

RSA®Conference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN
ELEMENT

SESSION ID: SEM-M03F

Ransomware: Partnering for Recovery



Deborah Blyth

Chief Information Security Officer
State of Colorado
@debbiblyth

#RSAC

2018 Ransomware Attack: Colorado Department of Transportation (CDOT)

THE DENVER POST

SamSam virus demands bitcoin from CDOT, state shuts down 2,000 computers

Colorado investigators call in FBI, work through the night

Ransomware Hits CDOT Computers

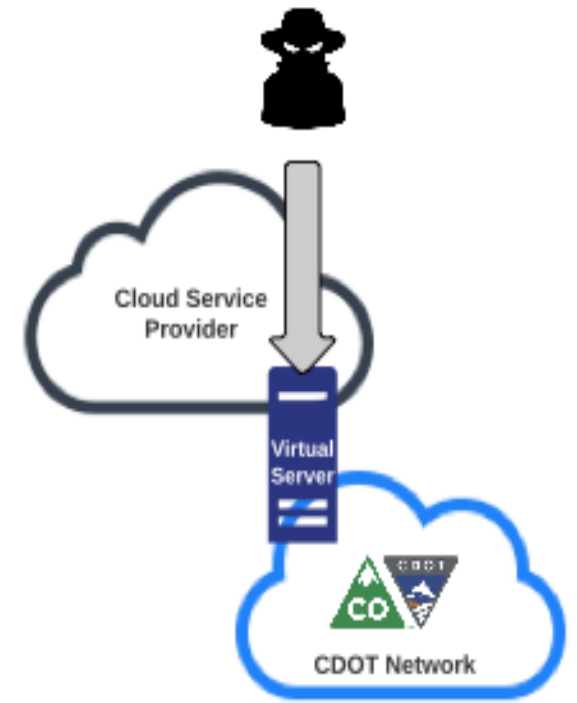
February 21, 2018 at 5:56 pm Filed Under: Colorado Department of Transportation, Ransomware

CBS 4 CBS Denver



SamSam Ransomware Attack: CDOT

- Misconfigured virtual server
- Virtual server connected to the CDOT network
- Brute force attack (account compromise)
 - Started the day the server came online
 - Server was compromised within 48 hours
 - 40,000 password attempts
- Attacker installed and launched the CDOT ransomware attack



SamSam Ransomware Attack: CDOT Impact


Impact to CDOT Business Operations

- ~1300 workstations
- ~400 servers
- Databases and software applications
- All VoIP phones
- SAP – financial systems used for paying employees and vendors



We Thought We Were Clean...

Hit again!

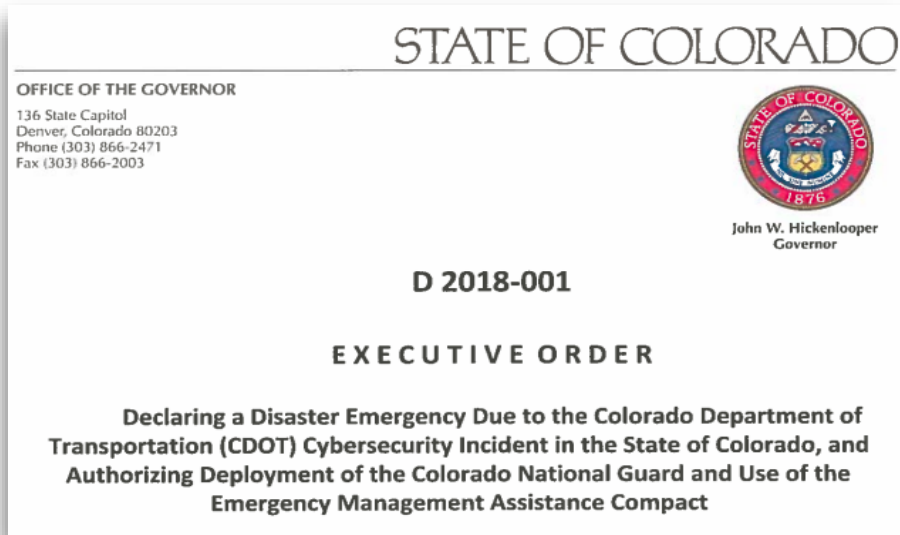


The video player shows a news report from 9news.com. The video frame displays a close-up of hands typing on a laptop keyboard, overlaid with a green digital rain effect, reminiscent of the Matrix. The video player interface includes a progress bar at 00:48 / 01:55, a 'Next' button, and a 'More Videos' link. Below the video player, the headline reads 'More malicious activity on CDOT computers reported'. The sub-headline states: 'Eight days into a ransomware attack, state information technology officials detected more malicious activity on computer systems at the Colorado Department of Transportation.'

More malicious activity on CDOT computers reported

Eight days into a ransomware attack, state information technology officials detected more malicious activity on computer systems at the Colorado Department of Transportation.

SamSam Ransomware Attack: Recovering CDOT



Key Response Partners onsite

- State Agencies

- Governor's Office of Information Technology (OIT)
- Colorado Department of Transportation (CDOT)
- Colorado Office of Emergency Management
- State Fusion Center
- Colorado National Guard

- Federal Partners

- FBI, DHS, US-CERT, FEMA

- Vendor Partners

- Four security tools vendors
- Incident Response Team



CDOT Contributing Factors and Enabling Recovery

- Contributing Factors
 - Remote Desktop open to the internet
 - Lack-of cloud training and cloud governance
 - Domain Administrator account in use
- Things that enabled recovery
 - Network segmentation
 - Backups
 - Partnerships



RSA®Conference2020

Building Security Resilience

Colorado: Building Security Resilience

- New Endpoint Detection and Response toolset – across all agencies
- New CDOT firewall
- Firewall rules tightened across the state
- 2-Factor Authentication for all remote access and vendor access



Colorado: Building Security Resilience

We had the right efforts underway, but...

- We need to be **faster** at implementing security projects
- Need better controls in place for privileged accounts
- Need better cloud training and governance
- Need better visibility into internal traffic



Colorado: Building Security Resilience

Security Operations budget approved + \$11.8 Million

- The majority of the funding is for this year
- To implement the projects to fill known gaps
- Including necessary resources to implement quickly
- Ongoing annual cybersecurity budget raised to 5% of overall statewide IT spend



RSA®Conference2020

Recommendations for Building Security Resilience

What should you do now?

Building Security Resilience – Next Week

Next week you should:

- Chose a framework to help you benchmark where you are in your program
- Start forming those critical response partnerships
 - Who will you call when there is an incident?
 - Who will you share information and how will you do it?
 - Educate your Public Information Officer



Building Security Resilience – Next 3 Months

In the first three months following this presentation you should:

- Assess your program against those foundational elements
- Meet with your stakeholders to get their support and priorities
- Consult with your important partnerships to get their input
- Create your security strategy



Building Security Resilience – Next 6-12 Months

Within six to twelve months you should:

- Create a prioritized plan for implementing security improvements
- Build a business case to request funding
- Build a version of your security vision and roadmap that is high level and used to get stakeholder buy-in



RSA[®]Conference2020

Thank you! Questions?

Deborah.Blyth@state.co.us