Trellix detecta colaboración entre ciber criminales y naciones-estado

- *El reporte destaca nuevos lenguajes de programación para desarrollo de malware, adopción de GenAI malicioso*
- *Hay una notoria aceleración en la actividad de amenazas geopolíticas*

SAN JOSE, Calif. – 16 de noviembre de 2023 – Trellix, la empresa de ciberseguridad que ofrece el futuro de la detección y respuesta extendidas (XDR), publicó hoy el **Informe Sobre Amenazas Cibernéticas de noviembre de 2023**, desde el Centro de Investigación Avanzada (ARC). Trellix observó indicadores de colaboración entre grupos de ransomware y actores de amenazas persistentes avanzadas (APT), respaldados por naciones-estado, adopción y uso de lenguajes de programación menos conocidos para malware y ciberdelincuentes que desarrollan herramientas de IA generativa (GenAI).

"A medida que avanza la tecnología, también lo hace el cibercrimen, y comprender el panorama cambiante es vital para que los CISO y los equipos de SecOps se adelanten a las amenazas", dijo John Fokker, director de Inteligencia de Amenazas del Centro de Investigación Avanzada Trellix. “Los ciberdelincuentes son cada vez más ágiles, organizados y políticamente alineados. Es imperativo que los defensores recurran a la inteligencia sobre amenazas para maximizar su postura de seguridad con recursos limitados".

El último Informe sobre amenazas cibernéticas del Centro de investigación avanzada Trellix incluye:

- **GenAI malicioso:** los ciberdelincuentes eluden las protecciones para aprovechar herramientas comúnmente conocidas y utilizan GenAI para mejorar las campañas de phishing. La escala y la velocidad cada vez mayores de los ataques de phishing indican que es posible que GenAI malicioso ya esté implementándose en la actualidad.
- **Actividad de amenazas geopolíticas:** la actividad de amenazas a los Estados-Nación aumentó más del 50% en los últimos seis meses debido a la escalada del conflicto en Rusia y Ucrania; la intensificación de la actividad cibernética en Israel justo antes y durante el conflicto; y los ataques de partes probablemente afiliadas a China contra Taiwán, de cara a sus elecciones de 2024.
- **Desarrollos de ransomware:** las detecciones globales y los incidentes reportados por la industria, particularmente en el segundo trimestre, reflejan variaciones inusuales en las familias de ransomware, así como en los países e industrias objetivo. El Centro de Investigación Avanzada de Trellix también observó una fragmentación de grandes grupos de ransomware, con la introducción de grupos más pequeños y más ataques centrados en la filtración de datos.
- **Colaboración clandestina:** los últimos seis meses demostraron un aumento en los actores de amenazas que colaboran activamente en los foros de la Dark Web. Esto abarcó grupos que se unieron formalmente (“The Five Families”), una escalada en la

venta/compartición de vulnerabilidades de día cero, esfuerzos conjuntos de desarrollo de PoC para acelerar los exploits y más.

- **Malware políglota:** la ciber crisis, que es en sí misma una crisis múltiple porque multiplica las amenazas, y el aumento del malware políglota lo exacerba aún más. Los nuevos lenguajes de programación se están convirtiendo en opciones populares de malware, el Golang registra un alto uso para ransomware (32%), puertas traseras (26%) y troyanos (20%).

El panorama de la ciberseguridad experimenta perturbaciones periódicamente a medida que los acontecimientos geopolíticos y económicos crean un mundo cada vez más complicado e incierto. Diariamente surgen nuevos actores cibernéticos y constantemente se descubren nuevas vulnerabilidades, exploits y tácticas. El análisis integral proporcionado por el Centro de Investigación Avanzada de Trellix sirve como un recurso vital para que los CISO de hoy comprendan y mitiguen los riesgos de ciberseguridad en evolución en un mundo interconectado.

El **Informe sobre Amenazas Cibernéticas de noviembre de 2023** incluye datos patentados de la red de sensores de Trellix, investigaciones sobre la actividad cibercriminal y de los estados-nación realizadas por el Centro de Investigación Avanzada de Trellix, e inteligencia de código abierto y cerrado. El informe se basa en la telemetría relacionada con la detección de amenazas, cuando la Plataforma XDR de Trellix detecta y reporta un archivo, URL, dirección IP, correo electrónico sospechoso, comportamiento de la red u otro indicador.

Recursos adicionales:

- Informe sobre Ciber Amenazas: noviembre de 2023 (en inglés)
- Centro de Investigación Avanzada de Trellix
- Boletín informativo de LinkedIn del Centro de investigación avanzada Trellix

Fuente: Trellix

.