RANSOMWARE GUIDE

SEPTEMBER 2020

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Overview

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. In recent years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.

Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. Malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion. The monetary value of ransom demands has also increased, with some demands exceeding US $1 million. Ransomware incidents have become more destructive and impactful in nature and scope. Malicious actors engage in lateral movement to target critical data and propagate ransomware across entire networks. These actors also increasingly use tactics, such as deleting system backups, that make restoration and recovery more difficult or infeasible for impacted organizations. The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organizations large and small.

These ransomware best practices and recommendations are based on operational insight from the Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC). The audience for this guide includes information technology (IT) professionals as well as others within an organization involved in developing cyber incident response policies and procedures or coordinating cyber incident response.

This *Ransomware Guide* includes two resources:
Part 1: Ransomware Prevention Best Practices
Part 2: Ransomware Response Checklist

CISA recommends that organizations take the following initial steps:

- Join an information sharing organization, such as one of the following:
  - Multi-State Information Sharing and Analysis Center (MS-ISAC): **https://learn.cisecurity.org/ms-isac-registration**
  - Election Infrastructure Information Sharing and Analysis Center (EI-ISAC): **https://learn.cisecurity.org/ei-isac-registration**
  - Sector-based ISACs - National Council of ISACs: **https://www.nationalisacs.org/member-isacs**
  - Information Sharing and Analysis Organization (ISAO) Standards Organization: **https://www.isao.org/information-sharing-groups/**
- Engage CISA to build a lasting partnership and collaborate on information sharing, best practices, assessments, exercises, and more.
  - SLTT organizations: **CyberLiaison_SLTT@cisa.dhs.gov**
  - Private sector organizations: **CyberLiaison_Industry@cisa.dhs.gov**

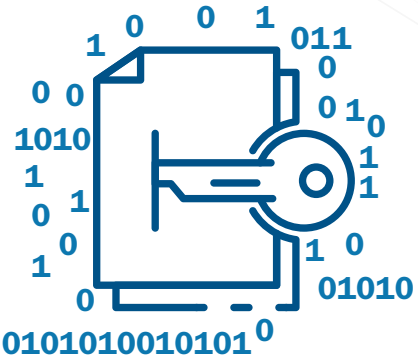
Engaging with your ISAC, ISAO, and with CISA will enable your organization to receive critical information and access to services to better manage the risk posed by ransomware and other cyber threats.

Part 1: Ransomware Prevention Best Practices

Be Prepared

Refer to the best practices and references below to help manage the risk posed by ransomware and support your organization's coordinated and efficient response to a ransomware incident. Apply these practices to the greatest extent possible based on availability of organizational resources.

- It is critical to maintain offline, encrypted backups of data and to regularly test your backups. Backup procedures should be conducted on a regular basis. It is important that backups be maintained offline as many ransomware variants attempt to find and delete any accessible backups. Maintaining offline, current backups is most critical because there is no need to pay a ransom for data that is readily accessible to your organization.
  - Maintain regularly updated "gold images" of critical systems in the event they need to be rebuilt. This entails maintaining image "templates" that include a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.
  - Retain backup hardware to rebuild systems in the event rebuilding the primary system is not preferred.
    - Hardware that is newer or older than the primary system can present installation or compatibility hurdles when rebuilding from images.
  - In addition to system images, applicable source code or executables should be available (stored with backups, escrowed, license agreement to obtain, etc.). It is more efficient to rebuild from system images, but some images will not install on different hardware or platforms correctly; having separate access to needed software will help in these cases.
- Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident.
  - Review available incident response guidance, such as the *Public Power Cyber Incident Response Playbook* (**https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf**), a resource and guide to:
    - Help your organization better organize around cyber incident response, and
    - Develop a cyber incident response plan.
  - The Ransomware Response Checklist, which forms the other half of this *Ransomware Guide*, serves as an adaptable, ransomware-specific annex to organizational cyber incident response or disruption plans.



