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

#StopRansomware Guide

Publication: October 2023

Change Record

Version	Date	Revision/Change Description	Section/Page Affected
1.0	September 2020	Initial Version	
2.0	May 2023	See “What’s New” on p.3.	Updates throughout.
3.0	October 2023	• Initial Access Vector bullet added for internet-facing vulnerabilities. • Updated guidance on hardening SMB. • Added information about threat actors impersonating employees. • Added guidance on hardening web browsers. • Added a bullet about abnormal amounts of data outgoing over any ports. • Added Acknowledgements section.	• Initial Access Vector: Internet-Facing Vulnerabilities and Mitigations p.7. • Part 1: Ransomware and Data Extortion Preparation, Prevention, and Mitigation Best Practices, pages 8, and 9. • Initial Access Vector: Advanced Forms of Social Engineering p.14. • General Best Practices and Hardening Guidance, p.20. • Part 2: Ransomware and Data Extortion Response Checklist p. 24. • Acknowledgements, p.30.

INTRODUCTION

Ransomware is a form of malware designed to encrypt files on a device, rendering them and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Over time, malicious actors have adjusted their ransomware tactics to be more destructive and impactful and have also exfiltrated victim data and pressured victims to pay by threatening to release the stolen data. The application of both tactics is known as "double extortion." In some cases, malicious actors may exfiltrate data and threaten to release it as their sole form of extortion without employing ransomware.

These ransomware and associated data breach incidents can severely impact business processes by leaving organizations unable to access necessary data to operate and deliver mission-critical services. The economic and reputational impacts of ransomware and data extortion have proven challenging and costly for organizations of all sizes throughout the initial disruption and, at times, extended recovery.

This guide is an update to the Joint Cybersecurity and Infrastructure Security Agency (CISA) and Multi-State Information Sharing & Analysis Center (MS-ISAC) Ransomware Guide released in September 2020 (see What's New) and was developed through the JRTF. This guide includes two primary resources:

- Part 1: Ransomware and Data Extortion Prevention Best Practices
- Part 2: Ransomware and Data Extortion Response Checklist

This guide was developed through the U.S. Joint Ransomware Task Force (JRTF).

The JRTF, co-chaired by CISA and FBI, is an interagency, collaborative effort to combat the growing threat of ransomware attacks. The JRTF was launched in response to a series of high-profile ransomware attacks on U.S. critical infrastructure and government agencies. The JRTF:

1. Coordinates and streamlines the U.S. Government's response to ransomware attacks and facilitates information sharing and collaboration between government agencies and private sector partners.
2. Ensures operational coordination for activities such as developing and sharing best practices for preventing and responding to ransomware attacks, conducting joint investigations and operations against ransomware threat actors, and providing guidance and resources to organizations that have been victimized by ransomware.
3. Represents a significant step forward in enabling unity of effort across the U.S Government's efforts to address the growing threat of ransomware attacks.

For more info on JRTF, see cisa.gov/joint-ransomware-task-force.

Part 1 provides guidance for all organizations to reduce the impact and likelihood of ransomware incidents and data extortion, including best practices to prepare for, prevent, and mitigate these incidents. Prevention best practices are grouped by common initial access vectors. Part 2 includes a checklist of best practices for responding to these incidents.

These ransomware and data extortion prevention and response best practices and recommendations are based on operational insight from CISA, MS-ISAC, the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI), hereafter referred to as the authoring organizations. 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.

The authoring organizations recommend that organizations take the following initial steps to prepare and protect their facilities, personnel, and customers from cyber and physical security threats and other hazards:

- Join a sector-based information sharing and analysis center (ISAC), where eligible, such as:
    - MS-ISAC for U.S. State, Local, Tribal, & Territorial (SLTT) Government Entities - learn.cisecurity.org/ms-isac-registration. MS-ISAC membership is open to representatives from all 50 states, the District of Columbia, U.S. Territories, local and tribal governments, public K-12 education entities, public institutions of higher education, authorities, and any other non-federal public entity in the United States.
    - Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC) for U.S. Elections Organizations - learn.cisecurity.org/ei-isac-registration. See the National Council of ISACs for more information.
- Contact CISA at CISA.JCDC@cisa.dhs.gov to collaborate on information sharing, best practices, assessments, exercises, and more.
- Contact your local FBI field office for a list of points of contact (POCs) in the event of a cyber incident.

Engaging with peer organizations and CISA enables your organization to receive critical and timely information and access to services for managing ransomware and other cyber threats.

What's New

Since the initial release of the Ransomware Guide in September 2020, ransomware actors have accelerated their tactics and techniques.

To maintain relevancy, add perspective, and maximize the effectiveness of this guide, the following changes have been made:

- Incorporated the #StopRansomware effort into the title.
- Added recommendations for preventing common initial infection vectors, including compromised credentials and advanced forms of social engineering.
-

> #StopRansomware is CISA and FBI's effort to publish advisories for network defenders that detail network defense information related to various ransomware variants and threat actors. Visit stopransomware.gov to learn more and to read the joint advisories.

- Expanded the ransomware response checklist with threat hunting tips for detection and analysis.
- Mapped recommendations to CISA's Cross-Sector Cybersecurity Performance Goals (CPGs).

Part 1: Ransomware and Data Extortion Preparation, Prevention, and Mitigation Best Practices

These recommended best practices align with the CPGs developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. For more information on the CPGs and recommended baseline protections, visit CISA's Cross-Sector Cybersecurity Performance Goals.

Preparing for Ransomware and Data Extortion Incidents

Refer to the best practices and references listed in this section to help manage the risks posed by ransomware and to drive a coordinated and efficient response for your organization in the event of an incident. Apply these practices to the greatest extent possible pending the availability of organizational resources.

- **Maintain offline, encrypted backups of critical data**, and regularly test the availability and integrity of backups in a disaster recovery scenario [CPG 2.R]. Test backup procedures on a regular basis. It is important that backups are maintained offline, as most ransomware actors attempt to find and subsequently delete or encrypt accessible backups to make restoration impossible unless the ransom is paid. Ransomware actors often hunt for and collect credentials stored in the targeted environment and use those credentials to attempt to access backup solutions; they also use publicly available exploits to target unpatched backup solutions.

  Automated cloud backups may not be sufficient because if local files are encrypted by an attacker, these files will be synced to the cloud, possibly overwriting unaffected data.

