EVIDEN

Case study

Digital Forensics and Incident Response

Public sector company

Enterprise falls to Ryuk ransomware

Ransomware is dangerous, complex, and constantly evolving. But it can be stopped.

In this incident, the organization was compromised by a ransomware attack because they had a low-security profile, no MFA, improper segmentation, no security monitoring, and no in-house security talent or a managed security vendor to fill the gaps in their defense.

Thankfully, we could still respond successfully to this incident and stop the attack before they suffered significant harm.

To show you how we stopped this attack and how you could too, we will outline:

- A detailed timeline of the incident and our response
- How to successfully prevent, detect, and respond against attacks like this
- How you can develop the ability to stop attacks like this

What happened: Timeline of the attack and our response

Here's what happened during the attack and how we evicted the attacker.

25th June:

A domain admin of the client receives an email with a wire transfer in .xslx. The file contains a trick bot trojan dropper. The admin tries to remove the malware on his own, unsuccessfully. On day four, the attacker deploys and finds keys to the kingdom on the admin's computer. The attacker uses a self-propagating trick bot through SMB to move laterally.

10th July:

The attacker accesses Domain Controller (DC). They launch Group Policy Management, create new group policies, schedule tasks with logon scripts, and spread the encryptor with psexec via DC. They encrypt the servers over the weekend. Our client learned of the infection late weekend and contacted us on Monday morning.

12th July:

A few of the client's critical servers are encrypted. We collect data and conduct an initial investigation. We learn that the entire domain is compromised by Ryuk ransomware. We split our workstreams into recovery and investigation, and secured evidence from our client's critical servers before taking further action.

15th July:

We see the attacker uploaded offensive tools to the compromised admin account to access the central network. The attackers lacked accounts to access AD and exploited a ZeroLogon vulnerability instead. They compromised most of our client's domains, added Cobalt Strike, and waited to trigger the attack.

14th July:

We discovered malicious implants on most servers where Cobalt Strike was installed. We see the backup servers and infrastructure were also infected with ransomware payloads that weren't yet triggered. We identified that the ransomware group was Avvadon and that they had not yet exfiltrated any data.

13th July:

We see the attacker uploaded offensive tools to the compromised admin account to access the central network. The attackers lacked accounts to access AD and exploited a ZeroLogon vulnerability instead. They compromised most of our client's domains, added Cobalt Strike, and waited to trigger the attack.

16th July:

We confirm the attacker does not have persistence access. Our recovery team expands our client's trust bubble and rebuilds their servers. We close all possible backdoors.

19th July:

We helped the client restore their systems and recover or restore most of their data. Some data was lost due to incomplete backups.

20th July:

We provide a detailed incident report and customized recommendations. Eviden helps the client create a robust threat detection and response system.

Lessons learned: How to stop this attack

To keep your organization safe against attacks like this, you must take a few fundamental actions:

Prevention

- Establish Multi-Factor Authentication and Zero Trust segmentation
- Perform fundamental security hygiene and vulnerability management
- Close unnecessary connections from high-risk attack pathways, such as SMB
- Establish and maintain comprehensive security monitoring tools
- Maintain complete and timely backups of all critical data
- Develop in-house security talent or contract. 24x7 MSSP or MDR provider

Detection

- Don't ignore commodity malware and threats
- Use MDR and EDR for TTP monitoring
- Focus on Active Directory to prevent lateral movement
- Combine threat intelligence, threat hunting, auto-containment, and SOC
- Establish visibility into your supply chain and manage it
- Ensure proper logging to perform an effective investigation
- Be aware of your threat landscape

Response

- Maintain an incident response
- playbook and perform tabletop exercises
- Create a crisis team and streamline communication channels with stakeholders
- Use trusted bubbles and build a recovery on top of the investigation
- Accelerate breach containment and management with a mature CMDB and asset management process
- Prepare and test your backup and recovery plan before a breach
- Implement post-incident recommendations from your IR team

An ounce of prevention: Prepare to stop this attack ransomware

These security lessons are simple, but they can be challenging to bring to life. This is why Eviden has put together a comprehensive framework for Ransomware defense aligned to the NIST framework.

To learn more about Eviden security solutions, schedule a noobligation consultation with an Eviden Digital Security expert and begin to build or augment your ransomware defense.

Connect with us

eviden.com