Ransomware Infection Vector: Internet-Facing Vulnerabilities and Misconfigurations

- Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface.
  - CISA offers a no-cost Vulnerability Scanning service and other no-cost assessments: **https://www.cisa.gov/cyber-resource-hub**.
- Regularly patch and update software and OSs to the latest available versions.
  - Prioritize timely patching of internet-facing servers—as well as software processing internet data, such as web browsers, browser plugins, and document readers—for known vulnerabilities.
- Ensure devices are properly configured and that security features are enabled. For example, disable ports and protocols that are not being used for a business purpose (e.g., Remote Desktop Protocol [RDP] – Transmission Control Protocol [TCP] Port 3389).
- Employ best practices for use of RDP and other remote desktop services. Threat actors often gain initial access to a network through exposed and poorly secured remote services, and later propagate ransomware. See CISA Alert AA20-073A, Enterprise VPN Security (**https://us-cert.cisa.gov/ncas/alerts/aa20-073a**).
  - Audit the network for systems using RDP, close unused RDP ports, enforce account lockouts after a specified number of attempts, apply multi-factor authentication (MFA), and log RDP login attempts.
- Disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB. Threat actors use SMB to propagate malware across organizations. Based on this specific threat, organizations should consider the following actions to protect their networks:
  - Disable SMBv1 and v2 on your internal network after working to mitigate any existing dependencies (on the part of existing systems or applications) that may break when disabled.
    - Remove dependencies through upgrades and reconfiguration: Upgrade to SMBv3 (or most current version) along with SMB signing.
  - Block all versions of SMB from being accessible externally to your network by blocking TCP port 445 with related protocols on User Datagram Protocol ports 137–138 and TCP port 139.

Ransomware Infection Vector: Phishing

- Implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity (e.g., phishing) or incidents. Conduct organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails.
- Implement filters at the email gateway to filter out emails with known malicious indicators, such as known malicious subject lines, and block suspicious Internet Protocol (IP) addresses at the firewall.
- To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification. DMARC builds on the widely deployed sender policy framework and Domain Keys Identified Mail protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email.
- Consider disabling macro scripts for Microsoft Office files transmitted via email. These macros can be used to deliver ransomware.

Ransomware Infection Vector: Precursor Malware Infection

- Ensure antivirus and anti-malware software and signatures are up to date. Additionally, turn on automatic updates for both solutions. CISA recommends using a centrally managed antivirus solution. This enables detection of both "precursor" malware and ransomware.
  - A ransomware infection may be evidence of a previous, unresolved network compromise. For example, many ransomware infections are the result of existing malware infections, such as TrickBot, Dridex, or Emotet.
  - In some cases, ransomware deployment is just the last step in a network compromise and is dropped as a way to obfuscate previous post-compromise activities.
- Use application directory allowlisting on all assets to ensure that only authorized software can run, and all unauthorized software is blocked from executing.
  - Enable application directory allowlisting through Microsoft Software Restriction Policy or AppLocker.
  - Use directory allowlisting rather than attempting to list every possible permutation of applications in a network environment. Safe defaults allow applications to run from PROGRAMFILES, PROGRAMFILES(X86), and SYSTEM32. Disallow all other locations unless an exception is granted.
- Consider implementing an intrusion detection system (IDS) to detect command and control activity and other potentially malicious network activity that occurs prior to ransomware deployment.

CISA offers a no-cost Phishing Campaign Assessment and other no-cost assessments: **https://www.cisa.gov/cyber-resource-hub**.

For more information on DMARC, see: **https://www.cisecurity.org/blog/how-dmarc-advances-email-security/** and

https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-EnhanceEmailandWebSecurity_S508C.pdf.

Funded by CISA, the MS-ISAC and EI-ISAC provide the Malicious Domain Blocking and Reporting (MDBR) service at no-cost to members. MDBR is a fully managed proactive security service that prevents IT systems from connecting to harmful web domains, which helps limit infections related to known malware, ransomware, phishing, and other cyber threats. To sign up for MDBR, visit: **https://www.cisecurity.org/ms-isac/services/mdbr/.**

CISA and MS-ISAC encourage SLTT organizations to consider the Albert IDS to enhance a defense-in-depth strategy. CISA funds Albert sensors deployed by the MS-ISAC, and we encourage SLTT governments to make use of them. Albert serves as an early warning capability for the Nation's SLTT governments and supports the nationwide cybersecurity situational awareness of CISA and the Federal Government. For more information regarding Albert, see: **https://www.cisecurity.org/services/albert-network-monitoring/.**

Ransomware Infection Vector: Third Parties and Managed Service Providers

- Take into consideration the risk management and cyber hygiene practices of third parties or managed service providers (MSPs) your organization relies on to meet its mission. MSPs have been an infection vector for ransomware impacting client organizations.
  - If a third party or MSP is responsible for maintaining and securing your organization's backups, ensure they are following the applicable best practices outlined above. Using contract language to formalize your security requirements is a best practice.
- Understand that adversaries may exploit the trusted relationships your organization has with third parties and MSPs. See CISA's APTs Targeting IT Service Provider Customers (**https://us-cert.cisa.gov/APTs-Targeting-IT-Service-Provider-Customers**).
  - Adversaries may target MSPs with the goal of compromising MSP client organizations; they may use MSP network connections and access to client organizations as a key vector to propagate malware and ransomware.
  - Adversaries may spoof the identity of—or use compromised email accounts associated with—entities your organization has a trusted relationship with in order to phish your users, enabling network compromise and disclosure of information.

