CDOT Cyber Incident

After-Action Report

Releasable to the Public

July 17, 2018

INCIDENT OVERVIEW

Incident Name	CDOT Cyber Incident
Incident Dates	On or about 18 Feb 2018 to Present
Situation	Between 21-23 Feb 2018, a threat actor executed a ransomware attack on that ultimately affected roughly half of the department's computers. Despite immediate action by CDOT and OIT, CDOT suffered a second attack on 01 Mar. On 03 Mar, CDOT, OIT, and DHSEM formed a Unified Command Group (UCG) to provide direction and control for incident responders. On 08 Mar, the UCG completed Phase 1 (Containment) objectives and shifted to Phase 2 (Eradication) operations. On 09 Mar, the UCG completed Phase 2 (Eradication) objectives and shifted to Phase 3 (Recovery) operations. Recovery operations continued for several weeks.
Mission Area(s)	Response and Recovery
Threat or Hazard	Ransomware Cyber Attack
Participating Organizations	Colorado Department of Transportation Colorado Governor's Office of Information Technology Colorado Division of Homeland Security and Emergency Management Colorado Army National Guard Colorado Bureau of Investigation Federal Bureau of Investigation Department of Homeland Security-Cyber Department of Homeland Security-Infrastructure Protection Department of Homeland Security-Hunt and Incident Response Team Federal Emergency Management Agency Federal Emergency Management Agency-MERS Private cybersecurity contractors
Point of Contact	Michael Willis Director, Office of Emergency Management Colorado Division of Homeland Security and Emergency Management

Incident Summary

On or about 18 Feb 2018, a threat actor gained access to the CDOT network and installed the SamSam ransomware malware variant. On Wednesday, 21 Feb, OIT declared a security incident when the ransomware became active and infected approximately 150 servers and 2000 workstations.

On Friday, 23 Feb, OIT executed a remediation plan to get CDOT back online safely. The OIT team worked through the weekend to assess, cleanse, and restore systems prioritized by CDOT.

On Monday, 26 Feb, leadership representatives from CDOT and OIT established a coordinated incident response team.

By Wednesday, 28 Feb, with the assistance of private sector partners and security tool vendors, OIT believed it had fully contained the malware and began bringing CDOT systems back online for restoration.

On Thursday, 01 Mar, OIT discovered new attacker activity overnight and what was initially believed to be a new type of malware on CDOT systems—even on the newly cleaned and restored systems. At this point, CDOT and OIT leadership notified the State Emergency Operations Center (SEOC) and requested that the Governor activate the Colorado National Guard to provide additional support. The Governor made a verbal emergency declaration to access funding and granted verbal approval to activate the National Guard. Future analysis would determine that it was a second infection of SamSam.

On Friday, 02 Mar, the National Guard arrived at CDOT headquarters and assisted OIT in creating an operational plan to identify and defeat the malware and threat actor(s). This allowed for a detailed targeted forensics analysis to combat the attacker and the malware. The State Emergency Operations Center (SEOC) increased its Activation Level from IV to III to provide support and coordination to CDOT and OIT.

On Saturday, 03 Mar, CDOT, OIT, and DHSEM formed a Unified Command Group (UCG) to provide direction and control for incident responders. CDOT was tasked with focusing on continuity of operations while OIT focused on ransomware containment, eradication, and recovery. OIT successfully blocked the SamSam ransomware from a single data point and developed a plan to test this solution on other machines for proof of success.

On Sunday, 04 Mar, the UCG developed a four-phase campaign to eliminate the threat, return CDOT to full operational capability, and to harden Colorado State Agencies against further attacks. The four phases were:

1. Containment
2. Eradication
3. Recovery
4. Sustainment

On Monday, 05 Mar, the SEOC increased its Activation Level to Level I (Full Activation).

