simples pero potentes. Sin embargo, si se logra establecer una base sólida de seguridad, seremos

El año 2016 trajo un menor número de casos de brechas masivas en el sector, pero lamentablemente esto no significa que el problema esté resuelto.

capaces de reducir tanto los efectos de futuras amenazas de malware como los riesgos que traigan aparejadas las nuevas tecnologías.

La importancia de evaluar los riesgos y corregir las deficiencias

En WeLiveSecurity ya hablamos sobre la importancia de la evaluación de riesgos en la industria sanitaria. **Al categorizar regularmente los activos y los métodos de transmisión, es posible identificar posibles vulnerabilidades y riesgos.** Si se toman en cuenta la probabilidad y el costo potencial de estos riesgos, se puede tener una idea de las cosas que necesitan abordarse con mayor urgencia. **En el caso del ransomware, la evaluación del riesgo puede ayudar a resolver la situación de diversas maneras:**

- ¿Qué activos corren el riesgo de ser cifrados por el ransomware?
- ¿Qué métodos de transmisión le permiten al ransomware acceder a la red?
- ¿Qué métodos le permiten a la amenaza recibir comandos externos para cifrar archivos?
- ¿Cuál es la probabilidad de que la organización se vea afectada por esta amenaza?
- ¿Cuál es el daño monetario potencial que puede provocar un ataque exitoso?

Los activos que corren el riesgo de ser cifrados son, por desgracia, casi todos los datos o sistemas a los que se puede acceder desde la red o Internet. Los ataques de ransomware a menudo se originan por correos electrónicos de phishing que contienen archivos maliciosos o enlaces a través de los cuales se descargan los archivos maliciosos. Por lo tanto, el método de transmisión en este caso sería el correo electrónico, con un enfoque en la ingeniería social. El malware normalmente necesita ser capaz de comunicarse con su canal de Comando y Control para recibir instrucciones, lo que muchas variantes hacen utilizando los protocolos comunes como HTTP o HTTPS. Aunque los detalles de los daños monetarios varían de una organización a otra, la probabilidad de ser víctima de un ataque es actualmente muy alta para todos los sectores y tamaños de empresas. **Para reducir el riesgo, se pueden hacer varias cosas.** Por ejemplo:

- **Crear backups periódicos** y luego verificarlos es una forma muy efectiva de mitigar los daños una vez que un sistema o una red es víctima de un ataque.
- **Segregar la red** limita los efectos del malware una vez que éste ingresa a los sistemas.
- **Filtrar el correo electrónico** en busca de spam y de phishing, así como bloquear los tipos de archivos más populares utilizados por los autores de malware, ayuda a disminuir el riesgo de que el malware llegue hasta los usuarios.
- **Educar a los usuarios** desde que ingresan a la empresa y ofrecer capacitaciones periódicas disminuye las probabilidades de que ejecuten un archivo de malware.
- **Animar a los usuarios** a enviar los correos electrónicos o los archivos sospechosos al personal de TI o de seguridad ayuda a aumentar la eficacia de los métodos de filtrado.
- **Usar un software antimalware** en la puerta de enlace, en la red y en los endpoints ayuda a identificar el malware y a evitar que entre en la red, o a reducir el daño ocasionado en caso de que el archivo malicioso logre evadir las defensas iniciales de los sistemas.
- **El firewall y el software de prevención** de intrusiones ayudan a identificar el tráfico de red desconocido o no deseado.

Estos pasos no solo mitigarán el riesgo de un ataque de ransomware: también ayudarán a prevenir una variedad de otros tipos de ataques. Evaluar en forma exhaus-

Los activos que corren el riesgo de ser cifrados son, por desgracia, casi todos los datos o sistemas a los que se puede acceder desde la red o Internet.

tiva los riesgos y mejorar la postura global de seguridad de una organización reduce significativamente la frecuencia y la gravedad de todo tipo de problemas de seguridad.

Dispositivos médicos y para monitorear la actividad física

A medida que la industria médica se vuelve más informatizada, es mayor la cantidad de profesionales de la salud y los pacientes que comienzan a utilizar dispositivos médicos y aquellos diseñados para monitorear la actividad física. **Estos dispositivos suelen estar repletos de información confidencial;** sin embargo, la seguridad y la privacidad en general son una preocupación secundaria. **Como hemos visto al analizar la tendencia del ransomware, el riesgo de tener información de alta confidencialidad sin una base sólida de seguridad puede ocasionar graves problemas.** Pero como esta tecnología es bastante nueva, ahora es un buen momento para centrar nuestra atención en cómo proteger los equipos.

Dispositivos médicos en redes de instituciones de salud

Los dispositivos médicos utilizados en las redes de hospitales pueden ser máquinas grandes y costosas, que con frecuencia usan sistemas operativos comunes (y con demasiada frecuencia obsoletos) como Windows XP Embedded. A menudo proporcionan un fácil acceso al resto de la red hospitalaria donde se guardan muchos tipos de datos confidenciales: información financiera para la facturación, información de identidad para brindar seguros médicos, así como información relacionada con la salud generada por las visitas de los pacientes. **Desde una perspectiva criminal, estos datos son sumamente lucrativos: tienen el potencial de ser diez veces más valiosos que los detalles de las tarjetas de crédito o débito.** Los dispositivos médicos de los hospitales suelen utilizar un sistema operativo similar al que usan los equipos de escritorio, por lo que **es posible aplicar la misma tecnología y las mismas técnicas para protegerlos.** Sin embargo, **si un dispositivo tiene un sistema operativo obsoleto** (y potencialmente sin soporte) **se le deberá dar una protección adicional significativa.** Hasta puede ser preferible mantener la máquina completamente desconectada de todas las redes, aunque aún así se deberá proteger contra amenazas que se puedan propagar por medios extraíbles.

El riesgo de tener información de alta confidencialidad sin una base sólida de seguridad puede ocasionar graves problemas.

Dispositivos médicos y de monitoreo en el hogar

Los dispositivos médicos y de monitoreo de actividad utilizados en el hogar suelen ser muy pequeños para que se puedan usar o implantar sin resultar intrusivos. La mayoría utiliza sistemas operativos Linux o basados en Linux. Pueden estar conectados a Internet u ofrecer sincronización con un dispositivo móvil o equipo de escritorio; y al igual que los dispositivos que se usan en hospitales, también suelen actualizarse con poca frecuencia... cuando se actualizan. **Aunque un dispositivo utilizado por el paciente en su casa no suele almacenar información de tarjetas de pago, puede tener otros datos que a los delincuentes les interesaría robar o modificar,** tales como: la dirección de correo electrónico, el nombre de usuario, la contraseña y los datos de GPS, incluyendo la dirección particular o laboral. Además, el dispositivo podría indicar cuando el usuario está fuera de casa o dormido. **Un ataque a un dispositivo médico implantable podría permitir que los delincuentes hicieran una serie de cambios a las medidas prescritas, lo que podría causar problemas médicos graves (o incluso mortales).**

En cuanto a un dispositivo médico personal, es de suma importancia evitar que se use para dañar a los usuarios o comprometer su privacidad. Es evidente que un ataque a una bomba de insulina o un marcapasos con conexión a Internet será significativamente diferente a un ataque a un dispositivo para monitorear la actividad física. Las medidas de seguridad necesarias para proteger los

dispositivos serán las mismas, aunque una bomba de insulina o un marcapasos pueden tener activados ajustes más estrictos en forma predeterminada.

