9/4/2019

Georgia Department of Human Services

Office of Information Technology

Information Security Briefing

Ransomware

Venkat Krishnan, Chief Information Officer & Randy Coleburn, Chief Information Security Officer


stronger families
FOR A STRONGER GEORGIA

Agenda

- Ransomware
  - What is it?
  - How is it transmitted?
  - Recent Attacks—*The Threat is real!*
- How can we defend against ransomware?
- What are we doing now to protect the agency?
- What additional steps are we investigating?
- Responding to a ransomware attack

What is Ransomware?

- Malicious software that denies availability of information and/or systems until a ransom is paid
  - File encryption is most common approach
- Victims are faced with the choice of:
  - Paying untrustworthy criminals an expensive ransom to decrypt their files, or
  - Total loss – *unless unaffected backups are available for recovery*
- Even when backups are available:
  - Productivity is lost,
  - Reputation/customer trust is marred,
  - Recovery expenses are incurred, and
  - The business is disrupted

How is Ransomware transmitted?

- Most often, the entry vector is through “social-engineering” attacks sent via e-mail. (“the clever manipulation of the natural human tendency to trust”)

- Once the victim is tricked into downloading or executing the malware:
  - it leverages system vulnerabilities to spread across the enterprise undetected
  - before crippling operations and demanding the ransom

- Criminals create many ransomware variants to evade detection and thwart recovery.

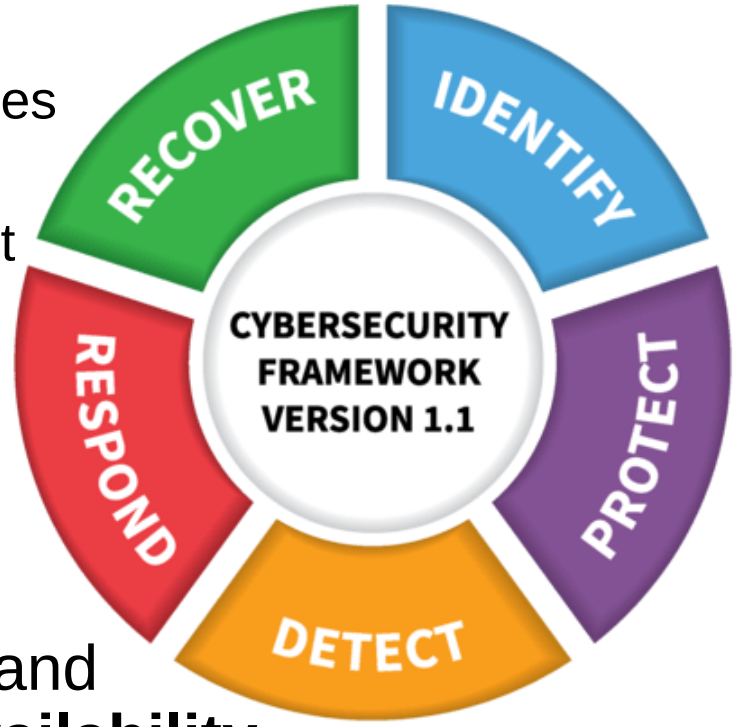
- “Ryuk” is a variant that recently has affected state and local governments. (Ryuk is a fictional character in the manga series *Death Note*)

Recent Attacks—*The threat is real!*

- July 24, 2019: Louisiana declares state of emergency after ransomware hit three public school districts.
- July 2019: Ransomware attacks in Georgia
  - Administrative Office of the Courts (AOC)
  - Lawrenceville Police Department
  - Henry County government
- April 2019: Augusta, Maine, suffered a highly-targeted malware attack that froze the city's entire network and forced the city center to close
- March 2019: Jackson County, Georgia, officials paid cybercriminals $400,000 after a cyberattack shut down the county's computer systems.
- 2018: City of Atlanta, Georgia, millions of dollars spent in repair costs + irretrievable data

How can we Defend against Ransomware?