General Best Practices and Hardening Guidance

- Employ MFA for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.
  - If you are using passwords, use strong passwords (**https://us-cert.cisa.gov/ncas/tips/ST04-002**) and do not reuse passwords for multiple accounts. Change default passwords. Enforce account lockouts after a specified number of login attempts. Password managers can help you develop and manage secure passwords.
- Apply the principle of least privilege to all systems and services so that users only have the access they need to perform their jobs. Threat actors often seek out privileged accounts to leverage to help saturate networks with ransomware.
  - Restrict user permissions to install and run software applications.
  - Limit the ability of a local administrator account to log in from a local interactive session (e.g., "Deny access to this computer from the network.") and prevent access via an RDP session.

- Remove unnecessary accounts and groups and restrict root access.
- Control and limit local administration.
- Make use of the Protected Users Active Directory group in Windows domains to further secure privileged user accounts against pass-the-hash attacks.
- Audit user accounts regularly, particularly Remote Monitoring and Management accounts that are publicly accessible—this includes audits of third-party access given to MSPs.

- Leverage best practices and enable security settings in association with cloud environments, such as Microsoft Office 365 (**https://www.us-cert.cisa.gov/ncas/alerts/aa20-120a**).
- Develop and regularly update a comprehensive network diagram that describes systems and data flows within your organization's network (see figure 1). This is useful in steady state and can help incident responders understand where to focus their efforts.
  - The diagram should include depictions of covered major networks, any specific IP addressing schemes, and the general network topology (including network connections, interdependencies, and access granted to third parties or MSPs).
- Employ logical or physical means of network segmentation to separate various business unit or departmental IT resources within your organization as well as to maintain separation between IT and operational technology.

