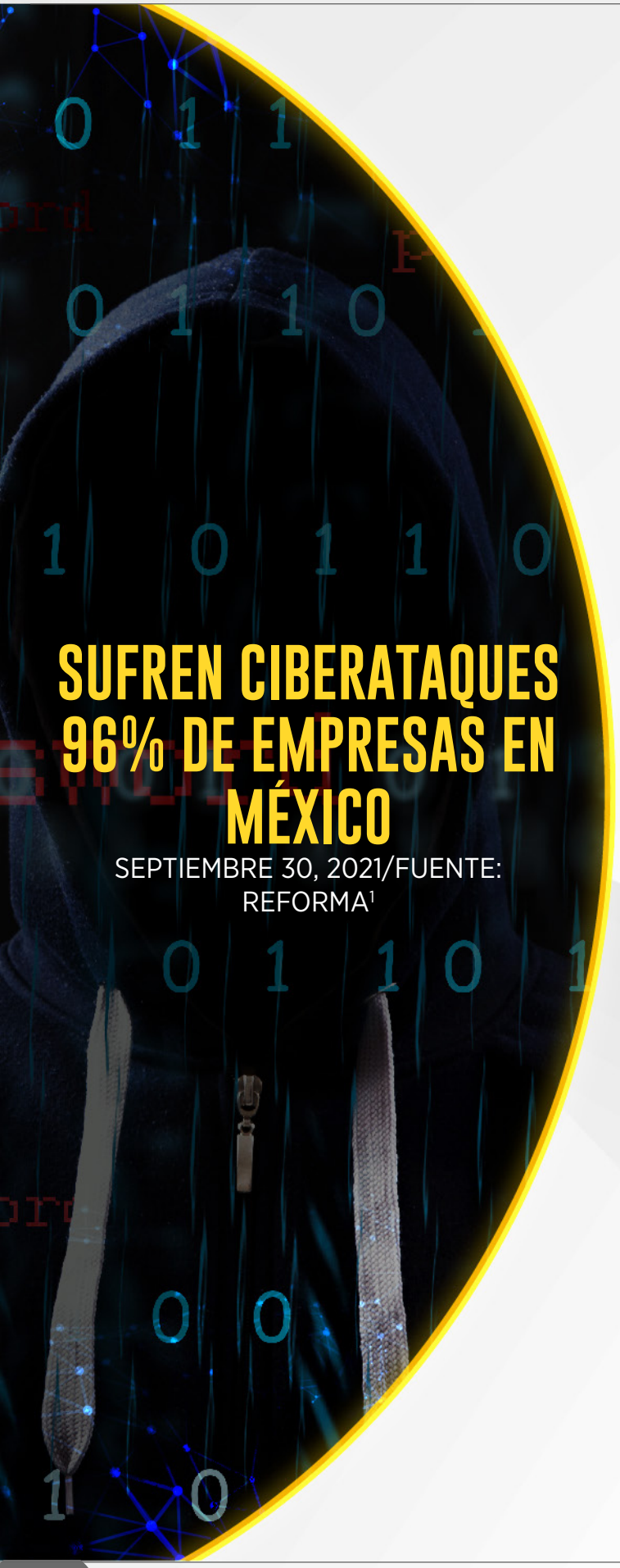
NEWSLETTER | totalsec

Expertos en Ciberseguridad

No. 291 | Sep 27 - Oct 01



SUFREN CIBERATAQUES 96% DE EMPRESAS EN MÉXICO

SEPTIEMBRE 30, 2021/FUENTE: REFORMA[1]

En el último año, 96 por ciento de las empresas mexicanas sufrió un ataque cibernético con impacto en el negocio, según un estudio que se aplicó a 155 encuestados realizado por la empresa especializada Tenable.

De acuerdo al informe 'Más allá de los límites: El futuro de la ciberseguridad en el nuevo mundo laboral', poco más del 80 por ciento se enfrentó a cuatro o más ciberataques. "El 96 por ciento reportó algún ataque, 74 por ciento de esos casos fueron por la nueva forma de trabajo, por aplicaciones o por esquemas que tuvieron que adaptarse para el tema de la pandemia al trabajo remoto, un porcentaje altísimo a mi parecer."

