COHESITY

City government restores services less than 24 hours after ransomware investigation begins

CERT Cyber Event Response Team

Industry:
State and local government

Target: VMware

Initial Attack Vector:
Compromised credentials

Overview

For this city, data security is critical to protect residents' and employees' personally identifiable information (PII) and to avoid interruption in city services, including online payment of taxes and fees that fund essential city services.

Adversary tactics, techniques, and procedures (TTPs)

The city was attacked by a ransomware-as-a-service group that typically gains initial access by exploiting public-facing vulnerabilities, and has been observed to self-propagate. More recently the group has been observed using valid credentials with VPN accounts. In some cases the attacker exfiltrates data prior to encrypting systems, and has recently targeted VMware ESXi hosts directly.

"Government facilities were the third largest critical infrastructure sector targeted by ransomware attacks in 2023."

Source: FBI Internet Crime Report 2023

1: Detect

On a Sunday evening, an employee discovers that all applications are offline, quickly realizing that three separate virtual machine (VM) environments have been encrypted. Services are down for residents and the workforce.

2: Respond

While initiating the response, the city's incident response partner, Surefire Cyber, develops reasonable confidence about which ransomware group is behind the attack. As Surefire focuses on the forensic investigation, the Cohesity CERT (Cyber Event Response Team) is called in to focus on the Cohesity environment. Cohesity CERT delivers the following:

- Access to all available backup data
- A posture review report that highlights drift from recommended settings
- Details of all platform login data, compared against the customer digital forensics and incident response (DFIR) analysis
- Assistance with data and system restores to further the investigation and confirm mitigation steps

3: Recover

Cohesity CERT facilitates the transition from response to recovery by providing the servers and objects that Surefire needs for mitigation, validation, and documentation. The Cohesity Instant Volume Mount capability streamlines the process and ensures that each recovered server's operating system remains benign until all checks are completed. At this point the systems are returned to service—less than 24 hours after the investigation begins.

This response highlights the difference between traditional backups and a robust, fortified data management platform for cyber incident response. Trust, visibility, and quick access to data can shave hours, or even days, from the time to recover.

Cohesity CERT recommendations for cyber resilience

- Configure quorum feature for operations typically associated with an administrator role. Quorum adds an additional layer of protection from compromised credentials or insider threats by adding a time-based, multi-user approval flow.
- Assign minimum required user privileges using role-based access (RBAC).
- For workloads that do not require a very low recovery time objective (RTO), create an administratively isolated backup copy in Cohesity FortKnox, a software-as-a-service (SaaS) offering.
- Expand out-of-band threat hunting and data classification capabilities using Cohesity DataHawk.

5000144-001-EN 1-2025