Protección de dispositivos médicos

Los fabricantes de dispositivos médicos para uso personal o en hospitales tienen en sus manos la oportunidad de iniciar un cambio hacia una mayor seguridad, mediante la seria consideración de este problema desde la fase de diseño. **Hay varias medidas que deberían tomar** para hacerlos más seguros:

- **Diseñar teniendo en cuenta la privacidad:** Lee sobre los siete principios de la Privacidad por diseño (en inglés).
- **Cifrar datos:** Proteger los datos con cifrado fuerte, tanto los guardados en disco como los que se encuentran en tránsito. Por ejemplo, cuando se envían por correo electrónico, por la Web o por mensajería instantánea, o cuando se sincronizan con el equipo del usuario.
- **Clarificar las opciones de almacenamiento de datos:** Darles a los usuarios la capacidad de almacenar localmente los datos monitoreados, en vez de que tengan que dejarlos en la nube.
- **Autenticar el acceso a las cuentas:** Verificar que los usuarios sean quienes dicen ser. Es imprescindible que se autentiquen antes de que visualicen, compartan o modifiquen la información almacenada en los dispositivos implantados, dado que las consecuencias de su uso indebido son significativamente más costosas. Por lo tanto, es necesario que los fabricantes suministren múltiples factores de autenticación para el acceso a las cuentas online.
- **Crear un mecanismo de protección integrado en caso de fallas:** Los errores ocurren. Por eso, los productos deberán ofrecer la posibilidad de revertirse a un estado predeterminado que mantenga el acceso a las funcionalidades críticas y no ponga en peligro a los usuarios cuando se produzca algún problema.
- **Asumir que el código se puede llegar a usar con fines maliciosos:** El código legítimo puede manipularse para que el dispositivo ejecute código no autenticado. Es de vital importancia manejar los errores teniendo siempre en cuenta esta posibilidad para que los dispositivos no se puedan utilizar maliciosamente.
- **Prepararse para vulnerabilidades:** Establecer y publicar una política de revelación responsable para informar las vulnerabilidades. regiones en el futuro previsible. A pesar de las dificultades actuales, existe la oportunidad de llevar a cabo una transformación significativa que podría servirles a otras industrias.
- **Prepararse para posibles brechas de seguridad:** Es necesario crear un plan de respuesta a incidentes para poder reaccionar correctamente en caso de una fuga de datos. De esta forma, en el caso de una emergencia, tu respuesta será más rápida y te permitirá elegir tus palabras sabiamente.
- **Prepararse para el escrutinio gubernamental:** Hay diversas organizaciones, como la Comisión Federal de Comercio (FTC) y la Administración de Alimentos y Drogas (FDA) en los Estados Unidos, que monitorean de cerca el ámbito de los dispositivos médicos, por lo que implementar cambios ahora puede ayudar a evitar problemas legales y multas considerables en el futuro.

Es probable que la seguridad de la industria de la salud se convierta en el foco de atención pero también puede ser un modelo de cambio positivo, a medida que la Internet de las Cosas se abre paso en nuestros hogares y lugares de trabajo.

Aunque un dispositivo utilizado por el paciente en su casa no suele almacenar información de tarjetas de pago, puede tener otros datos que a los delincuentes les interesaría robar o modificar.

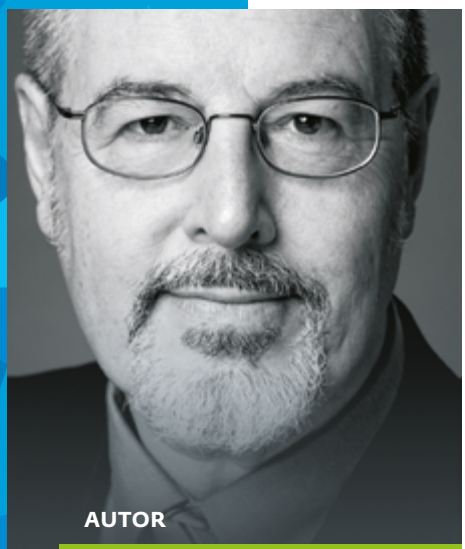
La industria de la salud puede convertirse en un modelo de cambio positivo., a medida que la Internet de las Cosas se abre paso en nuestros hogares y lugares de trabajo.

Amenazas para infraestructuras críticas: la dimensión de Internet

- Definición de incidentes
- Incidentes problemáticos
- Un panorama preocupante

AUTOR

Cameron Camp
Malware Researcher



AUTOR

Stephen Cobb
Senior Security Researcher

7

Amenazas para infraestructuras críticas: la dimensión de Internet.

Los ataques cibernéticos a la infraestructura crítica fueron una tendencia clave en 2016, y lamentablemente se cree que continuarán llegando a los titulares y complicando la vida cotidiana de las personas durante 2017.

A comienzos del año 2016 fue publicado en WeLiveSecurity el análisis que hizo Anton Cherepanov sobre Black Energy, un código malicioso utilizado en los ataques contra las compañías eléctricas ucranianas, que resultaron en cortes de electricidad por varias horas para cientos de miles de hogares en esa parte del mundo. Sin embargo, antes de discutir este y otros incidentes, será útil que definamos con un poco más de precisión la terminología. Al parecer, "infraestructura" puede significar cosas diferentes para diferentes personas, y no todo el mundo está de acuerdo en lo que significa "crítica" en este contexto.

Definición de incidentes

En Estados Unidos, el Departamento de Seguridad Nacional (DHS, por sus siglas en inglés) está encargado de proteger la infraestructura crítica, que se clasifica en 16 sectores distintos, "*cuyos activos, sistemas y redes, ya sean físicos o virtuales, son tan vitales para los Estados Unidos que su incapacidad o destrucción tendrían un efecto debilitante sobre la seguridad, la seguridad económica nacional, la salud o seguridad pública nacional, o cualquier combinación de éstas*".

Si te interesa, encontrarás enlaces a las definiciones detalladas de los 16 sectores en dhs.gov, pero aquí al menos queremos mencionar sus títulos para que tengas una idea de lo omnipresente que es la infraestructura crítica:

- → Instalaciones químicas
- → Instalaciones comerciales
- → Comunicaciones
- → Fabricación crítica
- → Represas
- → Bases industriales de defensa
- → Servicios de emergencia
- → Energía
- → Servicios financieros
- → Alimentación y agricultura
- → Instalaciones gubernamentales
- → Salud pública
- → Tecnología de la información
- → Reactores, materiales y residuos nucleares
- → Sistemas de transporte
- → Sistemas de agua y agua residual

Todos estos sectores dependen en cierta medida de la infraestructura digital conocida como Internet, pero a veces hay cierta confusión entre la infraestructura crítica y la infraestructura de Internet. La diferencia es clara si nos fijamos en dos incidentes clave que ocurrieron en 2016: las interrupciones de energía ucranianas mencionadas al principio, y el fenómeno conocido como el ataque de denegación de servicio distribuido a Dyn mediante dispositivos de la Internet de las Cosas (IoT por sus siglas en inglés) previamente infecta-

Al parecer, "infraestructura" puede significar cosas diferentes para diferentes personas, y no todo el mundo está de acuerdo en lo que significa "crítica" en este contexto.

dos, que tuvo lugar el 21 de octubre (y que abreviaremos como 21/10).