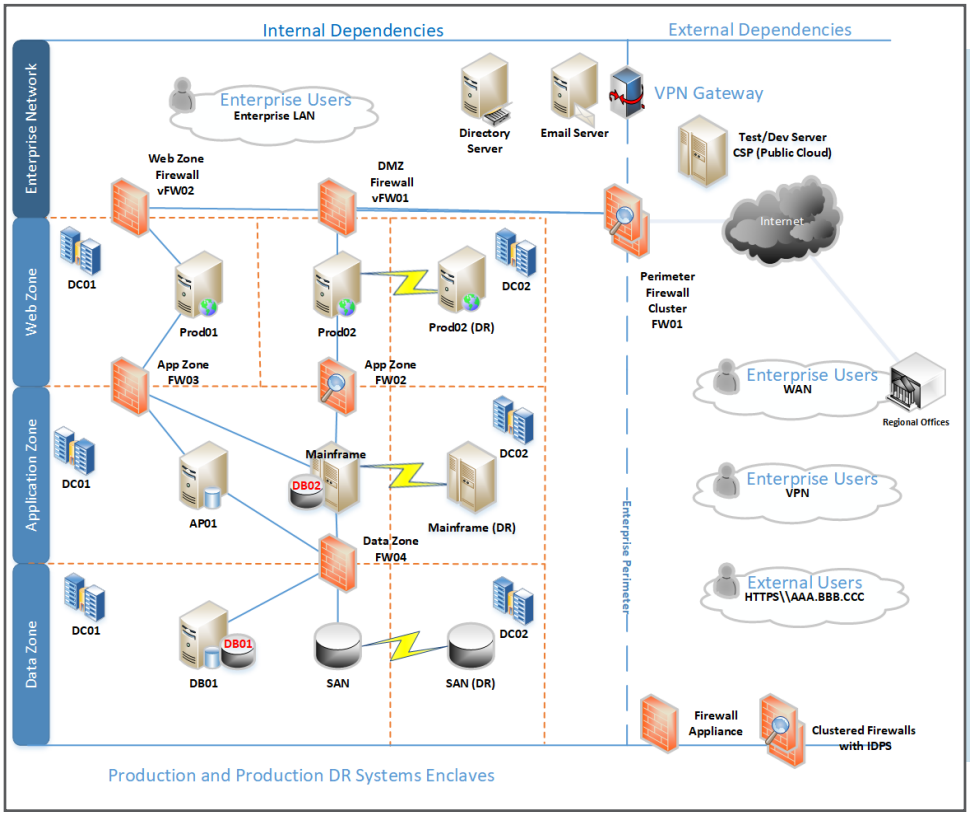


Figure 1. Example Network Diagram

This will help contain the impact of any intrusion affecting your organization and prevent or limit lateral movement on the part of malicious actors. See figures 2 and 3 for depictions of a flat (unsegmented) network and of a best practice segmented network.

- Network segmentation can be rendered ineffective if it is breached through user error or non-adherence to organizational policies (e.g., connecting removable storage media or other devices to multiple segments).

- Ensure your organization has a comprehensive asset management approach.
  - Understand and inventory your organization's IT assets, both logical (e.g., data, software) and physical (e.g., hardware).
  - Understand which data or systems are most critical for health and safety, revenue generation, or other critical services, as well as any associated interdependencies (i.e., "critical asset or system list"). This will aid your organization in determining restoration priorities should an incident occur. Apply more comprehensive security controls or safeguards to critical assets. This requires organization-wide coordination.
  - Use the MS-ISAC Hardware and Software Asset Tracking Spreadsheet: **https://www.cisecurity.org/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet/**.

- Restrict usage of PowerShell, using Group Policy, to specific users on a case-by-case basis. Typically, only those users or administrators who manage the network or Windows OSs should be permitted to use PowerShell. Update PowerShell and enable enhanced logging. PowerShell is a cross-platform, command-line, shell and scripting language that is a component of Microsoft Windows. Threat actors use PowerShell to deploy ransomware and hide their malicious activities.
  - Update PowerShell instances to version 5.0 or later and uninstall all earlier PowerShell versions. Logs from PowerShell prior to version 5.0 are either non-existent or do not record enough detail to aid in enterprise monitoring and incident response activities.
    - PowerShell logs contain valuable data, including historical OS and registry interaction and possible tactics, techniques, and procedures of a threat actor's PowerShell use.
  - Ensure PowerShell instances (use most current version) have module, script block, and transcription logging enabled (enhanced logging).