  - Maintain and regularly update "golden images" of critical systems. This includes maintaining image "templates" that have 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 [CPG 2.O].
    - Use infrastructure-as-code (IaC) to deploy and update cloud resources and keep backups of template files offline to quickly redeploy resources. IaC code should be version controlled and changes to the templates should be audited.
    - Store applicable source code or executables with offline backups (as well as escrowed and license agreements). Rebuilding from system images is more efficient, but some images will not install on different hardware or platforms correctly; having separate access to software helps in these cases.

  - Retain backup hardware to rebuild systems if rebuilding the primary system is not preferred.
    - Consider replacing out-of-date hardware that inhibits restoration with up-to-date hardware, as older hardware can present installation or compatibility hurdles when rebuilding from images.
  - Consider using a multi-cloud solution to avoid vendor lock-in for cloud-to-cloud backups in case all accounts under the same vendor are impacted.
    - Some cloud vendors offer immutable storage solutions that can protect stored data without the need for a separate environment. Use immutable storage with caution as it does not meet compliance criteria for certain regulations and misconfiguration can impose significant cost.

- **Create, maintain, and regularly exercise a basic cyber incident response plan (IRP) and associated communications plan that includes response and notification procedures** for ransomware and data extortion/breach incidents [CPG 2.S]. Ensure a hard copy of the plan and an offline version is available.
  - Provide data breach notifications to third parties and regulators consistent with law.
  - Ensure the IRP and communications plan are reviewed and approved by the CEO, or equivalent, in writing and that both are reviewed and understood across the chain of command.
  - Review available incident response guidance, such as the Ransomware Response Checklist in this guide and Public Power Cyber Incident Response Playbook to:
    - Help your organization better organize around cyber incident response.
    - Draft cyber incident holding statements.
    - Develop a cyber IRP.
  - Include organizational communications procedures as well as templates for cyber incident holding statements in the communications plan. Reach a consensus on what level of detail is appropriate to share within the organization and with the public and how information will flow.
- **Implement a zero trust architecture** to prevent unauthorized access to data and services. Make access control enforcement as granular as possible. ZTA assumes a network is compromised and provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per request access decisions in information systems and services.

Preventing and Mitigating Ransomware and Data Extortion Incidents

Refer to the best practices and references listed in this section to help prevent and mitigate ransomware and data extortion incidents. Prevention best practices are grouped by common initial access vectors of ransomware and data extortion actors.

Initial Access Vector: Internet-Facing Vulnerabilities and Misconfigurations

- **Do not expose services, such as remote desktop protocol, on the web**. If these services must be exposed, apply appropriate compensating controls to prevent common forms of abuse and exploitation. All unnecessary OS applications and network protocols are disabled on internet-facing assets. [CPG 2.W]
- **Conduct regular vulnerability scanning to identify and address vulnerabilities**, especially those on internet-facing devices, to limit the attack surface [CPG 1.E].
    - CISA offers a no-cost Vulnerability Scanning service and other no-cost assessments: cisa.gov/cyber-resource-hub [CPG 1.F].
- **Regularly patch and update software and operating systems to the latest available versions**.
    - Prioritize timely patching of internet-facing servers—that operate software for processing internet data, such as web browsers, browser plugins, and document readers—especially for known exploited vulnerabilities.
    - The authoring organizations—aware of difficulties small and medium business have keeping internet-facing servers updated—urge migrating systems to reputable "managed" cloud providers to reduce, not eliminate, system maintenance roles for identity and email systems. For more information, visit NSA's Cybersecurity Information page Mitigating Cloud Vulnerabilities.
- **Ensure all on-premises, cloud services, mobile, and personal (i.e., bring your own device [BYOD]) devices are properly configured and security features are enabled**. For example, disable ports and protocols that are not being used for business purposes (e.g., Remote Desktop Protocol [RDP]—Transmission Control Protocol [TCP] Port `3389`) [CPG 2.X].
    - Reduce or eliminate manual deployments and codify cloud resource configuration through IaC. Test IaC templates before deployment with static security scanning tools to identify misconfigurations and security gaps.
    - Check for configuration drift routinely to identify resources that were changed or introduced outside of template deployment, reducing the likelihood of new security gaps and misconfigurations being introduced. Leverage cloud providers' services to automate or facilitate auditing resources to ensure a consistent baseline.
- **Limit the use of RDP and other remote desktop services**. If RDP is necessary, apply best practices. Threat actors often gain initial access to a network through exposed and poorly secured remote services, and later traverse the network using the native Windows RDP client. Threat actors also often gain access by exploiting virtual private networks (VPNs) or using compromised credentials. Refer to CISA Advisory: Enterprise VPN Security.
    - Audit the network for systems using RDP, close unused RDP ports, enforce account lockouts after a specified number of attempts, apply multifactor authentication (MFA), and log RDP login attempts.
    - Update VPNs, network infrastructure devices, and devices being used to remote in to work environments with the latest software patches and security configurations.

  - Implement MFA on all VPN connections to increase security. If MFA is not implemented, require teleworkers to use passwords of 15 or more characters.

- Disable Server Message Block (SMB) protocol version 1 and upgrade to version 3 (SMBv3) after mitigating existing dependencies (on existing systems or applications), as they may break when disabled. SMBv3 was first released as part of updates to Microsoft Windows 8 and Windows Server 2012, Apple OS X 10.10, and Linux kernel 3.12.
- Harden SMBv3 by implementing the following guidance as malicious actors use SMB to propagate malware across organizations.
  - Require the use of SMBv 3.1.1. This version contains enhanced security protections, including pre-authentication integrity, enhanced AES encryption, and signing cryptography. SMBv 3.1.1 protocol is supported natively in Windows, Apple, and Linux kernel, as well as many other third-party storage systems. In Microsoft Windows 10 and Windows Server 2019, Windows 11 Preview Build 25951, and later, you can mandate SMBv 3.1.1 protections such as dialect client negotiation. For more information, see Microsoft's Protect SMB traffic from interception | Use SMB 3.1.1 and SMB dialect management now supported in Windows Insider.
  - Block unnecessary SMB communications:
    - Block external access of SMB to and from organization networks by blocking TCP port 445 inbound and outbound at internet perimeter firewalls. Block TCP ports `137`, `138`, `139`. **Note:** SMBv2 and later does not use NetBIOS datagrams. Continuing to use SMBv2 does not have significant risks and can be used where needed. It is recommended to update it to SMBv3 where feasible.
    - Block or limit internal SMB traffic so that communications only occur between systems requiring it. For instance, Windows devices need SMB communications with domain controllers to get group policy, but most Windows workstations do not need to access other Windows workstations.
    - Configure Microsoft Windows and Windows Server systems to require Kerberos-based IP Security (IPsec) for lateral SMB communications to prevent malicious actors from accessing communications over SMB by detecting systems that are not members of an organization's Microsoft Active Directory domains.
    - Disable the SMB Server service ("Server") on Microsoft Windows and Windows Server devices in instances where there is no need to remotely access files or to name pipe application programming interfaces (APIs).
    - For more information guidance, see Microsoft's Secure SMB Traffic in Windows Server.
  - Consider requiring SMB encryption. To guarantee that SMB 3.1.1 clients always use SMB Encryption, you must disable the SMB 1.0 server. For more information, refer to Microsoft's SMB security enhancements | Enable SMB Encryption and Reduced performance after SMB Encryption or SMB Signing is enabled
  - If SMB encryption is not enabled, require SMB signing for both SMB client and server on all systems. This will prevent certain adversary-in-the-middle and pass-the-hash attacks.