"Creo que lo que demuestra es un impacto directo en la forma de cambio de trabajo", dijo Francisco Ramírez de Arellano, vicepresidente de Tenable para Latinoamérica y el Caribe, en entrevista con REFORMA. Las afectaciones más reportadas por las empresas atacadas fueron provocadas porque alguna vulnerabilidad en los sistemas o aplicaciones que están utilizando los equipos.

"No nada más está enfocado en un solo sector sino son muchas verticales, hablamos del financiero, manufactura, ese tipo de lugares, por supuesto Gobierno, y el común denominador es que todos están preocupados por la creciente ola de ataques y que no se ve que vaya a parar."

Más de 91 mil millones de intentos de ciberataques se registraron en América Latina y el Caribe en el primer semestre de 2021

"Solo se ve que aumenta conforme más dispositivos están conectados a la red y más aumentan este tipo de ataques", mencionó Ramírez de Arellano.

Según cifras de Tenable, en los próximos dos años las organizaciones aumentarán en 88 por ciento su inversión en seguridad de redes; 79 por ciento en la gestión de vulnerabilidades y 75 por ciento en seguridad en la nube.

Por otra parte, cifras de la firma Fortinet indican que más de 91 mil millones de intentos de ciberataques se registraron en América Latina y el Caribe en el primer semestre de 2021, de los cuales el 67 por ciento fueron en México. Telecomunicaciones, manufactura y la industria automotriz son los sectores en los que aumentó el número de ciberataques, comentó Arturo Torres, estratega de FortiGuard Labs para América Latina y el Caribe a Grupo REFORMA.

Además, ataques a infraestructuras críticas, como el que ocurrió con Colonial Pipeline, seguirán ocurriendo. "El tema de infraestructuras críticas va a seguir siendo el foco principal por la criticidad que maneja", agregó Torres.

Además, con la adopción de los dispositivos de internet de las cosas, como los que se usan para casas o edificios inteligentes, están cobrando relevancia entre los ciberatacantes, aseguró el estratega.

[1]Fuente: https://www.reforma.com/aplicacioneslibre/preacceso/articulo/default.aspx?__rval=1&urlredirect=/sufren-ciberataques-96-de-empresas-en-mexico/ar2268302

ATAQUES CIBERNÉTICOS A INDUSTRIA DEL 'GAMING' CRECEN 340% DURANTE PANDEMIA

SEPTIEMBRE 24, 2021/FUENTE: MILENIO[2]

Entre 2019 y 2020, periodo en el que la pandemia del covid-19 se extendió por todo el mundo, la industria de los videojuegos reportó un **incremento de ataques cibernéticos de 340 por ciento** alrededor del mundo.

De acuerdo con un estudio de la firma Akamai, que se dedica a proveer servicios y aplicaciones de seguridad de internet, detalló que, **durante el último año, se registraron más de 240 millones de ataques de aplicaciones web** dirigidos a la industria.

Según el informe, **59 por ciento fueron SQL Injection (SQLi)**, que tiene como objetivo las **credenciales de inicio de sesión de los jugadores y su información personal**, el cual creció 224 por ciento entre 2019 y 2020.

En este periodo, hubo alrededor de 11 mil millones de ataques de relleno de credenciales contra jugadores. **El ataque de robo de credenciales es uno de los tipos más comunes para el control de cuentas**, principalmente debido al uso de información "reciclada" por parte de los usuarios.

Por otro lado, **hubo una caída del 20 por ciento en los ataques DDoS.** Pero a pesar de eso, todavía representaron 46 por ciento del tráfico DDoS observado por Akamai el año pasado.

Se estima que **el mercado global de videojuegos sigue creciendo en todo el mundo**, según una encuesta de Newzoo, la industria del gaming llegará a 175 mil millones dólares en el mundo en 2021.

