MANDIANT®

RESUMO DA SOLUÇÃO

Mitigação de Ameaças Ransomware Estratégicas com o Mandiant Managed Defense

VANTAGENS

- **Veja os alertas que importam**
  Recrute um especialista para monitorar alertas de tecnologia em seu ambiente e identificar, investigar e priorizar. Em troca, você obtém um conjunto estreito de prioridades, enriquecido com contexto.
- **Exponha atacantes ocultos**
  Detecte violações ocultas e ataques cibernéticos em potencial com a caça proativa de ameaças mapeada para o framework MITRE ATT&CK.
- **Interrompa e responda rapidamente**
  Os especialistas do Managed Defense apoiam sua resposta a ataques com o conhecimento coletivo e a experiência dos responsáveis pela resposta a incidentes e analistas de segurança da Mandiant.
- **Aumente o nível da sua equipe**
  Nossa equipe de especialistas designados em segurança treina, aconselha e trabalha com sua equipe, para transmitir seus conhecimentos diferenciados em cibersegurança e criar uma compreensão mais profunda de seu ambiente.
- **Aumente suas defesas**
  Reforce sua postura de segurança com avaliações e recomendações contínuas, informadas pela inteligência de ameaças relevantes.

Os ataques de ransomware aumentaram rapidamente sua frequência e gravidade desde 2017. O que inicialmente era considerado um incômodo foi adotado por atacantes sofisticados em ataques complexos e em várias fases, combinando criptografia com ameaça de exposição dos dados. Nesse mesmo período, esses agentes se expandiram da ampla disseminação dessa ameaça de malware para atacar organizações e setores específicos, inclusive cidades inteiras. Atualmente, o custo total de um ataque de ransomware pode chegar a milhões de dólares.

A evolução dessa ameaça levou muitas organizações a avaliar, desenvolver e atualizar possíveis táticas anti-ransomware para acelerar sua resposta. Um recurso de detecção e resposta gerenciada (MDR) eficaz, como o Mandiant Managed Defense, pode reduzir o risco de ameaças como ransomware que são implantados estrategicamente por grupos APT e garantir aos seus executivos e ao conselho de diretores que os recursos de segurança estão disponíveis. Alcançar esses recursos internamente pode levar tempo e exigir recursos.

O Managed Defense Ajuda a Combater o Ransomware

Para organizações que enfrentam táticas e ameaças avançadas de ransomware, o Managed Defense oferece o suporte de especialistas que respondem e protegem contra adversários motivados todos os dias.

Veja as Principais Ameaças em Todos os Vetores de Ameaças

Os atacantes que desejam usar ransomware podem entrar no ambiente de uma vítima por meio de uma variedade de vetores de ameaça, incluindo Remote Desktop Protocol, e-mails de spear phishing com links ou anexos maliciosos ou por meio de um drive-by-download de um site malicioso. Após o comprometimento, esses atacantes identificam os principais sistemas e dados para maximizar a chance de sucesso de sua missão.

Para a maioria das organizações, obter visibilidade e controle sobre toda a empresa, desde a miríade de endpoints até o perímetro de rede atualmente em rápida expansão, é crucial para detectar um ataque sofisticado pós-comprometimento. Em vez de parar no endpoint, o Managed Defense mantém a visibilidade da rede de ponta a ponta, para identificar comportamentos anômalos e priorizar alertas críticos para investigação. Além disso, os especialistas da Mandiant podem usar a atividade de e-mail para identificar novas tendências de atacantes e mecanismos de entrega de ransomware.

