Conoce las predicciones de Trellix sobre las ciber amenazas para 2023

*Por John Fokker**
Director de Inteligencia de Amenazas de Trellix

Cada año compartimos nuestras observaciones de cómo será el siguiente año en ciber amenazas. El equipo del Centro de Investigación Avanzada de Trellix reportó que para 2022 teníamos predicciones sobre *hacktivismo*, guerra cibernética y ataques a las cadenas de proveedores de software.

Comenzamos 2022 con una vulnerabilidad para toda la industria en Log4J, que fue seguido por la guerra física y cibernética contra Ucrania. Terminamos el año observando *hactivistas* resolviendo el problema con sus propias manos, nuevos actores en operación y un escenario diferente pero cada vez más activo de ransomware.

Conforme la economía global continúa creando estrés político y divergencia, las organizaciones deben esperar un incremento en las actividades de los actores que buscan promover su propia agenda por ganancias políticas o financieras. Para engañar y vencer a los malhechores, y avanzar en forma proactiva las defensas, la industria de la ciberseguridad debe estar siempre alerta y siempre aprendiendo

De los reportes que estudian y explican las tendencias, podemos organizar mejor las acciones de nuestro sector. Yo sugiero mantener un ojo en cuatro actividades en 2023: geopolítica y conflictos, *hacktivismo*, más vulnerabilidades descubiertas (o redescubiertas) y ataques de phishing armado.

Geopolítica y conflictos

El alza de los ciberataques y campañas de desinformación motivados por geopolítica pueden continuar moldeando el paisaje de las ciber amenazas en 2023. Estos intentos fueron parte de esfuerzos de reconocimientos cada vez mayores, activos o pasivos, para apoyar el proceso de lanzamiento de misiles balísticos.

El *hacktivismo* en el centro del escenario

Dadas las tensiones globales de hoy, estamos viendo el resurgimiento del *hacktivismo* y esperamos que esto juegue un papel más importante en 2023. A medida que grupos débilmente organizados impulsados por la propaganda, se alinean por una causa común, pueden incrementar el uso de herramientas para expresar su enojo y causar disrupción. Como hay tensiones en diversas regiones, consideramos que el *hacktivismo* escalará conforme se adapta a la agenda política de partidos de oposición y ofrece una negación perfectamente plausible de las acciones, ya que son iniciadas y llevadas a cabo por activistas.

Más vulnerabilidades descubiertas (o redescubiertas)

Tanto los agentes de amenazas como los investigadores de seguridad incrementarán sus estudios en las estructuras subyacentes que son parte de la cadena de suministros. Como resultado, anticipamos ver más vulnerabilidades descubiertas (o redescubiertas) y

explotadas con amplio impacto, lo que no necesariamente llegará en la forma de un gran error de Microsoft, sino un marco del que nunca había oído y que todo mundo está usando. Por lo tanto, debemos incrementar nuestra visibilidad y profunda comprensión de exactamente cuál código estamos corriendo en nuestra organización.

Ataques de phishing armados

En 2023 se espera ver ataques armados de phishing a lo largo de servicios de comunicación de empresas y aplicaciones comúnmente usados. Los actores de amenazas alrededor del mundo pueden incrementar y ajustar sus métodos establecidos para infiltrar las redes de las organizaciones. Como la cultura del trabajo híbrido ha expandido las superficies de ataque hacia las redes y dispositivos domésticos que son vulnerables y están mal administrados, los agentes de amenazas se han beneficiado usando esto como un medio para apuntar fácilmente a las redes empresariales. Esto ha llevado a incrementos en los intentos de phishing hacia los negocios y, a cambio, las organizaciones se han enfocado en fortalecer sus perímetros y protección de servicio de correos.

Queremos que no solo responda a riesgos conocidos, sino que se anticipe a amenazas futuras con información de expertos de hacia dónde enfocar sus defensas. Resulta que predecir el futuro no es magia, solo requiere conocimiento de la industria y ciencia de datos vanguardista.

*John Fokker es actualmente el Director de Inteligencia de Amenazas en Trellix, que es la empresa resultado de la fusión entre McAfee y FireEye, creando una de las empresas de ciber seguridad más grandes del mundo. Cuenta con la plataforma abierta y nativa de detección y respuesta extendida (XDR) para ayudar a las organizaciones a enfrentar las amenazas más avanzadas de la actualidad y generar confianza en la protección y resiliencia de sus operaciones.