For more information on SMB signing, refer to Microsoft's Overview of Server Message Block Signing.

- Require Kerberos authentication by hardening Universal Naming Convention (UNC). OSs such as Microsoft Windows 10, Windows Server 2016, and later automatically harden UNC for connections to the Microsoft Active Directory domain via SYSVOL and NETLOGON shares. Additionally, network administrators can manually configure UNC hardening for servers and shares in any supported Microsoft Windows operating system. For more information, refer to Microsoft's Vulnerability in Group Policy could allow remote code execution. Using IP addresses to connect to SMB servers will result in the use of NTLM authentication unless you also configure the use of Kerberos SPNs with IP addresses, refer to Microsoft's Configuring Kerberos for IP Address.
- Use SMB over QUIC. Microsoft Windows 11, Windows Server 2022 Datacenter: Azure Edition, and Android clients with a third-party SMB client support use of SMB over QUIC, an alternative for SMB over TCP. The QUIC protocol is always Transport Layer Security (TLS) 1.3 encrypted and uses certificate authentication to encapsulate all SMB traffic—including SMB's own authentication—inside a VPN-like transport. SMB over QUIC allows mobile users to safely connect over the public internet to edge SMB resources, such as servers at the edge of organizational networks not completely behind a firewall, but also works on internal networks that require the highest SMB transport security. For more information, refer to Microsoft's SMB over QUIC.
- Log and monitor SMB traffic [CPG 2.T] to help flag potentially abnormal, harmful behaviors.

Initial Access Vector: Compromised Credentials

- **Implement phishing-resistant MFA for all services**, particularly for email, VPNs, and accounts that access critical systems [CPG 2.H]. Escalate to senior management upon discovery of systems that do not allow MFA, systems that do not enforce MFA, and any users who are not enrolled with MFA.
    - **Consider employing password-less MFA** that replace passwords with two or more verification factors (e.g., a fingerprint, facial recognition, device pin, or a cryptographic key).
- **Consider subscribing to credential monitoring services** that monitor the dark web for compromised credentials.
- **Implement identity and access management (IAM) systems** to provide administrators with the tools and technologies to monitor and manage roles and access privileges of individual network entities for on-premises and cloud applications.
- **Implement zero trust access control** by creating strong access policies to restrict user to resource access and resource-to-resource access. This is important for key management resources in the cloud.
- **Change default admin usernames and passwords** [CPG 2.A].
- **Do not use root access accounts for day-to-day operations**. Create users, groups, and roles to carry out tasks.

- **Implement password policies that require unique passwords of at least 15 characters**. [CPG 2.B] [CPG 2.C].
    - Password managers can help you develop and manage secure passwords. Secure and limit access to any password managers in use and enable all security features available on the product in use, such as MFA.
- **Enforce account lockout policies after a certain number of failed login attempts**. Log and monitor login attempts for brute force password cracking and password spraying [CPG 2.G].
- **Store passwords in a secured database and use strong hashing algorithms**.
- **Disable saving passwords to the browser in the Group Policy Management console**.
- **Implement Local Administrator Password Solution (LAPS)** where possible if your OS is older than Windows Server 2019 and Windows 10 as these versions do not have LAPS built in. **Note:** The authoring organizations recommend organizations upgrade to Windows Server 2019 and Windows 10 or greater.
- Protect against Local Security Authority Subsystem Service (LSASS) dumping:
    - **Implement the Attack Surface Reduction (ASR) rule for LSASS.**
    - **Implement Credential Guard for Windows 10 and Server 2016**. Refer to Microsoft Manage Windows Defender Credential Guard for more information. For Windows Server 2012R2, enable Protected Process Light (PPL) for Local Security Authority (LSA).
- **Educate all employees on proper password security in your annual security training** to include emphasizing not reusing passwords and not saving passwords in local files.
- **Use Windows PowerShell Remoting, Remote Credential Guard, or RDP** with restricted Admin Mode as feasible when establishing a remote connection to avoid direct exposure of credentials.
- **Separate administrator accounts from user accounts** [CPG 2.E]. Only allow designated admin accounts to be used for admin purposes. If an individual user needs administrative rights over their workstation, use a separate account that does not have administrative access to other hosts, such as servers. For some cloud environments, separate duties when the account used to provision/manage keys does not have permission to use the keys and vice versa. As this strategy introduces additional management overhead, it is not appropriate in all environments.

Initial Access 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 [CPG 2.I].
- **Implement flagging external emails in email clients**.
- **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 [CPG 2.M].

CISA offers a no-cost Phishing Campaign Assessment and other no-cost assessments. Visit cisa.gov/cyber-resource-hub.

- **Enable common attachment filters to restrict file types that commonly contain malware** and should not be sent by email. For more information, refer to Microsoft's post Anti-malware protection in EOP.
    - Review file types in your filter list at least semi-annually and add additional file types that have become attack vectors. For example, OneNote attachments with embedded malware have recently been used in phishing campaigns.
    - Malware is often compressed in password protected archives that evade antivirus scanning and email filters.
- **Implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification** to lower the chance of spoofed or modified emails from valid domains. DMARC protects your domain from being spoofed but does not protect from incoming emails that have been spoofed unless the sending domain also implements DMARC. DMARC builds on the widely deployed Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email. For more information on DMARC, refer to CISA Insights Enhance Email & Web Security and the Center for Internet Security's blog How DMARC Advances Email Security.

