Ransomware

Malware that infects computers and encrypts files until ransom is paid and attempts to spread to all connected systems and storage devices

Common Methods Used to Infect Devices

- **Phishing** emails tempting a user to click a corrupt link or open an infected attachment.
- "**Drive-by downloads**" - a program that automatically downloads from the internet without consent.
- **Internet-facing vulnerabilities** - devices and applications exposed to the internet increase risks and attack surface.
- **Misconfigured devices** – devices set up with unnecessary ports, protocols, accounts, and configurations.

Prevent Methods with Basic Cyber Hygiene

- **Know your data responsibilities.** Define data types (FCI, CUI, ECI, Classified, etc.). Document reporting requirements for associated federal entities. Keep internal and external contacts up-to-date, including law enforcement.
- Complete annual **Business Impact Analysis, Continuity Planning, Test Effectiveness**: define critical information and assets, set maximum tolerable downtime, and map interconnections.
- **Patch promptly**. Scan vulnerabilities weekly, prioritize and patch promptly, and segment systems which cannot be patched. Hold your organization resources accountable for addressing vulnerabilities promptly and reducing risks to the organization.
- **Back up Data** – set up regular (daily) isolated, encrypted backups requiring MFA to access.
- Prepare and Practice **Incident Response and Recovery** Plans – prepare for incident response and test restoring systems from backups.
- Run up-to-date **virus scanning** software with current signatures. Automatically scan downloads, emails, and flash drives.
- **Delete Suspect Emails** – Educate users to ID suspicious emails, not click, and report. Use email filtering tools.
- Use **Multi-factor Authentication** (MFA) on all devices and accounts. Make sure account holders with privileged access maintain a separate account for privileged account functions. Avoid using privileged accounts on standard activities (emailing, and Internet browsing) where possible. Use the **least user privilege** model.
- **Secure Your Server Message Block** (SMB) – SMB vulnerabilities allow their payloads to spread laterally through connected systems like a worm. Disable SMB protocols to prevent ransomware and other malware attacks.
- **Security Operations Center (SOC)** Capabilities – maintain up to date threat intelligence and respond to potential threats with a robust cybersecurity tool stack. If you do not have a SOC, ensure that the basic security functions are implemented.
- **Map interconnected systems** – make sure you know how systems are connected whether the systems are in your network, in the cloud, or connected from an externally managed network. For connections you do not control, **flow down all contractual requirements** and ensure each organizations knows their roles and responsibilities. Externally hosted (software as a service, infrastructure as a service, etc.) information systems should have a customer responsibility matrix that the organization supplies to you.
- **Disable unnecessary ports, protocols, and accounts** and change default account passwords.
- Pay attention to what devices are **internet enabled** – document IoT devices, its purpose, and disable unnecessary functions. **Segment the network with defense in depth practices**. Separate Operational Technology from Information Technology.
- **Block access** to known ransomware sites and be cautious of unknown sources.
- **Restrict unauthorized** devices, apps, software, and accounts. Use caution for BYOD programs and when teleworking.

Checklist for Guarding Against Ransomware

Planning, Prevention, and Preparation

- ☐ Maintain up-to-date inventory
  - ☐ Inventory of all IT and OT hardware, software, and firmware
  - ☐ Complete annual Business Continuity Plans and exercises: define critical assets, location of sensitive and critical data, and maximum tolerable downtime
  - ☐ Define all system interconnections
  - ☐ Ensure operational technology is segmented from information technology
  - ☐ Limit Internet exposure to reduce attack landscape where possible
  - ☐ Conduct Data Inventory
    - ☐ Create data flow map
    - ☐ Define data types, associated protection requirements, and reporting requirements
    - ☐ Define data ownership. If Federal Information or Federal Information Systems are involved, document Federal oversight points of contact (Cybersecurity, Safeguards and Security, Counterintelligence, and Officially Designated Federal Security Authority (ODFSA)) for notifications and obtain applicable departmental incident response procedures to follow, such as notification to iJC3 and IARC (as applicable)
- ☐ Prepare and Practice Incident Response and Recovery Plans – make sure that you have planned out all activities surrounding responding to incidents and test restoring systems from backups
- ☐ Conduct a Privacy Needs Assessment and Privacy Impact Assessment
- ☐ Maintain up-to-date network drawings and data flow diagrams
- ☐ Prevent unauthorized devices from connecting to the network
- ☐ Prevent unauthorized software from being installed
- ☐ Use Multi-factor Authentication (MFA) where possible
- ☐ Ensure all devices are running up-to-date anti-virus/anti-malware software
- ☐ Document all third-party providers (Software-as-a-Service, Platform-as-a-Service, Infrastructure-as-a-Service) to include all data types involved and network connections
  - ☐ Flow down all relevant contractual requirements to third-party providers
  - ☐ Complete a customer responsibility matrix with cloud providers to define roles & responsibilities
- ☐ Use email filtering tools to filter out spam and block spoofed emails and invalid domains (consider software that isolates files during on-access scans)
- ☐ Educate users to identify suspicious emails and respond to suspect emails (don't click, report immediately)
- ☐ Subscribe to intelligence data feeds that provides up-to-date information of known malicious websites and current attack techniques
- ☐ Act on intelligence data (block malicious sites, look for indicators of compromise)
- ☐ Change default device passwords, disable unnecessary ports, protocols, and remove unnecessary accounts
- ☐ Back up Data – set up regular (daily) offline, encrypted backups, and test backups to validate
- ☐ Conduct weekly vulnerability scans, prioritize and address vulnerabilities
- ☐ Patch promptly, including third-party software and firmware patching
- ☐ Encrypt data at rest and in transit
- ☐ Store backups in an encrypted format separate from the network
- ☐ Disable SMB protocols to prevent ransomware and other malware attacks
- ☐ Implement or subscribe to a Security Operations Center
- ☐ Utilize enhanced logging and alert for potential anomalous activities
- ☐ Control BYOD and implement secure telework policies.