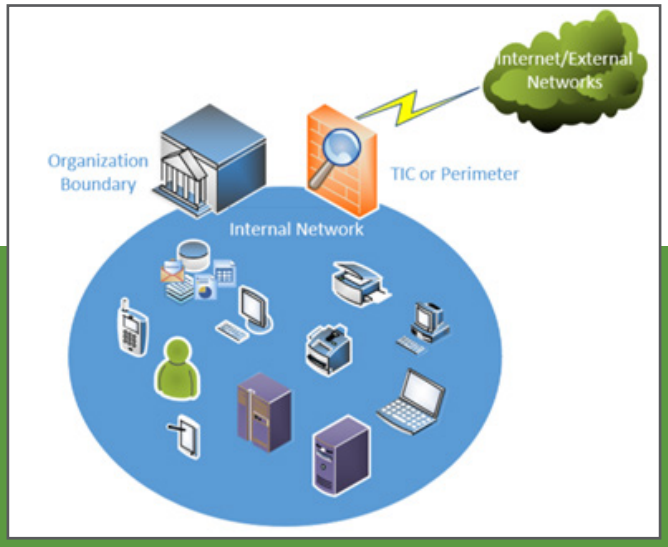


Figure 2. Flat (Unsegmented) Network

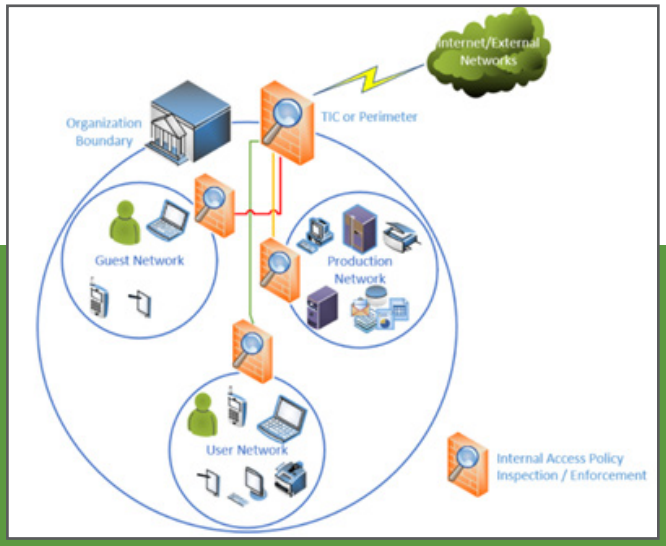


Figure 3. Segmented Network

- The two logs that record PowerShell activity are the “PowerShell” Windows Event Log and the “PowerShell Operational” Log. CISA recommends turning on these two Windows Event Logs with a retention period of 180 days. These logs should be checked on a regular basis to confirm whether the log data has been deleted or logging has been turned off. Set the storage size permitted for both logs to as large as possible.

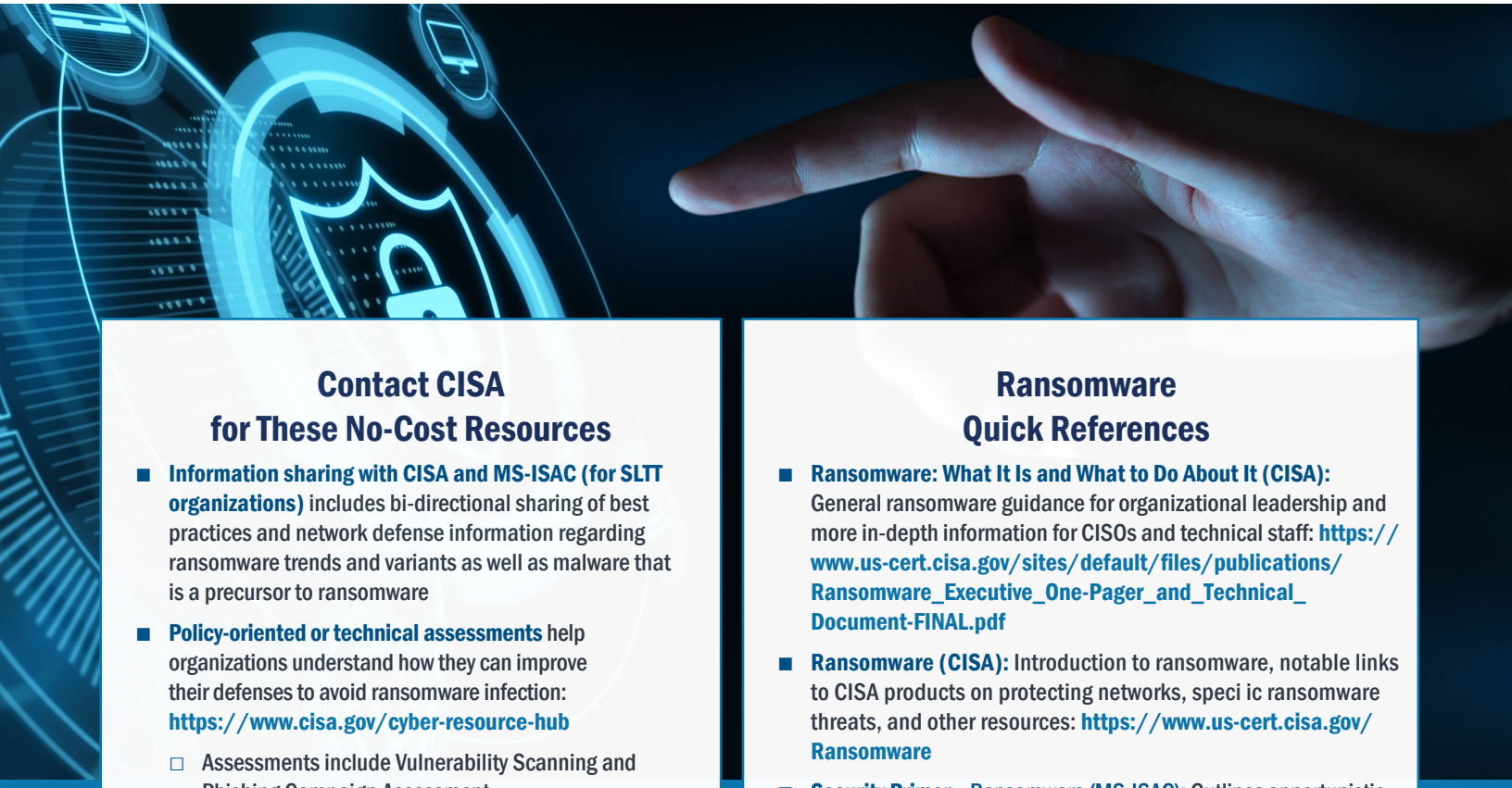
- Secure domain controllers (DCs). Threat actors often target and use DCs as a staging point to spread ransomware network-wide.
  - The following list contains high-level suggestions on how best to secure a DC:
    - Ensure that DCs are regularly patched. This includes the application of critical patches as soon as possible.
    - Ensure the most current version of the Windows Server OS is being used on DCs. Security features are better integrated in newer versions of Windows Server OSs, including Active Directory security features. Use Active Directory configuration guides, such as those available from Microsoft (**https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory**), when configuring available security features.
    - Ensure that no additional software or agents are installed on DCs, as these can be leveraged to run arbitrary code on the system.
    - Access to DCs should be restricted to the Administrators group. Users within this group should be limited and have separate accounts used for day-to-day operations with non-administrative permissions.
    - DC host firewalls should be configured to prevent internet access. Usually, these systems do not have a valid need for direct internet access. Update servers with internet connectivity can be used to pull necessary updates in lieu of allowing internet access for DCs.
  - CISA recommends the following DC Group Policy settings:

    (Note: This is not an all-inclusive list and further steps should be taken to secure DCs within the environment.)
    - The Kerberos default protocol is recommended for authentication, but if it is not used, enable NTLM auditing to ensure that only NTLMv2 responses are being sent across the network. Measures should be taken to ensure that LM and NTLM responses are refused, if possible.
    - Enable additional protections for Local Security Authentication to prevent code injection capable of acquiring credentials from the system. Prior to enabling these protections, run audits against the lsass.exe program to ensure an understanding of the programs that will be affected by the enabling of this protection.
    - Ensure that SMB signing is required between the hosts and the DCs to prevent the use of replay attacks on the network. SMB signing should be enforced throughout the entire domain as an added protection against these attacks elsewhere in the environment.

- Retain and adequately secure logs from both network devices and local hosts. This supports triage and remediation of cybersecurity events. Logs can be analyzed to determine the impact of events and ascertain whether an incident has occurred.

- Set up centralized log management using a security information and event management tool. This enables an organization to correlate logs from both network and host security devices. By reviewing logs from multiple sources, an organization can better triage an individual event and determine its impact to the organization as a whole.
- Maintain and back up logs for critical systems for a minimum of one year, if possible.

- Baseline and analyze network activity over a period of months to determine behavioral patterns so that normal, legitimate activity can be more easily distinguished from anomalous network activity (e.g., normal vs anomalous account activity).
  - Business transaction logging—such as logging activity related to specific or critical applications—is another useful source of information for behavioral analytics.



Contact CISA for These No-Cost Resources

- **Information sharing with CISA and MS-ISAC (for SLTT organizations)** includes bi-directional sharing of best practices and network defense information regarding ransomware trends and variants as well as malware that is a precursor to ransomware
- **Policy-oriented or technical assessments** help organizations understand how they can improve their defenses to avoid ransomware infection: **https://www.cisa.gov/cyber-resource-hub**
  - Assessments include Vulnerability Scanning and Phishing Campaign Assessment
- **Cyber exercises** evaluate or help develop a cyber incident response plan in the context of a ransomware incident scenario
- **CISA Cybersecurity Advisors (CSAs)** advise on best practices and connect you with CISA resources to manage cyber risk
- **Contacts:**
  - **SLTT organizations:** **CyberLiaison_SLTT@cisa.dhs.gov**
  - **Private sector organizations:** **CyberLiaison_Industry@cisa.dhs.gov**

Ransomware Quick References

- **Ransomware: What It Is and What to Do About It (CISA):** General ransomware guidance for organizational leadership and more in-depth information for CISOs and technical staff: **https://www.us-cert.cisa.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf**
- **Ransomware (CISA):** Introduction to ransomware, notable links to CISA products on protecting networks, speci ic ransomware threats, and other resources: **https://www.us-cert.cisa.gov/Ransomware**
- **Security Primer –** Ransomware (MS-ISAC): Outlines opportunistic and strategic ransomware campaigns, common infection vectors, and best practice recommendations: **https://www.cisecurity.org/white-papers/security-primer-ransomware/**
- **Ransomware: Facts, Threats, and Countermeasures (MS-ISAC):** Facts about ransomware, infection vectors, ransomware capabilities, and how to mitigate the risk of ransomware infection: **https://www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/**
- **Security Primer – Ryuk (MS-ISAC):** Overview of Ryuk ransomware, a prevalent ransomware variant in the SLTT government sector, that includes information regarding preparedness steps organizations can take to guard against infection: **https://www.cisecurity.org/white-papers/security-primer-ryuk/**

