MANDIANT®

SOLUTION BRIEF

Mitigation of Strategic Ransomware Threats with Mandiant Managed Defense

BENEFITS

- **See the alerts that matter**
  Enlist an expert to monitor technology alerts across your environment and identify, investigate and prioritize. In return you get a narrow set of priorities, enriched with context.
- **Expose hidden attackers**
  Detect hidden breaches and potential cyber attacks with proactive threat hunting mapped to the MITRE ATT&CK framework.
- **Quickly disrupt and respond**
  Managed Defense experts support your response to attacks with the collective knowledge and experience of Mandiant incident responders and security analysts.
- **Level up your team**
  Our designated team of security experts train, advise and work with your team to impart their differentiated cyber security knowledge and build a deeper understanding or your environment.
- **Elevate your defenses**
  Bolster your security posture with ongoing assessments and recommendations that are informed by relevant threat intelligence.

Ransomware attacks have rapidly increased in frequency and severity since 2017. What was initially considered a nuisance has been adopted by sophisticated attackers in complex, multi-phased attacks that combine data encryption with the threat of data exposure. In this same timeframe, these actors expanded from widely seeding this malware threat to targeting specific organizations and industries—including whole cities. Today, the total costs of a ransomware attack can climb into the millions of dollars.

This evolved threat has driven many organizations to assess, develop and update potential anti-ransomware tactics to accelerate their response. An effective managed detection and response (MDR) capability, such as Mandiant Managed Defense, can mitigate the risk of threats like ransomware that are strategically deployed by APT groups, and assure your C-suite and board of directors that security capabilities are in place. Achieving these capabilities in house can take time and resources.

Managed Defense Helps Combat Ransomware

For organizations facing advanced ransomware tactics and threats, Managed Defense offers support from experts who respond to and protect against motivated adversaries every day.

See Threats That Matter Across All Threat Vectors

Attackers that want to use ransomware can enter a victim's environment through a variety of threat vectors, including Remote Desktop Protocol, spear-phishing emails with malicious links or attachments or through a drive-by-download from a malicious website. Post-compromise, these attackers identify key systems and data to maximize their mission's chance for success.

For most organizations, gaining visibility and control over the entire enterprise, from the myriad of endpoints to today's rapidly extending network perimeter, is crucial in detecting a sophisticated attack post-compromise. Rather than stop at the endpoint, Managed Defense maintains end-to-end network visibility to identify anomalous behavior and prioritize critical alerts for investigation. In addition, Mandiant experts can use email activity to identify new attacker trends and ransomware delivery mechanisms.

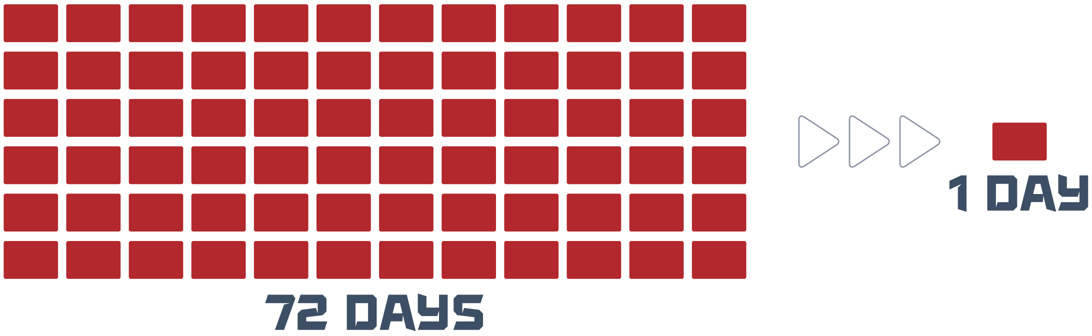
Recognize Ransomware Threat Patterns

An organization's access to skilled analysts with knowledge of ransomware attacker tactics, techniques and procedures is more important than ever. To achieve their objectives, strategic ransomware attackers need to establish a foothold first, and then maintain connectivity to the victim's environment. For example, Mandiant experts found that MAZE threat actors installed payloads on many servers and workstations after moving laterally through victims' networks. The group was then able to acquire and maintain access, escalate privileges and begin to move laterally.

In 2019 Mandiant found that for ransomware strategically deployed by APT threat groups among Incident Response customers, the average dwell time—before deploying the ransomware—was 72 days. While Managed Defense customers were also targeted with ransomware by APT threat groups, in nearly all cases the ransomware component was detected and mitigated before being deployed. This reduced customers' average dwell time for strategically deployed ransomware from 72 days to less than 24 hours. (Fig. 1).

Figure 1.

Managed Defense significantly reduced the dwell time of strategic ransomware for customers in 2019.



To detect such a strategic ransomware attack, organizations must first uncover these hidden attackers; many organizations do not employ skilled threat hunters who possess expert knowledge of current and historical attacker behavior. Managed Defense threat hunting teams rely on frontline cyber threat intelligence and unique incident response experience when hunting for strategic ransomware threats.

Respond Before Impact

Because it can infect and encrypt so quickly, quick and effective response to strategic ransomware is paramount. The wide range of recent ransomware attacks requires security teams to determine the full extent of attacker activity and thoroughly address it. Managed Defense offers around-the-clock monitoring and alert prioritization, so a prioritized alert can be swiftly scoped and investigated by a Mandiant expert.

Managed Defense leverages more than 15 years of high-profile incident response experience to provide rapid assessments and contain threats. Managed Defense consultants work with Mandiant Incident Response specialists to uncover and stop attacker activity in your environment. These rapid response engagements prevent customers from incurring the cost of a full incident response 98% of the time. Managed Defense findings are developed collaboratively with insights from your team and delivered via comprehensive reports in the Managed Defense portal.

To learn more about how Mandiant Managed Defense can help your organization uncover and respond to strategic ransomware, visit **www.fireeye.com/managed-defense**

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

About Mandiant Solutions

Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce business risk.

MANDIANT®