Breach response case study

Perimeter security services company

Evicting ransomware actors before encryption

Atos

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.

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.

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.

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.

23rd Feb:

It was time to evict the attacker. We presented a plan to the board, completed the bubble of trust, and placed anti-ransomware 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 Atos implemented were upgraded and became the official security program of the client.

6th Sep:

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

- Perform regular vulnerability scans, patching, and management of open exploits
- Establish Multi-Factor Authentication and Zero Trust segmentation
- Close all non-essential Active Directory connections to minimize the attack surface
- Maintain real-time visibility and data collection to accelerate investigation
- Minimize and monitor outbound connections to separate attackers from tools
- Maintain up-to-date backups and infrastructure separate from main network

Detection

- Perform security detection before Active Directory crashes
- Place analysts behind your AV/EDR/XDR tools
- Know your attackers and detect C2 activities, especially Cobalt Strike
- Monitor VPN connections and apply detection rules to them
- Perform network security monitoring and centralize your logs

Response

- Understand that response is slowed by heterogeneous infrastructure
- Prioritize which assets you must rebuild first during an incident
- Create a "bubble of trust" instead of rebuilding on compromise infrastructure
- Prepare task forces to support intervention based on your staff's strengths

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 Atos has put together a comprehensive framework for Ransomware defense aligned to the NIST framework. You can download this complimentary e-book here.

To learn more about Atos security solutions. Schedule a no-obligation consultation with an Atos Digital Security expert and begin to build or augment your ransomware defense.

About Atos

Atos is a global leader in digital transformation with 107,000 employees and annual revenue of over € 11 billion. European number one in cybersecurity, cloud and high performance computing, the Group provides tailored end-to-end solutions for all industries in 71 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea), listed on Euronext Paris and included in the CAC 40 ESG and Next 20 Paris Stock Indexes.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
atos.net
atos.net/career

Let's start a discussion together

For more information: breachresponse@atos.net