Trellix pronostica sobre las ciberamenazas para 2024

- *La firma se adelanta y alerta sobre tres grandes riesgos para el próximo año*

La necesidad de una inteligencia eficaz sobre amenazas a escala mundial crece a medida que los acontecimientos geopolíticos y económicos crean un mundo cada vez más complicado e incierto tanto para las empresas como para los consumidores. Los ciberdelincuentes evolucionan con nuevos actores y amenazas; además de nuevas formas de aprovechar o ejecutar tácticas. Los expertos en seguridad deben asumir que ninguna empresa o individuo está a salvo de una amenaza cibernética y que existe una urgencia cada vez mayor de monitorear e investigar las amenazas que reaparecen y evolucionan a un ritmo y escala acelerados.

El ransomware es una plaga presente para muchas organizaciones en todo el mundo a medida que estas familias aumentan en escala y sofisticación, incluida la coordinación y asociación con otros actores de amenazas a través de foros clandestinos. Las tácticas diseñadas para engañar a los usuarios y poner en peligro sus dispositivos o su información personal son cada vez más astutas y, al mismo tiempo, difíciles de detectar e identificar tanto para las víctimas como para las herramientas de seguridad. Además, es tendencia que los ciberataques aprovechen situaciones políticas, económicas y geográficas de instituciones o gobiernos de naciones-estado que practican el espionaje, experimentan guerra y desinformación.

“El panorama cibernético es más complejo que nunca. Los ciberdelincuentes, desde familias de ransomware hasta actores de Estados-Nación, se vuelven más inteligentes, rápidos y coordinados a la hora de reestructurar sus tácticas para seguir nuevos esquemas, y no anticipamos que eso cambie en 2024”, afirmó John Fokker, jefe de Inteligencia de Amenazas del Centro de Investigación Avanzada de Trellix. “Para romper con el aumento de ataques y comenzar a ser más astutos que los actores de amenazas; todas las industrias deben adoptar una estrategia cibernética que esté en constante alerta, sea procesable, comprensible y adaptable a nuevas amenazas. Así es como podemos garantizar una ventaja sobre los ciberdelincuentes durante el próximo año”.

Los expertos en ciberseguridad y los investigadores de amenazas del equipo del Centro de Investigación Avanzada Trellix han recopilado sus predicciones sobre tendencias, tácticas y amenazas para 2024. El estudio resulta en tres temas principales: inteligencia artificial, cambios en las tendencias de la ciberdelincuencia y amenazas emergentes y nuevos ataques.

Sobre IA, la especialista Shyava Tripathi aportó al estudio el tema “Desarrollo clandestino de LLM maliciosos”, donde menciona que herramientas como FraudGPT y WormGPT son prominentes en las redes cibercriminales. Los foros populares de la red oscura a menudo sirven como plataformas para el desarrollo coordinado de correos electrónicos de phishing, páginas web falsificadas, así como la creación de malware y vulnerabilidades diseñadas para evadir la detección de miles de usuarios. Estas aplicaciones de lenguaje (LLM) pueden ayudar a mitigar los considerables desafíos que enfrentan los ciberdelincuentes y que su uso malicioso se acelere en 2024.

Por su parte, el experto John Fokker aporta sobre el tema de ataques a la cadena de suministro y menciona que las soluciones de transferencia gestionada de archivos (MFT), diseñadas para intercambiar de forma segura datos confidenciales entre entidades, desempeñan un papel fundamental en las operaciones comerciales modernas y las empresas dependen en gran medida de éstas para facilitar el intercambio fluido de datos tanto interna como externamente.

Donde cualquier interrupción o compromiso de estos sistemas puede provocar un tiempo de inactividad operativo significativo, reputación empañada y pérdidas financieras. Esto los convierte en objetivos muy atractivos para los actores del ransomware que son conscientes de cómo el impacto potencial aumenta el alcance de sus demandas de extorsión, expone Fokker.

Para finalizar, en torno a la tercera tendencia de ciberseguridad, Manoj Reddy, del Centro de Investigación Avanzada de Trellix, agrega que las amenazas internas en las empresas y organizaciones han aumentado 47% en los últimos dos años, lo que provocó una pérdida total de 15.38 millones de dólares por la contención de estos incidentes. Esta amenaza vulnera la confidencialidad y la integridad de la organización al tiempo que ayuda a los adversarios a recopilar inteligencia, llevar a cabo operaciones de sabotaje y utilizar métodos de suplantación para lograr sus objetivos.

Reddy concluye que a medida que los dispositivos conectados sigan proliferando y las fuerzas de trabajo híbridas y remotas persistan, las amenazas internas seguirán creciendo. La naturaleza de las amenazas internas presenta un desafío formidable para las personas, los procesos y la tecnología. Es esencial que las organizaciones identifiquen, evalúen, detecten y gestionen estas amenazas internas en el panorama de amenazas actual para conservar la confianza de las partes interesadas