EVIDEN

Case study

Digital Forensics and Incident Response

Insurance company

Large backups destroyed, 15,000+ devices encrypted

As Gartner notes, ransomware activities “are at an all-time high during the global health emergency. Cybercriminals are becoming more sophisticated, organizing as groups and sharing techniques, data and results of prior exploitations.”

With the right security capabilities, any organization can prevent, detect, and respond to any ransomware attack that comes their way — without suffering significant harm.

In the incident illustrated in this case study, this organization was compromised by a ransomware attack because they lacked security controls like Secure Email Gateway (SEG), Secure Web Gateway (SWG), segmentation, analytics-based threat detection, and immutable backups. This lack of basic security controls created a perfect storm that led to a significant attack — one that we were able to stop.

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

This ransomware attack demonstrates how elusive an attack pattern can be and how attackers have learned to evade detection by leveraging legitimate connections and disabling conventional monitoring tools. Thankfully, we could still stop this incident before the attackers caused significant harm. Here’s what happened during the attack and how we evicted the attacker.

5th March:

Attackers breach an employee’s workstation using a fake and malicious browser update delivered through a legitimate website. The attacker gains elevated privileges on the system and then moves laterally. They then breach and establish persistence on multiple devices.

5th – 21st March:

The attackers use legitimate tools and credentials to conduct reconnaissance, establish persistence, and avoid detection. They disable security tools and monitoring and destroy the company’s backups. They launch a ransomware payload that encrypts over 15,000+ devices.

22nd March:

The targeted company contacts our CSIRT. Our team collects data and creates a coordinated response with the client’s teams. We identify the attack encrypted remote worker devices logged into the client’s VPN. As a containment measure, systems globally are disconnected during initial forensics.

25th March:

A parallel team had already set up a ‘bubble of trust’ and started bringing up critical systems online from the 23rd. We slowly expand the bubble and evict the attacker. We close back doors and monitor the environment for a return.

24th March:

We brief their crisis cell. The stolen files include PII including names, medical information, employee benefits data, former employees and their dependents, as well as 10% of their customers. We help our client report the breach to authorities and work with law enforcement. No ransom will be paid.

22nd – 24thMarch:

We implement supplemental security monitoring and identify the initial intrusion point and vector. We learn the attack uses the Phoenix CryptoLocker variant and accessed files using MEGASync, a legitimate tool, before copying and uploading them to their cloud via MegaNZ.

26th March:

We confirm the attackers have not viewed the files accessed and work with law enforcement to seize their MEGASync account. The cloud storage platform confirms that the data was not shared outside the account. The client notifies its customers about the compromise.

30th March:

We fully restore our client’s systems and recover and restore most data (some were lost when backups were destroyed). Our client upgrades the security we set up and also sets up new backup and recovery systems.

31stMarch:

We provide a detailed incident report, offer customized recommendations, and send a thank-you note to law enforcement for timely intervention.

Lessons learned: How to stop this attack

In this incident, the attacker moved quickly through the client's systems, built a significant foothold, and exfiltrated a large volume of data in just a few weeks. It was fortunate that the client called us in before that data had been viewed and shared and that we could stop the attack quickly.

You can prevent attacks like this— or at least detect them much earlier in their progression — by developing a few fundamental security capabilities.

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, hardcoded passwords in scripts and applications
- Isolate legacy systems that can't be adequately patched
- Implement tamper-resistant backups
- Deploy agents with application controls (blacklist/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

Learn more about Eviden DFIR

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 DFIR services, schedule a noobligation consultation with an Eviden Digital Security expert and begin to build or augment your ransomware defense.

Connect with us

eviden.com

ECT-230613-SJ-CASE STUDIES- LARGE BACKUPS DESTROYED, 15,000+ DEVICES ENCRYPTED-