FIREEYE™

FICHA TÉCNICA

Servicios de respuesta ante incidentes

Investigar, contener y corregir los incidentes de seguridad críticos mediante velocidad, adaptabilidad y eficiencia

CASO PRÁCTICO: RESPUESTA ANTE INCIDENTES (IR) DE MANDIANT EN ACCIÓN

Una firma multinacional de servicios profesionales con decenas de miles de computadoras en todo el mundo contrató a Mandiant para responder a una vulneración de datos potencial de datos críticos de los clientes.

Día 1: los consultores de Mandiant empezaron a implementar en 18 000 sistemas su tecnología de usuario final basada en la nube en un lapso de cuatro horas de recibir la notificación.

- La investigación empezó ese mismo día.
- En un lapso de cuatro horas de haber iniciado la investigación se confirmó que existía evidencia de una vulneración.

Día 6: se completó la mayor parte del trabajo de investigación. Se llevó a cabo el análisis de más de 18 000 usuarios finales con un análisis profundo de respuesta en vivo de 80 sistemas.

Día 7: se llevó a cabo la contención sin ningún tipo de instrucción comercial. Los expertos de Mandiant continuaron con la supervisión de la red a fin de garantizar que el perpetrador de la amenaza no volviera a intentar una vulneración.

Día 11: el cliente volvió a su actividad de negocio usual.

Todo el trabajo se llevó a cabo de forma remota.

FireEye Mandiant ha sido el líder en cuanto a ciberseguridad e inteligencia 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 tácticas, técnicas y procedimientos que cambian rápidamente.

Combinamos la experiencia en investigación y remediación que hemos obtenido al brindar respuesta a miles de incidentes, gracias a la información de inteligencia sobre amenazas líder en la industria y a las tecnologías de red y usuario final de vanguardia de FireEye.

El trabajo de Mandiant en los incidentes de mayor envergadura y más publicitados certifica de forma única que nuestros expertos cuentan con experiencia para ayudar a los clientes en todos los aspectos de una respuesta ante incidentes: desde una respuesta técnica hasta la gestión de la crisis.

Ayudamos a que los clientes investiguen e implementen las medidas de corrección de forma más rápida y eficiente, a fin de que retomen aquello que es más importante: sus negocios.

Descripción general

El uso de soluciones en la nube y en el sitio permite que las investigaciones comiencen de inmediato, mientras se gestionan las preocupaciones de privacidad de datos de los clientes. En cuestión de horas, los responsables de la respuesta ante incidentes de Mandiant pueden empezar a analizar el tráfico de la red y la información proveniente de miles de usuarios finales. El acceso sin precedentes a la información de inteligencia sobre amenazas desde las primeras líneas de la investigación de los ataques y otras fuentes de inteligencia brinda a los equipos de respuesta ante incidentes de Mandiant la posibilidad de conocer las tácticas, técnicas y procedimientos (TTP) más recientes de los atacantes.

Los expertos de Mandiant comprenden que una respuesta integral ante incidentes y vulneraciones va mucho más allá de la investigación técnica, la contención y la recuperación. Por lo tanto, brindamos ayuda con respecto a las comunicaciones ejecutivas y a la gestión de crisis, como por ejemplo, las consideraciones legales, normativas y de relaciones públicas. La gestión de crisis es un elemento fundamental en el control de los daños a la reputación y a las responsabilidades legales.

Tabla 1. Tipos de incidentes que solemos gestionar.

Robo de propiedad intelectual	Robo de secretos comerciales u otro tipo de información confidencial.
Delitos financieros	Robo de datos de tarjetas de pago, transferencias de fondos ACH/EFT ilícitas, extorsión y ransomware.
Información Personal de Identificación (PII)	Exposición de la información que se utiliza para identificar de manera única a las personas.
Información de Salud Protegida (PHI)	Exposición de la información de salud protegida.
Amenazas internas	Actividad indebida o ilegal llevada a cabo por empleados, proveedores y otros usuarios internos.
Ataques destructivos	Ataques cuya única intención es provocar dificultades a la organización víctima haciendo que la información o los sistemas no pueden recuperarse.

