FIREEYE™

FICHA TÉCNICA

Operaciones del equipo de emergencias (Red Team Operations, RTO)

Ponga a prueba su capacidad para proteger sus activos más críticos de un ataque selectivo del mundo real

VENTAJAS

- Saber si sus datos críticos están en riesgo y qué tan fácilmente puede ser obtenidos por un perpetrador
- Evaluar la seguridad de su entorno contra un atacante realista y "sin restricciones"
- Poner a prueba la capacidad de su equipo de seguridad interna para prevenir, detectar y responder a incidentes en un entorno controlado y realista
- Identificar y mitigar las vulnerabilidades de seguridad complejas antes de que un atacante las explote
- Obtener un análisis de riesgos basados en hechos y recomendaciones para mejorar el nivel de seguridad

Por qué Mandiant

Mandiant, una empresa de FireEye, ha sido el líder en cuanto a ciberseguridad e información de ciberamenazas desde 2004. Nuestros responsables de la respuesta ante incidentes han estado en las primeras líneas de las brechas más complejas en todo el mundo. Tenemos una comprensión exhaustiva en lo que respecta a perpetradores existentes y emergentes, además de sus herramientas, tácticas y procedimientos que cambian rápidamente.

Descripción general del servicio

La investigación de las operaciones del equipo de emergencias consiste de un escenario de ataque realista y "sin restricciones" en su entorno. El equipo de emergencias de Mandiant usa cualquier método no destructivo necesario para lograr un conjunto de objetivos de la misión acordados conjuntamente mientras simula el comportamiento del atacante. El equipo de emergencias imita estrechamente los métodos de ataque activos y encubiertos de un atacante real mediante el uso de TTP vistos en investigaciones reales y recientes de respuesta ante incidentes. Esto ayuda a evaluar la capacidad de su equipo de seguridad para detectar y responder a un escenario de atacante activo.

Objetivos de muestra		
Robar correos electrónicos de ejecutivos o desarrolladores	Irrumpir en un entorno segmentado que contenga datos críticos o confidenciales del negocio	Tomar el control de un dispositivo automatizado, como un dispositivo IoT, un dispositivo médico o un dispositivo de fabricación

Metodología

Las operaciones del equipo de emergencias comienzan cuando se determina de manera conjunta si el equipo de emergencias debe tener o no algún conocimiento del entorno. Mandiant aplica su experiencia en la industria para identificar objetivos que representan riesgos primarios para sus funciones principales de negocio.

Las investigaciones de las operaciones del equipo de emergencias siguen las fases del ciclo de vida del ataque.