Incidentes problemáticos

Los ataques de suministro de energía eléctrica en Ucrania fueron posibles por la infraestructura de Internet. Los atacantes usaron el correo electrónico y otras formas de conectividad por Internet para ingresar a las computadoras en red de la empresa de energía eléctrica. En algunas organizaciones atacadas, la falta de impedimentos efectivos les permitió a los atacantes acceder, a través de Internet, a las aplicaciones que controlan remotamente la distribución de electricidad. El investigador de ESET Robert Lipovsky puso los ataques en contexto de este modo: *"El 23 de diciembre de 2015, alrededor de la mitad de los hogares en la región ucraniana llamada Ivano-Frankivsk (con una población de 1,4 millones de habitantes) se quedaron sin electricidad durante varias horas"*. **Un corte de energía como éste es claramente un ataque a la infraestructura crítica, así como una posible prueba para planificar ataques futuros.**

El incidente del 21/10 fue una serie de grandes ataques de Denegación de Servicio Distribuido (DDoS) que hicieron uso de decenas de millones de dispositivos conectados a Internet (denominados colectivamente la Internet de las Ccosas o IoT) para llegar a los servidores de una empresa llamada Dyn, que proporciona el Servicio de Nombres de Dominio (DNS) a muchas empresas estadounidenses conocidas. DNS es la "libreta de direcciones" para Internet; un sistema para asegurarse de que las solicitudes de información en Internet se entreguen al host correcto (servidor, equipo portátil, tableta, smartphone, heladera inteligente, etc.). **El efecto de los ataques del 21/10 fue impedir o retrasar el tráfico a sitios web, servidores de contenido de Internet y otros servicios de Internet, como el correo electrónico.**

Debido a la naturaleza altamente interdependiente de los servicios de Internet, **los ataques del 21/10 tuvieron un impacto negativo,** sus daños colaterales provocaron una reacción en cadena que afectó a un porcentaje significativo de empresas comerciales de los Estados Unidos, a pesar de que no eran el blanco directo del ataque.

Imagina a una empresa que vende software online, cuya tienda en la Web no es uno de los objetivos de los atacantes, pero que de todas formas el tráfico a su sitio se ve interrumpido porque no es posible acceder a los servidores que distribuyen los anuncios online para vender sus productos. Las páginas web del sitio de la empresa no se llegan a cargar correctamente debido a que dependen de una red de distribución de contenido (CDN) que es temporalmente inaccesible. Incluso cuando los clientes pueden completar sus compras online, algunos no logran llegar al servidor de contenido para descargar el producto que acaban de comprar. Otros no pueden activar su compra porque el servidor de licencias de software agota el tiempo de espera. Los clientes, frustrados, envían un correo electrónico a la empresa. Las líneas telefónicas de atención al cliente comienzan a sonar. Se cambia el saludo inicial del contestador automático de la empresa para informar sobre la situación. Las campañas de anuncios online y las compras por palabras clave en motores de búsqueda se suspenden para ahorrar dinero y reducir la frustración entre los clientes potenciales. Se pierden ingresos. El personal se desvía de sus deberes normales.

Por supuesto, durante el 21/10, distintas empresas se vieron afectadas de manera diferente. Algunas experimentaron interrupciones prolongadas, otras quedaron offline por solo unos minutos, pero incluso un minuto de tiempo en Internet puede representar una gran cantidad de transacciones. Por ejemplo, los ingresos minoristas online de Amazon por minuto superan los USD 200.000. En ese mismo minuto, más

Claramente, los ataques del 21/10 demostraron cuán vital es la infraestructura de Internet para el comercio diario, pero ¿fue también un ataque a la infraestructura crítica?.

de 50.000 apps se descargan desde la tienda de aplicaciones móviles de Apple. **Claramente, los ataques del 21/10 demostraron cuán vital es la infraestructura de Internet para el comercio diario, pero ¿fue también un ataque a la infraestructura crítica?**

No escuchamos que los ataques del 21/10 hayan afectado a los sectores críticos, como el transporte, el agua, la agricultura, la energía, etc. Sin embargo, **no es difícil ver cómo variaciones posibles de los ataques del 21/10 a los servidores DNS podrían afectar los elementos de la infraestructura crítica,** como la venta de pasajes aéreos, las comunicaciones en la cadena de suministro, o incluso la distribución de energía eléctrica. Y también es posible ver estos ataques como parte de un patrón, como indicó el tecnólogo de seguridad Bruce Schneier: *"Durante el último año o dos, se han estado probando las defensas de las empresas que trabajan con los sectores críticos de Internet"*.

Un panorama preocupante

La tendencia probable para 2017 es que los atacantes sigan sondeando la infraestructura crítica a través de la infraestructura de Internet. Distintos tipos de atacantes seguirán buscando maneras de causar daño, denegar el servicio o secuestrar datos para pedir un rescate.

También se espera que haya más ataques a la misma infraestructura de Internet, interrumpiendo el acceso a datos y servicios. Y por supuesto, algunos de esos datos y servicios podrían ser vitales para el buen funcionamiento de una o más de las 16 categorías de infraestructura crítica mencionadas. Por ejemplo, algunos cibercriminales han mostrado su interés por atacar datos y sistemas médicos, y es probable que esta tendencia sea global. Al mismo tiempo, sabemos que hay en marcha muchos esfuerzos en diferentes países con el objetivo de mejorar la seguridad cibernética de los sistemas que apoyan la infraestructura crítica. En los Estados Unidos, existen 24 Centros de Intercambio y Análisis de Información (ISAC) que cubren la mayoría de los aspectos de los 16 sectores de infraestructura crítica y que proporcionan canales de comunicación e intercambio de conocimientos en materia de seguridad cibernética. En septiembre, el Industrial Internet Consortium publicó un proyecto de seguridad para la industria de la Internet de las Cosas con el objetivo de llegar a un consenso generalizado de la industria sobre cómo proteger este sector en rápido crecimiento.

Esperamos sinceramente que esfuerzos como este, y otros en todo el mundo, obtengan el respaldo y los recursos que necesitan para tener éxito. Sin embargo, para que esto suceda **hará falta mucho más que buenas intenciones. Incluso podría requerir la presión política de la gente más propensa a sufrir los ataques cibernéticos a la infraestructura crítica: el electorado.** Por ejemplo, podríamos argumentar que el proyecto de ley para otorgarle al gobierno de los Estados Unidos más poder para proteger la red eléctrica ante ciberataques fue un éxito rotundo. De hecho, en abril de 2016, el Senado de los Estados Unidos aprobó el proyecto con apoyo bipartidista. Sin embargo, aunque 2017 se acerca rápidamente, la ley aún no está vigente.

A medida que el paisaje global se vuelve cada vez más interconectado e interdependiente (superando las fronteras políticas, físicas e ideológicas), **nos espera una mezcla interesante y compleja de reacciones políticas y sociales de los Estados-Nación** que ahora necesitan luchar con las implicaciones de un ataque a dicha infraestructura crítica y que, de ocurrir, necesitarán tener preparada una respuesta defensiva y/u ofensiva apropiada para el ataque. **Probablemente estemos subestimando la situación si solo dijéramos que nos espera un año desafiante por delante.**

No es difícil ver cómo variaciones posibles de los ataques del 21/10 a los servidores DNS podrían afectar los elementos de la infraestructura crítica.

Desafíos e implicaciones de legislaciones sobre ciberseguridad

- Ciberseguridad: organización, colaboración y difusión en el orbe
- Desafíos e implicaciones en la promulgación de leyes relacionadas con la ciberseguridad
- Hacia el desarrollo y divulgación de la cultura de ciberseguridad

AUTOR

Miguel Angel Mendoza
Security Researcher

8

Desafíos e implicaciones de legislaciones sobre ciberseguridad

El impacto de la tecnología ha alcanzado a casi todos los aspectos de la sociedad y lo seguirá haciendo en los próximos años.

