Argentina sufrió más de 1.590 millones de intentos de ciberataques en el 2019 y los bancos fueron los principales objetivos

12/03/2020

El líder global en soluciones de ciberseguridad amplias, integradas y automatizadas, anunció los hallazgos para el 2019 de su plataforma Fortinet Threat Intelligence Insider Latin America, herramienta que recopila y analiza miles de incidentes de ciberseguridad a nivel global.

Los datos de la plataforma Fortinet revelaron la alarmante realidad del cibercrimen en América Latina y el Caribe, registrando 85 billones de intentos de ciberataques en el 2019. En Argentina, se registraron más de 1.590 millones de intentos de ciberataque el año pasado. Eso se traduce a alrededor de 4,4 millones de intentos por día, la mayoría de los cuales siguen la tendencia de Latinoamérica y están especialmente diseñados para entrar en redes bancarias, obtener información financiera y robar dinero, informaron desde la compañía.

Entre las amenazas más detectadas durante el 2019, se encuentran dos ataques dirigidos específicamente al sector bancario: DoublePulsar y Emotet. DoublePulsar es un ataque tipo “backdoor” que ha sido utilizado por el ransomware WannaCry y en intrusiones a bancos de la región en 2018.

“Teniendo en cuenta que aprovecha vulnerabilidades ya resueltas, su uso continuo evidencia la gran huella de software sin actualizaciones en Argentina que afecta tanto a

empresas como a individuos. Por su parte, Emotet es un botnet dirigido a bancos que permite que un atacante remoto puede emitir comandos para realizar diferentes operaciones como descargas de malware y ransomware", indicaron en el documento.

"Los datos de nuestra plataforma Fortinet Threat Intelligence Insider Latin America revelan un gran aumento de amenazas y el creciente desafío al que se enfrentan los bancos y las empresas en general para asegurar sus redes. El cibercrimen es uno de los mayores riesgos de hoy y continúa evolucionando en Argentina a un nivel alarmante, tanto en cantidad como en sofisticación. Ante este panorama de amenazas, las empresas y las instituciones financieras en particular se ven obligadas a repensar sus estrategias de ciberseguridad para asegurar la continuidad del negocio", señaló Gustavo Maggi, Director Regional de Fortinet para Sudamérica Este.

Otros resultados destacados, incluidos en la investigación publicada por Fortinet son:

· Fuerte aumento en la actividad de malware, exploits y botnets que ingresa a través de ataques de ingeniería social como el phishing. Las amenazas varían desde descargas no deseadas y troyanos que permiten tomar control de dipositivos infectados hasta explotación de vulnerabilidades. Muchas amenazas también buscan propagar malware para robar información crítica. La educación y concientización de los usuarios se vuelve clave.

· Las criptomonedas como uno los objetivos más buscados por los cibercriminales. Una gran parte de los ataques de criptominería a nivel mundial fue detectada en América Latina y el Caribe. El 84% del troyano W64/CoinMiner y el 77% del malware Riskware/CoinMiner a nivel mundial en el 2019 fue dirigido hacia la región.

"Como líderes en ciberseguridad, en Fortinet tenemos un fuerte compromiso con la recopilación, el análisis y el intercambio

de inteligencia crítica de amenazas a medida que el crimen se traslada de manera acelerada al ciberespacio. Las empresas no pueden proteger lo que no pueden ver, por lo que el intercambio de información sobre amenazas ayuda a las organizaciones a construir la estrategia de ciberseguridad integral y proactiva que los entornos digitales requieren para abarcar los ciber riesgos globales de hoy", agregó Maggi.

La plataforma Fortinet Threat Intelligence Insider Latin America es una herramienta en línea gratuita que ofrece hallazgos trimestrales de amenazas del laboratorio de inteligencia de Fortinet, FortiGuard Labs, para 10 países de la región. Además de información local sobre intentos de ataques a la ciberseguridad, ofrece resúmenes ejecutivos y mejores prácticas de seguridad.