COHESITY

Leading lender restores data after attack, expedites recovery of time-sensitive files

CERT Cyber Event Response Team

Industry:
Financial services

Target: Unknown

Initial Attack Vector:
Unconfirmed access through phishing, moving to out-of-band management on critical server

Overview

Data security and cyber resilience are crucial for this consumer lending company, which has a fiduciary responsibility to protect customers' personally identifiable information (PII) and private financial data. Data loss or prolonged recovery times can delay loan closing, prevent customers from making payments, and cause reputational damage.

Adversary tactics, techniques, and procedures (TTPs)

Affiliates using this ransomware as a service tend to exploit vulnerabilities in public-facing systems or to use valid credentials for initial access. Once inside, attackers use a number of living-off-the-land techniques to further the attack, resulting in exfiltrated data and encrypted systems.

> "After standing up a new server and firewall, the customer engaged us to guide them through restoring data in the most efficient and secure way."

Greg Tucker, Global Escalation Leader, Cohesity CERT

1: Detect

It's 1:00 a.m., and the lender's IT team receives an alert of suspicious activity consistent with a ransomware attack. The IT team immediately powers off the Cohesity cluster as a precaution while they determine the scale and scope of the attack. They also disconnect the network to keep the threat from spreading. An incident response firm identifies the ransomware based on the attacker's TTPs.

2: Respond

The IT team begins preparing a new environment to restore files, including a brand-new VMware ESXi host and firewall. Early in the process, they contact Cohesity CERT (Cyber Event Response Team) for expert-led data restoration and operational recovery. Cohesity CERT:

- Freezes the cluster to preserve potential evidence and assess the scope of the attack
- Gathers logs for forensic analysis by Cohesity security engineers, who confirm the Cohesity backups are available and show no signs of unauthorized access

3: Recover

The lender's CIO urgently needs a folder for a time-critical accounting matter. Cohesity CERT delivers by immediately spinning up a new VM and cloning the folder. When the new infrastructure is ready, the lender's IT team successfully restores all data from the Cohesity backups—with Cohesity CERT on standby to resolve any issues.

Cohesity CERT recommendations to strengthen security posture

- Verify that the Cohesity cluster has not drifted from the recommended security configuration, and confirm the use of DataLock and MFA.
- Assign roles with least privilege required, and configure proper audit logging and alerting to an external collector.
- For more sensitive operations, follow the separation-of-duties principle for oversight and human-based authentication.

5000141-001-EN 1-2025