Gran parte de las actividades de la actualidad no se entenderían sin los sistemas de información, los dispositivos electrónicos o las redes de datos, una tendencia que conduce hacia la hiperconectividad. De forma paralela **aparecen nuevas amenazas y vulnerabilidades, determinantes para los riesgos que siguen aumentado en cantidad, frecuencia o impacto.** Por lo tanto, la trascendencia de la tecnología para las sociedades actuales y los riesgos asociados a su uso, muestran **la necesidad de proteger la información y otros bienes a distintos niveles y ámbitos, ya no solo en las industrias, empresas o usuarios, sino incluso para los países mismos.** Por ello, diversas legislaciones en el mundo instan a aumentar y mejorar la seguridad a partir de criterios objetivos de moralidad y ética.

La promulgación de leyes relacionadas con el ámbito de la ciberseguridad plantea la importancia de contar con marcos normativos de aplicación a gran escala, que contribuyen a reducir incidentes de seguridad, combatir delitos informáticos, al tiempo que desarrollan y permean una cultura de ciberseguridad. Pero más allá de los beneficios que las legislaciones pueden traer a la seguridad de los datos, la realidad es que **existen distintas tensiones, posturas y contrapuntos que hacen de su implantación una tarea no tan sencilla.** En la presente sección repasaremos algunas de las legislaciones más significativas a nivel mundial y algunos de los retos actuales y futuros a los que se enfrentan los Estados, empresas y usuarios/ciudadanos alrededor del mundo.

Ciberseguridad: organización, colaboración y difusión en el orbe

En los últimos tiempos se ha observado una tendencia hacia el desarrollo de nuevas legislaciones relacionadas con la ciberseguridad a nivel global. A partir de la colaboración entre los sectores público y privado para el intercambio de información y la creación de los organismos de seguridad cibernética en los países, **se pretende contar con las herramientas para hacer frente a los riesgos de la era digital y legislar en materia de delitos informáticos.**

Unión Europea

Recientemente la Unión Europea adoptó la Directiva NIS para la seguridad de redes y sistemas de información, que busca la promulgación de legislaciones que instan a los países miembros a estar equipados y preparados para dar respuesta a incidentes, a través de contar con un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) y una autoridad nacional competente en la materia. La creación de una red CSIRT pretende promover la cooperación rápida y eficaz, el intercambio de información relacionada con riesgos y el desarrollo de una cultura de seguridad entre los sectores esenciales para la economía y sociedad, como el energético, transporte, financiero, salud o infraestructura digital. Las nuevas leyes buscan generar un mismo nivel de desarrollo en las capacidades de ciberseguridad, para evitar incidentes que atenten contras las actividades económicas, la infraestructura, la confianza de

Más allá de los beneficios que las legislaciones pueden traer a la seguridad de los datos, la realidad es que existen distintas tensiones, posturas y contrapuntos que hacen de su implantación una tarea no tan sencilla.

usuarios o el funcionamiento de sistemas y redes críticos para cada país.

Estados Unidos

A finales de 2015 el Congreso de los Estados Unidos aprobó la denominada Ley de Ciberseguridad, para proteger al país de ataques cibernéticos de forma responsable y con la suficiente rapidez para atender las emergencias, a través de un marco que promueve el intercambio de información sobre amenazas informáticas entre el sector privado y el gobierno. De acuerdo con la ley, la información sobre una amenaza que se encuentra en un sistema puede ser compartida con el propósito de prevenir ataques o mitigar riesgos que pudiera afectar otras empresas, organismos o usuarios. A través del uso de controles de seguridad, la recopilación de información y otras medidas de protección, las organizaciones y el gobierno pueden coordinar acciones de inteligencia y de defensa.

Latinoamérica

En un informe de reciente publicación se aplicó un modelo para determinar la capacidad de seguridad cibernética, en los países de Latinoamérica y el Caribe. Este documento resalta la importancia de la divulgación responsable de información en las organizaciones del sector público y privado cuando se identifica una vulnerabilidad. También, destaca la importancia de los marcos legislativos, la investigación, el tratamiento de pruebas electrónicas, así como la formación de jueces y fiscales en el ámbito de ciberseguridad. La adhesión a convenios internaciones como el de Budapest y la firma de acuerdos transfronterizos para la cooperación, son otros aspectos determinantes. Del mismo modo, el uso de tecnologías de seguridad y la aplicación de buenas prácticas, son consideradas para la formación de una "sociedad cibernética resiliente".

Asia - Pacífico

Otro estudio que busca conocer el nivel de madurez en ciberseguridad, enfocado a los países de la región Asia-Pacífico, también considera las legislaciones como un indicador básico para el panorama de seguridad. Durante 2016, varios países de esta región han liberado nuevas políticas o estrategias de ciberseguridad, así como la actualización de marcos normativos existentes, para adaptarse a nuevos retos y temas emergentes. Por ejemplo, Australia ha puesto en marcha una estrategia de seguridad cibernética, que considera fondos adicionales y pretende un mayor compromiso del sector privado con la policía cibernética del país. Otros países, como Nueva Zelanda, han emitido estrategias nacionales de seguridad cibernética, centradas en la mejora de su capacidad de resiliencia, la cooperación internacional y la respuesta a delitos informáticos.

Desafíos e implicaciones en la promulgación de leyes relacionadas con la ciberseguridad

El estado actual de los riesgos presenta la necesidad de contar con marcos normativos para la gestión de la seguridad, una tendencia en el ámbito organizacional. De forma similar, **cuando hacemos referencia a las legislaciones nos referimos a la aplicación de normativas a gran escala, en busca de la reglamentación en ciberseguridad a nivel país.**

Generalmente las legislaciones resultan eficaces cuando se busca normar las conductas. Sin embargo, **existen retos que deben ser superados para una efectiva aplicación de las leyes.** Por ejemplo, el informe Global Agenda Council on Cybersecurity plantea los desafíos a los cuales se enfrentan los países que han comenzado a legislar en el tema, a partir del Convenio de Budapest. Sin embargo, también pueden presentarse con otros convenios de alcance global o regional, e incluso con iniciativas locales específicas. Antecedentes muestran que dada la influencia de la tecnología

El estado actual de los riesgos presenta la necesidad de contar con marcos normativos para la gestión de la seguridad.

y los hábitos arraigados en torno a ella, la implantación de una legislación puede impactar en diversos intereses que van desde empresas tecnológicas hasta los mismos usuarios. **A partir de estas tensiones se originan diferentes conflictos y retos que vamos a repasar a continuación.**

Retraso en la publicación de leyes

Varios elementos determinan la creación de leyes en diferentes países, por lo que su promulgación depende de una multiplicidad de factores, por ejemplo, cuestiones políticas o de otra naturaleza que afectan iniciativas locales, o la adhesión a acuerdos internacionales que fomentan el mismo nivel de desarrollo para la colaboración transfronteriza.

Sin embargo, por estas mismas condiciones y características, las legislaciones se ven aplazadas. Por ejemplo, durante 2016 casi la mitad de los países que han ratificado su participación en el Convenio de Budapest tomaron una década o más para completar dicha ratificación, entre otras razones, debido al retraso en el desarrollo de sus leyes. Además de que el convenio se enfoca solo en algunos aspectos legales dentro de la gama de posibilidades relacionadas con el ámbito de la ciberseguridad.

