Cyberkraft

Colorado DOT Lessons Learned from 2018 Ransomware Attacks

Background

From February 21-23, 2018, a threat actor executed a ransomware attack on the Colorado Department of Transportation (CDOT) that ultimately affected roughly half of the Department's computers. Despite immediate action by CDOT and Governor's Office of Internet Technology (OIT), CDOT suffered a second attack on March 1, 2018 that was discovered to pose risk to other state resources. On March 3, CDOT, OIT, and the Colorado Division of Homeland Security and Emergency Management (DHSEM) formed a Unified Command Group (UCG) to provide direction and control for incident responders. On March 8, the UCG completed Phase 1 (Containment) objectives and shifted to Phase 2 (Eradication) operations. On March 9, the UCG completed Phase 2 (Eradication) objectives and shifted to Phase 3 (Recovery) operations.

Root cause analysis revealed several vulnerabilities related to a newly created, Internet-accessible virtual server with direct connection directly into the CDOT network and administrative privileges that did not have OIT security controls in place. This server was compromised within two days of creation and was under SamSam ransomware attack within one additional day. Containment, eradication, and recovery of services required approximately four weeks.

Though CDOT operations were degraded, CDOT continued to execute its core mission to provide a multi modal transportation system for Colorado. This success may be attributed to a sound Continuity of Operations Plan that allowed CDOT to continue to operate and an OIT response that brought in the right people at the right time to contain and eradicate the threat. The creation of the UCG provided a clear direction and control structure that unified and focused the efforts of the numerous government agencies and private contractors involved. Though the State effectively responded to and recovered from this incident without paying the ransom, the threat to the State and its networks remains.

Lessons Learned

CDOT's experience offers various lessons regarding the hardening of networks, creating and rehearsing a cyber incident response plan, and allocating resources to both the necessary personnel and technology to effectively mitigate, respond to, and recover from future cyber-attacks.

Segment your network to isolate any potential malware. Network segmentation allowed OIT to isolate the malware within one department, protecting both the CDOT Intelligent Transit System and the cloud-based backup system. Though the effects on CDOT were significant, this segmentation directly contributed to containment of the malware and prevented the spread throughout the Colorado State Network (CSN).

Make the implementation of endpoint detection and response toolsets a top priority. While a Security Analytics and Endpoint Detection and Response toolset had recently been purchased, implementation was still being coordinated according to a per-agency project plan, with the CDOT network scheduled for implementation the week after the ransomware hit the agency. If the toolset had been fully implemented, it would have alerted earlier and may have completely contained the outbreak.

Ensure there are no outdated systems in use that provide easy backdoors to attackers. A couple of outdated systems were discovered in the agency environment. The attackers utilized these outdated systems to establish staging environments and persistent backdoors into the environment. These systems were easy targets and easily penetrated, since security patches were no longer being released by the vendor. These systems have since been depreciated and replaced.

Initiate protocols for centralized logging. OIT has a large logging initiative underway to ensure that all critical and essential systems and infrastructure components are sending security logs to a centralized log collection and analysis tool to filter the most significant security data.

Implement current system backups and segment them from the network. The successful FY17 completion of Colorado's system backup strategy, Backup Colorado, meant that OIT was confident in the offline backups of the servers and ability to recover data files. Backup Colorado was a key to successfully recovering from this incident and a significant factor in the decision not to pay the ransom. The backup solution provided two advantages. First, it was segmented from the network, making it inaccessible to the adversary; second, the solution's ability to detect malware protected the data and provided one of the first indicators of the attack.

Protect network diagrams and ensure familiarity with the agency network. Diagrams of the network were stored on systems which had been encrypted by the ransomware. As a result, incident response teams had to recreate the diagrams from memory and knowledge of the

network. It is possible that a better understanding of the environment would have highlighted risks requiring a higher level of urgency for replacement than was in progress.

Employ sufficient firewall personnel. Following significant turnover of subject matter experts in the Security Operations Center, OIT was forced to solicit less knowledgeable volunteers from other state agencies and public sector entities to help with the firewall monitoring, investigation, and work that needed to occur. OIT is deploying tools with automated security response capabilities to handle the repeatable, lower-skill, mundane tasks, thereby creating more interesting and fulfilling work, as a way to retain their scarce human resources.

Maintain strong partnerships with cloud service providers to provide higher visibility into the cloud. The virtual server instance was created only two days prior to the attacker gaining access. While a penetration test was conducted a few months previously, because this system's internet address was not on the state network it would have never been detected. A solid partnership with cloud service providers and tools to gain visibility into cloud services are needed to detect poorly configured systems that might put state data and networks at risk.

Ensure that cyber incident response plans are fully integrated and operationalized. OIT has a cyber incident response plan and did use it for this incident, however the plan was not as operational as it could have been and was not rehearsed often enough to facilitate confident employment of the plan. As a result, a systematic approach to an escalating cyber incident did not exist. Integrated and supporting operational plans promote commonly understood roles, responsibilities, escalation triggers, and expected responses to those triggers. Such plans also ensure supporting functions, such as internal/external communications, response team life support and vendor integration are addressed pre-incident. Once such plans are in place, a deliberate training and exercise program that includes both cyber response and business continuity is necessary to rehearse and test the plans.