Malicious Domain Blocking and Reporting (MDBR) is a no-cost service for SLTT organizations that is funded by CISA, the MS-ISAC, and the EI-ISAC. This fully managed security service prevents IT systems from connecting to harmful web domains and protects against cyber threats, including:

- Malware,
- Ransomware, and
- Phishing.

To sign up for MDBR, visit cisecurity.org/ms-isac/services/mdbr/.

- **Ensure macro scripts are disabled for Microsoft Office files transmitted via email**. These macros can be used to deliver ransomware [CPG 2.N]. **Note:** Recent versions of Office are configured by default to block files that contain Visual Basic for Applications (VBA) macros and display a Trust Bar with a warning that macros are present and have been disabled. For more information, refer to Microsoft's Macros from the internet will be blocked by default in Office. See Microsoft's Block macros from running in Office files from the Internet for configuration instructions to disable macros in external files for earlier versions of Office.
- **Disable Windows Script Host (WSH)**. Windows script hosting provides an environment in which users can execute scripts or perform tasks.

Initial Access Vector: Precursor Malware Infection

- **Use automatic updates for your antivirus and anti-malware software and signatures**. Ensure tools are properly configured to escalate warnings and indicators to notify security personnel. The authoring organizations recommend 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 QakBot, Bumblebee, and Emotet.
    - In some cases, ransomware deployment is the last step in a network compromise and is dropped to obscure previous post-compromise activities, such as business email compromise (BEC).

> CISA and MS-ISAC encourage SLTT organizations to use Albert IDS to enhance a defense-in-depth strategy. Albert serves as an early warning capability for U.S. SLTT governments and supports nationwide cybersecurity situational awareness and defense. For more information regarding Albert, visit cisecurity.org/services/albert-network-monitoring/.

- **Use application allowlisting and/or endpoint detection and response (EDR) solutions** on all assets to ensure that only authorized software is executable and all unauthorized software is blocked.
    - For Windows, enable Windows Defender Application Control (WDAC), AppLocker, or both on all systems that support these features.
        - WDAC is under continuous development while AppLocker will only receive security fixes. AppLocker can be used as a complement to WDAC, when WDAC is set to the most restrictive level possible, and AppLocker is used to fine-tune restrictions for your organization.
    - Use allowlisting rather than attempting to list and deny every possible permutation of applications in a network environment.
    - Consider implementing EDR for cloud-based resources.
- **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.
    - Ensure that the IDS is centrally monitored and managed. Properly configure the tools and route warnings and indicators to the appropriate personnel for action.
- **Monitor indicators of activity and block malware file creation with the Windows Sysmon utility**. As of Sysmon 14, the `FileBlockExecutable` option can be used to block the creation of malicious executables, Dynamic Link Library (DLL) files, and system files that match specific hash values.

Initial Access Vector: Advanced Forms of Social Engineering

- **Create policies to include cybersecurity awareness training** about advanced forms of social engineering for personnel that have access to your network. Training should include tips on being able to recognize illegitimate websites and search results. It is also important to repeat security awareness training regularly to keep your staff informed and vigilant.
- **Implement Protective Domain Name System (DNS).** By blocking malicious internet activity at the source, Protective DNS services can provide high network security for remote workers. These security services analyze DNS queries and take action to mitigate threats—such as malware, ransomware, phishing attacks, viruses, malicious sites, and spyware—leveraging the existing DNS protocol and architecture. SLTT's can implement the no-cost MDBR service. See NSA's and CISA's Selecting a Protective DNS Service.
- **Consider implementing sandboxed browsers** to protect systems from malware originating from web browsing. Sandboxed browsers isolate the host machine from malicious code.

Advanced forms of social engineering include:

- Search Engine Optimization (SEO) poisoning, also known as search poisoning: When malicious actors create malicious websites and use SEO tactics to make them show up prominently in search results. SEO poisoning hijacks the search engine results of popular websites and injects malicious links to boost their placement in search results. These links then lead unsuspecting users to phishing sites, malware downloads, and other cyber threats.
- Drive-by-downloads (imposter websites): When a user unintentionally downloads malicious code by visiting a seemingly legitimate website that is malicious. Malicious actors use drive-by downloads to steal and collect personal information, inject trojans, or introduce exploit kits or other malware to endpoints. Users may visit these sites by responding to a phishing email or by clicking on a deceptive pop-up window.
- "Malvertising": Malicious advertising that cybercriminals use to inject malware to users' computers when they visit malicious websites or click an online advertisement. Malvertising may also direct users to a corrupted website where their data can be stolen, or malware can be downloaded onto their computer. Malvertising can appear anywhere, even at sites you visit as part of your everyday web browsing.
- Impersonating employees: Ransomware actors have posed as company IT and/or helpdesk staff in phone calls or SMS messages to obtain credentials from employees and gain access to the network.

Initial Access Vector: Third Parties and Managed Service Providers

- **Consider 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 numerous client organizations [CPG 1.I].
    - 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. Use contract language to formalize your security requirements as a best practice.

> Malicious actors may exploit the trusted relationships your organization has with third parties and MSPs.
>
> - Malicious actors 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.
> - Malicious actors may spoof the identity of—or use compromised email accounts associated with—entities your organization has a trusted relationship with to phish your users, enabling network compromise and disclosure of information.

- **Ensure the use of least privilege and separation of duties when setting up the access of third parties**. Third parties and MSPs should only have access to devices and servers that are within their role or responsibilities.
- **Consider creating service control policies (SCP) for cloud-based resources to prevent users or roles, organization wide, from being able to access specific services or take specific actions within services.** For example, the SCP can be used to restrict users from being able to delete logs, update virtual private cloud (VPC) configurations, and change log configurations.

General Best Practices and Hardening Guidance

- **Ensure your organization has a comprehensive asset management** approach [CPG 1.A].
    - Understand and take inventory of your organization's IT assets, logical (e.g., data, software) and physical (e.g., hardware).
    - Know which data or systems are most critical for health and safety, revenue generation, or other critical services, and understand any associated interdependencies (e.g., "system list 'A' used to perform 'X' is stored in critical asset 'B'"). 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.
    - Ensure you store your IT asset documentation securely and keep offline backups and physical hard copies on site.

