MANDIANT®

RESUMEN DE LA SOLUCIÓN

Mitigación de amenazas estratégicas de ransomware con Mandiant Managed Defense

VENTAJAS

- **Vea las alertas importantes**
  Solicite ayuda a un experto para supervisar las alertas tecnológicas en su entorno e identificar, investigar y priorizar. A cambio, obtiene un conjunto limitado de prioridades, enriquecido con contexto.
- **Exponga a los atacantes ocultos**
  Detecte las vulneraciones ocultas y los ataques cibernéticos potenciales mediante una cacería de amenazas proactiva asignada al marco MITRE ATT&CK.
- **Interrumpa y responda rápidamente**
  Los expertos de Managed Defense respaldan su respuesta a los ataques con el conocimiento colectivo y la experiencia de los analistas de seguridad y los responsables de la respuesta a incidentes de Mandiant.
- **Eleve el nivel de su equipo**
  Nuestro equipo designado de expertos en seguridad capacita, asesora y trabaja con su equipo para impartir su conocimiento diferenciado en ciberseguridad y generar una comprensión más profunda de su entorno.
- **Eleve sus defensas**
  Refuerce su nivel de seguridad con evaluaciones y recomendaciones continuas que se basan en la inteligencia sobre amenazas relevante.

La frecuencia y la gravedad de los ataques de ransomware aumentaron rápidamente desde 2017. Lo que inicialmente se consideró solo una molestia ha sido adoptado por los atacantes sofisticados en complejos ataques de múltiples fases que combinan el cifrado de datos con la amenaza de la exposición de datos. En este mismo margen de tiempo, estos perpetradores pasaron de sembrar ampliamente esta amenaza de malware a atacar organizaciones e industrias específicas, incluidas ciudades enteras. Hoy en día, los costos totales de un ataque de ransomware pueden ascender a millones de dólares.

Esta amenaza evolucionada ha llevado a muchas organizaciones a evaluar, desarrollar y actualizar posibles tácticas antirransomware para acelerar su respuesta. Una capacidad de detección y respuesta gestionada (Managed Detection and Response, MDR) eficazmente, como Mandiant Managed Defense, puede mitigar el riesgo de amenazas como el ransomware que implementan estratégicamente los grupos de APT y asegurar a su cuerpo directivo y a la junta directiva que las capacidades de seguridad están en su lugar. Lograr estas capacidades internamente puede requerir tiempo y recursos.

Managed Defense ayuda a combatir el ransomware

Para las organizaciones que enfrentan amenazas y tácticas avanzadas de ransomware, Managed Defense ofrece el apoyo de expertos que responden y protegen contra adversarios motivados todos los días.

Vea las amenazas importantes en todos los vectores de amenazas

Los atacantes que desean utilizar ransomware pueden ingresar al entorno de la víctima a través de una variedad de vectores de amenazas, incluido el Protocolo de escritorio remoto, correos electrónicos de phishing selectivo con enlaces o archivos adjuntos maliciosos o mediante una descarga involuntaria desde un sitio web malicioso. Después de la vulneración, estos atacantes identifican sistemas y datos clave para maximizar las posibilidades de éxito de su misión.

Para la mayoría de las organizaciones, ganar visibilidad y control sobre toda la empresa, desde la gran cantidad de endpoints hasta el perímetro de red que se extiende rápidamente en la actualidad, es crucial para detectar un ataque sofisticado después de la vulneración. En lugar de detenerse en el endpoint, Managed Defense mantiene la visibilidad integral de la red para identificar el comportamiento anómalo y priorizar las alertas críticas para la investigación. Además, los expertos de Mandiant pueden utilizar la actividad del correo electrónico para identificar nuevas tendencias de atacantes y mecanismos de entrega de ransomware.

Reconocer patrones de amenazas de ransomware

El acceso de una organización a analistas capacitados con conocimiento de las tácticas, técnicas y procedimientos de los atacantes de ransomware es más importante que nunca. Para lograr sus objetivos, los atacantes estratégicos de ransomware primero deben establecer su presencia y luego mantener la conectividad con el entorno de la víctima. Por ejemplo, los expertos de Mandiant descubrieron que los perpetradores de MAZE instalaron cargas útiles en muchos servidores y estaciones de trabajo después de desplazarse lateralmente a través de las redes de las víctimas. Luego, el grupo pudo adquirir y mantener el acceso, realizar la escalación de privilegios y comenzar a desplazarse lateralmente.

En 2019, Mandiant descubrió que para el ransomware implementado estratégicamente por grupos de amenazas de APT entre los clientes de respuesta a incidentes, el tiempo de permanencia promedio, antes de implementar el ransomware, era de 72 días. Si bien los grupos de amenazas de APT también atacaron a los clientes de Managed Defense con ransomware, en casi todos los casos el componente de ransomware se detectó y mitigó antes de su implementación.

Figura 1.

En 2019 Managed Defense redujo considerablemente el tiempo de permanencia del ransomware estratégico para los clientes.

Esto redujo el tiempo de permanencia promedio de los clientes para el ransomware implementado estratégicamente, de 72 días a menos de 24 horas. (Fig. 1).

Para detectar un ataque de ransomware estratégico de este tipo, primero las organizaciones deben identificar a estos atacantes ocultos; muchas organizaciones no emplean cazadores de amenazas capacitados que posean un conocimiento experto del comportamiento actual e histórico de los atacantes. Los equipos de cacería de amenazas de Managed Defense confían en la inteligencia sobre ciberamenazas de primera línea y la experiencia única de respuesta a incidentes cuando buscan amenazas estratégicas de ransomware.

Responder antes del impacto

Debido a que puede infectar y cifrar muy rápidamente, la respuesta rápida y eficaz al ransomware estratégico es primordial. La amplia gama de ataques de ransomware recientes requiere que los equipos de seguridad determinen el alcance total de la actividad del atacante y la aborden en profundidad. Managed Defense ofrece supervisión y priorización de alertas de manera continua, por lo que un experto de Mandiant puede determinar el alcance e investigar rápidamente una alerta priorizada.

Managed Defense aprovecha más de 15 años de experiencia en respuesta a incidentes de alto perfil para brindar evaluaciones rápidas y contener las amenazas. Los consultores de Managed Defense trabajan con los especialistas de respuesta a incidentes de Mandiant para identificar y detener la actividad de los atacantes en su entorno. Estas operaciones de respuesta rápida evitan que los clientes incurran en el costo de una respuesta completa a incidentes el 98 % de las veces. Los hallazgos de Managed Defense se desarrollan en colaboración con la información de su equipo y se entregan a través de informes integrales en el portal de Managed Defense.

Para obtener más información sobre cómo Mandiant Managed Defense puede ayudar a su organización a identificar y responder al ransomware estratégico, visite **www.fireeye.com/managed-defense**

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

Acerca de Mandiant

Solutions Mandiant Solutions reúne la experiencia en inteligencia sobre amenazas y de primera línea más importante del mundo con una validación de la seguridad continua a fin de armar a las organizaciones con las herramientas necesarias para aumentar la eficacia de la seguridad y reducir el riesgo comercial.

MANDIANT®