# CITY HELD FOR RANSOM:

## Do Not Let This Happen to You!

**September 17, 2023**

65 YEARS
OF EXCELLENCE *and* COUNTING
IGFOA ANNUAL CONFERENCE
*peoria, il september 17-19, 2023*

# Speakers

**Dr. Linda Moore**, City Treasurer, *City of Quincy*

**Mr. Tony Collings**, Cybersecurity State Coordinator, *Cybersecurity & Infrastructure Security Agency* (CISA)

**Moderator: Elizabeth Holleb**, CPA, Finance Director and Treasurer, *City of Lake Forest*

# Learning Objectives

- Learn about the City of Quincy's ransomware experience;
- Identify best practices to keep communities safe from cyber threats;
- Understand the steps needed for an actionable emergency response plan; and
- Know where to go for help and resources.

# The Situation: City Under Attack

- Saturday, May 7, 2022
  - Technical difficulties or cyber attack?
    - Computers were “slow”
    - Servers became inaccessible
    - Police printers/computers not working
    - VOIP telephones stopped working
    - IT specialist was locked out of network and saw typing on boss’ computer screen, but boss was at home and not accessing the system
  - Immediate Response
    - Shut down all non-essential computers
    - Disconnect entire environment from the Internet
    - Disconnect from other locations to isolate City Hall network
    - City Administration notified
    - Begin assessment of damage
    - Monday morning
      - Employees told not to log in to the computers
      - Contacted cyber insurance carrier – followed their expert legal counsel advice and technical guidance (KROLL and Mullen Couglin)
      - Contacted FBI and other federal and state authorities as advised by expert legal counsel
    - Back to the old ways – paper journals, paper checks, no emails, no phones

# The Impact: Rumors Fly

- Monday, May 9 — Computers are down, no phones, no email – what's going on?
- Tuesday, May 10 — Media starts asking questions
  Bank personnel asking questions – engaged bank fraud prevention group
- Thursday, May 12 — Department Heads informed of cyber "incident" – no personal information
  - Financial systems unaffected
  - Stand alone laptop in one room for financial system access (G/L, payroll, A/P)
- Friday, May 13 — Employees Received a Letter that Payroll would be "manual"
  - All a/p checks also manual
  - With no file access, work arounds created for most processes
- Thursday, May 19 — Treasurer Told to Wire the Ransom – disguised as "Cyber Security Consulting Services"
- June 9 — Treasurer's Electronic Receipt Book available
- 6-9 weeks Later — Most departments were back online
  - Notified that archives were held and personal information could be jeopardized
  - Scope: Treasurer had 2371 files including pension files to review; Police had 5x that amount
- 6 months Later — Multi-factor authentication required for login
- 495 days Later — Still no QuickBooks Access, computer slowdowns standard, video surveillance unavailable, Still not 100%

# What You Need to Know:

- The Response Plan
  - Immediate Mitigation
  - Investigate the Impact
  - Communicate to Everyone
  - Adapt for Ongoing Operations
- Questions to Ask/Things to Do
  - Do you have Cyber Insurance? How much coverage?
  - Do you have a Crisis Management (Incident Response) Plan?
    - What is your role?
    - Do you have an Emergency Phone Tree?
  - Firewalls! Firewalls! Firewalls!
  - Don’t Wait - Tell the Truth!

U.S. Department of Homeland Security

# CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

DEFEND TODAY,
SECURE TOMORROW

PRESS ANY KEY!

# Ransomware Quiz

**When was the first Ransomware attack?**

# Ransomware – a brief history

- 1989 - It was delivered on floppy disk. Ransom - $189
- In 2010, ransomware was a little more a blip on most organization cybersecurity radar
- 2013, CryptoLocker appeared
- In 2020, ransomware jumped to the top of the list of threats

# SophosLabs – How Ransomware Attacks whitepaper 2019 Unit 42 Ransomware Threat Report 2022

**Dividing ransomware into categories**

**Cryptoworm** - A standalone ransomware that replicates itself to other computers for maximum reach and impact.

**Automated Active Adversary** – Here, the ransomware is deployed by attackers who use tools to automatically scan the internet for IT systems with weak protection. When such systems are found, the attackers establish a foothold and from there carefully plan the ransomware attack for maximum damage. For example, services that are openly exposed to the internet – like the Remote Desktop Protocol (RDP) – are a sought-after entry point as they are susceptible to a brute-force password-guessing attack. Although victims may believe they are targeted, the attack is usually opportunistic.