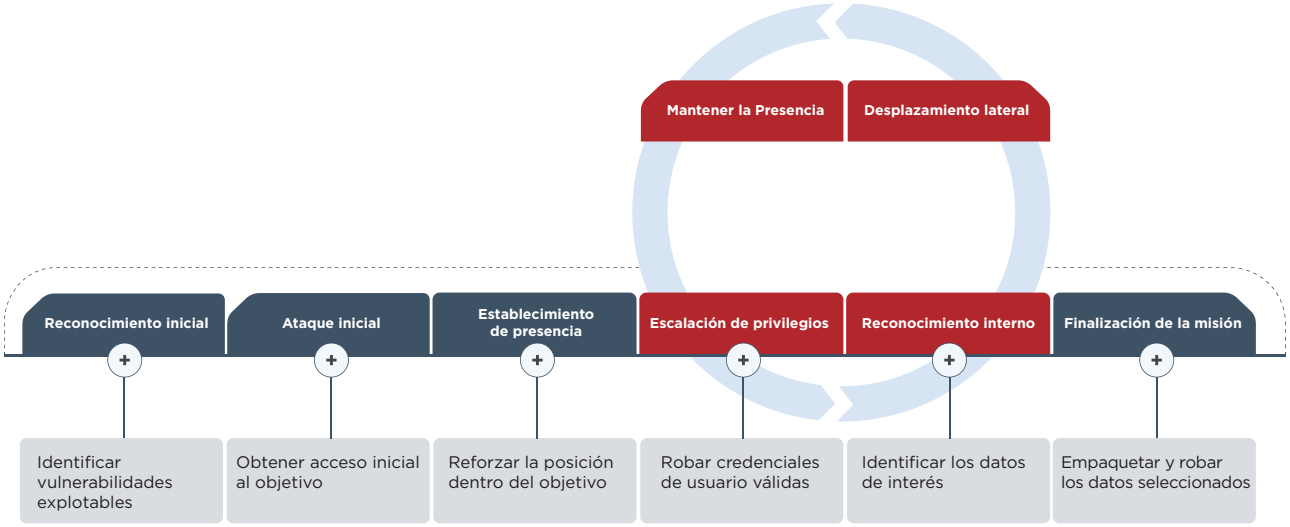

Figura 1. Ciclo de vida de ataque.

Una vez que se establecen los objetivos, el equipo de emergencias comienza realizando un reconocimiento inicial. Mandiant aprovecha una combinación de repositorios de información exclusiva, además de herramientas y técnicas de inteligencia de código abierto (Open-Source Intelligence, OSINT) para realizar reconocimientos en el entorno seleccionado.

Mandiant intenta obtener acceso inicial al entorno seleccionado mediante al explotar las vulnerabilidades o realizar un ataque de ingeniería social. Mandiant aprovecha las técnicas utilizadas por los atacantes del mundo real para obtener acceso privilegiado a estos sistemas.

Una vez que se obtiene el acceso, el equipo de emergencias intenta la escalación de privilegios para establecer y mantener la persistencia dentro del entorno mediante la implementación de una infraestructura de comando y control, tal como lo haría un atacante.

Después de que se establecen los sistemas de persistencia y comando y control dentro del entorno, el equipo de emergencias intenta cumplir con sus objetivos a través de cualquier medio no disruptivo necesario.

Por qué elegir las operaciones del equipo de emergencias
Las operaciones del equipo de emergencia se recomiendan para las organizaciones que desean hacer lo siguiente:

- *Capacidades de detección y respuesta de prueba.* Los equipos de seguridad se preparan para los incidentes del mundo real, pero debe confirmar que pueden responder correctamente, sin riesgo real.
- *Aumentar la conciencia y demostrar el impacto.* El equipo de emergencias de Mandiant se comportan como atacantes del mundo real, trabajan para vulnerar su entorno desde internet utilizando información solo disponible en Internet. Las investigaciones exitosas del equipo de emergencias pueden ayudar a justificar el aumento de los presupuestos de seguridad e identificar brechas que requieren mayor inversión.

LO QUE OBTIENE

- Resumen para ejecutivos y directores
- Detalles técnicos con información paso a paso que le permite recrear nuestros hallazgos
- Análisis de riesgos basado en hechos para que sepa que un hallazgo crítico es relevante para su entorno
- Recomendaciones tácticas para una mejora inmediata
- Recomendaciones estratégicas para la mejora a largo plazo
- Experiencia invaluable para responder a un incidente del mundo real sin la presión de una vulneración potencial que aparezca en los titulares de los periódicos

Para obtener más información sobre FireEye, visite: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

Acerca de FireEye, Inc.
FireEye es una empresa de seguridad basada en inteligencia. FireEye, que funciona como una extensión escalable y transparente de las operaciones de seguridad del cliente, ofrece una sola plataforma que combina tecnologías innovadoras de seguridad, inteligencia sobre amenazas similar a los de una Nación y los servicios de consultoría de fama mundial de Mandiant®. Gracias a este enfoque, FireEye elimina la complejidad y la carga de la seguridad cibernética para las organizaciones que desean estar preparadas y responder ante los ataques cibernéticos, además de prevenirlos.