Actividad de ciber amenazas en México en el primer semestre de 2023

Por Erika Urbina y Stephen Fallas*

Uno de los principales objetivos de Trellix, a través de su Centro de Investigación Avanzada (ARC), es analizar las distintas ciber amenazas que acechan en las distintas regiones del mundo, para tratar de entender lo que buscan los ciber criminales cuando organizan los ataques a diversas organizaciones de los países.

En el caso de México, y tal y como se dio a conocer a través de un webinar el 17 de agosto, se proporcionó un reporte con una descripción general de alto nivel sobre el panorama de amenazas observadas en México durante el primer semestre de 2023, utilizando información extraída de la plataforma de inteligencia, en este se dio a conocer información acerca de los actores detectados, las industrias afectadas, los artefactos y herramientas utilizadas, así como las actividades, entre otros.

Entre los datos más destacados que se dieron a conocer están los siguientes:

- El 45.5% de las actividades observadas están relacionadas con la industria de la Educación.
- El actor APT40 representa el 53.9% de la actividad observada.
- PowerSploit & Cobalt Strike es la principal herramienta utilizada con un 8.2% del total.
- Las familias de Ransomware con más presencia son DarkPower, Revil y Cuba.
- Los principales TTP de Mitre ATT&CK utilizadas en las campañas de ransomeware son Datos Cifrados (T1486) así como el Descubrimiento de Archivos y Directorios (T1083)
- El sector con más actividad de ransomware fue Educación con el 58.16%.

Durante el periodo hubo **26,885,500 detecciones totales** de direcciones IP, archivos y URLs maliciosos, las principales **campañas detectadas** que los actores de amenazas utilizan para atacar organizaciones en México fue de **80,496**.

El total de detecciones de hash de **archivos maliciosos** en formatos MD5, que se clasifican por reputación y puntuación de confianza, fue de **6,078,686**; y el número de **detecciones de ransomware**, que incluye a varias familias de este tipo de amenazas, fue de **69,722**. Las 5 principales familias de ransomware detectadas son DarkPower, REvil, Cuba e Industrial Spy y Lockbit.

Actividad de Ciber Amenazas

Los grupos de ransomware buscan extorsionar a sus víctimas mediante la publicación de su información en sitios web denominados “sitios de fuga”, utilizando la exposición para impulsar negociaciones estancadas con las víctimas o cuando se rechaza el pago del rescate.

La matriz de MITRE ATT&CK contiene un conjunto de técnicas utilizadas por los adversarios para lograr un objetivo específico, estos objetivos se clasifican como tácticas en la matriz

ATT&CK. Los objetivos se presentan linealmente desde el punto de reconocimiento hasta el objetivo final de exfiltración o “impacto”.

Durante el primer semestre de 2023, los grupos **APT40**, **MuddyWater** y **Gamaredon** fueron los tres grupos de amenazas más activos en el país. Las herramientas de amenazas más utilizadas fueron **PowerSploit**, **Cobalt Strike**, **China Chopper**, **Gh0st RAT** y **Empire**.

Todos estos grupos de amenazas tienen distintas motivaciones, técnicas, objetivos y usos de los datos robados. Durante los siguientes meses se estará monitoreando la actividad de estos grupos para evaluar si los datos del periodo indican un resurgimiento de los grupos en el escenario global.

Conclusión

México no está exento de sufrir diversos ataques cibernéticos de todo tipo, sobre todo porque su economía está en crecimiento y la actividad industrial se diversifica. Esto lo hace atractivo para grupos de ciber delincuentes que buscan obtener beneficios utilizando diversas técnicas para infiltrarse en los sistemas de todo tipo de organizaciones, en busca de información que les sirva para extorsionar tanto a las personas como a las organizaciones, en su beneficio.

Por ello es cada vez más importante contar con todo tipo de medidas de seguridad en los sistemas y con la gente necesaria, implementando una arquitectura de seguridad que se adapte fácilmente a las amenazas emergentes. Esto puede mejorar de manera significativa la resiliencia de una organización contra los ataques cibernéticos, minimizando las interrupciones y asegurando la continuidad operativa.

Trellix ofrece en este sentido su plataforma abierta y nativa con capacidades **XDR** (detección y respuesta extendida), ofreciendo a los equipos de Operaciones de Seguridad una mejor visibilidad, mayor facilidad de uso y una más rápida respuesta ante cualquier posible amenaza antes de que esta cause daños importantes en la organización. Trellix ofrece una amplia gama de controles de seguridad y XDR en su clase, incluyendo seguridad para Endpoints y redes, protección de datos, seguridad de colaboración. seguridad en la nube e Inteligencia de Amenazas, trabajando juntos para ofrecer la mejor protección a las organizaciones.

---

*Erika Urbina es la Country Manager de Trellix para México y Stephen Fallas es un Estratega de Arquitectura de Seguridad de Trellix para Latinoamérica, quien tiene una vasta experiencia de 23 años como especialista en seguridad de la información, con diversas certificaciones internacionales.