> **Tip:** To facilitate asset tracking, use MS-ISAC's Hardware and Software Asset Tracking Spreadsheet.

- **Apply the principle of least privilege to all systems and services** so that users only have the access they need to perform their jobs [CPG 2.E]. Malicious actors often leverage privileged accounts for network-wide ransomware attacks.
    - Restrict user permissions to install and run software applications.
    - Restrict user/role permissions to access or modify cloud-based resources.
    - Limit actions that can be taken on customer-managed keys by certain users/roles.
    - Block local accounts from remote access by using group policy to restrict network sign-in by local accounts. For guidance, refer to Microsoft's Blocking Remote Use of Local Accounts and Security identifiers.
    - Use Windows Defender Remote Credential Guard and restricted admin mode for RDP sessions.
    - Remove unnecessary accounts and groups and restrict root access.
    - Control and limit local administration.
    - Audit Active Directory (AD) for excessive privileges on accounts and group memberships.
    - Make use of the Protected Users AD group in Windows domains to further secure privileged user accounts against pass-the-hash attacks.
    - Audit user and admin accounts for inactive or unauthorized accounts quarterly. Prioritize review of remote monitoring and management accounts that are publicly accessible—this includes audits of third-party access given to MSPs.
- **Ensure that all hypervisors and associated IT infrastructure, including network and storage components, are updated and hardened**. Emerging ransomware strategies have begun targeting VMware ESXi servers, hypervisors, and other centralized tools and systems, which enables fast encryption of the infrastructure at scale. For more information about ransomware resilience and hardening of VMware and other virtualization infrastructure, see:
    - NIST Special Publication (SP 800-125A Rev.1): Security Recommendations for Server-based Hypervisor Platforms
    - VMware: Cloud Infrastructure Security Configuration & Hardening
- **Leverage best practices and enable security settings in association with cloud environments**, such as Microsoft Office 365.
    - Review the shared responsibility model for cloud and ensure you understand what makes up customer responsibility when it comes to asset protection.
    - Backup data often; offline or leverage cloud-to-cloud backups.
    - Enable logging on all resources and set alerts for abnormal usages.
    - Enable delete protection or object lock on storage resources often targeted in ransomware attacks (e.g., object storage, database storage, file storage, and block storage) to prevent data from being deleted or overwritten, respectively.
    - Consider enabling version control to keep multiple variants of objects in storage. This allows for easier recovery from unintended or malicious actions.

  - Where supported, when using custom programmatic access to the cloud, use signed application programming interface (API) requests to verify the identity of the requester, protect data in transit, and protect against other attacks such as replay attacks.
  - For more information, refer to CISA Cybersecurity Advisory Microsoft Office 365 Security Recommendations.

- **Mitigate the malicious use of remote access and remote monitoring and management (RMM)** software:
  - Audit remote access tools on your network to identify current or authorized RMM software.
  - Review logs for execution of RMM software to detect abnormal use, or RMM software running as a portable executable.
  - Use security software to detect instances of RMM software only being loaded in memory.
  - Require authorized RMM solutions only be used from within your network over approved remote access solutions, such as VPNs or virtual desktop interfaces (VDIs).
  - Block both inbound and outbound connections on common RMM ports and protocols at the network perimeter.

- **Employ logical or physical means of network segmentation by implementing** ZTA and separating various business units or departmental IT resources within your organization and maintain separation between IT and operational technology [CPG 2.F]. Network segmentation can help contain the impact of any intrusion affecting your organization and prevent or limit lateral movement on the part of malicious actors. Organizations should use due diligence when segmenting networks and ensure network security policies are in place and adhered to because segmentation can be rendered ineffective if it is breached through user error or non-adherence to policies (e.g., connecting removable storage media or other devices to multiple segments).

- **Develop and regularly update comprehensive network diagram(s) that describes systems and data flows within your organization's network(s)** (see Figure 1) [CPG 2.P]. This is useful in steady state and can help incident responders understand where to focus their efforts. See Figure 2 and Figure 3 for depictions of a flat (unsegmented) network and of a best practice segmented network.
  - The diagram should include depictions of major networks, any specific IP addressing schemes, and the general network topology including network connections, interdependencies, and access granted to third parties, MSPs, and cloud connections from external and internal endpoints.
  - Ensure you securely store network documentation and keep offline backups and hard copies on site.