Leyes alejadas del contexto y el tiempo

Relacionado con el punto anterior, es preciso considerar también que la tecnología avanza a un ritmo rápido, por lo que el desarrollo de normas puede retrasarse considerablemente con relación a los avances tecnológicos. Del mismo modo en el que las organizaciones continuamente actualizan sus normativas respecto a los cambios en los riesgos y las nuevas tecnologías, **las leyes deben estar a la vanguardia en cuanto a los temas presentes y emergentes que pueden ser regulados.**

Por lo tanto, quizá la manera de subsanar esta disparidad es **adoptar el enfoque de la regulación hacia las conductas humanas, más que a las tecnologías que pueden quedar obsoletas en periodos relativamente cortos.** Ésta puede llegar a ser la manera más confiable de que dichas regulaciones sean efectivas, pero también es preciso marcar que a futuro podría suponer el surgimiento de tensiones. Un ejemplo de esto podría estar tratando de regular comportamientos que, en ocasiones, se convierten en leyes tácitas, como el uso de las redes sociales, que no están respaldadas por las legislaciones.

Heterogeneidad técnica y legal

A lo anterior se suma el hecho de que **los países se encuentran en condiciones diferentes para sumarse a convenios internacionales o regionales,** que incluso determinan las iniciativas propias para el desarrollo de sus leyes. Las brechas legales y técnicas, dificultan los esfuerzos para dar respuesta, investigar y enjuiciar incidentes de ciberseguridad, y se convierten en un inhibidor de la colaboración internacional. Por ejemplo, iniciativas regionales o bilaterales se desarrollan para necesidades específicas, tal es el caso del Escudo de Privacidad entre la Unión Europea y Estados Unidos, un marco que busca proteger los derechos fundamentales de cualquier persona de la UE, cuyos datos personales se transfieren a empresas de EU. Esto sin duda no considera la colaboración con otros países o regiones.

Conflictos de leyes y principios básicos

En este mismo contexto, las legislaciones generalmente son eficaces cuando se trata de regular el comportamiento, sin embargo, no existen leyes perfectas, y por el contrario son susceptibles de ser mejoradas, sobre todo si se considera que **existen proyectos que podrían atentar contra los principios sobre los que se sustentan Internet e incluso en contra de algunos derechos humanos.** Con base en la idea de que Internet es libre y no tiene fronteras, mientras que las legislaciones aplican en el ámbito de los países, existen casos donde se presentan

La tecnología avanza a un ritmo rápido, por lo que el desarrollo de normas puede retrasarse considerablemente con relación a los avances tecnológicos.

conflictos constitucionales o legales, principalmente sobre las acepciones y concepciones de privacidad o libertad de expresión. **En este caso, puede hacer acto de presencia nuevamente el eterno debate entre la privacidad y la seguridad.**

Limitantes en el ámbito de aplicación

En el mismo orden de ideas, la ausencia de legislaciones o acuerdos en aspectos puntuales, merma la colaboración internacional e incluso dentro de un mismo territorio. **Los sectores público y privado se enfrentan a un reto de acceso a la información para las investigaciones, con las implicaciones de seguridad, derecho a la privacidad e intereses comerciales, principalmente de las empresas de tecnología.** Como ejemplo se tiene el conocido caso que confrontó al FBI y Apple donde una jueza estadounidense solicitó la colaboración del gigante tecnológico para desbloquear el iPhone de un terrorista involucrado en un atentado, o bien, el caso reciente donde un juez de Río de Janeiro ordenó el bloqueo de WhatsApp en todo Brasil y multas a Facebook. Sin duda, **sucesos de esta naturaleza evidencian la necesidad de acuerdos locales y transfronterizos para la colaboración,** que eviten la transgresión entre los intereses de una y otra parte.

Hacia el desarrollo y divulgación de la cultura de ciberseguridad

La promulgación de leyes relacionadas con la ciberseguridad ha cobrado relevancia a nivel internacional desde hace años a raíz de la cantidad, frecuencia e impacto de incidentes registrados en todo el mundo. Distintas iniciativas consideran la legislación en la materia como un elemento fundamental para aumentar el nivel de madurez en los países. **El propósito, por lo tanto, es contar con las medidas legales para la protección a distintos niveles y ámbitos.** Por ello, las legislaciones también han comenzado a considerar los elementos necesarios para la seguridad de los países, desde su capacidad para responder a incidentes de gran escala, la protección de su infraestructura crítica, su capacidad para colaborar con otros países, e incluso considerando el desarrollo de una cultura de seguridad que pueda permear entre la población. **Todo esto sin dejar de lado temas ya conocidos, como la privacidad, protección de datos personales o los delitos informáticos.**

Nos encontramos ante una tendencia creciente en el desarrollo de nuevas legislaciones que determinan la manera de proteger los bienes de una nación en el contexto de la ciberseguridad, además, de impulsar la cooperación y la colaboración entre los sectores público y privado de cada país, así como a nivel internacional para contrarrestar las amenazas y ataques informáticos de la actualidad y emergentes. Sin embargo, **a pesar de las bondades que esto puede representar, existen desafíos que deben ser superados para lograr este propósito y comprender las características, necesidades y condiciones tanto del sector público como privado, y de todos los involucrados,** entre los que se encuentran las poblaciones en su carácter tanto de usuario como de ciudadano. Los obstáculos y limitaciones a la colaboración pueden incluir la falta de confianza, legislaciones poco efectivas e intereses distintos entre los diferentes sectores.

A partir de estos desafíos y tensiones, **se vislumbra la necesidad de definir las reglas claras para todos los participantes, quizá a partir de acuerdos internacionales, regionales o locales, que contemplen a todas las partes involucradas,** con el objetivo de que la legislación sea realmente efectiva, pueda ser aplicada y cumplida. Sin duda, **es un camino largo por recorrer, que requiere de la colaboración entre los gobiernos, la iniciativa privada, el sector académico y, por supuesto, de los usuarios;** todo lo anterior es necesario para lograr un propósito de mayor alcance, encaminado hacia el desarrollo de la cultura de ciberseguridad.

Los obstáculos y limitaciones a la colaboración pueden incluir la falta de confianza, legislaciones poco efectivas e intereses distintos entre los diferentes sectores.

Plataformas de juego: los riesgos potenciales de consolas integradas a computadoras

AUTOR

Cassius de Oliveira Puodzius
Security Researcher

9

Plataformas de juego: los riesgos potenciales de consolas integradas a computadoras

Los juegos emplean tecnologías de última generación compuestas por hardware y software avanzado para ofrecerles la mejor experiencia de entretenimiento a los usuarios.

Son tan populares y exitosos que convirtieron a la industria de los videojuegos en un sector sustancial del mercado global que, a pesar de las crisis financieras, ha estado creciendo rápidamente en el pasado y seguramente continúe expandiéndose en el futuro próximo.

La seguridad es un elemento clave para la industria de los videojuegos, dado que una cantidad innumerable de personas en todo el mundo gasta muchísimo dinero para jugar en diversas plataformas, ya sean consolas, PC o teléfonos móviles. Sin duda, esto **las convierte en objetivos de ataque sumamente valiosos para los hackers** de sombrero negro que buscan obtener fama, diversión o beneficios económicos.

Según el Informe sobre el mercado global de juegos en 2016 publicado por Newzoo, **el mercado del juego se incrementará un 8,5% durante 2016, por lo que sus ingresos alcanzarán casi los USD 100 mil millones.** Los juegos para dispositivos móviles tienen un papel importante en dicho crecimiento, ya que **los smartphones y las tabletas generarán USD 36,9 mil millones a finales de 2016, lo que representa el 37% del mercado total de la industria de juegos.** Se estima que **el crecimiento anual de este mercado para los próximos años será del 6,6%, con lo que sus ingresos alcanzarán los USD 118,6 mil millones para el año 2019.** La consolidación de los juegos para móviles y la experiencia cada vez más atractiva, gracias a la integración de diferentes plataformas, hacen que la industria de los videojuegos experimente un éxito constante. Por lo tanto, **la estrategia de crecimiento del mercado de videojuegos apunta a dos áreas principales: la diversificación y los juegos casuales.**

Panorama de amenazas en la industria de videojuegos

El modelo de negocio de la industria de los videojuegos ha evolucionado drásticamente en los últimos años, lo que se puede atribuir en parte a la necesidad de incorporar medidas de seguridad. Pero a pesar de ellas, **las amenazas continúan adaptándose a los cambios y poniendo en peligro a los gamers.**

En el pasado, los juegos generaban ingresos principalmente por la "venta de software empaquetado", donde los usuarios pagan una licencia por adelantado y tienen el derecho a jugar todo el tiempo que quieran. Aunque aún sigue siendo un modelo de negocio relevante, ha ido perdiendo protagonismo.

