MANDIANT
AHORA PARTE DE Google Cloud

Informe especial de M-Trends 2023

Resumen ejecutivo

La edición n.° 14 del informe M-Trends 2023 está disponible en www.mandiant.com/m-trends

En cifras: Los datos de M-Trends

La información proporcionada se basa en investigaciones de Mandiant Consulting realizadas entre el 1 de enero de 2022 y el 31 de diciembre de 2022.

¿Qué necesito saber?

- En todo el mundo, los ataques se detectan más rápido, con una mejora en las regiones de América y EMEA, pero no en la región de APAC.
- Los proveedores de seguridad y otras fuentes externas están notificando a las organizaciones sobre ataques de manera más frecuente de lo que los equipos internos de seguridad los descubren; sin embargo, cuando los equipos internos detectan ataques, es más rápido que cuando se los notifica un externo.
- Para obtener acceso a las organizaciones, los atacantes aprovechan lo que mejor funciona en distintas regiones: exploits en América, phishing en EMEA y ataques previos en APAC.

Consulte con su CISO

- ¿Cómo medimos nuestro tiempo de detección y de respuesta, y cuál es nuestro tiempo promedio desde la detección hasta la respuesta y la remediación?
- ¿Estamos preparados para detectar y responder a los malwares, exploits y vectores de infección inicial más comunes, como el phishing?
- ¿Cuál es nuestro protocolo cuando un tercero nos notifica que posiblemente hemos sido atacados?
- ¿Cómo nos posicionamos para garantizar la mitigación de exploits para sistemas con vulnerabilidades conocidas?

Invasión de Ucrania

¿Qué necesito saber?

- Mandiant identificó un amplio espionaje cibernético, ataques cibernéticos disruptivos y destructivos y operaciones de información que condujeron a la invasión de Rusia a Ucrania el 24 de febrero de 2022 y que han continuado desde entonces.
- Las operaciones rusas han afectado los sistemas de control industrial e infraestructura crítica y, en algunos casos, fueron habilitadas mediante campañas realizadas y accesos obtenidos antes de la invasión.
- La invasión rusa a Ucrania ha demostrado la posible superposición de las operaciones cibernéticas y la guerra cinética como un nuevo estándar de facto.

Consulte con su CISO

- ¿Hemos tomado acciones para fortalecer nuestros sistemas contra ataques destructivos y disruptivos?
- ¿Cuáles fueron los resultados de la prueba más reciente de nuestro plan de respaldos y continuidad de las operaciones?
- ¿Deberíamos utilizar inteligencia de amenazas para combatir operaciones de información?

Operaciones financieras de Corea del Norte

¿Qué necesito saber?

- Junto con las misiones tradicionales de recolección de inteligencia y ataques disruptivos, en 2022, operadores de la República Popular Democrática de Corea (RPDC) demostraron más interés en robar y utilizar criptomonedas.
- Estas operaciones han sido muy lucrativas y es probable que continúen ininterrumpidamente durante 2023.

Consulte con su CISO

- ¿Cuán preparados estamos para lidiar con las amenazas financieras más relevantes para nuestra organización?

Cambiar el enfoque y técnicas poco comunes

¿Qué necesito saber?

- Atacantes con menos habilidades técnicas están causando un gran impacto en las organizaciones.
- Estas operaciones condujeron al robo de datos y propiedad intelectual, así como daño significativo a la reputación.
- Estos atacantes parecen estar más motivados por la notoriedad que por dinero o espionaje, han demostrado capacidad de improvisación y están dispuestos a utilizar sobornos e incluso intimidación o amenazas para lograr sus objetivos.

Consulte con su CISO

- ¿Cómo estamos minimizando el riesgo de que la ingeniería social y otras amenazas similares alcancen a nuestros empleados?
- ¿Qué programas tenemos para proteger a nuestros empleados, especialmente ejecutivos y empleados altamente visibles de estos tipos de ataques?
- ¿Cómo reaccionaríamos si se robara información propietaria o con datos personales del cliente y se la utilizara para extorsionarnos?
- ¿Tenemos un procedimiento para adquirir rápidamente criptomonedas en respuesta a una amenaza de extorsión?

Enfoque en la nube: Caso de estudio de un Red Team

¿Qué necesito saber?

- Los proyectos de Red Team ayudan a las organizaciones a evaluar las capacidades de su programa de seguridad frente a escenarios de ataque del mundo real y a mejorar sus posturas de seguridad.
- Mandiant le demostró a una empresa de servicios públicos de qué manera los atacantes pueden obtener acceso a recursos críticos del entorno de tecnología operativa y de la nube.

Consulte con su CISO

- ¿Tenemos una visibilidad completa sobre cómo nuestra organización utiliza la nube exactamente?
- ¿Estamos periódicamente revisando para identificar errores de configuración que los atacantes pueden explotar?
- ¿Probamos nuestras implementaciones de arquitectura en la nube?

Campañas y eventos globales

¿Qué necesito saber?

- Para proteger mejor a los clientes durante 2022, el equipo de campañas y eventos globales de Mandiant investigó actividad rusa de espionaje, ransomware y vulnerabilidades significativas como Log4Shell.
- Mandiant comparte indicadores e inteligencia valiosa para ayudar a nuestros clientes y a la comunidad a protegerse de estas campañas.

Consulte con su CISO

- ¿Qué estamos haciendo para rastrear y corregir vulnerabilidades en nuestra red?
- ¿Cómo estamos utilizando la inteligencia de amenazas actual para la toma informada de decisiones?

APT42—Graduaciones notables

¿Qué necesito saber?

- APT42 es un grupo de amenazas con nexo iraní que realiza espionaje mediante ataques sofisticados de ingeniería social y phishing.
- La actividad de APT42 representa una amenaza para funcionarios de política exterior, comentaristas y periodistas que trabajan en proyectos relacionados con Irán, en especial aquellos en los Estados Unidos, el Reino Unido e Israel.

Consulte con su CISO

- ¿Qué pueden hacer nuestros equipos de seguridad, de TI y de negocios para proteger a todos los empleados?
- ¿Cómo estamos minimizando el riesgo de que las amenazas de ingeniería social alcancen a nuestros empleados?
- ¿Cómo concientizamos a nuestros empleados sobre el phishing y otros intentos de ingeniería social?

Más información en www.mandiant.com/m-trends

Mandiant

11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

Acerca de Mandiant

Mandiant es un líder reconocido en defensa cibernética dinámica, inteligencia de amenazas y servicios de respuesta a incidentes. Gracias a décadas de experiencia en el frente de batalla, Mandiant ayuda a las organizaciones a mejorar su preparación para defender y responder a las amenazas cibernéticas. Mandiant ahora es parte de Google Cloud.

MANDIANT
AHORA PARTE DE Google Cloud