Reporting Requirements when Federal Information or Federal Information Systems are involved

☐ Notify the appropriate cybersecurity personnel, safeguards and security personnel, and executive leadership, and provide regular updates

☐ Notify the appropriate Federal oversight individuals from Cybersecurity, Safeguards and Security, and/or Counterintelligence. Provide regular updates

☐ Follow Federal reporting requirements such as reporting the incident to iJC3

☐ Consult with Federal oversight personnel on reporting to the FBI, IG, and law enforcement agencies

☐ Based on requests and approval from the ODFSA, request assistance from CISA; MS-ISAC; and local, state, or federal law enforcement (e.g., Federal Bureau of Investigation [FBI], U.S. Secret Service [USSS])

☐ Refrain from external communications to the public or media without appropriate Federal approvals. Ensure that all staff know what to say if contacted by the media

☐ Notify relevant stakeholders such as IT departmental resources, managed service providers, cyber insurance company, and departmental leaders

Reporting Requirements when Federal Information or Federal Information Systems are **NOT** involved

☐ Notify the appropriate cybersecurity personnel, safeguards and security personnel, and executive leadership. Provide regular updates

☐ If extended identification or analysis is needed, CISA, MS-ISAC and local, state, or federal law enforcement may be interested in any of the following information that your organization determines it can legally share:

- Recovered executable file
- Copies of the readme file – DO NOT REMOVE the file or decryption may not be possible
- Live memory (RAM) capture from systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally)
- Images of infected systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally)
- Malware samples
- Names of any other malware identified on your system
- Encrypted file samples
- Log files (Windows Event Logs from compromised systems, Firewall logs, etc.)
- Any PowerShell scripts found having executed on the systems
- Any user accounts created in Active Directory or machines added to the network during the exploitation
- Email addresses used by the attackers and any associated phishing emails
- A copy of the ransom note
- Ransom amount and whether the ransom was paid
- Bitcoin wallets used by the attackers
- Bitcoin wallets used to pay the ransom (if applicable)
- Copies of any communications with attackers

☐ Refrain from external communications to the public or media without appropriate Federal approvals. Ensure that all staff know what to say if contacted by the media

☐ Notify relevant stakeholders such as IT departmental resources, managed service providers, cyber insurance company, and departmental leaders