**Ransomware-as-a-Service (RaaS)** – A ransomware sold on the dark web as a distribution kit to anyone who can afford it. These RaaS packages allow people with little technical skill to attack with relative ease. They are typically deployed via malicious spam e-mails (malspam), via exploit kits as a drive-by download, or semi-manually by automated active adversaries.

# FinCEN – 2021 report

- FinCEN said there were 1,489 ransomware incidents costing nearly **$1.2 billion in 2021**, a substantial rise from $416 million in damages recorded in 2020, according to the report.
- FinCEN's analysis covers 2021, with a focus on the second half of the year. The agency said four of the overall top five ransomware attacks reported during this period are **tied to Russia**. Around 75% of ransomware-related incidents are also related to the country.

# 2023 CISA Alerts

JUL 12, 2023 CYBERSECURITY ADVISORY | AA23-193A - Enhanced Monitoring to Detect APT Activity Targeting Outlook Online

JUL 06, 2023 CYBERSECURITY ADVISORY | AA23-187A - Increased Truebot Activity Infects U.S. and Canada Based Networks

JUN 14, 2023 CYBERSECURITY ADVISORY | AA23-165A - Understanding Ransomware Threat Actors: LockBit

JUN 07, 2023 CYBERSECURITY ADVISORY | AA23-158A - #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability

MAY 24, 2023 CYBERSECURITY ADVISORY | AA23-144A - People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

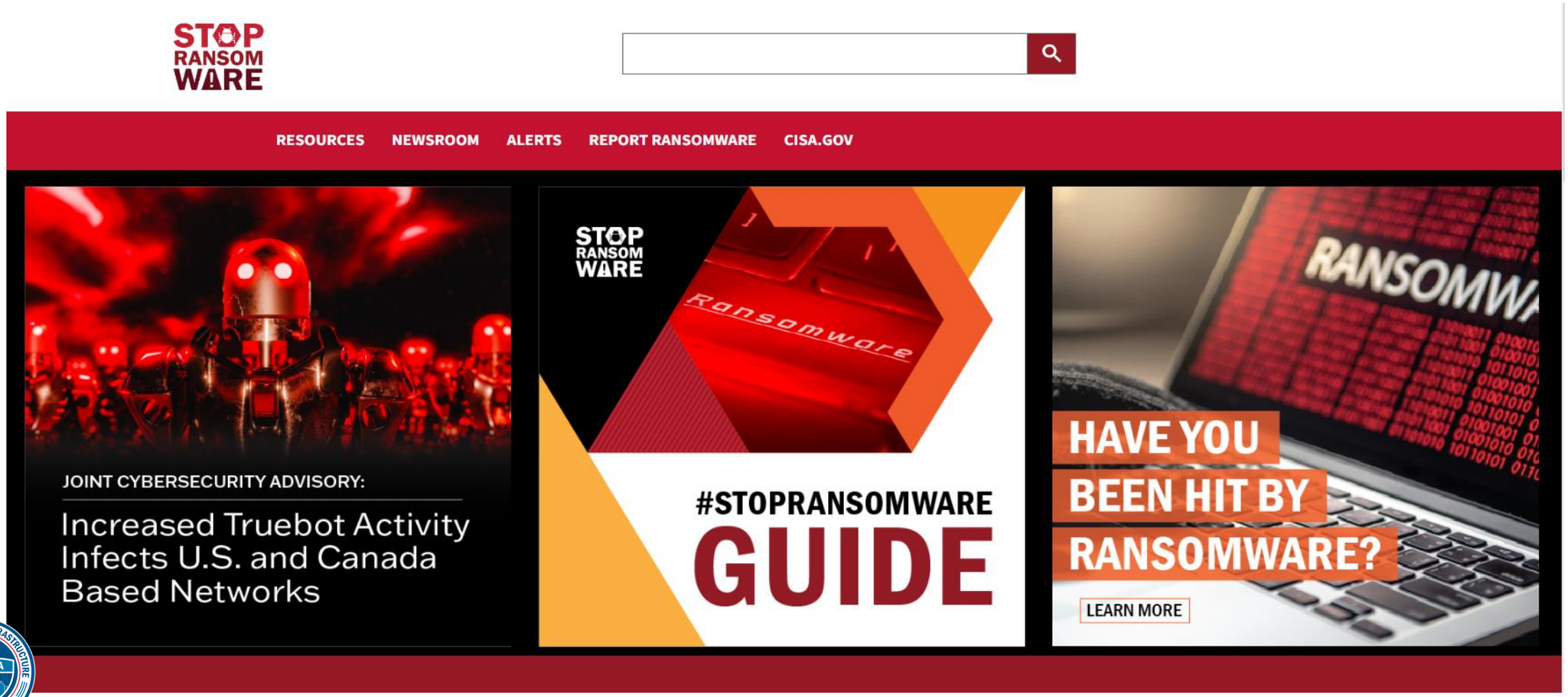
MAY 16, 2023 CYBERSECURITY ADVISORY | AA23-136A - #StopRansomware: BianLian Ransomware Group

