COHESITY

International nonprofit restores encrypted VMs

CERT Cyber Event Response Team

Industry:
Nonprofit

Target: VMware virtual machines

Initial Attack Vector:
Software vulnerability in firewall

Overview

This global nonprofit runs programs and camps for children and college students in 100+ countries. Data security is critical to protect logins and personally identifiable information (PII) for young people and hundreds of thousands of donors, and for resilient operations. Day-to-day operations such as fundraising and program management depend on VMware virtual machines (VMs).

Adversary tactics, techniques, and procedures (TTPs)

This ransomware has variants that target Windows systems and VMware ESXi virtual machines. Attackers typically gain access through VPNs not configured for multifactor authentication (MFA), RDP, spear phishing, and the abuse of valid credentials.

> "After determining techniques used for initial access and evicting the threat, it's a straightforward process to help our customers recover their data."

Greg Tucker, Cyber Incident Handler, Cohesity

1: Detect

As a 2024 summer weekend begins, the IT manager discovers that VMs are encrypted, as is the organization's compute environment. A ransom note from the Akira ransomware group is found. The organization contacts Cohesity Cyber Event Response Team (CERT) on day 2.

2: Respond

Fortunately, the firewall has already automatically disabled ports in response to the attack. To prevent further damage, the IT manager unplugs the network. As the organization's IT team begins rebuilding its servers, CERT takes the following actions to contain and investigate the threat:

- Freezes the cluster to preserve potential evidence and assess the scope of the attack
- Gathers logs for forensics analysis by Cohesity security engineers, who confirm the Cohesity backups are clean with no alteration
- Collaborates with the incident response partner to scan for indicators of compromise (IOC)

3: Recover

The IT team rebuilds the production servers over three days. During this time CERT advises the organization on the optimum method to restore VMs from the Cohesity backups, balancing speed against risk of reattack using the same tactics and techniques. When the target server has been prepared, CERT guides the organization through the process of restoring VMs. At CERT's recommendation, approximately 40% of critical VMs are restored with instant volume mounts, another 40% with file-level recovery, and 20% with VM recovery. With VMs restored, the organization resumes normal operations.

CERT's recommendations to strengthen data security and cyber resilience

- Immediately change passwords based on information from the investigation
- Validate that phishing-resistant MFA is enabled, especially on externally accessible systems like VPN
- Ensure that role-based access (RBAC) is used, with minimum required privileges
- Enable multi-person controls (Quorum) on critical systems
- Regularly audit domain user creation, setting up alerts when accounts are created with elevated privileges

5000140-001-EN 1-2025