Part 2: Ransomware Response Checklist

Should your organization be a victim of ransomware, CISA strongly recommends responding by using the following checklist. Be sure to move through the **first three steps in sequence.**

Detection and Analysis

☐ **1. Determine which systems were impacted, and immediately isolate them.**

- ☐ If several systems or subnets appear impacted, take the network offline at the switch level. It may not be feasible to disconnect individual systems during an incident.
- ☐ If taking the network temporarily offline is not immediately possible, locate the network (e.g., Ethernet) cable and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.
- ☐ After an initial compromise, malicious actors may monitor your organization's activity or communications to understand if their actions have been detected. Be sure to isolate systems in a coordinated manner and use out-of-band communication methods like phone calls or other means to avoid tipping off actors that they have been discovered and that mitigation actions are being undertaken. Not doing so could cause actors to move laterally to preserve their access—already a common tactic—or deploy ransomware widely prior to networks being taken offline.

Note: Step 2 will prevent you from maintaining ransomware infection artifacts and potential evidence stored in volatile memory. It should be carried out **only** if it is not possible to temporarily shut down the network or disconnect affected hosts from the network using other means.

☐ **2. Only in the event you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.**

☐ **3. Triage impacted systems for restoration and recovery.**

- ☐ Identify and prioritize critical systems for restoration, and confirm the nature of data housed on impacted systems.
  - Prioritize restoration and recovery based on a predefined critical asset list that includes information systems critical for health and safety, revenue generation, or other critical services, as well as systems they depend on.
- ☐ Keep track of systems and devices that are not perceived to be impacted so they can be deprioritized for restoration and recovery. This enables your organization to get back to business in a more efficient manner.

☐ **4. Confer with your team to develop and document an initial understanding of what has occurred based on initial analysis.**

☐ **5. Using the contact information below, engage your internal and external teams and stakeholders with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident.**

- ☐ Share the information you have at your disposal to receive the most timely and relevant assistance. Keep management and senior leaders informed via regular updates as the situation develops. Relevant stakeholders may include your IT department, managed security service providers, cyber insurance company, and departmental or elected leaders.

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 or not 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

Remember: Paying ransom will not ensure your data is decrypted or that your systems or data will no longer be compromised. CISA, MS-ISAC, and federal law enforcement do not recommend paying ransom.

- ☐ Consider requesting assistance from CISA; MS-ISAC; and local, state, or federal law enforcement (e.g., Federal Bureau of Investigation [FBI], U.S. Secret Service [USSS]). See contact information below.
- ☐ As appropriate, coordinate with communications and public information personnel to ensure accurate information is shared internally with your organization and externally with the public.
- ☐ The *Public Power Cyber Incident Response Playbook* (https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf) contains guidance for organizational communication procedures as well as templates for cyber incident holding statements for public consumption. Work with your team to develop similar procedures and draft holding statements as soon as possible, as developing this documentation during an incident is not optimal. This will allow your organization to reach consensus, in advance, on what level of detail is appropriate to share within the organization and with the public, and how information will flow.

Containment and Eradication

If no initial mitigation actions appear possible:

☐ 6. Take a system image and memory capture of a sample of affected devices (e.g., workstations and servers). Additionally, 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). The contacts below may be able to assist you in performing these tasks.

- ☐ 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).

☐ 7. Consult federal law enforcement regarding possible decryptors available, as security researchers have already broken the encryption algorithms for some ransomware variants.

To continue taking steps to contain and mitigate the incident:

☐ 8. Research the trusted guidance (i.e., published by sources such as government, MS-ISAC, reputable security vendor, etc.) for the particular 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.

☐ 9. Identify the systems and accounts involved in the initial breach. This can include email accounts.

☐ 10. Based on the breach or compromise details determined above, contain any associated systems that may be used for further or continued unauthorized access. Breaches often involve mass credential exfiltration. Securing the network and other information sources from continued credential-based unauthorized access may include the following actions:

- ☐ Disabling virtual private networks, remote access servers, single sign-on resources, and cloud-based or other public-facing assets.