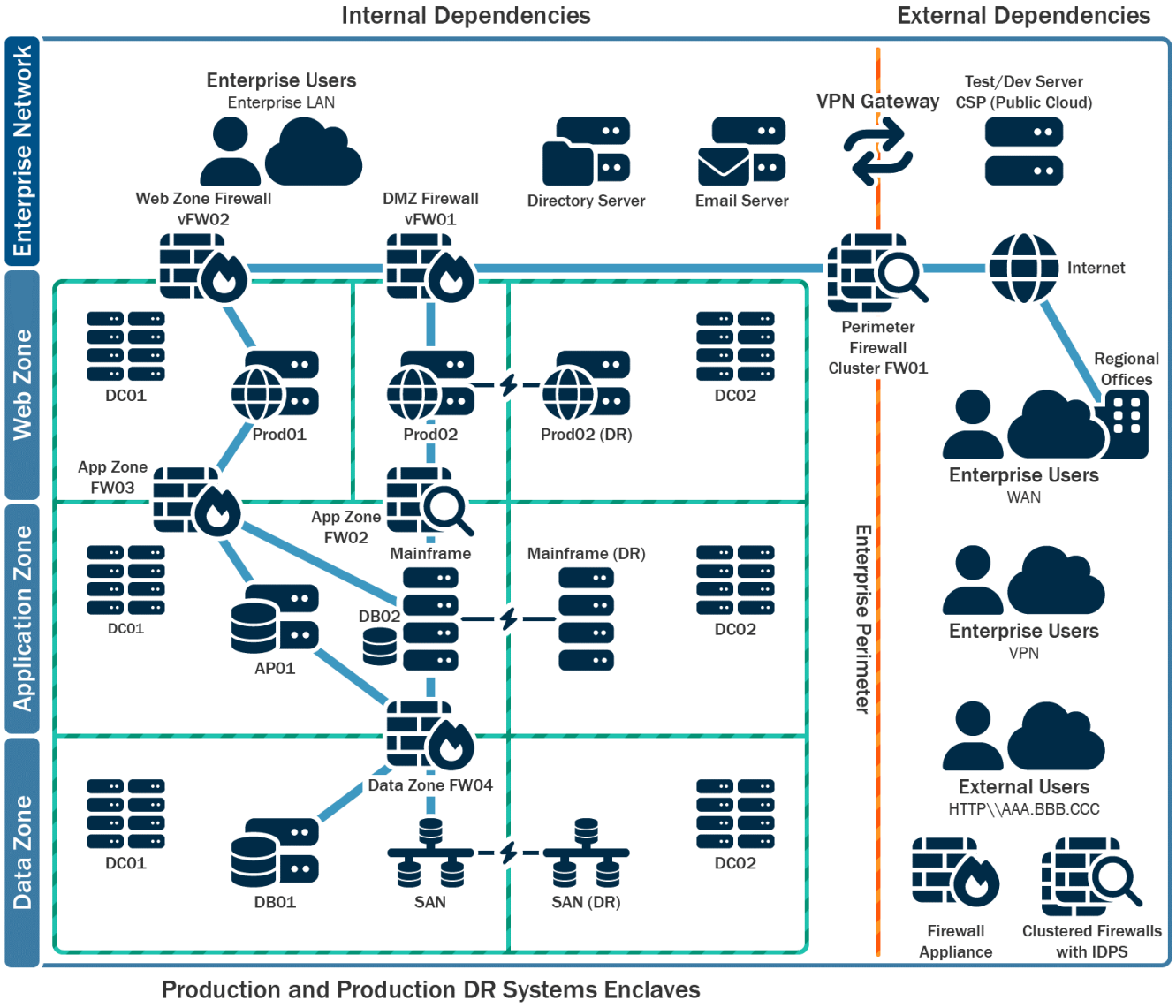

Figure 1: Example Network Diagram

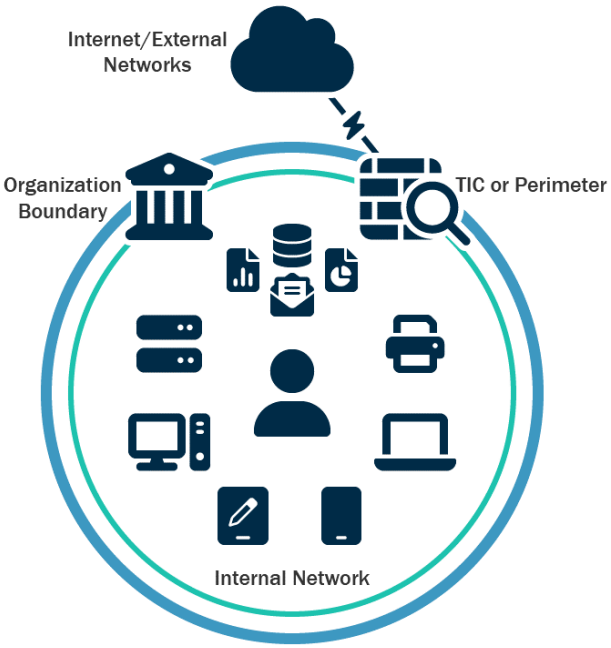

Figure 2: Flat (Unsegmented) Network

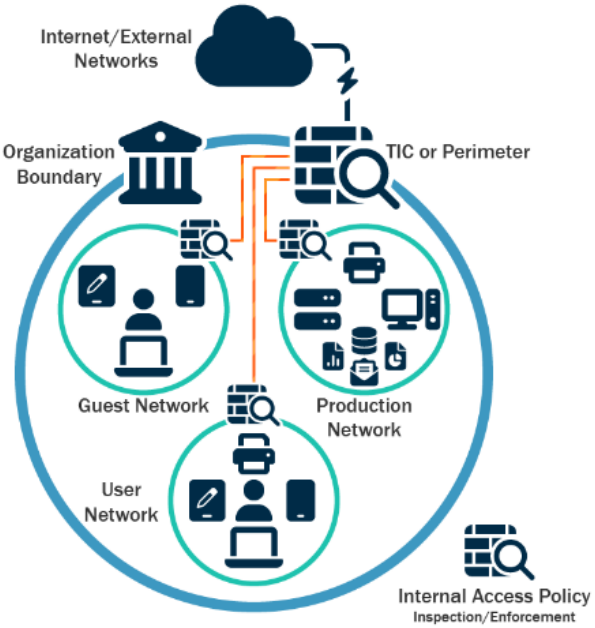

Figure 3: Segmented Network

- **Restrict usage of PowerShell to specific users on a case-by-case basis by using Group Policy**. Typically, only users or administrators who manage a network or Windows OS are permitted to use PowerShell. 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. For more information, refer to the joint Cybersecurity Information Sheet Keeping PowerShell: Security Measure to Use and Embrace.
    - Update Windows PowerShell or PowerShell Core to the latest version and uninstall all earlier PowerShell versions.
    - Ensure PowerShell instances, using the most current version, have module, script block, and transcription logging enabled (enhanced logging).
        - Logs from Windows 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.
        - Two logs that record PowerShell activity are the "PowerShell Windows Event" log and the "PowerShell Operational" log. The authoring organizations recommend turning on these two Windows Event Logs with a retention period of at least 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)**. Malicious actors often target and use DCs as a staging point to spread ransomware network wide. To secure DCs:
    - Use the latest version of Windows Server supported by your organization on DCs. Newer versions of Windows Server OS have more security features, including for Active Directory, integrated. For guidance on configuring available security features refer to Microsoft's Best Practices for Securing Active Directory.
        - The authoring organizations recommend using Windows Server 2019 or greater and Windows 10 or greater as they have security features, such as LSASS protections with Windows Credential Guard, Windows Defender, and Antimalware Scan Interface (AMSI), not included in older operating system
    - Ensure that DCs are regularly patched. Apply patches for critical vulnerabilities as soon as possible.
    - Use open-source penetration testing tools, such as BloodHound or PingCastle, to verify domain controller security.
    - Ensure that minimal software or agents are installed on DCs because these can be leveraged to run arbitrary code on the system.
    - Restrict access to DCs 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. For more information, refer to Microsoft's Securing Active Directory Administrative Groups and Accounts.
        - The designated admin accounts should only be used for admin purposes. Ensure that checking emails, web browsing, or other high-risk activities are not performed on DCs.
    - Configure DC host firewalls to prevent internet access. Usually, DCs do not need direct internet access. Servers with internet connectivity can be used to pull necessary updates in lieu of allowing internet access for DCs.
    - Implement a privileged access management (PAM) solution on DCs to assist in managing and monitoring privileged access. PAM solutions can also log and alert usage to detect unusual activity.
    - Consider disabling or limiting NTLM and WDigest Authentication, if possible. Include their use as criteria for prioritizing upgrading legacy systems or for segmenting the network. Instead use modern federation protocols (e.g., SAML, OIDC or Kerberos) for authentication with AES-256 bit encryptionhttps://cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf. If NTLM must be enabled:
        - Enable Extended Protection for Authentication (EPA) to prevent some NTLM-relay attacks. For more information, refer to Microsoft Mitigating NTLM Relay Attacks on Active Directory Certificate Services (AD CS).
        - Enable NTLM auditing to ensure that only NTLMv2 responses are sent across the network. Measures should be taken to ensure that LM and NTLM responses are refused, if possible.