Una de las razones por las que las empresas desarrolladoras de juegos comenzaron a dejar de usar este modelo es la piratería. Por ejemplo, Nintendo, un gigante de la industria del juego, argumenta: "La piratería sigue siendo una grave amenaza para el negocio de Nintendo y para las más

La seguridad es un elemento clave para la industria de los videojuegos, dado que una cantidad innumerable de personas en todo el mundo gasta muchísimo dinero para jugar.

de 1.400 empresas desarrolladoras que trabajan con el objetivo de ofrecer juegos únicos e innovadores para esta plataforma".

A pesar de los esfuerzos de la industria para implementar medidas que combatan la piratería, **hemos estado presenciando ataques continuos a consolas durante más de una década.** Un ejemplo es el lanzamiento de un hack para PlayStation 4 por parte del grupo failoverflow, que aunque no llevó directamente a la piratería, tuvo un efecto secundario que habilitaba la consola para este tipo de ataques.

Para combatir la piratería y diversificar el modelo de negocio de los juegos, en los últimos años, la industria ha estado mejorando "otros formatos de entrega". **Tales formatos incluyen suscripciones, juegos digitales completos, contenidos digitales como complementos, juegos para móviles y redes sociales,** así como otras formas de venta diferentes al tradicional software de juego empaquetado.

Este novedoso modelo de negocio es mucho más dependiente de Internet que la tradicional "venta de software empaquetado". Por otra parte, las plataformas de juegos con conexión de red generan riesgos de seguridad informática, ya que **los ciberdelincuentes pueden aprovechar vulnerabilidades con el fin de controlarlas remotamente o instalar malware para obtener acceso a la información confidencial de los jugadores.**

Sin embargo, los juegos online no son exactamente una moda nueva. En sus versiones para PC existen desde los albores de Internet, debido a su soporte de hardware. Con la expansión de Internet de banda ancha, los juegos online comenzaron a lanzar títulos muy exitosos con soporte para un gran número de jugadores, convirtiéndose en lo que se conoce como videojuego multijugador masivo online (del inglés MMO). Por ejemplo, en 2010, el juego World of Warcraft (WoW) alcanzó los 12 millones de suscriptores en todo el mundo.

De esta manera, a medida que el modelo de negocio va evolucionando, también atrae nuevos tipos de amenazas. Los juegos online se ven ante la necesidad de hacer frente a las amenazas comunes del mundo cibernético, como el malware oculto en los programas de instalación, que incluye troyanos en el software del juego, o las campañas maliciosas, que se hacen pasar por juegos populares para distribuir malware o robar las cuentas de los jugadores. Sin embargo, también hay otros tipos de conductas ilegales que se aprovechan de los juegos online.

A medida que los jugadores se sumergen en el juego, no es nada raro que el mundo virtual se mezcle con la realidad. **Los ciberdelincuentes se aprovechan de esta transición entre los dos mundos y usan los juegos online para lavar dinero.**

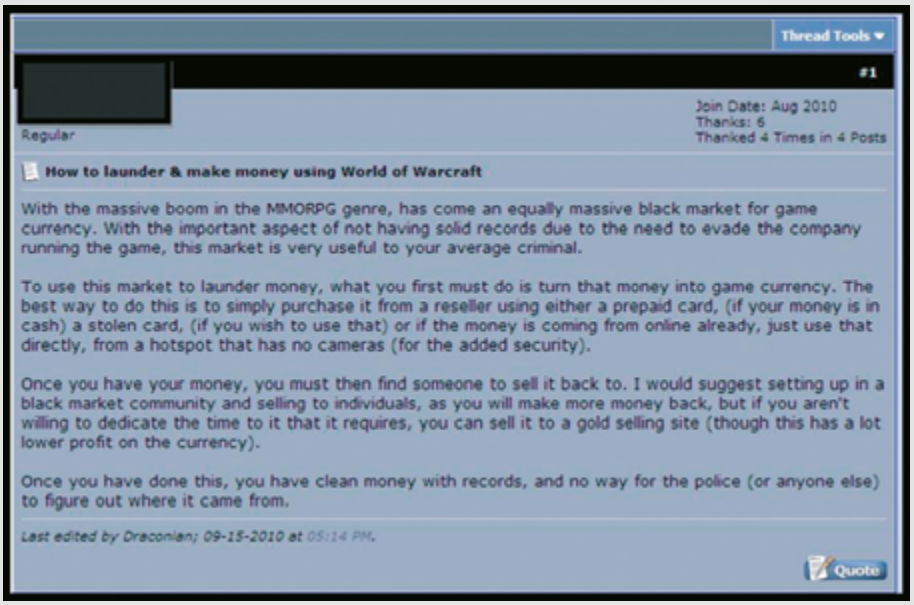
Esta posibilidad surge cuando se comercializan objetos virtuales en sitios de comercio electrónico como eBay, donde los elementos del juego que fueron robados de las cuentas de otros jugadores o comprados con dinero ilícito se venden a otros jugadores a cambio de dinero real y limpio. En el caso de WoW, este tipo de incidente fue lo suficientemente importante como para hacer que Blizzard emitiera una alerta de seguridad tras una serie de inicios de sesión no autorizados y reportes de jugadores sobre estafas de "lavado de dinero" durante 2013.

Otra forma en que los delincuentes intentan obtener los datos de los usuarios es atacando directamente a los desarrolladores de juegos. Blizzard, Steam, Sony (entre otros) fueron víctimas de brechas de datos que ocasionaron riesgos como el lavado de dinero (ya mencionado) o la pérdida financiera para la empresa y sus clientes, en el caso del robo de tarjetas de crédito e información personal de los clientes.

Pero a pesar de las amenazas informáticas,

A medida que el modelo de negocio va evolucionando, también atrae nuevos tipos de amenazas.

Post de un foro que explica cómo lavar dinero ilícito con juegos MMO



Fuente: **Laundering Money Online: a review of cybercriminals' methods** por Jean-Loup Richet.

los juegos de consola empezaron a pasar al mundo online hace unos diez años; después de todo, es un mercado enorme y rico. Los gigantes de las consolas de juegos como Microsoft (Xbox), Nintendo (Wii) y Sony (PlayStation) lanzaron Xbox live (2002), Nintendo Wi-Fi Connection (2005) y PlayStation Network (alias PSN, 2006), respectivamente.

Todas estas iniciativas se basan en servicios de entrega online diseñados para proporcionar juegos multijugador y medios digitales, y fueron objeto de varias reformas desde su creación. Por ejemplo, Nintendo Wi-Fi Connection fue reemplazado por Nintendo Network (alias NN) en 2012. En total, **sus comunidades de red comprenden casi 185 millones de miembros. El elevado número de miembros convirtió a estas redes de juego en grandes objetivos de ataque** para el hacktivismo. En la víspera de Navidad de 2014, un equipo conocido como Lizard Squad llevó a cabo varios ataques exitosos de denegación de servicio distribuido (DDoS) contra Playstation Network y Xbox Live, dejándolos sin servicio por varias horas, y solo se detuvo cuando le regalaron 3000 vouchers para el servicio de almacenamiento en la nube con cifrado MegaPrivacy.

