COHESITY

Local law enforcement agency confidently restores dispatch system used as a staging area for ransomware attack

CERT Cyber Event Response Team

Industry:
State and local government

Target: VMware

Initial Attack Vector:
Vulnerability in VPN appliance

Overview

This county law enforcement agency has almost 1,000 employees serving half a million residents. Cyber resilience is crucial because personnel rely on law enforcement and public safety applications to protect life and property. The agency is also obligated to protect residents' personally identifiable information (PII), including social security numbers and addresses collected when residents call 911.

Adversary tactics, techniques, and procedures (TTPs)

Affiliates of this ransomware-as-a-service group gain initial access through unpatched vulnerabilities in public-facing systems and compromised accounts, sometimes through an access broker. Attackers then use a variety of tools to rapidly enumerate the network, move laterally, and elevate privileges. The ransomware avoids detection in various ways and can move to the impact stage within hours of initial access.

"Ransomware attacks on state and local governments were 51% more prominent during the first eight months of 2023 than they were during the same period a year earlier."

Center for Internet Security

1: Detect

Late one evening, an agency IT specialist sees a flurry of alerts about unusual activity in the computer-aided dispatch (CAD) system. The alerts come from the virtual security operations center (Arctic Wolf Networks) and the antivirus client.

2: Respond

To contain the attack, the county's IT specialist proactively turns off the CAD system, and the county temporarily reverts to manual dispatch methods. A Cohesity partner, Arctic Wolf, determines that the system had been used as a staging area to deploy the ransomware. The county's quick action stopped the attack in its tracks, before any data could be exfiltrated or encrypted. The cyber response partner's investigation determines that the attackers entered the network by exploiting a vulnerability on the VPN appliance. As the agency begins restoring the network, Cohesity CERT (Cyber Event Response Team) is contacted to recover the CAD server.

3: Recover

Cohesity CERT takes steps to confirm that the backups are accessible, then validates that the security posture of the Cohesity environment aligns with hardening recommendations. For extra assurance, Cohesity CERT reviews audit logs for indicators that credentials may have been compromised. Cohesity CERT finds no evidence that the Cohesity environment was accessed and confirms that the backups are ready for restores. The most time-consuming step is setting up the replacement VPN appliance to restore network functions. When that's done, Cohesity CERT guides the county team through restoring a full copy of the CAD server to another location. At this point the county's automated dispatch operations fully resume.

Cohesity CERT recommendations

The county already followed recommended data security practices from Cohesity CERT:

- Storing an administratively isolated backup copy in Cohesity FortKnox, a software-as-a-service (SaaS) offering
- Using multifactor authentication
- Setting a time-based lock on backup snapshots (DataLock)

5000145-001-EN 1-2025