- The NIST Cyber Security Framework (CSF) prescribes 5 core functions that form the basis of achieving cybersecurity outcomes, including protection against Ransomware.
  - **Identify**—you can't secure what you don't understand
  - **Protect**—implement safeguards to ensure delivery of critical services
  - **Detect**—identify occurrence of a cybersecurity event
  - **Respond**—take action to contain and limit the impact of an incident
  - **Recover**—maintain resilience and restore capabilities/services impaired by an incident



- Security practitioners devise a combination of **Preventative**, **Detective**, and **Corrective** security controls (applied before, during, and after an incident) using **People**, **Process**, and **Technology** to implement the CSF and achieve the objectives of **Confidentiality**, **Integrity** and **Availability**.

What are we doing at DHS to Prevent Ransomware?

- Keeping computers and software updated and patched
- Conducting routine vulnerability testing and hardening security configurations to meet federal guidelines
- Deployed new, scenario-based FY 2020 security awareness training:
  - Teaches users to exercise good judgment before clicking on hyperlinks in e-mails or downloading or opening e-mail attachments
  - Demonstrates how to avoid social-engineering attacks
  - Emphasizes access controls and provides techniques for strong passwords
  - Provides information on how to report incidents and suspected threats

What are we doing at DHS to Prevent Ransomware?

- Mandating all Data Sharing Agreements (DSAs) and all DHS websites and communications links to use Transport Layer Security (TLS) v1.2
- Using Trend-Micro Deep Security tool at NADC and for IES/Gateway to watch for indicators of compromise and block intrusion attempts
- Ensuring up-to-date McAfee Endpoint Security (ENS) on all systems
- Deploying McAfee Active Response (MAR) tool across DHS
- Reviewing / updating business continuity (BC) and disaster recovery (DR) plans and developing scenario-response playbooks

What are we doing at DHS to Prevent Ransomware?

- Enforcing host checks on all computers connecting via VPN
  - Current anti-virus/malware & patches
- Leveraging new GTA/GETS SOC* & SIEM* capabilities and event log correlation
- Using Microsoft Advanced Threat Protection for Office-365 and e-mail
- Additional rules enforced on emails with embedded links to run a security safety check when user attempts to open links

(*__SOC__ = Security Operation Center; __SIEM__ = Security Information & Event Management)

What additional steps are we investigating?

- Recommending that GTA/GETS:
  - Implement Domain Name System Security (DNSSEC) enterprise-wide
  - Implement standards for e-mail authentication, including:
    - **DMARC** = Domain-based Message Authentication, Reporting & Conformance
    - **SPF** = Sender Policy Framework
    - **DKIM** = Domain Keys Identified Mail

    These standards reduce e-mail fraud and impersonation.

- Planning to deploy additional, periodic security training and reinforcement using new Proofpoint platform available via GETS
- Application whitelisting and sandboxing
- Review network segmentation/quarantine capabilities with GTA/GETS

What additional steps are we investigating?

- Review backup schedules and isolation capabilities to ensure backups are adequate and isolated to prevent entry of ransomware

- Test all backups for successful, malware-free restoration
- Conduct incident response, business continuity and disaster recovery exercises
- Perform penetration testing (hacking) of computer systems and critical applications to discover and close security gaps
- Reduce/restrict usage of privileged admin accounts and automate elevation of privileges to install approved software and printers

Responding to a Ransomware Attack

- Isolate the infected computer immediately
  - Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking additional networked devices/data stores.
- Isolate or power-off affected devices that have not yet been corrupted
  - Affords more time to clean and recover data, contain damage, and prevent worsening conditions
- Immediately secure backup data or systems by taking them offline
  - Ensure backups are free of malware
- Engage additional resources as warranted
  - (e.g., National Guard, GBI, FBI, Homeland Security, MS-ISAC*)
- Change all online account passwords after removing infected system
- Implement incident response and business continuity plans

(*MS-ISAC = Multi-State Information Sharing & Analysis Center)

Questions?

Contact:

Venkat R. Krishnan
Chief Information Officer
Department of Human Services
Email: **Venkat.Krishnan@dhs.ga.gov**
Phone: 404-657-3759

Randy C. Coleburn
Chief Information Security Officer
Department of Human Services
Email: **Randy.Coleburn@dhs.ga.gov**
Phone: 404-651-9876