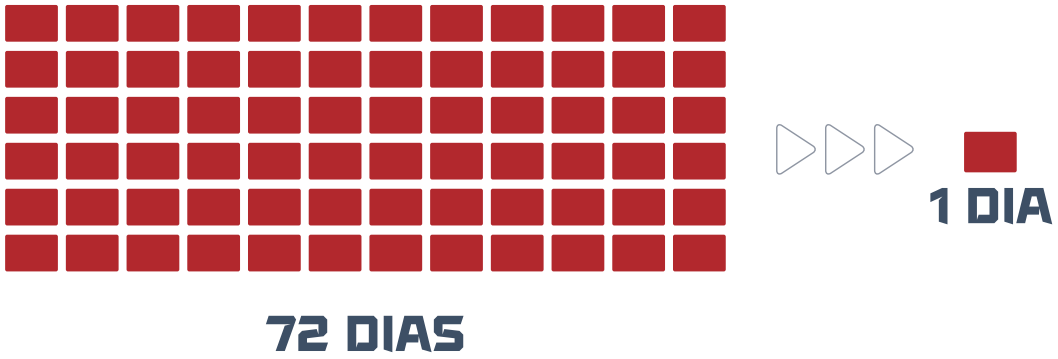
Reconhecer Padrões de Ameaça de Ransomware

O acesso de uma organização a analistas qualificados com conhecimento de táticas, técnicas e procedimentos de atacantes de ransomware é mais importante do que nunca. Para atingir seus objetivos, os atacantes de ransomware estratégico precisam primeiro estabelecer uma posição e, em seguida, manter a conectividade com o ambiente da vítima. Por exemplo, os especialistas da Mandiant descobriram que os agentes da ameaça MAZE instalaram payloads em muitos servidores e estações de trabalho depois de moverem-se lateralmente pelas redes das vítimas. O grupo foi então capaz de adquirir e manter acesso, escalar privilégios e começar a se mover lateralmente.

Em 2019, a Mandiant descobriu que, para o ransomware implantado estrategicamente por grupos de ameaças APT entre clientes de Resposta a Incidentes, o tempo médio de permanência — antes de implantar o ransomware — era de 72 dias. Embora os clientes do Managed Defense também tenham sido alvos de ransomware por grupos de ameaças APT, em quase todos os casos o componente ransomware foi detectado e mitigado antes de ser implantado. Isso reduziu o tempo médio de permanência do ransomware implantado estrategicamente nos clientes de 72 dias para menos de 24 horas. (Fig. 1).

Figura 1.

O Managed Defense reduziu significativamente o tempo de permanência do ransomware estratégico nos clientes em 2019.



Para detectar um ataque de ransomware estratégico, as organizações devem primeiro descobrir esses atacantes ocultos. Muitas organizações não empregam caçadores de ameaças qualificados que possuam conhecimento especializado sobre o comportamento atual e histórico do atacante. As equipes de caça a ameaças do Managed Defense contam com inteligência de linha de frente contra ameaças cibernéticas e experiência única de resposta a incidentes ao procurar ameaças de ransomware estratégicos.

Responder Antes do Impacto

Como ele pode infectar e criptografar com tanta rapidez, a resposta rápida e eficaz ao ransomware estratégico é fundamental. A ampla gama recente de ataques de ransomware exige que as equipes de segurança determinem a extensão total da atividade do atacante e a resolvam completamente. O Managed Defense oferece monitoramento ininterrupto e priorização de alertas, de modo que um alerta priorizado pode ser avaliado rapidamente e investigado por um especialista da Mandiant.

O Managed Defense aproveita os mais de 15 anos de experiência em resposta a incidentes de alto padrão para fornecer avaliações rápidas e conter ameaças. Os consultores do Managed Defense trabalham com os especialistas de resposta a incidentes da Mandiant para descobrir e interromper a atividade do atacante em seu ambiente. Esses compromissos de resposta rápida evitam, em 98% das vezes, que os clientes incorram no custo de uma resposta a incidentes completa. As descobertas do Managed Defense são desenvolvidas em colaboração com os insights de sua equipe e entregues por meio de relatórios abrangentes no seu portal.

Para saber mais sobre como o Mandiant Managed Defense pode ajudar sua organização a descobrir e responder ao ransomware estratégico, visite **www.fireeye.com/managed-defense**

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

Sobre as soluções Mandiant

As soluções Mandiant reúnem a inteligência de ameaças líder no mundo e conhecimento de linha de frente especializado com validação de segurança contínua para capacitar as empresas com ferramentas que aumentam a eficácia da segurança e reduzem riscos de negócios.

MANDIANT®