COHESITY

Hospital emerges successfully from ransomware attack, recovers payroll system by deadline

CERT Cyber Event Response Team

Industry: Healthcare

Target: Unknown

Initial Attack Vector: Active Directory

Overview

This North American hospital provides care for people with chronic diseases. Cyber resilience is critical for patient safety and operations, and data security is vitally important to protect personal health information (PHI) and personally identifiable information (PII) for patients and staff.

Adversary tactics, techniques, and procedures (TTPs)

It appears that the attackers used valid credentials for initial access and privilege escalation, concluding with encrypted VMs. No ransom note was found.

> **"The first step in our response is to contain the attack. This helps to manage risk and to minimize some of the noise to help expedite the response process."**
>
> William Wells, Tech Lead, Cohesity CERT

1: Detect

In 2024, the hospital IT team discovers that both data centers are down and the VMware environment is compromised. Active Directory fails first, followed by critical core infrastructure. That same day the IT team opens a case with Cohesity CERT (Cyber Event Response Team).

2: Respond

Cohesity CERT takes the following actions to contain and investigate the threat:

- Disconnects all systems connected to the Cohesity cluster to prevent exposure to attack.
- Changes all cluster passwords and freezes the cluster to preserve potential evidence.
- Gathers logs for analysis to confirm there are no signs of unauthorized access to Cohesity backups.

Immediately after freezing the cluster, Cohesity CERT meets with hospital IT staff to determine which VMs to recover first, including the domain controller, health scanning system, and payroll system.

3: Recover

Working into the night, Cohesity CERT guides the hospital IT staff through repairing core infrastructure, using an encrypted messaging service for privacy. Once the environment is prepared, a Cohesity CERT engineer helps the hospital restore its 32 encrypted VMs—beginning with a 400 GB VM needed for tomorrow's payroll run. Within 3.5 hours, all but two VMs have been restored using the Cohesity Instant Volume Mount capability and then validated for release to production. On the advice of Cohesity CERT, the IT team waits to bring each restored VM online until the incident response firm can verify that the attack signature is not present. The hospital resumes normal business operations three days after the attack, meeting the payroll deadline.

Cohesity CERT recommendations to strengthen resilience

- Consider adding another backup copy in Cohesity FortKnox, an administratively isolated cloud vault.
- Regularly check that users have the minimum privileges to do their jobs—the principle of least privilege.

5000142-001-EN 1-2025