A esta altura, está claro que el panorama de amenazas en la industria de los videojuegos es todo un desafío. Sin embargo, no es tan sorprendente si tenemos en cuenta el tamaño, la riqueza y el crecimiento de este segmento del mercado. Las empresas desarrolladoras de juegos están realizando grandes inversiones para hacer frente a las amenazas informáticas, al tiempo que buscan expandirse lanzando juegos para un mayor número de plataformas y atrayendo a más personas.

Convergencia y amenazas futuras

El número cada vez más elevado de jugadores y la mayor cantidad de transacciones monetarias integradas a los juegos plantean grandes desafíos de seguridad para el

La integración de las consolas de juegos con las computadoras y dispositivos móviles está creciendo rápidamente, lo que podría tener un impacto significativo para la seguridad de la información de los juegos en los próximos años.

futuro. Por otra parte, **la integración de las consolas de juegos con las computadoras y dispositivos móviles está creciendo rápidamente, lo que podría tener un impacto significativo para la seguridad** de la información de los juegos en los próximos años.

El Informe sobre el mercado global de juegos en 2016 publicado por Newzoo revela que **el 87% de los gamers que usan consolas también juegan en la PC,** y la escogen como el "centro para gestionar los juegos de consola". Para apoyar esta afirmación, se destaca que tanto la PC como el móvil son dispositivos esenciales, mientras que las consolas de videojuegos no lo son. Por otra parte, también se remarca que las PC son dispositivos mucho más adecuados para intercambiar contenidos online que las consolas, y además los usuarios de PC actualizan sus equipos con más naturalidad que los usuarios de consolas.

Microsoft define su estrategia de convergencia con la frase "compra una vez, juega en todas partes". En 2013, contrató a Jason Holtman (quien anteriormente estaba a cargo del popular Steam en la empresa Valve) para dirigir la evolución de su plataforma de juego. El proceso se describió como "la idea de jugar en tu consola Xbox, y luego pasar a tu PC y seguir jugando desde donde dejaste, sin tener que volver a comprar el juego o repetir los mismos niveles".

De hecho, los fabricantes de consolas ya están poniendo en práctica esta idea de un modo u otro. Wii U es capaz de retransmitir los juegos en GamePad, mientras que PlayStation 4 los retransmite en Vita. En el caso de la Xbox de Microsoft, el objetivo es retransmitir los juegos en la PC.

A comienzos de 2015, Microsoft anunció sus planes de renovar la aplicación Xbox App para PC lanzada en 2012, para suministrar acceso a Xbox Live, control remoto y función de segunda pantalla para Xbox. A partir de 2015, Xbox y Windows 10 están estrechamente integrados para crear el entorno de juego ideal de Microsoft.

Pocos meses después del anuncio, se lanzó la compatibilidad de Xbox con la PC en la conferencia de desarrolladores de juegos GDC 2015. El turno para Xbox App para iOS y Android llegó en 2016, cuando la app volvió a cambiar de nombre y se renovó para incluir funcionalidades de Windows 10 Xbox App.

Tal integración podría permitir que el spyware que se ejecuta en computadoras y dispositivos móviles infectados se colara en los chats de los jugadores y obtuviera acceso a las contraseñas de diferentes aplicaciones, que antes quedaban restringidas solamente a las consolas Xbox.

Hasta el momento, **puede parecer que la evolución de los juegos de consola hacia otras plataformas es un movimiento unilateral, pero no es cierto.** Valve, una empresa de videojuegos estadounidense que se especializa en juegos online para PC, se encamina en la dirección opuesta.

Su cartera de productos incluye títulos de gran éxito como Half-Life, Counter-Strike y Dota. Por otra parte, Valve es el propietaria de Steam, la mayor plataforma de juegos online del mundo y uno de los objetivo de ataque de TeslaCrypt, un ransomware que cifra más de 185 tipos diferentes de archivos asociados a los juegos.

En 2015, Steam anunció su récord de 125 millones de usuarios activos en todo el mundo. Su sitio web proporciona estadísticas en tiempo real sobre la plataforma, que muestra **un pico de casi 12,5 millones de usuarios registrados en las últimas 48 horas** (en el momento de redactar este informe).

En mayo de 2014, Steam lanzó una funcionalidad llamada "Retransmisión en casa". Ahora, los jugadores que tienen varios equipos donde ejecutan Steam dentro de la

La integración entre consolas y otros dispositivos podría permitir que el spyware que se ejecuta en computadoras y dispositivos móviles infectados se colara en los chats de los jugadores y obtuviera acceso a las contraseñas de diferentes aplicaciones, que antes quedaban restringidas solamente a las consolas.

misma red pueden usar esta funcionalidad para hacer instalaciones remotas, iniciar juegos y jugar desde equipos diferentes.

De esta forma, los usuarios pueden jugar a un juego de PC en un equipo de gama baja que esté conectado a la PC principal, y ni siquiera es necesario que ambos equipos tengan el mismo sistema operativo. Por otro lado, la Retransmisión en casa les otorga acceso completo a los equipos de escritorio remoto, es decir que un atacante podría aprovechar esta funcionalidad para moverse lateralmente en redes complejas.

A finales de 2013, Valve lanzó SteamOS, un sistema operativo basado en Linux diseñado para ejecutar los juegos de Steam. Su desarrollo sentó las bases para el lanzamiento de Steam Machine, la estrategia de Valve para ganar cuota de mercado en el segmento de juegos de consola, en noviembre de 2015; se trata de un equipo de juego similar a una consola que ejecuta SteamOS y les permite a los usuarios jugar a juegos de Steam (online) en una pantalla de televisión. Aunque no se sabe a ciencia cierta qué desarrolladores de juegos tendrán éxito en su estrategia de diversificación, al menos **podemos decir que la convergencia es un elemento fundamental en la industria del juego.**
Hasta los dispositivos wearables se están convirtiendo en plataformas de juego. Después del éxito rotundo de Pokémon GO, una app lanzada en 2016 que superó los 500 millones de descargas en todo el mundo, Niantic Labs anunció que ya está programado el lanzamiento de una app del juego para Apple Watch.

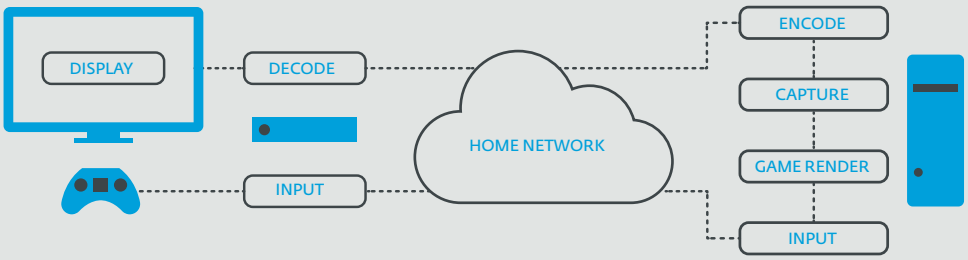
Desde el punto de vista de la seguridad, la convergencia acarrea grandes preocupaciones, ya que habrá más datos valiosos transmitiéndose desde y hacia muchos dispositivos y plataformas diferentes. Además, **habrá más recursos disponibles en riesgo potencial de que un atacante los use** como parte de sus nuevos tipos de botnets, cuyo objetivo es controlar los dispositivos de la Internet de las cosas (IoT).