MAY 11, 2023 CYBERSECURITY ADVISORY | AA23-131A - Malicious Actors Exploit CVE-2023-27350 in PaperCut MF and NG

MAY 09, 2023 CYBERSECURITY ADVISORY | AA23-129A - Hunting Russian Intelligence “Snake” Malware

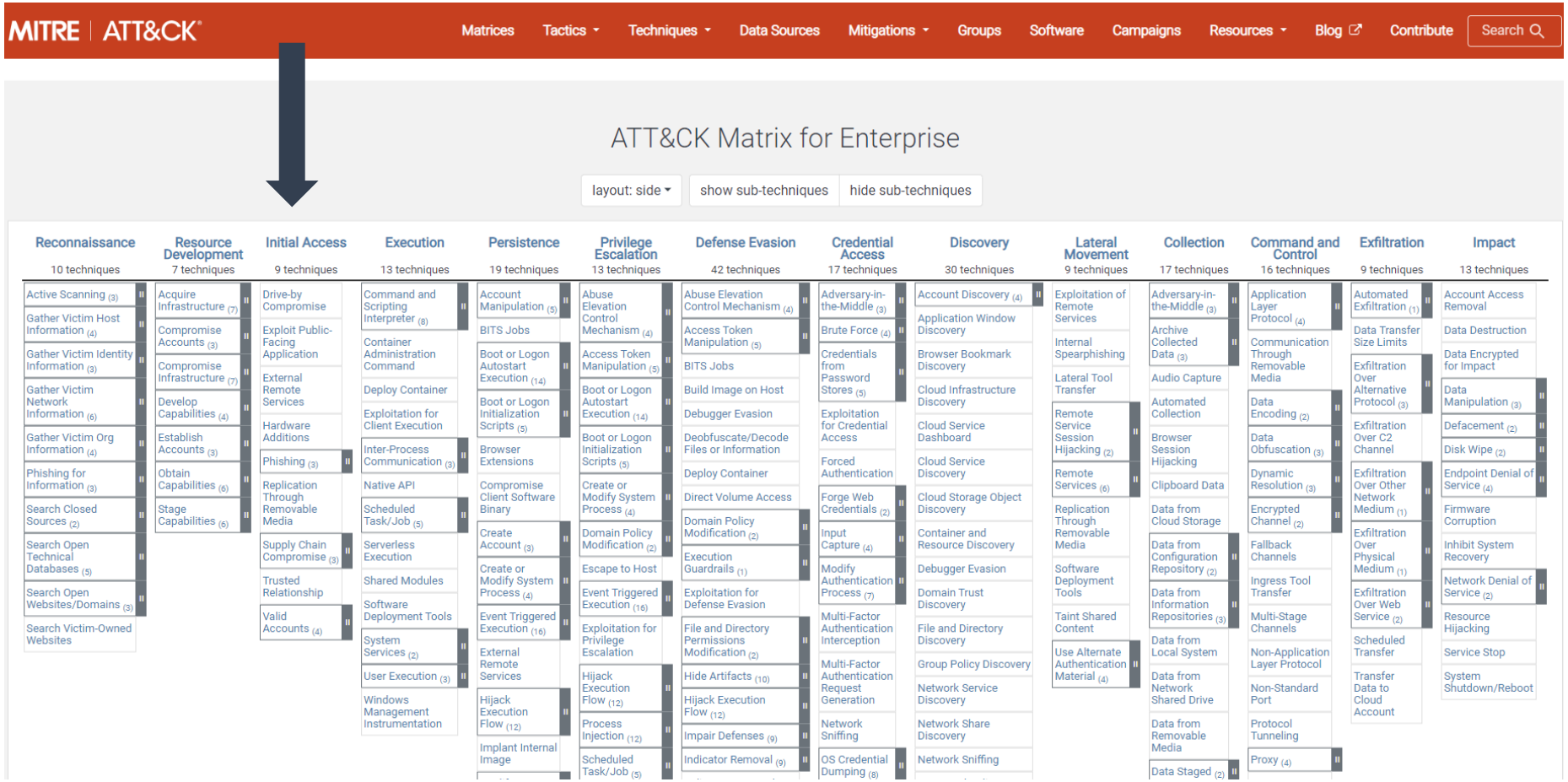
APR 18, 2023 CYBERSECURITY ADVISORY | AA23-108 - APT28 Exploits Known Vulnerability to Carry Out Reconnaissance and Deploy Malware on Cisco Routers

