Mandiant

Solution Brief

Combating Ransomware

Multifaceted extortion blends the impact of a data breach with the already painful impact of ransomware. A data breach can result in greater reputational damage, regulatory fines, class action lawsuits, and derailed digital transformation initiatives. These consequences were not typically seen with ransomware before 2019.[1]

Defend against the attackers' top choice for multifaceted extortion

Ransomware and multifaceted extortion have become top cybersecurity threats for organizations of all shapes and sizes. Ransomware actors have intensified their attack campaigns by threatening critical infrastructure shutdowns, risking public health and safety, diverting vital public resources, disrupting educational institutions and impacting data privacy. Dwell time was less than a week in 56.5% of the ransomware-related intrusions that Mandiant investigated in 2024, as attackers are incentivized to complete their objectives without being detected.[2]

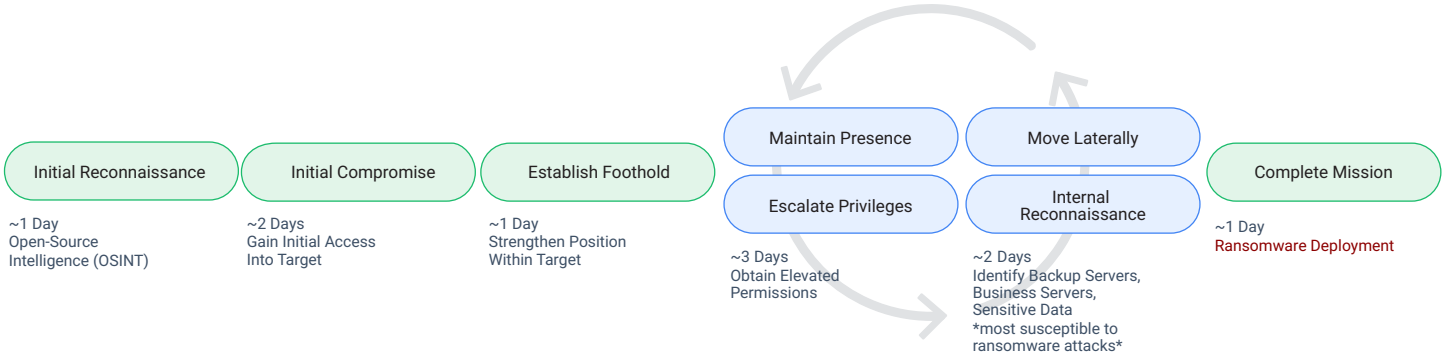
Ransomware actors are becoming increasingly aggressive, turning once relatively simple attacks into more elaborate—and lucrative—multifaceted extortion operations. Multifaceted extortion involves multiple attack points, including ransomware encryption, data theft and public "naming and shaming" of the victim organizations, all of which presents a more profound risk to organizations.

Security conscious organizations know that the best ransomware defense is ransomware preparedness. Assessing and mitigating your organization's ransomware risks and understanding your team's ransomware response capabilities can help you prevail against ransomware attacks.

The highest reported ransomware payment is $75 million USD,[3] with the initial demand being an even higher $150 million USD.

1 Mandiant (2021), M-Trends 2021.
2 Mandiant (2025), M-Trends 2025.
3 Bloomberg (Sep 18, 2024) Gang Got $75 Million for Cencora Hack in Largest Known Ransom

Anatomy of a targeted ransomware attack

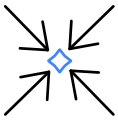


The objectives of ransomware defenses

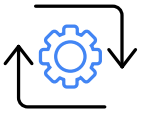
When ransomware is successfully deployed, organizations often experience technical and non-technical challenges that can cripple their operations. To counter the frequently seen combination of poor visibility into the effectiveness of controls and detection environments and the advanced techniques, skills, and resources of threat actors, organizations must have a holistic risk mitigation strategy, from the Board level to security practitioners.

Ideally, every organization should strive to catch a ransomware attack at its earliest stages and understand their ability to prevent ransomware deployment.

Stop an attack before ransomware deployment



Accelerate response of the attack



Resume operations of the organization

How Mandiant helps address this challenge

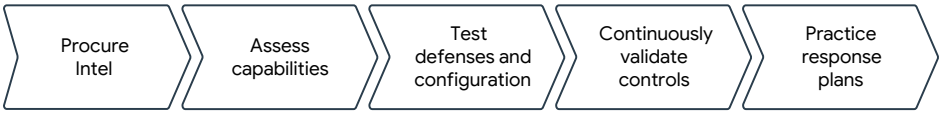
Many organizations victimized by ransomware have turned to Mandiant to help them respond. With extensive experience on the frontlines, Mandiant has developed expertise and intelligence to understand who the attackers are, how they operate, and ultimately, how to counter them.