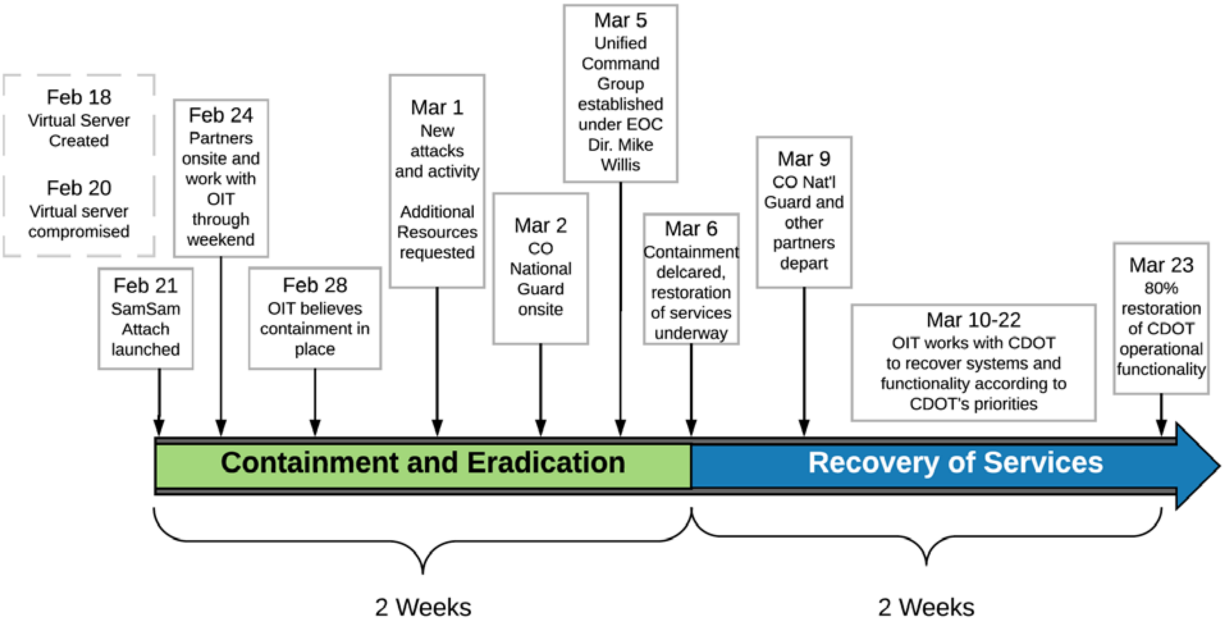
On Thursday, 08 Mar, the campaign completed Phase 1 (Containment) objectives and shifted to Phase 2 (Eradication) operations.

On Friday, 09 Mar, the campaign completed Phase 2 (Eradication) objectives and shifted to Phase 3 (Recovery) operations. CDOT and OIT assumed combined command of the recovery phase on 10 Mar.

On Wednesday, 14 Mar, the Unified Command Group was disestablished and turned over incident direction and control a combined CDOT-OIT team.

As of Friday, 23 Mar, CDOT had nearly 80% of their operational functionality restored. Recovery operations continued for several weeks.