Containment and Analysis

- ☐ Determine what systems, information, and users are impacted
- ☐ Isolate impacted systems and user accounts
- ☐ To prevent unauthorized monitoring, use out of band communications such as cellular phones
- ☐ Maintain chain of custody of affected systems and information. Take care to preserve evidence that is highly volatile in nature—or limited in retention—to prevent loss or tampering (e.g., system memory, Windows Security logs, data in firewall log buffers)
- ☐ Take a system image and memory capture of a sample of affected devices (e.g., workstations and servers)
- ☐ Collect any relevant logs as well as samples of any "precursor" malware binaries and associated observables or indicators of compromise (e.g., suspected command and control IP addresses, suspicious registry entries, or other relevant files detected)
- ☐ Consult federal law enforcement regarding possible decryptors available
- ☐ Research the trusted guidance (i.e., published by sources such as government, MS-ISAC, reputable security vendor, etc.) for the ransomware variant and follow any additional recommended steps to identify and contain systems or networks that are confirmed to be impacted
- ☐ Kill or disable the execution of known ransomware binaries; this will minimize damage and impact to your systems. Delete other known, associated registry values and files
- ☐ Disable VPN's, remote access servers, single sign-on resources, and cloud-based or other public facing assets
- ☐ In the event you learn that server-side data is being encrypted by an infected workstation, quick-identification steps are to:
    - ☐ Review Computer Management > Sessions and Open Files lists on associated servers to determine the user or system accessing those files
    - ☐ Review file properties of encrypted files or ransom notes to identify specific users that may be associated with file ownership
    - ☐ Review the TerminalServices-RemoteConnectionManager event log to check for successful RDP network connections
    - ☐ Review the Windows Security log, SMB event logs, and any related logs that may identify significant authentication or access events
    - ☐ Run Wireshark on the impacted server with a filter to identify IP addresses involved in actively writing or renaming files (e.g., "smb2.filename contains cryptxxx")
    - ☐ Conduct an examination of existing organizational detection or prevention systems (antivirus, Endpoint Detection & Response, IDS, Intrusion Prevention System, etc.) and logs. Doing so can highlight evidence of additional systems or malware involved in earlier stages of the attack
- ☐ Look for evidence of precursor "dropper" malware. A ransomware event may be evidence of a previous, unresolved network compromise. Many ransomware infections are the result of existing malware infections such as TrickBot, Dridex, or Emotet. - Operators of these advanced malware variants will often sell access to a network
- ☐ Conduct extended analysis to identify outside-in and inside-out persistence mechanisms
    - Outside-in persistence may include authenticated access to external systems via rogue accounts, backdoors on perimeter systems, exploitation of external vulnerabilities, etc
    - Inside-out persistence may include malware implants on the internal network or a variety of living-off-the-land style modifications (e.g., use of commercial penetration testing tools like Cobalt Strike; use of PsTools suite, including PsExec, to remotely install and control malware and gather information regarding—or perform remote management of—Windows systems; use of PowerShell scripts)
    - Identification may involve deployment of endpoint detection and response solutions, audits of local and domain accounts, examination of data found in centralized logging systems, or deeper forensic analysis of specific systems once movement within the environment has been mapped out

Recovery

☐ Rebuild systems based on a prioritization of critical services (e.g., health and safety or revenue generating services), using pre-configured standard images, if possible. This should be already defined in the Contingency Plan and Business Impact Analysis

☐ After the rebuild completes, issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility

☐ Apply patches, upgrade software, and take other security precautions not previously taken

☐ Reconnect systems and restore data from offline, encrypted backups based on a prioritization of critical services. Be careful not to re-infect clean systems during recovery. For example, if a new Virtual Local Area Network has been created for recovery purposes, ensure only clean systems are added to it

☐ Closely monitor traffic and proceed with caution, promptly responding to any anomalous behavior

Post-Incident Activities

☐ Document lessons learned from the incident and associated response activities to inform updates to—and refine—organizational policies, plans, and procedures and guide future exercises of the same

☐ Consider sharing lessons learned and relevant indicators of compromise with CISA and other trusted agencies

References and Resources

- DOE O 205.1C. 1.
- Cybersecurity Act of 2015, Pub. L. No. 114-113, enacted 12-18-2015.
- Presidential Policy Directive (P.P.D) 41, Federal Government Coordination Architecture for Significant Cyber Incidents, dated 7-26-2016.
- E.O. 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, dated 5-11-2017.
- US-CERT,0 Federal Incident Notification Guidelines, dated 4-1-2017.
- DOE O 150.1A, Continuity Programs.
- DOE O 470.4, Safeguards and Security Program.
- DOE O 471.6, Information Security.
- DOE O 473.3, Protection Program Operations.
- CNSS Policies, Directives, Instructions and Issuances located at https://www.cnss.gov/CNSS/
- NIST Framework for Improving Critical Infrastructure Cybersecurity.
- NIST FIPS 140-2, Security Requirements for Cryptographic Modules.
- NIST SP 800-34, Contingency Planning Guide for Federal Information Systems.
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View.
- NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.
- NIST SP 800-61, Computer Security Incident Handling Guide.
- NIST SP 800-82, Guide to Industrial Control System (ICS) Security.
- NIST SP 800-150, Guide to Cyber Threat Information Sharing
- NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.
- Upon voluntary request, CISA and MS-ISAC can assist with analysis (e.g., phishing emails, storage media, logs, malware) at no cost in understanding the root cause of an incident, even in the event additional remote assistance is not requested:
    - CISA – Advanced Malware Analysis Center: https://www.malware.uscert.gov/MalwareSubmission/ pages/submission.jsf
    - MS-ISAC – Malicious Code Analysis Platform (SLTT organizations only): https://www.cisecurity.org/ spotlight/cybersecurity-spotlightmalware-analysis/
        - Scans a suspicious file or Uniform Resource Locator (URL) against several antivirus vendors to determine if it matches known malicious signatures
        - Runs a file or URL in a sandbox to analyze behavior
        - Provides a user with a summary report of malware behavior, including files accessed, tasks created, outbound connections, and other behavioral traits
        - Users can opt to keep submissions private and make direct requests for assistance from MS-ISAC; users can also mark submissions for sharing with CISA Email: mcap@cisecurity.org to set up an account
        - Remote Assistance – Request via CISA Central or MS-ISAC Security Operations Center – Request via CISA Central or MS-ISAC Security Operations Center