MANDIANT

SOLUTION BRIEF

COMBATING RANSOMWARE

Defend against the attackers' top choice for multifaceted extortion

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]

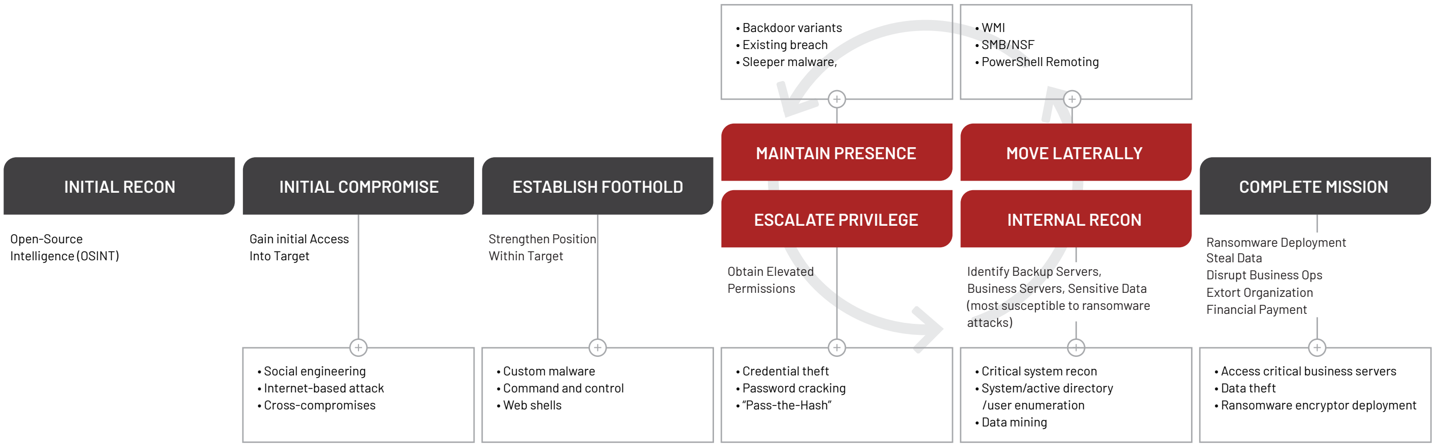
Ransomware and multifaceted extortion have become top cyber security threats for organizations of all shapes and sizes. Ransomware actors have intensified their attack campaigns by threatening critical infrastructure shutdowns, risking public health and safety, diverting vital public resources, disrupting educational institutions and impacting data privacy. The average downtime experienced from a ransomware attack is 21 days.[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.

In March 2021, one of the largest US insurance companies publicly reported a ransom payment of $40 million,[3] the largest known ransomware payment to-date.

[1] FireEye (2021). M-Trends 2021.
[2] Coveware (February 1, 2021). Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands.
[3] Business Insider (May 22, 2021). One of the biggest US insurance companies reportedly paid hackers $40 million ransom after a cyberattack.

Anatomy of a targeted ransomware attack



INITIAL RECON
Open-Source Intelligence (OSINT)

INITIAL COMPROMISE
Gain initial Access Into Target
- Social engineering
- Internet-based attack
- Cross-compromises

ESTABLISH FOOTHOLD
Strengthen Position Within Target
- Custom malware
- Command and control
- Web shells

MAINTAIN PRESENCE
- Backdoor variants
- Existing breach
- Sleeper malware,

MOVE LATERALLY
- WMI
- SMB/NSF
- PowerShell Remoting

ESCALATE PRIVILEGE
Obtain Elevated Permissions
- Credential theft
- Password cracking
- "Pass-the-Hash"

INTERNAL RECON
Identify Backup Servers, Business Servers, Sensitive Data (most susceptible to ransomware attacks)
- Critical system recon
- System/active directory /user enumeration
- Data mining

COMPLETE MISSION
Ransomware Deployment
Steal Data
Disrupt Business Ops
Extort Organization
Financial Payment
- Access critical business servers
- Data theft
- Ransomware encryptor deployment

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.

Stop an attack before ransomware is deployed

Accelerate response and **minimize impact** of an attack

Allow the organization to **resume operations**

Ideally, every organization should strive to catch a ransomware attack at its earliest stages to prevent deployment. Early detection of the intrusion allows an organization to accelerate their response, minimize the impact of ransomware and swiftly resume business operations.

