Lessons Learned: Ransomware in Atlanta

National Conference of State Legislatures
May 28, 2020

Jonathan Jesse, Senior Systems Engineer, Forescout
Yejin Jang, Government Affairs Director, Forescout
About Forescout + Speakers

Jonathan Jesse
Senior Systems Engineer, Forescout

Yejin Jang
Government Affairs Director, Forescout
Agenda

- Key Cybersecurity Principles
- Atlanta Ransomware Timeline
- Ransomware Details
- Lessons Learned
- Model Legislation (Texas HB 4214)
Center for Internet Security (CIS) Top 20 Controls

Source: https://www.cisecurity.org/controls/
**Timeline + Ransomware Details**

- **January 2018**
  - Audit results released
  - 100 government servers running unsupported Windows software

- **March 2018**
  - Atlanta announces ransomware attack

- **June 2018**
  - 424 applications not working (some critical)

- **Oct. 2018**
  - Gary Brantley starts as CIO

- **Nov. 2018**
  - DOJ indicts Iranian hackers
Stages of a SamSam Ransomware Outbreak

1) Vulnerability exists or remediating vulnerabilities not 100% complete/effective (SamSam uses JBOSS or RDP)

2) Exploitation/penetration occurs via stolen/compromised credentials (“brute force”)

3) Privileges elevated via Domain Controllers

4) Identify vulnerable systems-actor tests waters identifying those systems he can command, what systems are “manageable” via credentials (write a empty text file to a directory)

5) Deploy the Payload - executable, script

6) Execute Payload

7) Encrypt systems (e.g.-file extension changed to “.sorry”, “.imsorry”)

8) Demand Ransom

"Be aware of how your network is configured and what software you use on a regular basis. By knowing what your system looks like and how it works, you will be able to identify problems when they occur."

"Patch systems regularly and use automated patching when possible."

"Know what is connected to and running on your network."
Lessons Learned

CIS Controls™

Basic
1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational
17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Source: https://www.cisecurity.org/controls/

- Governance
  - People
  - Processes
  - Tools
- Disaster Recovery
- When it happens...
  - Communication
Sec. 2054.137. INFORMATION SECURITY CONTINUOUS MONITORING PROGRAM. (a) In this section:
(1) "Common control" means a security control that is inherited by one or more information resources technologies.
(2) "Program" means the information security continuous monitoring program described by this section.
(b) Each state agency shall:
(1) develop and maintain an information security continuous monitoring program that:
   (A) allows the agency to maintain ongoing awareness of the security and vulnerabilities of and threats to the agency’s information resources;
   (B) provides a clear understanding of organizational risk and helps the agency set priorities and manage the risk consistently;
   (C) addresses how the agency conducts ongoing authorizations of information resources technologies and the environments in which those technologies operate, including the agency’s use of common controls;
   (D) aligns with the continuous monitoring guidance, cybersecurity framework, and risk management framework published in Special Publications 800-137 and 800-53 by the United States Department of Commerce National Institute of Standards and Technology;
   (E) addresses critical security controls, including hardware asset management, software asset management, configuration management, and vulnerability management; and
   (F) requires the integration of cybersecurity products;
   (2) establish a strategy and plan to implement a program for the agency;
   (3) to the extent practicable, establish information security continuous monitoring as an agency-wide solution and deploy enterprise information security continuous monitoring products and services;
   (4) submit specified security-related information to the dashboard established under Subsection (c)(3);
   (5) evaluate and upgrade information resource technologies and deploy new products, including agency and component information security continuous monitoring dashboards, as necessary to support information security continuous monitoring and the need to submit security-related information requested by the department;
   (6) require that external service providers hosting state information meet state information security requirements for information security continuous monitoring; and
   (7) ensure the agency has adequate staff with the necessary training to meet the objectives of the program.
(c) The department shall:
(1) oversee the implementation of this section by each state agency;
(2) monitor and assist each state agency in implementation of a program and related strategies; and
(3) establish a statewide dashboard for information security continuous monitoring that provides:
   (A) a government-wide view of information security continuous monitoring; and
   (B) technical specifications and guidance for state agencies on the requirements for submitting information for purposes of the dashboard.
THANK YOU

Jonathan.Jesse@forescout.com
Yejin.Jang@forescout.com