Top 5 Amenazas a la seguridad, conócelas y protege tu empresa!

Las empresas y organizaciones han dado grandes pasos frente a los ataques de seguridad, incrementando recursos que las empresas han destinado para la ciberseguridad. Sin embargo, ante la mayor investigación y protección contra las amenazas, los ciber atacantes continúan cambiando su modo de actuar y ampliando sus objetivos, en numerosas ocasiones con unos presupuestos más elevados que los encargados de defender.

Los atacantes se han sofisticados y cada vez más buscan objetivos precisos y que ofrezcan una recompensa económica elevada, en lugar de ataques a gran escala al mayor número de usuarios posibles. De acuerdo a lo que hemos visto en materia de seguridad, compartimos las 5 amenazas de seguridad que estarán presentes a lo largo del 2019.

1. RANSOMWARE: EL MALWARE MAS RENTABLE

No es una amenaza nueva, pero es el tipo de Malware que mas crece. Este software malicioso se utiliza para bloquear el acceso a archivos o determinadas partes del dispositivo, con el objetivo de pedir un rescate a cambio de eliminar estas restricciones. Los ataques con ransomware siguen evolucionando y cada vez mas se dirigirán hacia las grandes organizaciones, que tienen la capacidad de pagar rescates más altos para recuperar el acceso a sus datos.

Los códigos maliciosos continúan siendo una de las principales amenazas, al tiempo que también son utilizados para llevar a cabo ataques. Además, de acuerdo con el ESET Security Report 2018, las infecciones por malware se presentan como la principal causa de incidentes de seguridad en las empresas latinoamericanas.

Los Laboratorios de Investigación de ESET reciben diariamente más de 300,000 muestras únicas de malware, lo que muestra un panorama del problema, sobre todo si consideramos que se desarrollan amenazas de este estilo para prácticamente todos los sistemas operativos

2. CRIPTOJACKING

Se trata de una amenaza que comenzaron a identificar a principios de agosto de 2018 y que tiene como principio el secuestro de la capacidad de procesamiento de un equipo ajeno para ganar dinero mediante la minería de criptomonedas. Una de las formas de infectar los dispositivos es a través de scripts que se ejecutan en el navegador de los usuarios. En otras palabras, basta con que el usuario visite un sitio web que contenga el código para que su procesador sea utilizado para minar alguna *criptodivisa*. El criptojacking comenzó a tener una gran actividad hacia finales del año pasado, siendo la amenaza más detectada por la telemetría de ESET a nivel mundial entre diciembre de 2017 y junio de 2018.

En lo que va de 2019, en la región latinoamericana, casi la mitad de las detecciones se concentra en dos países: Colombia (58,69%) Perú (30,72%) y México (17,41%), seguidos por Ecuador (8,89%), Brasil (7,73%) y Argentina (7,08%).

3. ATAQUES DE PHISHING

Si bien se trata de un ataque conocido y utilizado desde hace años, las **recientes campañas de propagación muestran nuevas características**. Por ejemplo, ahora los sitios web de phishing utilizan certificados de seguridad.

De acuerdo con el Antiphishing Working Group, durante el segundo trimestre de 2018, alrededor del 35% de los ataques de phishing registrados se alojaron en sitios web con el protocolo HTTPS, cifra que significa un importante incremento en comparación con el casi 5% de los casos de sitios falsificados con certificados SSL, reportados hacia finales de 2016.

Prácticamente la totalidad de las grandes empresas, han adoptado protocolos HTTPS ara cifrar la información y que esta no pueda ser utilizada por los atacantes. Sin embargo, en los últimos años, los cibercriminales han descubierto en estos protocolos una forma muy eficaz para maquillar sus acciones y hacer que se perciban como seguras. EN el 2018, el tráfico HTTPS cifrado que encubría malware y otras actividades maliciosas se multiplique por cinco.

4. EXPLORACIÓN DE VULNERABILIDADES

Método comúnmente utilizado por atacantes, con algunos datos interesantes de revisar, como los que se presentan a continuación.

Hacia finales de 2018 destacábamos que se trataba del año con el mayor número de vulnerabilidades reportadas (14,714 para ser precisos), superando por mucho los registros de años anteriores, sin embargo, en lo que va de 2019 esta cifra ha sido superada. De acuerdo con datos de CVE Details, a pesar de que aún no concluye el año, ya se han registrado más 15,300 vulnerabilidades.

5. CIBEREXTORSIONES

Durante 2018 aparecieron diversas estafas circulando a través del correo que se enfocaban en engañar a los usuarios a partir de la supuesta obtención de información que los comprometía. En varias de estas campañas existía algún elemento en particular, como un dato específico, que hacía creer al usuario que podría no tratarse de un engaño.

Un ejemplo es la campaña en la cual los cibercriminales enviaban un correo electrónico con la contraseña de los usuarios como parte del asunto del mensaje, en un intento por demostrar que tenían sus datos personales y que la extorsión que detallaban en el texto del correo era real. Se estima que esta campaña en particular logró recaudar cerca de medio millón de dólares.

Otro ejemplo de este tipo de estafas tenía la particularidad de que el correo electrónico llegaba al usuario desde su propia cuenta, lo que hacía suponer que el atacante tenía acceso a la cuenta de la potencial víctima. A través de un mensaje intimidatorio, el atacante hacía creer al usuario que poseía su información, por lo que solicitaba un pago (en Bitcoins) para “no revelar” los datos que supuestamente tenía en su poder.

Recientemente, se han identificado más campañas con el mismo modo de operación, y aunque parezca difícil de creer, continúan siendo efectivas para los atacantes.