How Mandiant helps address this challenge

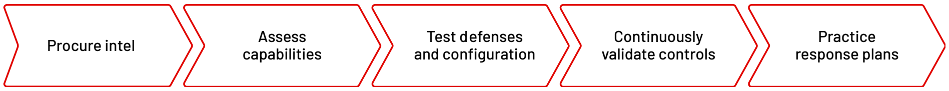
Many organizations victimized by ransomware have turned to Mandiant to help them respond to their incident. With experience on the frontlines of hundreds of such incidents, Mandiant has developed expertise and intelligence to understand who the attackers are, how they operate and ultimately, how to counter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

Mandiant has the unique ability to find the intrusions that precede ransomware deployment quickly and at scale. Through automated solutions and comprehensive services, your organization can prepare, prevent and respond to ransomware and multifaceted extortion attacks. Mandiant solutions bolster both your preparedness and cyber defense to help protect against multifaceted extortion attacks.

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.

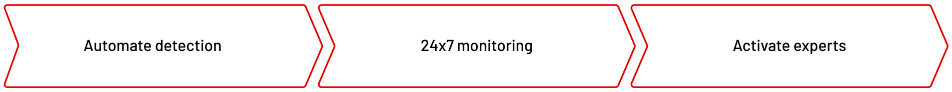
Mandiant can help you prepare your specific environment with the Mandiant Advantage platform and services. The platform offers access to timely, relevant and easy to consume threat insights that accelerate security decision making to mitigate risk. You'll gain visibility, evidence and confidence in your cyber readiness against ransomware through automated testing programs that give you real data on how your security controls are performing. Our frontline experts can better prepare you and your team to mitigate threats, reduce business risk and lessen the impact of ransomware.


Procure intel
Assess capabilities
Test defenses and configuration
Continuously validate controls
Practice response plans

Prevent

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

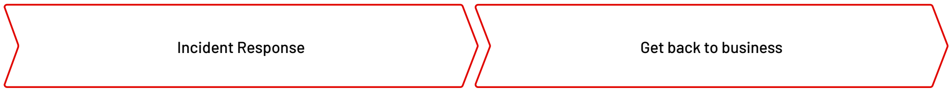
With Mandiant Advantage, response readiness services and on-demand access to Mandiant cyber defense experts, security teams can identify active and past compromises quickly and stop attackers before they cause damage to their organization. Security teams get an early knowledge advantage through automated 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.


Automate detection
24x7 monitoring
Activate experts

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 you recover your business operations after a breach.


Incident Response
Get back to business

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 threat 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	Delivery
Mandiant Advantage Threat Intelligence	Provide your organizations with visibility into the latest ransomware threats directly from the frontlines.	Mandiant Advantage
Ransomware Defense Assessment	Evaluate your ability to prevent, detect, contain and remediate ransomware by assessing the impact an attack could have on your internal network.	Mandiant Consulting Services
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.	Mandiant Consulting Services
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.	Mandiant Consulting Services
Mandiant Advantage Ransomware Defense Validation	Discover how effective you will be against the top ransomware families from the field. Continuously evaluate your ability to detect and contain an attack. Identify changes required to help ensure your defenses can block or contain modern ransomware.	Mandiant Advantage
Tabletop Exercise – Technical and Executive	Evaluate your ransomware incident response plan through scenario gameplay. Mandiant identifies gaps between your documented and expected response versus what actually happens during a real-world attack.	Mandiant Consulting Services
Prevent		
Mandiant Advantage Automated Defense	Access automated Mandiant expertise to rapidly identify indicators of compromise (IOCs) from active and targeted ransomware in your environment. Reduce threat actor dwell time and lessen the impact of an attack with real-time awareness at machine speed, scale and consistency.	Mandiant Advantage
Mandiant Advantage Managed Defense	Enlist Managed Defense experts for 24/7 support to minimize your risk from strategic ransomware threats to protect your organization from extortion, ransom, downtime and theft.	Mandiant Managed Services
Expertise On Demand	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.	Mandiant Consulting Services
Respond		
Incident Response Service	Activate the best-in-business response experts to complete in-depth attack analysis, perform crisis management over the complete attack lifecycle and help recover business operations after a breach.	Mandiant Consulting Services
Incident Response Retainer	Retain Mandiant incident response experts on standby with a competitive 2-hour service level agreement (SLA) option that enables faster and more effective response to cyber incidents.	Mandiant Consulting Services

Conclusion

With Mandiant you can address the challenge of ransomware and mitigate or 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.

Learn more at **https://www.mandiant.com/ransomware-solutions**

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant® has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.