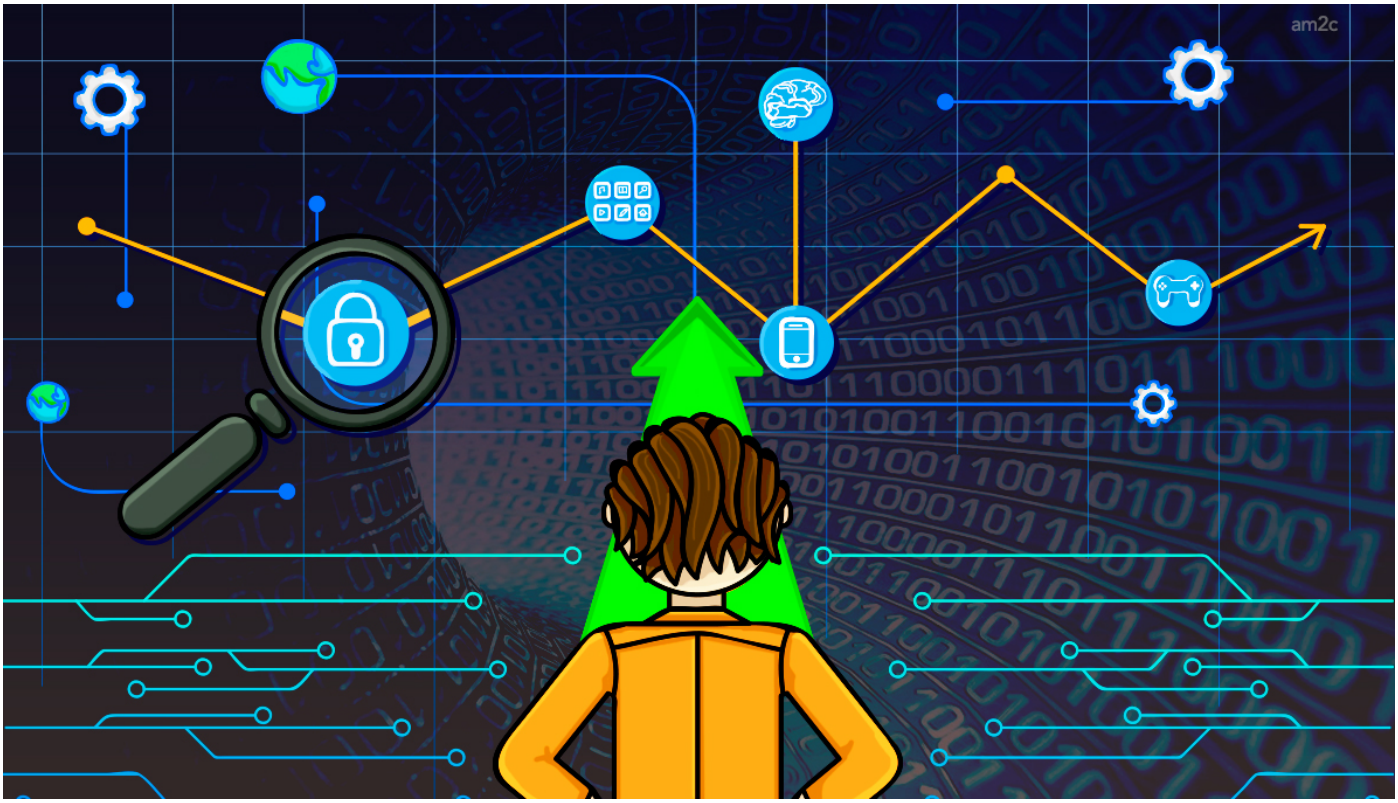
TENDENCIAS DE SEGURIDAD 2017, ¿ESTÁS PREPARADO?

Camilo Gutiérrez Amaya

dispositivos móviles

numero-28



Desde 2009 el equipo de investigación de ESET realiza el Informe de Tendencias a partir de la revisión de los acontecimientos recientes más importantes en materia de seguridad informática. En 2017 se elaboró un documento con nueve tendencias que abarcan diversos temas como el Ransomware de las Cosas, las infraestructuras críticas, las vulnerabilidades, entre otras. En este artículo se resaltarán dos de ellas: la seguridad en dispositivos móviles y las amenazas en plataformas de videojuegos.