    - Enable additional protections for LSA Authentication to prevent code injection capable of acquiring credentials from the system. Prior to enabling these protections, run audits against `lsass.exe` to ensure an understanding of the programs that will be affected by the enabling of this protection.

- **Retain and adequately secure logs from network devices, local hosts, and cloud services**. This supports triage and remediation of cybersecurity events. Logs can be analyzed to determine the impact of events and ascertain if an incident has occurred [CPG 2.T].
    - Set up centralized log management using a security information and event management tool [CPG 2.U]. This enables an organization to correlate logs from both network and host security devices. By reviewing logs from multiple sources, an organization can triage an individual event and determine its impact to the organization.
    - Maintain and back up logs for critical systems for a minimum of one year, if possible.
- **Establish a security baseline of normal network traffic and tune network appliances to detect anomalous behavior**. Tune host-based products to detect anomalous binaries, lateral movement, and persistence techniques.
    - Consider using business transaction logging—such as logging activity related to specific or critical applications—for behavioral analytics.
- **Conduct regular assessments** to ensure processes and procedures are up to date and can be followed by security staff and end users.
- **Enable tracking prevention** to limit the vectors that ad networks and trackers can use to track user information.
- **Enable website typo protection** to limit the possibility of logging onto spoofed websites or other potential malicious links that could compromise a browser.
- **Enable browser-based AV** for active scanning while browsing as an added layer of defense.
- **Block website notifications by default** to limit site's ability to track user data that can be exploited.

Part 2: Ransomware and Data Extortion Response Checklist

Should your organization be a victim of ransomware, follow your approved IRP. The authoring organizations strongly recommend responding by using the following checklist. Be sure to move through the **first three steps in sequence.**

> **The authoring organizations do not recommend paying ransom**. Paying ransom will not ensure your data is decrypted, that your systems or data will no longer be compromised, or that your data will not be leaked.
>
> Additionally, paying ransoms may pose sanctions risks. For information on potential sanctions risks, see U.S. Department of the Treasury Office of Foreign Assets Control (OFAC) memorandum from September 2021, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. The updated advisory states that Treasury's Office of Foreign Assets Control (OFAC) would consider 'mitigating factors' in related enforcement actions. Contact your local FBI field office, in consultation with OFAC, for guidance on mitigating penalty factors after an attack.

Detection and Analysis

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.

- ☐ **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.
  - ☐ Prioritize isolating critical systems that are essential to daily operations.
  - ☐ If taking the network temporarily offline is not immediately possible, locate the network cable (e.g., ethernet) and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.
  - ☐ For cloud resources, take a snapshot of volumes to get a point in time copy for reviewing later for forensic investigation.
  - ☐ After an initial compromise, malicious actors may monitor your organization's activity or communications to understand if their actions have been detected. Isolate systems in a coordinated manner and use out-of-band communication methods such as phone calls 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 or deploy ransomware widely prior to networks being taken offline.

- ☐ **2. Power down devices if you are unable to disconnect them from the network to avoid further spread of the ransomware infection.**

  Note: This step will prevent your organization 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.

☐ **3. Triage impacted systems for restoration and recovery.**
- ☐ Identify and prioritize critical systems for restoration on a clean network 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. Examine existing organizational detection or prevention systems (e.g., antivirus, EDR, IDS, Intrusion Prevention System) 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, such as Bumblebee, Dridex, Emotet, QakBot, or Anchor. A ransomware event may be evidence of a previous, unresolved network compromise.
    - 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 to further extort the victim and pressure them into paying.
    - Malicious actors often drop ransomware variants to obscure post-compromise activity. Care must be taken to identify such dropper malware before rebuilding from backups to prevent continuing compromises.

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

☐ **6. Initiate threat hunting activities.**
- ☐ For enterprise environments, check for:
    - Newly created AD accounts or accounts with escalated privileges and recent activity related to privileged accounts such as Domain Admins.
    - Anomalous VPN device logins or other suspicious logins.
    - Endpoint modifications that may impair backups, shadow copy, disk journaling, or boot configurations. Look for anomalous usage of built-in Windows tools such as `bcdedit.exe`, `fsutil.exe` (deletejournal), `vssadmin.exe`, `wbadmin.exe`, and `wmic.exe` (shadowcopy or shadowstorage). Misuse of these tools is a common ransomware technique to inhibit system recovery.
    - Signs of the presence of Cobalt Strike beacon/client. Cobalt Strike is a commercial penetration testing software suite. Malicious actors often name Cobalt Strike Windows processes with the same names as legitimate Windows processes to obfuscate their presence and complicate investigations.

- Signs of any unexpected usage of remote monitoring and management (RMM) software (including portable executables that are not installed). RMM software is commonly used by malicious actors to maintain persistence.
- Any unexpected PowerShell execution or use of PsTools suite.
- Signs of enumeration of AD and/or LSASS credentials being dumped (e.g., Mimikatz, `Sysinternals` `ProcDump`, or `NTDSutil.exe`).
- Signs of unexpected endpoint-to-endpoint (including servers) communications, for example, Address Resolution Protocol (ARP) poisoning of an endpoint or command and control traffic relayed between endpoints.
- Potential signs of data being exfiltrated from the network, which may include:
    - Abnormal amount of data outgoing over any port. Open source software can tunnel data over various ports and protocols. For example, ransomware actors have used Chisel to tunnel Secure Shell (SSH) over HTTPS port `443`. Ransomware actors have also used Cloudflared to abuse Cloudflare tunnels to tunnel communications over HTTPS.
    - Presence of Rclone, Rsync, and various web-based file storage services, and FTP/SFTP, which are common tools for data exfiltration (and also used by threat actors to implant malware/tools on affected networks.)
- Newly created services, unexpected scheduled tasks, unexpected software installed, unusual files created, legitimate processes with unexpected child processes, etc.