Incident Timeline

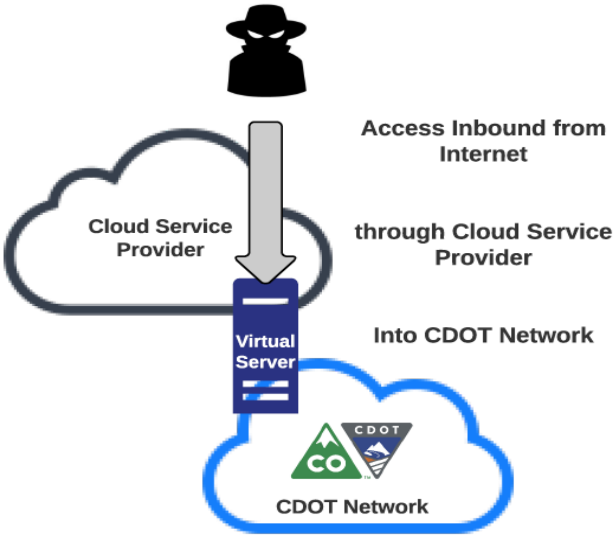

Feb 18
Virtual Server Created
Feb 20
Virtual server compromised
Feb 21
SamSam Attach launched
Feb 24
Partners onsite and work with OIT through weekend
Feb 28
OIT believes containment in place
Mar 1
New attacks and activity
Additional Resources requested
Mar 2
CO National Guard onsite
Mar 5
Unified Command Group established under EOC Dir. Mike Willis
Mar 6
Containment delcared, restoration of services underway
Mar 9
CO Nat'l Guard and other partners depart
Mar 10-22
OIT works with CDOT to recover systems and functionality according to CDOT's priorities
Mar 23
80% restoration of CDOT operational functionality
Containment and Eradication
Recovery of Services
2 Weeks
2 Weeks

Root Cause

A virtual server was created on February 18, 2018. The virtual server was directly connected into the Colorado Department of Transportation (CDOT) network, as if it was a local on premise system. The virtual server instance also had an internet address and did not have OIT's standardized security controls in place. The account utilized to establish the connection into the CDOT network was a domain administrator account - this is the highest level privileged account, and means that 1) the account cannot be disabled for too many failed login accounts, and 2) it provides the highest level of access to the agency domain controllers (gatekeepers for all access to everything in the department).

Later, OIT was informed by the vendor that when an external IP address is requested, the vendor automatically opens the Remote Desktop protocol to the internet. The Remote Desktop protocol is how this attack was initiated.

An attacker discovered this system available on the internet, broke into the Administrator account using approximately 40,000 password guesses until the account was compromised. From there, the attacker was able to access CDOT's environment as the domain administrator, installing and activating the ransomware attack.



The virtual server was built on 2/18. The brute force attack began the same day. The system was compromised on 2/20. The ransomware attack was launched on 2/21.

Protecting the Rest of the State

The OIT Security Operations team noticed that the attackers were attempting to break into systems that are shared across all agencies - the team took these down, and disconnected the OIT network from CDOT to ensure the attack could not spread.

Traffic Operations is separated from CDOT's business network by a next generation firewall which detected and blocked the ransomware from entering its network. Upon detecting the malware, the Traffic Operations team disconnected their network from the CDOT network to ensure their operation remained functional and not impacted.

Security Operations quickly deployed a newly acquired Security Analytics and Endpoint Detection and Response toolset with a very aggressive security policy, to CDOT and the rest of the state, to ensure that malware and ransomware behaviors would be detected and blocked. Prior to the attack, four state agencies had already received with this toolset and CDOT was scheduled for deployment the next week. Security Operations launched this statewide deployment starting the day of the attack.

Security Operations upgraded the standard endpoint security agents to a next-generation agent which incorporates threat intelligence information into the workstation protection to ensure that malicious-appearing behaviors would be captured and blocked. This had been implemented across approximately 50% of the agencies but was accelerated to aide with protecting the state.

The successful completion of “Backup Colorado” during FY17, Colorado's system backup strategy, meant that OIT was confident in the offline backups of the servers and would not need to pay ransom to recover data files.

Potential Opportunities to Prevent or Lessen Impact of the Incident

New tool fully implemented – If a recently purchased Security Analytics and Endpoint Detection and Response toolset had been fully implemented, it would have alerted earlier and may have completely contained the outbreak. This tool had recently been purchased, and implementation was being coordinated according to a per-agency project plan. The tool had been successfully implemented at four agencies. The project plan had the CDOT network scheduled for implementation the week after the ransomware hit the agency.

Monitoring - With 8.4 million security events per day, there may be important security events that are missed due to the sheer volume of the events. OIT has deployed a Security Analytics and Endpoint Detection and Response toolset to help discover anomalous events. OIT is exploring alternatives to have more people monitoring the state network.

Logging - OIT has a very 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. This effort has progressed and improved year over year; however, OIT needs to accelerate this process.

Privilege Access Management – OIT has implemented security enhancements for privileged accounts.

Cloud Governance, Security, and Training - OIT is looking into what responsibilities cloud service providers should have for alerting when poorly configured cloud services may put the state network at risk. So far, there does not appear to be a good partnership in this area. Additionally, OIT's personnel need to be better trained and knowledgeable on deploying cloud services securely and mitigating risks related to cloud based systems.

