COHESITY

When ransomware hits, retailer restores critical VM and domain controller just hours after contacting CERT

CERT Cyber Event Response Team

Industry:
Retail

Target: VMware vSphere and NAS

Initial Attack Vector:
An admin disabled the lockout policy, allowing a brute-force attack on a domain admin account

Overview

This U.S. retail chain operates in multiple states. An on-premises VMware environment and network-attached storage (NAS) are backed up to a Cohesity-managed cloud.

Adversary tactics, techniques, and procedures (TTPs)

Affiliates of the ransomware-as-a-service group behind the attack evade detection by deploying the malware using legitimate Windows tools such as PowerShell and Remote Desktop. They often use "double-extortion" tactics, encrypting data and also threatening to expose sensitive data such as personally identifiable information (PII).

> "After we restore the first VM or domain controller, customers typically are comfortable handling restores on their own. We're there for support in case they run into issues that sometimes crop up with networks, firewalls, or new servers."

Greg Tucker, Global Escalations Leader, Cohesity CERT

1: Discover

On a late afternoon in 2025, the retailer's IT team receives an alert of suspicious activity from the endpoint detection and response (EDR) system. The VMware ESX hypervisor and vCenter management platform are encrypted and inoperable. The IT team immediately contains the threat by disconnecting the VMware environment, and contacts an incident response (IR) firm. The firm later determines that attackers staged the ransomware three weeks before launching the attack.

2: Respond

At 5:33 p.m., the retailer opens a case with Cohesity Cyber Event Response Team (CERT). Within 20 minutes CERT has initiated validation and collection protocols to gather audit logs in support of the larger response. The impacted environment has already been contained, so CERT deploys a new SaaS connector on a clean subnet. On the 7:00 PM checkpoint call, CERT confirms that no malicious access to the Cohesity environment has been observed in the log review. Efforts shift to data recovery.

3: Recover

With the threat contained, the retailer's IT team provisions a new, standalone VMware ESXi host where the Cohesity backups can be safely restored. Following guidance from CERT, the team follows a controlled process to manage risk and make sure the threat does not compromise the new environment. When the host is ready, CERT connects it to the Cohesity-managed cloud and registers the host as a new data source. As the retailer's IT team watches and learns, CERT restores a critical VM and the domain controller on the new ESXi host. The retailer's IT team takes over from here—with CERT standing by to help—recovering and restoring other critical VMs and domain controllers on the new host. The IT team wipes existing hosts, engages the IR firm to confirm that no malware remains, redeploys VMware, and then restores the remaining VMs and NAS files from the Cohesity backups.

$0 Ransom paid

<1 Day to restore critical VM and domain server

0 Data loss

Cohesity CERT recommendations

- ↗ Enforce password policies, including regular changes, and use phishing-resistant MFA
- ↗ Never disable the count lockout policy on servers
- ↗ Regularly verify that Cohesity security features are enabled, including multifactor authentication and a policy-based lock on backups (DataLock)