En cuanto a los dispositivos móviles, es necesario pensar en los diferentes aspectos de seguridad que deben tener implementadas las plataformas, como el modelo de distribución de aplicaciones, la creciente cantidad de malware móvil o el desarrollo seguro en el contexto de incorporación de otras tecnologías, como la realidad aumentada y la realidad virtual a estos dispositivos.

Por otra parte, la industria de los videojuegos ha adquirido cada vez mayor relevancia, con una amplia variedad de usuarios con equipos de gran capacidad de procesamiento a su disposición, convirtiéndolos en un objetivo muy atractivo para los cibercriminales. 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.

Por lo tanto, la seguridad debe comenzar a ser considerada en los nuevos desarrollos tecnológicos que día con día se incorporan a nuestras actividades cotidianas, lo que se traduce en la aplicación de medidas de protección en distintos niveles y en diferentes ámbitos.

MOBILE: EL MALWARE Y SU REALIDAD… ¿AUMENTADA?

En un principio se esperaba que los dispositivos móviles evolucionaran 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 el contexto de la revolución socio-tecnológica, los nuevos desarrollos incorporan nuevos riesgos de seguridad que afectan la información digital e incluso al bienestar de los usuarios.

En la actualidad, el malware móvil va en aumento y cada vez es más complejo. Ante esta situación, en el desarrollo de software debe implementarse medidas de seguridad desde etapas tempranas y no como hoy en día, que se aplaza hasta etapas tardías del proyecto, en el mejor de los casos, o bien cuando se encuentran en producción. Dejando de lado las aplicaciones que deben cumplir estándares de seguridad, pocos desarrolladores se preocupan por realizar exhaustivos controles sobre sus productos antes de liberarlos al público.

En conjunto con el desarrollo seguro de aplicaciones, las bibliotecas de anuncios publicitarios también tendrán un rol importante en la seguridad, ya que son utilizadas por los desarrolladores en plataformas como una forma de ingresos, donde los usuarios no suelen estar dispuestos a pagar por conseguir la funcionalidad de las aplicaciones. Usualmente encontramos al menos una de ellas por aplicación y muchas veces contienen algún tipo de API insegura que podría ser explotada para la instalación de malware o el robo de información.

Adicionalmente, a estos errores involuntarios en el proceso de desarrollo también se suman aquellas creaciones maliciosas cuya propagación en ocasiones es favorecida por las políticas poco restrictivas en repositorios de aplicaciones, que encubren involuntariamente a los cibercriminales bajo la fiabilidad de las tiendas de aplicaciones oficiales. 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 repositorios, disponibles para ser descargada por los usuarios.

En suma, el crecimiento del malware móvil es una realidad innegable que veníamos previendo desde hace 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; en 2016 este número ascendió a 300 nuevas variantes mensuales (en iOS el número es de dos mensuales), por lo que no debería sorprendernos que este incremento continúe durante los próximos meses y años.