Por otro lado, de acuerdo con datos de la consultora **The Competitive Intelligence Unit** (The CIU) presentados durante la Gaming Geek, **la industria de los videojuegos en México alcanzó un valor de mercado de 32 mil 229 millones de pesos durante 2020**, es decir, 4.4 por ciento más con respecto al año anterior.

A su vez, **el número de gamers alcanzó 72.3 millones al finalizar 2020**, lo que significa un aumento de 5.5 por ciento con respecto al 2019.

El informe detalla que **los criminales están centrando algunos de sus esfuerzos en estafar jugadores móviles** que buscan gastar dinero real en artículos del juego, como máscaras y mejoras de personajes personalizados, toda vez que existen estas modalidades en múltiples juegos.

> El robo de identidad se elevó 224 por ciento entre 2019 y 2020; se estima que al cierre del año este mercado tendrá un valor de 175 mil mdd

Los delincuentes usan plataformas de internet, como la empresa multinacional llamada Codashop, una página que se dedica a vender créditos, o cupones de aplicaciones y juegos online.

En ella, los usuarios no requieren crear un inicio de sesión, por lo que **los ataques de phishing sólo tienen una moderada tasa de éxito contra jugadores experimentados**, reveló el informe.

Sin embargo, **los delincuentes suelen implementar estos sitios web** como parte de una campaña más amplia dirigiendo el tráfico de usuarios hacia ellos, **a través de mensajes de chat, publicaciones en foros y correo electrónico.**

[2]Fuente: https://www.milenio.com/negocios/ataques-ciberneticos-industria-gaming-crece-340-pandemia

DETECTAN APPS MALICIOSAS QUE AFECTAN A MILLONES DE USUARIOS DE ANDROID

SEPTIEMBRE 29, 2020/FUENTE: EXPANSIÓN[3]

Recientemente fue descubierta una agresiva campaña de servicios premium móviles descargables en Google Play con más de 10 millones de víctimas en todo el mundo.

El hallazgo a cargo de Zimperium zLabs , expone que esta campaña de estafa masiva se ocultan tras aplicaciones de aspecto benigno, pero una vez instaladas comienzan a hacer cargos monetarios a sus usuarios.

De acuerdo al descubrimiento de la empresa, una agresiva campaña de servicios Premium móviles afectó a más de 10 millones de personas en todo el mundo. “La cantidad total robada podría ascender a cientos de millones de euros”, detalla el reporte.

Las aplicaciones maliciosas en Android actúan como troyanos, lo que permite aprovechar las interacciones del usuario para aumentar la propagación y la infección.

“Estas aplicaciones maliciosas de Android parecen inofensivas al mirar la descripción de la tienda y los permisos solicitados, pero esta falsa sensación de confianza cambia cuando a los usuarios se les cobra mes tras mes por el servicio premium al que se suscriben sin su conocimiento y consentimiento”, explica Zimperium.

La campaña de estafa, a la que han llamado GriftHorse, fue descubierta debido al aumento de alertas específicas del motor de detección de malware en dispositivos de Zimperium, z9, el cual detectó la verdadera naturaleza de las apps.

Se calcula que cerca de 10 millones de usuarios fueron afectados por alrededor de 200 aplicaciones maliciosas localizadas en Google Play

El trabajo sugiere que el grupo de amenazas ha estado ejecutando desde noviembre de 2020, y fueron inicialmente distribuido a través de Google Play y tiendas de aplicaciones de terceros.

Zimperium zLabs asegura que ya ha notificado a Google sobre los hallazgos, señalando que el gigante de internet verificó la información y elimino las aplicaciones.

“Sin embargo, las aplicaciones maliciosas todavía están disponibles en repositorios de aplicaciones de terceros no seguros, lo que resalta el riesgo de descargar aplicaciones a terminales móviles y datos de usuario y que necesitan seguridad avanzada en el dispositivo”, advierte Zimperium.

