COHESITY

Auto parts manufacturer recovers more than 100,000 encrypted files

CERT Cyber Event Response Team

Industry: Manufacturing

Target: VMware virtual machines

Initial Attack Vector: Vulnerability in VMware

Overview

A division of a global auto parts enterprise operates a manufacturing plant and R&D center. Damaged or encrypted virtual machines (VMs) and databases exact a high cost on the multi-billion dollar business, including revenue interruption, potential compliance violations, and reputational damage. For cyber resilience, the company maintains one immutable Cohesity backup on-premises and another administratively isolated copy in Cohesity FortKnox, a software-as-a-service (SaaS) offering.

Adversary tactics, techniques, and procedures (TTPs)

The ransomware that hit the company encrypts VM images hosted on VMware ESXi servers. Attackers can also gain initial access to victim networks via RDP, drive-by compromise, phishing, abuse of valid credentials, and exploitation of public-facing applications.

> **"Manufacturing is one of the seven industries most vulnerable to cyberattacks."**

Source: 2024 Cohesity global cyber resilience report

1: Detect

In late 2023 an IT administrator discovers that all VMs have been encrypted.

2: Respond

The manufacturer contacts Cohesity CERT (Cyber Event Response Team) the morning after the attack. Cohesity CERT works in partnership with the company's incident response firm, **Fenix24**, to contain and investigate the threat. The investigation identifies the threat actor and reveals that more than 100,000 files are locked up, some containing proprietary company information and personally identifiable information (PII). Working with the incident response firm, Cohesity CERT helps to bring data back from FortKnox, working with the IT and incident response teams to validate that the threat has been mitigated and that remediation steps are successful.

3: Recover

Cohesity CERT works alongside the manufacturer's IT team to prepare a target server. When the target is ready, Cohesity CERT begins restoring large VMs (>12 TB) from FortKnox. Normal operations resume weeks sooner than they would have otherwise, and the company avoids significant business disruption.

Cohesity CERT recommendations to strengthen cyber resilience

- Take care that backups do not share hardware with the workloads they are protecting
- Follow the 3-2-1+ backup rule for cyber resiliency: three copies, two different storage media, and one copy geographically separated *plus* administratively isolated
- Make sure that backups do not share infrastructure with production data
- Verify that backups are successful

© 2025 Cohesity, Inc. All Rights Reserved.

5000143-001-EN 1-2025