# Ransomware




https://www.cisa.gov/stopransomware

# MITRE ATT&CK




https://attack.mitre.org

# MITRE ATT&CK – Initial Access (9)

Phishing

Valid Accounts

External Remote Services

Replication Through Removable Media

Trusted Relationships

Hardware Additions

Drive-by Compromise

Supply Chain Compromise

Exploit Public-Facing Application

# MITRE ATT&CK – Initial Access (9)

Phishing

Valid Accounts

External Remote Services

Replication Through Removable Media

Trusted Relationships

Hardware Additions

Drive-by Compromise

Supply Chain Compromise

Exploit Public-Facing Application

# Phishing

- User training / continuous internal phishing campaigns
- Use Antivirus / Antimalware that can automatically quarantine suspicious files
- Disable Macros by Default
- Block attachment types like (.scr, .exe, .pif, . cpl) that are used for phishing

  If you can't block them – monitor use, consider an allow list of what programs can run in your environment

  (ISO, RAR, ZIP, LNK – containers – are the newest type of file being used)
- Use Network Intrusion Prevention System (NIPS) type products that can scan and remove malicious email attachments and links
- Software Configuration for email (anti-spoofing and authentication)

  SPF – IP addresses allowed to send for your domain

  DKIM – integrity of the message, signing email so it can be verified by recipient's mail

  DMARC – rules governing protecting domain from unauthorized use

# MITRE ATT&CK – Initial Access (9)

Phishing

Valid Accounts

External Remote Services

Replication Through Removable Media

Trusted Relationships

Hardware Additions

Drive-by Compromise

Supply Chain Compromise

Exploit Public-Facing Application

# External Remote Services

- Sign up for CISA's Cyber Hygiene (CyHy) vulnerability scanning – free

Change default user ids / passwords

- Disable or block remotely available services that are not used
- Require MFA for all remote access
- Limit Remote access to VPNs and other remote access services
- Network Segmentation / Firewall

# MITRE ATT&CK – Initial Access (9)

Phishing

Valid Accounts

External Remote Services

Replication Through Removable Media

Trusted Relationships

Hardware Additions

Drive-by Compromise

Supply Chain Compromise

Exploit Public-Facing Application

# Replication Through Removable Media

- Write a policy disallowing or restricting removable media without a written and approved business justification
  - Including cell phone connection with managed devices
- Limit the use of USB devices and removable media
  - Consider a “Box” type of service for external sharing of data, if needed
- Disable Autorun
- Block executables from running from a USB drive

# MITRE ATT&CK – Initial Access (9)

Phishing

Valid Accounts

External Remote Services

Replication Through Removable Media

Trusted Relationships

Hardware Additions

Drive-by Compromise

Supply Chain Compromise

Exploit Public-Facing Application

# Exploit Public Facing Applications

- Vulnerability Scans
  - IP – Sign up for CISA's Cyber Hygiene (CyHy) vulnerability scanning – free
- Change default user ids / passwords
- Patching (ongoing support) – Vulnerability Management Program
- Don't use unsupported / outdated systems
- Software Bill of Materials from vendors
- Secure by Design Coding
- 3rd Party application scanning and pen testing

# Incident Response

- Documented
- Tested
- Store it offline
  - Plan / Contacts / Configurations
- Updated based on Lessons Learned
- Don’t forget to notify external partners – CISA / FBI / Insurance Carrier
- Cyber Insurance – Know what you paid for!

# Incident Reporting

***STIC@illinois.gov or (877)-455-7842***

**When to Report:**

If there is a suspected or confirmed cyber attack or incident that:

- Affects core government or critical infrastructure functions;
- Results in the loss of data, system availability; or control of systems;
- Indication of malicious software present on critical systems

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

# We are the Nation's Risk Advisor

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure

Region 5 - Illinois
August 10, 2023

# THANK YOU & QUESTIONS

**Dr. Linda Moore**
City Treasurer, *City of Quincy*
lmoore@quincyil.gov

**Tony Collings**
Cybersecurity State Coordinator
*CISA*
tony.collings@cisa.dhs.gov

**CISA.Illinois.Cyber@cisa.dhs.gov**