Las víctimas de GriftHorse

Según la información recopilada, GriftHorse ha infectado más de 10 millones de dispositivos de las víctimas en los últimos meses.

El grupo de ciberdelincuentes detrás de la campaña GriftHorse ha construido un flujo de efectivo estable de fondos ilícitos de estas víctimas, generando millones en ingresos.

Zimperium explica que esta campaña maliciosa es "excepcionalmente versátil" y está dirigida a usuarios móviles de más de 70 países. También detalla que ésta se ha desarrollado activamente a partir de noviembre de 2020, y la última hora actualizada se remonta a abril de 2021.

[3]Fuente: https://expansion.mx/tecnologia/2021/09/29/detectan-apps-maliciosas-que-afectan-a-millones-de-usuarios-de-android

PANDEMIA ABRIÓ LA PUERTA A ATAQUES CIBERNÉTICOS EN EMPRESAS: ESTUDIO

SEPTIEMBRE 28, 2021/FUENTE: FORBES[4]

El 74% de los líderes de seguridad y negocios mexicanos considera que los ataques cibernéticos actuales provienen de la tecnología implementada durante la pandemia, reveló un estudio.

El informe "Más allá de los límites: El futuro de la ciberseguridad en el nuevo mundo laboral", de Cyber Exposure, Forrester Consulting y Tenable, consultó la opinión de más de 1,300 líderes de seguridad, ejecutivos y empleados remotos.

De acuerdo con la investigación, 8 de cada 10 líderes empresariales señalaron que sus empresas están más expuestas a riesgos y ataques cibernéticos ante la migración a la nube que tuvieron que hacer al recurrir al trabajo remoto por la pandemia de Covid-19.

"Si las estrategias de ciberseguridad no se ajustan a los cambios en los negocios, el riesgo de hoy podría convertirse en la realidad de mañana", subraya el documento.

Factores de riesgo de ataques cibernéticos

A partir del confinamiento causado por la pandemia, las redes corporativas se convirtieron en redes domésticas pasibles de ataques cibernéticos, ya que el 82% de los trabajadores remotos tiene 6 o más dispositivos conectados a redes de internet caseras.

El 59% de los encuestados reconoce que accede a datos de clientes con un dispositivo personal y el 40% a registros financieros.

El estudio muestra que 6 de cada 10 líderes no contemplan prácticas para evitar ataques cibernéticos en el hogar de cada empleado.

"La pandemia transformó totalmente la manera en que la mayoría de las organizaciones trabajan en México. Al haber tantos equipos de seguridad luchando por comprender y abordar estos nuevos riesgos, los atacantes encuentran tierra fértil para aprovechar la oportunidad", dijo Francisco Ramírez de Arellano, vicepresidente en Latinoamérica de Tenable.

El trabajo remoto llevó a que las empresas trasladaran sus operaciones a la nube, donde se enfrentan a más riesgos de ataques cibernéticos por falta de protección en las casas

En este sentido, el 77% de organizaciones en México migró a la nube algunas funciones críticas y el 19% lo hará en los próximos 2 años, por lo tanto el riesgo de ataques cibernéticos es mayor. Los ejecutivos consideran que el riesgo de seguridad aumenta, ya que 66% de las empresas registraron ataques que involucran activos en estas plataformas.

Los responsables consideran que estos recientes ataques cibernéticos se deben en un 59% por el uso de software de terceros y en 56% por la expansión en su cadena de suministro.

El documento plantea dos escenarios, uno repleto de ataques cibernéticos descontrolados y otro con un incremento de la productividad y operaciones del negocio de forma segura.

"Las estrategias del trabajo remoto e híbrido han llegado para quedarse, al igual que los riesgos que conllevan a menos que las organizaciones comprendan su nueva superficie de ataque", dijo Amit Yoran, CEO de Tenable.

[4]Fuente: https://www.forbes.com.mx/tecnologia-pandemia-abre-la-puerta-a-ataques-ciberneticos-en-empresas-estudio/

NEWSLETTER

totalsec
Expertos en Ciberseguridad