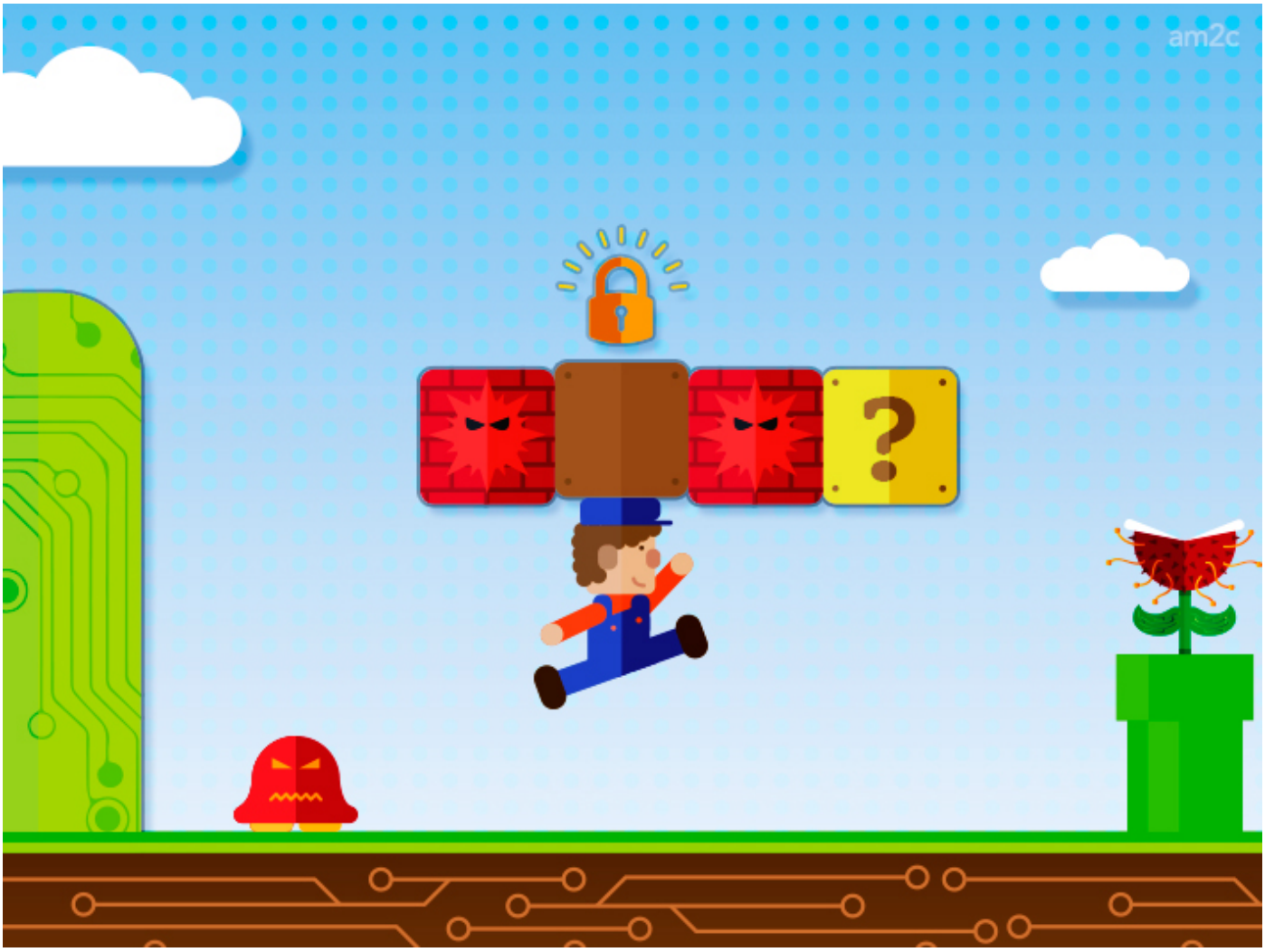
Además del aumento en la cantidad de nuevas variantes de códigos maliciosos, una gran preocupación para los usuarios móviles serán las vulnerabilidades no solo del sistema operativo sino también de las aplicaciones que utilizan. La reciente liberación de iOS 10 y Android 7.0 Nougat plantea algunas mejoras en el estado de la seguridad móvil, especialmente para este último sistema.

Por parte de Google comienzan a vislumbrarse esfuerzos por unificar 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 continuo programa de recompensa por errores como un medio para el

descubrimiento de vulnerabilidades. Otra característica 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 posean.

En este contexto, a medida que los usuarios desconozcan el peligro de instalar aplicaciones desde fuentes no confiables, la falta de implementación de prácticas de seguridad en el desarrollo de ellas y que los cibercriminales apuesten a nuevas campañas de Ingeniería Social a través de mercados oficiales, durante este año podremos observar más casos de malware móvil, aplicaciones falsas y una tendencia creciente a encontrar estafas móviles a través de WhatsApp y las redes sociales. En general, se presentarán riesgos de seguridad en las plataformas móviles, que requerirán la atención de todas las partes involucradas.