☐ 11. Additional suggested actions—server-side data encryption quick-identification steps:

- ☐ In the event you learn that server-side data is being encrypted by an infected workstation, quick-identification steps are to:

  1. Review Computer Management > Sessions and Open Files lists on associated servers to determine the user or system accessing those files.

  2. Review file properties of encrypted files or ransom notes to identify specific users that may be associated with file ownership.

  3. Review the TerminalServices-RemoteConnectionManager event log to check for successful RDP network connections.

  4. Review the Windows Security log, SMB event logs, and any related logs that may identify significant authentication or access events.

  5. 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").

☐ 12. 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.

Upon voluntary request, CISA and MS-ISAC can assist with analysis (e.g., phishing emails, storage media, logs, malware) at no cost to support your organization 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.us-cert.gov/MalwareSubmission/pages/submission.jsf**
- MS-ISAC – Malicious Code Analysis Platform (SLTT organizations only): **https://www.cisecurity.org/spotlight/cybersecurity-spotlight-malware-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 (see contact information below)

- ☐ 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. Malicious actors will sometimes use this access to exfiltrate data and then threaten to release the data publicly before ransoming the network in an attempt to further extort the victim and pressure them into paying.
  - Malicious actors often drop manually deployed ransomware variants on a network to obfuscate their post-compromise activity. Care must be taken to identify such dropper malware before rebuilding from backups to prevent continuing compromise.

☐ 13. 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.

☐ 14. 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.

☐ 15. Once the environment has been fully cleaned and rebuilt (including any associated impacted accounts and the removal or remediation of malicious persistence mechanisms) issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility. This can include applying patches, upgrading software, and taking other security precautions not previously taken.

☐ 16. Based on established criteria, which may include taking the steps above or seeking outside assistance, the designated IT or IT security authority declares the ransomware incident over.

Recovery and Post-Incident Activity

☐ 17. Reconnect systems and restore data from offline, encrypted backups based on a prioritization of critical services.

- ☐ Take care 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.

☐ 18. 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.

☐ 19. Consider sharing lessons learned and relevant indicators of compromise with CISA or your sector ISAC/ISAO for further sharing and to benefit others within the community.

Contact Information

Consider filling out the following contact information for ready use should your organization become a victim of a ransomware incident. Consider contacting these organizations for mitigation and response assistance or for purpose of notification.

State and Local Response Contacts:		
Contact	**24x7 Contact Information**	**Roles and Responsibilities**
IT/IT Security Team - Centralized Cyber Incident Reporting		
Departmental or Elected Leaders		
State and Local Law Enforcement		
Fusion Center		
Managed/Security Service Providers		
Cyber Insurance		

Federal Asset Response Contacts

Upon voluntary request, federal asset response includes providing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents while identifying other entities that may be at risk, assessing potential risks to the sector or region, facilitating information sharing and operational coordination, and providing guidance on how to best use federal resources and capabilities.

What You Can Expect:

- Specific guidance to help evaluate and remediate ransomware incidents
- Remote assistance to identify the extent of the compromise and recommendations for appropriate containment and mitigation strategies (dependent on specific ransomware variant)
- Phishing email, storage media, log and malware analysis, based on voluntary submission (full-disk forensics can be performed on an as-needed basis)
- Contacts:
  - CISA:
    - **https://us-cert.cisa.gov/report**, **Central@cisa.gov** or (888) 282-0870
    - Cybersecurity Advisor (**https://www.cisa.gov/cisa-regions**): [Enter your local CISA CSA's phone number and email address.]
  - MS-ISAC:
    - **soc@msisac.org** or (866) 787-4722

Federal Threat Response Contacts

Upon voluntary request, federal threat response includes law enforcement and national security investigative activity: collecting evidence and intelligence, providing attribution, linking related incidents, identifying additional affected entities, identifying threat pursuit and disruption opportunities, developing and executing action to mitigate the immediate threat, and facilitating information sharing and operational coordination with asset response.

What You Can Expect:

- Assistance in conducting a criminal investigation, which may involve collecting incident artifacts, to include system images and malware samples.
- Contacts:
  - FBI:
    - **https://www.fbi.gov/contact-us/field-offices**
    - [Enter your local FBI field office POC phone number and email address.]
  - USSS:
    - **https://www.secretservice.gov/contact/field-offices/**
    - [Enter your local USSS field office POC phone number and email address.]

DEFEND TODAY,
SECURE TOMORROW

CISA.GOV

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®