Mandiant has the unique ability to find the intrusions that precede ransomware deployment quickly and at scale. Through automated solutions and comprehensive services from Mandiant, your organization can prepare, prevent, and respond to ransomware and multifaceted extortion attacks effectively.

Prepare

Ready your cyber defenses against ransomware and multifaceted extortion campaigns through threat intelligence, security program assessment, controls validation, and hands-on operational exercises—with on-demand access to Mandiant frontline experts.

Gain visibility, evidence, and confidence in your cyber readiness against ransomware through testing programs that provide real data on your ability to effectively prevent ransomware. Mandiant frontline visibility, ransomware intelligence, and innovative expertise can better prepare your team to prevent or lessen the impact of ransomware.



Prevent

Identify the activity that precedes ransomware deployment and activate mitigation strategies to avoid a major ransomware and multifaceted extortion incident.

With Mandiant, response readiness services and on-demand access to cyber defense experts, security teams can identify active and past compromise quickly and stop attackers before they cause damage to their organization. Security teams get an early knowledge advantage through automated modules that identify critical indicators of compromise (IOCs). Managed detection and response services provide specialized expertise, such as integration of attacker research to detect malicious activity faster and the effective prioritization of mitigation efforts.

Respond

Reduce the impact of ransomware and multifaceted extortion attacks with swift and decisive action.

Mandiant provides access to incident response experts so you can rapidly and effectively respond to ransomware and multifaceted extortion attacks. These specialists complete in-depth attack analysis, perform crisis management across the full attack lifecycle, and help recover your business operations after a breach.

Benefits

- Access to the most up-to-date frontline threat intelligence enables understanding of the identity, targets, timing, motivation, and methods of the latest threat actors.
- Prioritize and focus efforts with intelligence on the specific threats facing your industry and organization, test security controls, and remediate vulnerabilities.
- Minimize the impact of an attack and reduce security incident response time.
- Safely test your organization against real-world ransomware attack scenarios to identify existing misconfigurations in your environment and help improve or develop a more robust security posture.

Offerings

Table 1. Offerings.	
Prepare	
Solution	**Description**
Threat Intelligence	Provide your organization with visibility into the latest ransomware threats directly from the frontlines.
Ransomware Defense Assessment	Evaluate your organization's ability to detect, contain, and remediate ransomware within your specific environment—before it cripples your operations.
Active Directory Security Assessment	Assess existing misconfigurations, process weaknesses, and exploitation methods within your Active Directory—the most abused network service by attackers to escalate privileges in a successful ransomware and multifaceted extortion attack.
Red Team for Ransomware	Evaluate your ability to protect your most critical assets through real-world ransomware attack scenarios. Mandiant experts emulate tactics, techniques, and procedures (TTPs) seen in an actual ransomware incident to identify weaknesses and recommend effective improvements.
Ransomware Defense Validation	Continuously test endpoint security controls against the latest ransomware families within your production environment.
Tabletop Exercise – Technical and Executive	Evaluate your ransomware incident response plan through scenario gameplay. Identify gaps between your documented and expected response versus what actually happens during a real-world attack.
Cloud Security Assessment	Protect your cloud environments against targeted threats with technical configuration assessments and scenario-based exercises.
Prevent	
Mandiant Threat Defense	Combat ransomware threats with Mandiant Threat Defense. Get comprehensive active threat detection, hunting, and rapid response from Mandiant experts, delivered natively in Google SecOps, to protect against extortion, downtime, and theft.
Mandiant Retainer	Request investigations into ransomware threats with the click of a button–when you need it. Our experts will respond with commentary and analysis based on the collective threat intelligence, and expertise of Mandiant.
Respond	
Incident Response Service	Activate frontline response experts to complete in-depth attack analysis, perform crisis management over the complete attack lifecycle, and help recover business operations after a breach.
Incident Response Retainer	Retain Mandiant incident response experts on standby with a competitive 2-hour response time that enables faster and more effective attention to and remediation of cyber incidents.

Conclusion

With Mandiant you can address the challenges of ransomware and significantly minimize the overall impact of this attack type. After identifying the critical assets that attacks can reach in your environment, you can uncover technical and operational weaknesses and in turn make both strategic and tactical improvements to your overall security program.