FIREEYE | MANDIANT

CASE STUDY

Modern Ransomware and Incident Response Solutions

End-to-end response to a government agency's ransomware attack

GLOBAL CYBER SECURITY SOLUTIONS

Mandiant partners with international, federal, state, and local governments to deliver holistic cyber security capabilities through a solution-based model in five areas:

- Single point of customer success and accountability
- Cyber security thought leadership and trusted advisor
- Operational security program transformation
- Custom end-to-end services and mission support
- Simplify capacity building on a global scale

The approaches and practices used for government sectors are regularly applied to clients in every other industry.

A Modern Threat

Ransomware is one of the most prevalent cyber threats, affecting multinational companies, as well as state and local governments—at all levels.

Specifically, state and local government organizations find themselves in the crosshairs of ransomware criminals with increasing frequency. Experts agree that prevention is the best mode of defense and many organizations make every attempt to prevent a ransomware event, but budget, misaligned decision-making and other factors may inhibit deployment.

The goal of cyber adversaries using ransomware as an attack vector is simple: gain control, incite panic and receive payment. To effectively defend against ransomware, it's critical to consider attacker motivations and connections between attack vectors.

The ability of a security team to properly assess this threat vector, stop its proliferation, remove its foreign artifacts and maintain business continuity is paramount to mitigating ransomware.

Government agencies and their associated groups have recently been targeted by adversaries seeking significant monetary compensation to release critical resources such as 911 emergency response recordings, criminal court documents and healthcare administration files. An end-to-end cyber security approach is needed to combat these harmful threats.

The Catalyst

Mandiant Consulting received a call from the Chief Information Security Officer (CISO) of a highly populated North American city to assist with the immediate investigation and remediation of a ransomware attack.

The adversary had gained access to a weak network password and used it to lock down the city's internal network, creating deep concerns surrounding a potential shutdown of the city's entire infrastructure—including their 911 dispatch center and property tax administration agency.

With approval from the city's mayor, the CISO worked closely with Mandiant experts to execute a comprehensive security plan to eradicate the ransomware threat within their environment, apply proper remediation efforts and ultimately improve the city's end-to-end security posture.

Mandiant consultants rapidly ramped up their ransomware attack investigation, working hand-in-hand with city personnel on initial incident triage.

Search and Rescue
Given the existence of the FireEye technology stack in the client's environment, Mandiant consultants were able to initiate two preliminary actions to assess the ransomware event before an expert arrived on-site. First, the FireEye Endpoint Security agent and FireEye Network Security and Forensics software was deployed onto the infected systems, to immediately begin monitoring the ransomware threat remotely.

Next, Mandiant consultants correlated their findings using proprietary adversary-based intelligence derived from frontline Mandiant incident responders, to aggregate and cross-reference malicious cyber data in the client's environment.

Rapid Incident Response
Within one day, two Mandiant experts—an incident responder and a reverse engineer—arrived onsite to help the city's local team triage the ransomware event and prevent the spread of malware. The reverse engineer examined the specific malware mechanism and unencrypted captured artifacts directly related to the attack. The response expert discovered back doors and additional snares established by the attacker within the city's network.

In parallel, a Mandiant malware threat hunter, uniquely equipped with Mandiant Threat Intelligence, collected and analyzed pertinent data and artifacts directly related to the ransomware attack (such as encrypted files and corrupted metadata) that were found on the deployed Endpoint Security appliance and Network Security software. Mandiant experts were then able to make new connections between the attacker and the agency's specific environment.

Over the two week engagement, Mandiant experts identified and neutralized the ransomware threat to the city's environment.

Advanced Cyber Defense
For advanced, long-term security, the Mandiant team recommended its Managed Defense offering for additional protection as part of a ransomware response methodology. This managed detection and response (MDR) service provided the city with a remote 24x7 security operations center (SOC) capability for attacker monitoring and threat hunting at the highest level of cyber defense.

Within 30 days of employing Mandiant Managed Defense, Mandiant consultants blocked a new ransomware variant with a FireEye Email Security agent after the targeted threat bypassed the city's existing non-FireEye email security tool. The city continues to use Mandiant Managed Defense as its primary detection and response service for optimal cyber defense coverage today.

Security Remediation
Following the initial triage, Mandiant Incident Response experts helped to rebuild the city's infrastructure, detail the various security gaps, mature the city's security posture and create an effective incident response plan. In addition to providing a report on security program weaknesses, Mandiant remediation consultants stayed in contact with the city's IT department to shepherd them through the process of rebuilding their networks. The consultants provided step-by-step support to ensure the city would get back to business as usual, as quickly as possible.

After remediation, Mandiant consultants followed up with a Ransomware Defense Assessment to evaluate the city's ability to prevent, detect, contain and remediate the next ransomware attack. As part of the assessment, they conducted multiple ransomware-focused workshops with the city's personnel and simulated the behavior of ransomware and ransomware operators to uncover ransomware-specific security issues that affected their environment. The strategic and tactical recommendations from the Ransomware Defense Assessment will help to significantly reduce the impact and scope that a ransomware attack would have on the city in the future.

Next, Mandiant experts performed a Tabletop Exercise in collaboration with the city's security leadership team to sync their security efforts with effective best practices. Through dedicated onsite workshops, Mandiant experts tested the team's newly developed incident response plan through roundtable scenario gameplay that incorporated common adversary behaviors and techniques seen by Mandiant responders in real-world attacks on the frontlines.

Mandiant consultants also identified areas for increased response efficiencies and created best practice domain playbooks to address specific factors that made their organization susceptible to similar ransomware attacks. Mandiant concluded the engagement with a comprehensive report to address critical gaps in the city's security program and prepare for future ransomware events.

Overall, the results conveyed the critical need for further mitigation recommendations to the city's infrastructure, including:

- Network segmentation for better control of traffic flow across the network
- Tighter access controls that use least privilege and need-to-know best practices to limit control of vital parts within the network
- Regular evaluation and testing to ensure that network backups are working properly
- Implementation of multi-factor authentication to require more than one simple password to access vital systems

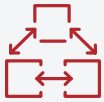
Conclusion

Holistic and strategic cyber security approaches should go beyond fixing the problem. Mandiant experts provide next steps that client organizations should take after the immediate threat is solved. In this case, the city was equipped with the power and support of Mandiant incident response, malware analysis, threat intelligence, and managed detection services to effectively defend against future ransomware attacks.

The fastest and most effective defense against targeted ransomware attacks is to employ a single integrated team of industry recognized experts to protect an organization's critical assets and program processes. Mandiant expertise serves as that single point of customer success and accountability.

The full suite of Mandiant Solutions, including frontline incident response and expertise, Managed Defense and Threat Intelligence alongside FireEye technologies, offers the most comprehensive approach to ransomware attacks and overall cyber security in the industry.

MITIGATION RECOMMENDATIONS



SEGMENT NETWORKS

IMPLEMENT TIGHT ACCESS CONTROLS

REGULARLY EVALUATE AND TEST BACK-UP STRATEGIES

REQUIRE MULTI-FACTOR AUTHENTICATION

To learn more, visit **www.FireEye.com**

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

About FireEye

At FireEye, our mission is to relentlessly protect organizations with innovative technology, intelligence and expertise gained on the frontlines of cyber attacks. Learn how at **www.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.