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 ofrecer la mejor experiencia de entretenimiento a los usuarios. Dado que una cantidad

innumerable de personas en todo el mundo gasta recursos para jugar en diversas plataformas, ya sean consolas, PC o teléfonos móviles, sin duda, esto las convierte en objetivos sumamente valiosos para los atacantes que buscan obtener fama, beneficios económicos o simplemente por diversión. Por esta razón, la seguridad es un elemento clave para la industria de los videojuegos.

El modelo de negocio de esta industria ha evolucionado en los últimos años. En el pasado, los juegos generaban ingresos principalmente por la venta de software empaquetado, en los cuales los usuarios pagaban una licencia por adelantado y tenían el derecho a jugar todo el tiempo que quisieran. Actualmente, los modelos involucran una mayor cantidad de transacciones monetarias, a través de la integración de consolas con computadoras y dispositivos móviles, lo que podría tener un impacto significativo para la seguridad de la información en los próximos años.

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 incluyen troyanos en el software del juego, o las campañas maliciosas, que se hacen pasar por juegos populares para distribuir códigos maliciosos o robar las cuentas de los jugadores. Sin embargo, también hay otros tipos de conductas ilegales que se aprovechan de los juegos online.

Conforme los jugadores se sumergen en el juego, es común que el mundo virtual se mezcle con la realidad; los cibercriminales se aprovechan de esta transición entre los dos mundos y usan los juegos online para obtener beneficios, principalmente económicos. Esta posibilidad surge cuando se comercializan objetos virtuales en sitios de comercio electrónico, en los cuales los elementos del juego, que fueron robados de las cuentas de otros jugadores o comprados con dinero ilícito, se venden a cambio de dinero real.

Otra forma a través de la cual los delincuentes intentan obtener los datos de los usuarios es atacando directamente a los desarrolladores de juegos, quienes han sido víctimas de brechas de datos; esto ha derivado en incidentes como la pérdida financiera para la empresa y sus clientes, robo de tarjetas de crédito e información personal, entre otros. Además de los riesgos conocidos, se identifican otro tipo de amenazas que se relacionan con el uso popular de los videojuegos.

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 solo por habilitar el uso de juegos en sus redes. El simple hecho de tener una consola de juegos dentro de la oficina puede exponer a toda la empresa a ataques dirigidos, los cuales utilizan la plataforma de juego como puerta de entrada a la red corporativa.

Como se observa, existe un panorama amplio de amenazas que atentan contra los gamers, al igual que los dispositivos móviles, resulta necesario que las partes interesadas que van desde los desarrolladores de videojuegos y consolas hasta los jugadores continúen aplicando medidas de seguridad con el propósito de minimizar los riesgos asociados a esta forma de entretenimiento.

SEGURIDAD EN DIFERENTES ÁMBITOS Y DISTINTOS NIVELES: HACIA EL DESARROLLO DE LA CULTURA DE 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 actuales no se entenderían sin los sistemas de información, los dispositivos electrónicos o las redes de datos, lo que genera una tendencia que conduce hacia la hiperconectividad.

Al analizar el estado y la evolución de la tecnología hay un aspecto a resaltar: cada vez existen más dispositivos, más tecnologías y, por lo tanto, un mayor número de desafíos para mantener la seguridad de la información. Nuevas herramientas que facilitan la comunicación y diversas actividades, como los dispositivos móviles, o que ofrecen entretenimiento, como los videojuegos, se popularizan y evolucionan continuamente.

Sin embargo, 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 sea que hablemos de las infraestructuras críticas, el Internet de las Cosas, los dispositivos móviles o los videojuegos, la seguridad de la información adquiere mayor relevancia. Diferentes sectores son requeridos para la mejora y el aumento de la seguridad, desde la iniciativa privada con productos y servicios seguros, los gobiernos con normas y legislaciones, el sector académico con investigaciones y educación, hasta usuarios conscientes de la seguridad. Todo lo anterior para lograr un objetivo de mayor alcance: desarrollar y divulgar la cultura de ciberseguridad.

SI QUIERES SABER MÁS, CONSULTA:

- Riesgos de seguridad en Android
- Información sensible en dispositivos móviles
- Dispositivos móviles: un riesgo de seguridad en las redes corporativas

---