Deepfakes, criptomonedas y wallets: los ciberataques a la cadena de suministro aumentarán

Un Informe sobre Predicciones Globales de Ciberseguridad 2022, realizado por Check Point® Software Technologies Ltd. (NASDAQ: CHKP), un proveedor líder de soluciones de ciberseguridad a nivel mundial, detalla los principales retos de seguridad a los que se enfrentarán las empresas durante el próximo año. Mientras los ciberdelincuentes siguen aprovechando el impacto de la pandemia de la COVID-19, también encontrarán nuevas oportunidades de ataque con las deepfakes, las criptodivisas, los wallets y mucho más.

Entre los aspectos más destacados del Informe sobre Predicciones Globales de Ciberseguridad 2022 se encuentran los siguientes:

- Vuelven las Fake News y las campañas de desinformación: a lo largo de 2021, se difundió información errónea sobre la pandemia de la COVID-19 y la correspondiente vacunación. En 2022, los grupos de ciberdelincuentes seguirán aprovechando las campañas de noticias falsas para ejecutar diversos ataques de phishing y estafas.

- Los ciberataques a la cadena de suministro siguen aumentando: los ataques a la cadena de suministro serán cada vez más comunes y los gobiernos comenzarán a legislar para hacer frente a estas amenazas y proteger las redes, así como a colaborar con los sectores privados y otros países para identificar y atacar a más grupos de amenaza a nivel mundial.
- La «guerra fría» cibernética se intensifica: la mejora de las infraestructuras y de las capacidades tecnológicas permitirán a los grupos terroristas y a los activistas políticos impulsar sus programas y llevar a cabo ataques más sofisticados y de mayor alcance. Los ciberataques se utilizarán cada vez más como conflictos indirectos para desestabilizar actividades a nivel mundial.
- Las filtraciones de datos son de mayor escala y más costosas: las filtraciones de datos se producirán con mayor frecuencia y a mayor escala y su recuperación costará más a las empresas y a los gobiernos. En mayo de 2021, el gigante estadounidense de los seguros pagó 40 millones de dólares en rescates a los ciberdelincuentes. Esto fue un récord, y es de esperar que los rescates exigidos por los atacantes aumenten en 2022.
- La criptodivisa gana popularidad entre los ciberdelincuentes: cuando el dinero se convierta en puro software, la ciberseguridad necesaria para protegerse de los atacantes que roban y manipulan bitcoins y altcoins cambiará de forma inesperada.
- Dispositivos móviles en el punto de mira: a medida que los monederos móviles y las plataformas de pago por móvil se utilicen con más frecuencia, los ciberdelincuentes evolucionarán y adaptarán sus técnicas para explotar la creciente dependencia de los dispositivos móviles.
- Los ciberdelincuentes aprovecharán las vulnerabilidades de los microservicios: con la arquitectura de microservicios adoptada por los proveedores de servicios en la nube (CSP), los ciberdelincuentes están utilizando las vulnerabilidades encontradas en ellos, para lanzar ataques a gran escala contra los CSP.
- La tecnología deepfake se convierte en un arma para los ataques: las técnicas de vídeo o audio falsos son ahora lo suficientemente avanzadas como para ser un arma y utilizarse para crear contenido dirigido a manipular opiniones, cotizaciones bursátiles o para obtener permisos y acceder a datos sensibles.
- El ransomware sigue haciendo su agosto: a nivel mundial en 2021, 1 de cada 61 empresas experimenta un ransomware cada semana. Los ciberdelincuentes seguirán atacando a las compañías que puedan permitirse pagar un rescate, y la sofisticación del ransomware aumentará en 2022. Veremos cómo utilizan cada vez más herramientas de penetración para personalizar los ataques en tiempo real y vivir y trabajar dentro de las redes de las víctimas.

«En 2021, los ciberdelincuentes adaptaron su estrategia de ataque para explotar temas de actualidad como vacunación, las elecciones y el cambio al trabajo híbrido, para atacar las cadenas de suministro y las redes de las empresas con el fin de lograr la máxima disrupción», alertan desde Check Point Software Technologies.

«La sofisticación y la escala de los ciberataques seguirán batiendo récords y podemos esperar un enorme aumento en el número de ransomware y ataques móviles. De cara al futuro, las empresas deben ser conscientes de los riesgos y asegurarse de que cuentan con las soluciones adecuadas para prevenir, sin interrumpir el flujo normal de la empresa, la mayoría de los ataques, incluidos los más avanzados. Para adelantarse a las amenazas, las organizaciones deben ser proactivas y no dejar ninguna parte de su superficie de ataque sin proteger o supervisar, o corren el riesgo de convertirse en la próxima víctima de complejos ataques dirigidos», concluyen los especialistas en ciberseguridad.

Fuente: Ámbito