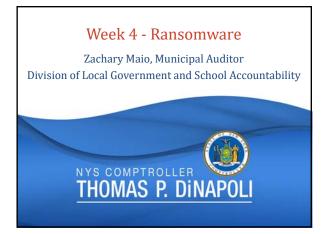
Cybersecurity for Local Governments and Schools A Weekly Cybersecurity Awareness Month Web Series NYS COMPTROLLER THOMAS P. DINAPOLI



Agenda

- Review of Wireless Technology & Security
- What is Ransomware?
- Headline Examples
- What is the impact?
- What can you do to lower your risk of becoming a victim of Ransomware?



What is Ransomware?

Ransomware - is a type of malware that when activated will encrypt all or most of your files and data so that it is inaccessible, or the system is inoperable. Following the encryption, a ransom is displayed requesting a monetary value in exchange for a key to decrypt your files and data.





Atlanta

- Largest successful breach of security on major American City affecting more than 6 million people SamSam relied on Brute-forcing rather than phishing
- Impacted Services include:

 - Utility Parking Court Services
 - Police Records
- Judicial systems Many legal documents and police dash cams were permanently deleted



Deployment: March 22nd, 2018

Strain: SamSam

Demand: ~\$50,000

Cost YTD: \$2.6 million+



Texas

- 22 (smaller) cities/towns were impacted by this
- That attack target was the Munis' Managed Service Provider (MSP) TSM Consulting Services
- MSPs are far more likely to pay ransomware demand
- Some services affected:

 - Financial Operations Birth/death certificates not available online

 - Cannot Accept payments
 One town stated ALL services were impacted
- The malware was suspected to propagate itself through TMS's update distribution system



Deployment: August 16th, 2019

Strain: Sodinokibi

Cost YTD: TBD

Demand: \$2.5 million



Albany

- Alerts were triggered immediately resulting in an
- immediate system shutdown City had <u>daily</u> backups of critical systems and servers Took 2-3 months for restore all City Systems (done in-

- Took 2-3 months for restore all City Systems (done inhouse)
 All computers/laptops were scanned prior to being put back online
 Legacy Systems were not rebuilt
 Rebuild costs consisted of:
 Destroyed servers
 Upgraded Security software
 Firewall Insurance
 Other improvements
 2021 Update: Impacts criminal cases as 2018 internal affairs files were lost



Deployment: March 30, 2019

Strain: Ryuk

Demand: \$76,000

Cost to date: \$300,000



CIA Triad

<u>Confidentiality</u> - Only authorized users and processes should be able to access or modify data

Integrity - Data should be maintained in a correct state and nobody should be able to improperly modify it, either accidentally or maliciously

Availability - Authorized users should be able to access data whenever they need to do so





Ransomware Evolution

<u>Double Extortion</u> - Before encrypting your files attackers will also exfiltrate your critical data and extort the victim to pay another monetary amount so that the data is not released publicly or sold to other cyber criminals.

- Increases from an incident to a breach
- Increases the urgency to pay at lease one of the monetary extortion rates
- Can we really trust that the information is being deleted as promised?





What can you, as an end user, do to help prevent Ransomware?

- Don't click links and open email attachments from unknown sources
- · Verify Email sender's address is legitimate
- Do not visit websites you are unfamiliar with
- · Spot and report phishing attempts
- Don't postpone updates
- Use strong passwords/don't reuse passwords
- · NEVER share your password
- Only use approved software and hardware
- Do not attempt to download software without approval
- Do not follow directions from callers claiming to be Microsoft or an IT vendor
- Don't plug in unknown USB drives



What can you, as an organization, do to help prevent the impacts of Ransomware?

- Restrict user access
 - "Principle of Least Privilege"
 - Limit administrative access
- Apply software patches and updates in a timely manner
 - Operating system
 - 3rd party software
- Install and maintain end point security products
- Implement strong password requirements
- Provide employees with cybersecurity training regularly
- Maintain offline and offsite backups
- Enable and review Audit logs
- Adopt a breach notification policy or local law
- Adopt IT Contingency plan



Resources

Office of the State Comptrollers Office https://www.osc.state.ny.us/files/localgovernment/publications/pdf/ransomware.pdf

Multi-State Information Sharing & Analysis Center (MS-ISAC) https://cisecurity.org/ms-isac/

National Institute of Standards and Technology (NIST)

https://mst.gov

New York State Office of Information Technology Services (NYS ITS) https://its.ny.gov

Cybersecurity and Infrastructure Security Agency (CISA)

https://www.cisa.gov/stopransomware

https://www.nomoreransom.org/en/index.html



Thank You Division of Local Government and School Accountability LGSAAppliedTech@osc.ny.gov