LA DIFERENCIA DE MANDIANT

- **Experiencia en investigación:** Los investigadores de Mandiant han perfeccionado sus habilidades para llevar a cabo y corregir las investigaciones más grandes y complejas del mundo.
- **Inteligencia sobre amenazas:** Inteligencia líder en la industria reunida a partir de las primeras líneas de las respuestas ante incidentes, descubrimiento amplio de las técnicas profesionales del atacante e investigación mediante fuentes de datos de terceros, FireEye Dynamic Threat Intelligence recopilada por las tecnologías de FireEye y otras fuentes de información de FireEye Threat Intelligence.
- **Tecnología:** Los expertos de Mandiant usan las tecnologías de nube y en el sitio más recientes de FireEye lo que permite que las investigaciones empiecen de inmediato. Nuestras tecnologías permiten una respuesta rápida a una mayor escala, lo que brinda visibilidad al tráfico de la red y los usuarios finales que ejecutan Microsoft Windows, Linux y Mac OS X.
- **Gestión de crisis:** Los responsables de la respuesta ante incidentes tienen años de experiencia en asesoramiento a los clientes con respecto a las comunicaciones relacionadas con los incidentes, como por ejemplo, las comunicaciones ejecutivas, y los requisitos de relaciones públicas y de divulgación.
- **Análisis de malware:** Los expertos en ingeniería inversa de FireEye analizan el malware y escriben decodificadores y analizadores personalizados para brindar una perspectiva de las capacidades y los TTP que utilizan los atacantees.
- **Cobertura de respuesta ante incidentes 24/7:** Análisis de la actividad del atacante 24/7 durante la investigación y la corrección que proporciona FireEye Managed Defense.

Nuestro método

Las investigaciones de Mandiant incluyen análisis del host, de la red y basado en la red para obtener una evaluación integral y global del entorno. Nuestras acciones de respuesta están adaptadas para ayudar a que los clientes respondan a y se recuperen de un incidente, mientras gestionan los requisitos normativos y los daños a la reputación. Durante las investigaciones, los consultores de Mandiant por lo general identifican lo siguiente:

- Aplicaciones, redes, sistemas y cuentas de usuario que se vieron afectados
- Software malicioso y vulnerabilidades aprovechadas
- Acceso a o robo de información

Análisis de incidentes

1. **Implementación de tecnología/ investigación de indicios iniciales:** Implementar la tecnología más adecuada para una respuesta ante incidentes rápida e integral. De manera simultánea investigamos los indicios iniciales proporcionados por el cliente a fin de desarrollar indicadores de riesgo (Indicators of Compromise, IOC) que identificarán las actividades del agresor mientras recorren el entorno para detectar todos los indicadores de actividad maliciosa.
2. **Planificación de gestión de crisis:** Trabajar con los ejecutivos, los equipos legales, los líderes empresariales y el personal de seguridad sénior a fin de desarrollar un plan de gestión de crisis.
3. **Determinar el alcance de los incidentes:** Supervisar en tiempo real la actividad del atacante y buscar evidencia forense de actividades anteriores del atacante a fin de determinar el alcance del incidente.
4. **Análisis profundo:** analiza las acciones que llevó a cabo el atacante para determinar el vector inicial del ataque, establecer la cronología de la actividad e identificar el alcance de la intrusión. Esto puede incluir lo siguiente:
   - Análisis de respuesta en vivo
   - Análisis forense
   - Análisis del tráfico de la red
   - Análisis de registros
   - Análisis de malware
5. **Evaluación de los daños:** Identifica los sistemas, las instalaciones, aplicaciones afectados y la exposición de la información.
6. **Corrección:** desarrollar una estrategia de contención y corrección personalizada en función de las acciones del atacante y adaptarla a las necesidades empresariales a fin de eliminar el acceso del atacante y mejorar el nivel de seguridad del entorno con el objetivo de evitar o limitar los daños de ataques futuros.

Resultados

Informes ejecutivos, de investigación y corrección que soporten el escrutinio de terceros.

- **Resumen ejecutivo:** Resumen de alto nivel que explica la cronología del proceso de investigación, los resultados importantes y las actividades de contención/erradicación.
- **Informe sobre la investigación:** Detalles sobre la cronología del atacante y la ruta crítica (cómo el atacante operó en el entorno). Los informes incluyen una lista de las computadoras, ubicaciones y cuentas de usuario que se vieron afectados y la información que se robó o estuvo en riesgo.
- **Informe de la corrección:** Detalles de las medidas de contención/erradicación que se llevaron a cabo, incluyendo las recomendaciones estratégicas para mejorar el nivel de seguridad de la organización.

¿Sospecha que ocurrió un incidente? Envíenos un correo electrónico en **investigations@mandiant.com** o visite **https://www.fireeye.com/company/incident-response.html**

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.

FIREEYE™