EVIDEN

Case study

Digital Forensics and Incident Response

Perimeter security services company

Evicting ransomware actors before encryption

Ransomware is today's biggest threat, and it is only getting worse.

With the right security capabilities, any organization can prevent, detect, and respond to any ransomware attack that comes their way — without suffering significant harm. We wrote this case study to illustrate this point.

In this incident, our client was compromised by a ransomware attack because they had unpatched firewalls, no MFA, ineffective segmentation, and no efficient vulnerability management. This allowed the attacker to progress until it was almost too late... yet we could still resolve the incident before harm was done.

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 ransomware attacks

What happened: Timeline of the attack and our response

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

9th Feb, 11:00 am:

Our client finds suspicious activity in one of their domain controller servers. They had 20 physical sites with servers with one malfunctioning Active Directory (AD) instance. They find Mimikatz-like strings but do not progress in their investigation after one week.

16th Feb 10:00 am:

Our client calls our incident response hotline. Our Incident Response team collects data and organizes logistics. Our client has a large and diverse WAN, and it takes us half a day to get started. We see the attacker has control of the AD so we create an external channel.

17th - 18th Feb:

We launch security monitoring & begin our investigation. We find malicious traffic from a network and a compromised firewall. We learned the attack started five months ago. The attackers gained initial access by stealing an account from the firewall's memory and then used the public directory and account names to access an admin account.

22nd Feb:

During the investigation, we completed patching — and moved critical assets to a trusted bubble. We also ensured the attacker did not know we were performing investigation and remediation to prevent the attacker from triggering the payload.

21st Feb:

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.

19th - 20th Feb:

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.

23d Feb:

It was time to evict the attacker. We presented a plan to the board, completed the bubble of trust, and placed antiransomware features through new security tools. We ensured the network would isolate affected machines if the attacker began to encrypt them.

24th Feb:

We evicted the attacker and removed their back doors. A post-incident analysis was performed, and recommendations were shared with the client. The measures Eviden implemented were upgraded and became the official security program of the client.

6th March:

Our client has not experienced another incident, ransomware or otherwise, since.

Lessons learned: How to stop this attack

This incident could have been much worse. The attacker had lurked undetected in our client's network for five months, and they had already compromised Active Directory (and other assets) and established multiple active outbound connections.

However, this attack could have been easily prevented and was relatively simple to stop once detected. To keep your organization safe against attacks like this, you must take just a few fundamental actions.

Prevention

- Use MFA for external accesses
- Disable or delete accounts of former employees
- Manage unused service accounts
- Avoid discoverable, hardcoded passwords in scripts and applications
- Eliminate discoverable, hard-coded passwords in scripts and applications
- Isolate legacy systems that can't be adequately patched
- Implement tamper-resistant backups
- Deploy agents with application controls (black-list/whitelist servers and workstations)

Detection

- Establish broad detection across vectors to detect multi-channel attacks
- Perform analytics-based threat detection that goes beyond known signatures
- Monitor user behavior, even from legitimate tools, credentials, and websites
- Periodically check security monitoring to ensure it hasn't been disabled
- Maintain up-to-date threat intelligence for all ransomware variants
- Regularly verify your SIEM/MDR receives signals from your environment

Response

- Automate access reconciliation and policy validation
- User insider threat detection
- Ensure monitoring systems can ingest data from IAM systems
- Implement network-based detection tools for your perimeter
- Use MDR/XDR and correlate threat intel and signals from your environment

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