A nivel personal, **los juegos tienen acceso al tipo de información que buscan los ciberdelincuentes, como datos personales y números de tarjetas de crédito.** Además, con la expansión del juego a nuevas plataformas, el uso que hacen de los datos tiende a seguir evolucionando: por ejemplo, si la falla de seguridad de algún juego llega a un dispositivo wearable, los ciberdelincuentes podrían obtener acceso a los registros médicos de las víctimas.

A medida que la superficie de ataque se

Desde el punto de vista de la seguridad, la convergencia acarrea grandes preocupaciones, ya que habrá más datos valiosos transmitiéndose desde y hacia muchos dispositivos y plataformas diferentes.

Esquema de "Retransmisión en casa" de Steam.



Fuente: Steam

extiende y los juegos se basan cada vez más en modelos online, también crece la necesidad de elevar el nivel de seguridad. **Las amenazas que la industria del juego enfrenta en la actualidad comienzan a alcanzar las plataformas en las que antes no eran tan frecuentes,** mientras que el impacto de los incidentes de seguridad tiende a ser aún mayor.

Tanto hogares como empresas (especialmente hoy en día con la tendencia a permitir los videojuegos en el lugar de trabajo como estrategia para aumentar la productividad) **pueden quedar expuestos a las amenazas informáticas simplemente por habilitar el uso de juegos en sus redes.** El mero hecho de tener una consola de juegos dentro de la oficina puede exponer a toda la empresa a ataques dirigidos APT que utilizan la plataforma de juego como puerta de entrada a la red corporativa. Por otra parte, los incidentes de seguridad que afecten los juegos tendrán un mayor impacto potencial sobre los jugadores.

Por ejemplo, en noviembre de 2015, se divulgaron las claves privadas de Microsoft correspondientes a un certificado digital de "xboxlive.com". Como consecuencia, un atacante podría haber utilizado dichas claves para suplantar la identidad de los servidores de Microsoft, no solo para interceptar datos de los usuarios que usan la consola Xbox Live, sino también de quienes juegan en la PC y en dispositivos móviles.

Además del cuidado habitual que siempre debemos tener con los juegos online, especialmente con los más populares (como la app de Pokémon GO de 2016), **los desarrolladores de juegos deben tener en cuenta el incremento del flujo de datos entre dispositivos durante el juego, de modo de garantizar que los dispositivos de los jugadores no sean explotados con fines maliciosos** ni se conviertan en un punto de entrada de malware a las redes domésticas y corporativas.

Las amenazas que la industria del juego enfrenta en la actualidad comienzan a alcanzar las plataformas en las que antes no eran tan frecuentes, mientras que el impacto de los incidentes de seguridad tiende a ser aún mayor.

Conclusión

En esta nueva edición del artículo de Tendencias hemos tratado temas muy variados: desde cuestiones generales como las infraestructuras críticas o los retos en materia de legislación que deben afrontar los países, hasta cuestiones más cotidianas y cercanas al usuario final, como amenazas en dispositivos IoT o consolas de videojuegos.

Conclusión

A pesar de la diversidad y variedad en los temas tratados a lo largo de las diferentes secciones, hay algo que es común a todos: el factor humano.

Una frase que se ha convertido en casi un dogma en seguridad informática es que **los usuarios finales son el eslabón más débil en la cadena de seguridad,** y que este es comúnmente utilizado por los cibercriminales para propagar sus amenazas. Esto es algo que no se puede negar y **de allí la necesidad de que los usuarios y las empresas sepan de seguridad, de las amenazas, de cómo se propagan y qué medidas implementar para poder proteger su privacidad y su información.** Pero con la concepción actual de concientización no basta: la relevancia del factor humano debe pasar a otro nivel de importancia.

Estamos en un momento en que la aparición de nuevas aplicaciones y dispositivos se da de una manera acelerada: realidad virtual, realidad aumentada, integración de tecnologías a todos los niveles (desde consolas de juegos hasta dispositivos IoT), virtualización de servidores en el entorno corporativo y demás. **Todas estas innovaciones se podrían constituir (y seguramente eso suceda) como nuevos vectores de ataque** a aprovechar por los cibercriminales, y se suman al largo listado de vectores ya existentes.

Esta situación, además, se ve agravada cuando observamos que aún existen usuarios que caen fácilmente en campañas de phishing o descargan aplicaciones maliciosas a sus dispositivos, sin tenerlos protegidos de la manera adecuada. **Este panorama se vuelve menos alentador cuando vemos en el horizonte que todo parece estar preparado para que exploten amenazas como el RoT (Ransomware of Things).** En definitiva: estamos en una etapa en la que tenemos usuarios que utilizan tecnología de última generación, pero con conceptos de seguridad de hace más de 10 años.

En la medida en la que los usuarios no tomen real dimensión de las implicancias de seguridad que tiene el uso irresponsable de la tecnología, quedarán a merced de los ciberdelincuentes, quienes continuarán robando y tomando de rehén la información de las personas y las organizaciones.

Pero el avance vertiginoso de la tecnología nos plantea otros desafíos en los riesgos que afrontan los usuarios, y por lo tanto en su concientización. **Detrás de cada nueva aplicación o de cada nuevo dispositivo hay un grupo de personas que deberían pensar en la seguridad de la información desde el diseño.** El hecho de que haya más vulnerabilidades críticas no es un algo fortuito; es claro que cada vez la superficie de ataque es mayor, por lo cual es necesario considerar la seguridad desde la concepción del proyecto.

Asimismo, la concientización debería alcanzar a industrias y sectores que hasta el momento no estaban tan ligados a la seguridad de la información. Dados los datos sensibles que manejan, marcamos como tendencias importantes para el próximo año la seguridad en infraestructuras críticas y en el sector salud. Pero la **educación y concientización en estos ámbitos también deben ir acompañados de una correcta gestión y de controles efectivos,** además de complementarse con legislación y normativas.

Estamos en una etapa en la que tenemos usuarios que utilizan tecnología de última generación, pero con conceptos de seguridad de hace más de 10 años.

Más allá de que este repaso pueda sonar algo pesimista, **la realidad es que existen muchas posibilidades para poder hacer un uso seguro de la tecnología.** 2017 se perfila como un año en el que seguirán creciendo los desafíos en materia de seguridad y estamos en el momento justo para hacer frente a estos retos.

No se trata solamente de educar al usuario final; es necesario que los gobiernos adopten marcos legislativos que impulsen los temas de ciberseguridad, que van desde formalizar la educación en temas de seguridad hasta proteger adecuadamente las infraestructuras críticas. En este sentido, **también es preciso que las empresas se decidan a llevar adelante una gestión correcta de la seguridad de su información y que los desarrolladores no posterguen la seguridad de sus productos** en detrimento de la usabilidad.

La información y su manejo son aspectos clave en las sociedades actuales y, por lo tanto, su correcta protección se hace imprescindible. Pero **dada la multiplicidad de aspectos y de actores involucrados, nadie puede mirar al costado.** Así que es el momento de ocuparse de todas las aristas de la seguridad presentadas a lo largo de este informe, destacando que **se trata de un trabajo conjunto entre las diferentes partes involucradas:** desde los grandes fabricantes de tecnología, las empresas y los gobiernos hasta, por supuesto, los usuarios. **Si se logra llegar a consensos y acuerdos en torno a estos temas, el futuro de la seguridad de la información será promisorio.**

2017 se perfila como un año en el que seguirán creciendo los desafíos en materia de seguridad y estamos en el momento justo para hacer frente a estos retos.

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™