Potential Aids to the Attack / Delays in Recovery

Turnover and lack of firewall personnel - OIT had, and continues to be effected by turnover in areas of subject matter expertise. They lost knowledgeable personnel in the Security Operations Center over the last 6-7 months. All OIT firewall personnel departed in November for higher salaries elsewhere. While one of the positions had been recently filled, OIT solicited volunteers from other state agencies and public sector entities to help with the firewall monitoring, investigation and work that needed to occur. OIT is actively recruiting replacement employees; however, it has been a slow process as there is a lot of local competition for these valuable resources. OIT is currently supplementing with consultants and has a large documentation effort underway to help new employees and consultants come up-to-speed quickly. OIT is in the submission process with a Decision Item for FY19 Supplemental funding and FY20 funding to increase salary levels for these in-demand and hard-to-retain skills. The number one reason cited for the individuals leaving this group is recruitment by the private sector with higher salaries. OIT is also evaluating the use of a Managed Security Service to offload much of the work. This cost is also included in the FY19/FY20 Decision Item. Additionally, 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 our scarce human resources.

Separate internet access and outdated firewall - controls, protection, and visibility built into enterprise services, such as firewall services, were scheduled for implementation into the CDOT network as part of a planned building move in the upcoming weeks. As a result, the firewall had not yet been replaced and upgraded. The replacement effort would have resulted in a stricter policy and better visibility into and blocking of malicious traffic.

Outdated systems in use –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 are easy targets and easily penetrated, since security patches are no longer being released by the vendor. These systems have since been depreciated and replaced.

An isolated network and lack of 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.

Little visibility into the cloud - the virtual server instance was created only 2 days prior to the attacker gaining access. And while a penetration test was conducted in November, because this system’s internet address was not on the state network it would have never been detected. Better partnership with cloud service providers and better tools to gain visibility into cloud services is needed to detect poorly configured systems that might put state data and networks at risk.

Major Strengths

The major strengths identified during this incident are as follows:

1. **Interagency Coordination and Support**: In the span of less than one week, five state agencies, six federal partners, and four private cyber security contractors formed a unified team that identified, contained, and eradicated the malware that threatened to shut down CDOT.
2. **CDOT Continuity of Operations (COOP) Planning and Execution**: Through effective pre-incident COOP planning and execution, CDOT maintained its essential functions, ensuring minimum risk to life or safety on Colorado’s transportation networks while continuing its essential business functions.

3. **Incident Support Augmentation**: Forming a Unified Command Group and bringing in the emergency management resources of DHSEM allowed CDOT to focus on its COOP and for OIT to focus on the cyber response and recovery. Additionally, the cyber resources deployed by the Colorado National Guard provided significant support to incident command, threat identification and analysis, and technical expertise.
4. **Strategic Communications**: Early in the incident, CDOT began daily communications (e.g., Town Hall conference calls, emails, etc.) to keep employees informed and to maintain morale. Following the creation of the UCG, the Joint Information Center (JIC) ensured consistent messaging across agencies to both internal and external stakeholders.

Primary Opportunities for Improvement

The primary areas for improvement are as follows:

1. **Pre-incident planning and exercises:** The State Emergency Operations Plan and OIT Cyber Incident Response Plan were not integrated or operationalized. As a result, a systematic approach to an escalating cyber incident did not exist. Integrated and supporting operational plans would promote commonly understood roles, responsibilities, escalation triggers and expected responses to those triggers. These plans would also ensure supporting functions, such as internal/external communications, response team life support and vendor integration were addressed pre-incident. Once these 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.
2. **Commonly understood Incident Command System approach:** Though versed in cyber incident response, the OIT cyber response team was not versed in the Incident Command System approach. CDOT utilized ICS as part of their COOP and the UCG employed it once engaged. Having ICS trained personnel on the cyber incident response team would have facilitated a common approach to incident handling and may have reduced friction points between the response team and the CDOT COOP team. Anecdotally, it appears most state agencies do not have the level of ICS training necessary to successfully employ the system in an incident.
3. **Cyber Incident Response Capabilities Gap Analysis:** Pre-incident cyber gap analysis in two areas could have contributed to a more coordinated and efficient cyber incident response.
    a. Cyber Incident Response Plan (CIPR). Capabilities gap analysis in the CIRP could identify known gaps in OIT capabilities. These could then be mitigated through pre-event contracts or MOUs with other agencies (ie: National Guard).
    b. Continuity of Operations Plans (COOP). Though CDOT had a thorough COOP that was instrumental in continuing its mission, these plans did not account to the challenges related to a cyber incident. Plans considered loss of infrastructure and the requirement to move people to alternate worksites, however, these plans assumed that employees would take their computers with them and be able to establish connectivity with key online applications. All State Agencies could benefit from capabilities gap analysis in their COOP for a cyber incident response.
4. **Third Party Vendor Relationships:** There were a number of third party vendor allegations pertaining to vulnerabilities and weaknesses made at various levels of state government. This after action review addresses the principle vulnerabilities that contributed to the incident, including root cause analysis identifying a virtual server without standardized security controls. Several vendors leveraged these vulnerabilities as part of their effort to sell the State either products or services during incident response. While third party vendors provided critical technical capability, bending the incident into a high pressure sales campaign was distracting and unhelpful. Vendor insights were used during the after action review process and OIT is evaluating areas where enhanced vendor support might improve pre-incident security and post-incident response.

Recommendations

1. **SEOP Cyber Incident Annex:** *Improve*. Convene a cross-functional planning team to review and revise the SEOP Cyber Incident Annex with lessons learned from this incident and industry best practices and standards. This annex should address escalading cyber incidents, establish triggers for response actions, including establishing scalable command and control and assigning roles and responsibilities. Office of Primary Responsibility (OPR): DHSEM with OIT assistance
2. **Cyber Incident Response Plan:** *Improve*. 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. Further refinement of this plan with lessons identified during this incident, the incorporation of known malware response playbooks and deliberate rehearsals of the plan can make significant improvements for the next incident. OPR: OIT with OEM support.
3. **Integration of external assets:** *Improve.* Future cyber response will require external support from vendors, the National Guard and federal assets. Pre-incident planning and coordination will help ensure the right support is provided and integrated as rapidly as possible to facilitate a cohesive response effort that leverages the capabilities of each asset. OPR: OIT
4. **COOP Planning:** *Sustain/Improve*. Share CDOT best practices and lessons learned with other state agencies. Incorporated specific considerations for a cyber incident in COOPs. Traditional COOP planning focuses on the loss of access to a physical location (e.g., offices). This incident highlighted the importance of digital resiliency and the need to plan for loss of data and/or connectivity. As program manager for the State Agency COOP Program, DHSEM should develop and promulgate digital COOP planning guidance to State Agencies. OPR: DHSEM with CDOT assistance.
5. **Statewide Network Assessment and Hardening:** *Sustain*. As part of the response to and recovery from this incident, OIT completed an extensive analysis of the statewide network and implemented immediate solutions to harden the network. OIT should continue its current work to secure the network against future attacks. OPR: OIT
6. **Backup Colorado:** *Sustain:* 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 and, second, it has the ability to detect malware. The ability to detect malware protected the data and provided one of the first indicators of the attack. The State should continue to programmatically use the backup solution for backup and recovery. OPR: OIT
7. **Network Segmentation:** *Sustain:* Segmentation of the network allowed OIT to isolate the malware within one department, allowed for isolation, and therefore, protection of the CDOT Intelligent Transit System and also protected the cloud based backup system. Though the effects on CDOT were significant, this segmentation directly contributed to containment of the malware and prevent the spread throughout the Colorado State Network (CSN).

Conclusion

Though CDOT operations were degraded, CDOT continued to execute its core mission to provide 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. The State must remain vigilant against future attacks by continuing to harden its networks, improving and rehearsing its cyber incident response plans and sharing information about this attack with stakeholders and partner agencies. Additionally, the State must allocate resources to both the necessary personnel and technology to effectively mitigate, respond to and recover from future cyber-attacks.