☐ For cloud environments:

- Enable tools to detect and prevent modifications to IAM, network security, and data protection resources.
- Use automation to detect common issues (e.g., disabling features, introduction of new firewall rules) and take automated actions as soon as they occur. For example, if a new firewall rule is created that allows open traffic (`0.0.0.0/0`), an automated action can be taken to disable or delete this rule and send notifications to the user that created it as well as the security team for awareness. This will help avoid alert fatigue and allow security personnel to focus on critical issues.

Reporting and Notification

Note: Refer to the Contact Information section at the end of this guide for details on how to report and notify about ransomware incidents.

- ☐ **7.** Follow notification requirements as outlined in your cyber incident response and communications plan to **engage 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 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 [CPG 4.A].
  - ☐ Report the incident to—and consider requesting assistance from—CISA, your local FBI field office, the FBI Internet Crime Complaint Center (IC3), or your local U.S. Secret Service field office.
  - ☐ As appropriate, coordinate with communications and public information personnel to ensure accurate information is shared internally with your organization and externally with the public.

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 malware identified on your network.
- Encrypted file samples.
- Log files (e.g., Windows event logs from compromised systems, firewall logs).
- PowerShell scripts found having executed on the network.
- User accounts created in AD or machines added to the network during the exploitation.
- Email addresses used by the attackers and any associated phishing emails.
- Other communication accounts used by the attackers.
- A copy of the ransom note.
- Ransom amount and if 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.

- ☐ **8.** If the incident resulted in a data breach, **follow notification requirements as outlined in your cyber incident response and communications plans.**

Containment and Eradication

If no initial mitigation actions appear possible:

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

Upon voluntary request, CISA and MS-ISAC (for SLTT organizations) can assist with analysis of phishing emails, storage media, logs, and/or malware at no cost to help organizations understand the root cause of an incident.

- CISA – Advanced Malware Analysis Center: malware.us-cert.gov/
- MS-ISAC – Malicious Code Analysis Platform (SLTT organizations only): cisecurity.org/spotlight/cybersecurity-spotlight-malware-analysis/

- ☐ **10. Consult federal law enforcement, even if mitigation actions are possible, regarding possible decryptors available,** as security researchers may have discovered encryption flaws for some ransomware variants and released decryption or other types of tools.

To continue taking steps to contain and mitigate the incident:

- ☐ **11. Research trusted guidance** (e.g., published by sources such as the U.S. Government, MS-ISAC, or a reputable security vendor) 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.

- ☐ **12. Identify the systems and accounts involved in the initial breach.** This can include email accounts.

- ☐ **13.** Based on the breach or compromise details determined above, **contain associated systems that may be used for further or continued unauthorized access.** Breaches often involve mass credential exfiltration. Securing networks and other information sources from continued credential-based unauthorized access may include:
  - ☐ Disable virtual private networks, remote access servers, single sign-on resources, and cloud-based or other public-facing assets.

- ☐ **14.** If server-side data is being encrypted by an infected workstation, **follow server-side data encryption quick identification steps.**
  - ☐ 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 related logs that may identify significant authentication or access events.
  - ☐ Run packet capture software, such as 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`).

- ☐ **15. 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 EDR 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.

- ☐ **16. Rebuild systems based on prioritization of critical services** (e.g., health and safety or revenue-generating services), using pre-configured standard images, if possible. Use infrastructure as code templates to rebuild cloud resources.

- ☐ **17. Issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility** once the environment has been fully cleaned and rebuilt, including any associated impacted accounts and the removal or remediation of malicious persistence mechanisms. This can include applying patches, upgrading software, and taking other security precautions not previously taken. Update customer-managed encryption keys as needed.

- ☐ **18. The designated IT or IT security authority declares the ransomware incident over** based on established criteria, which may include taking the steps above or seeking outside assistance**.**

Recovery and Post-Incident Activity

- ☐ **19. 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 (VLAN) has been created for recovery purposes, ensure only clean systems are added.

- ☐ **20. 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.

- ☐ **21. Consider sharing lessons learned and relevant indicators of compromise with CISA or your sector ISAC** to benefit others within the community.

Contact Information

In responding to any cyber incident, federal agencies will undertake threat response; asset response; and intelligence support and related activities.

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.
- Assistance in conducting a criminal investigation, which may involve collecting incident artifacts, including system images and malware samples.

Federal Asset Response Contacts

Upon voluntary request, federal asset response includes furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery.

CISA:	cisa.gov/report Central@cisa.gov or call (888) 282-0870 Cybersecurity Advisor (cisa.gov/cisa-regions): [Enter your local CISA CSA's phone number and email address.]
MS-ISAC:	For SLTTs, email soc@msisac.org or call (866) 787-4722

Federal Threat Response Contacts

Upon voluntary request, or upon notification of partners, federal threat response includes conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response.

FBI:	fbi.gov/contact-us/field-offices [Enter your local FBI field office POC phone number and email address.]
USSS:	FBI Internet Crime Complaint Center (IC3) at ic3.gov secretservice.gov/contact/field-offices/ [Enter your USSS field office POC phone number and email address.]

Other Federal Response Contacts

NSA: Cybersecurity Collaboration Center Services and Contact Information

Other Response Contacts

Consider filling out Table 1 for use should your organization become affected by ransomware. Consider contacting these organizations for mitigation and response assistance or for notification.

Table 1: Response Contacts Information

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		

RESOURCES

CISA No-Cost Resources

- Information sharing with CISA and MS-ISAC (for SLTT organizations) is bi-directional. This includes 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: cisa.gov/cyber-resource-hub.
    - Assessments include no-cost vulnerability scanning.
- Cyber exercises evaluate or help develop a cyber incident response plan in the context of a ransomware incident scenario: cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages.
- CISA cybersecurity advisors advise on best practices and connect you with CISA resources to manage cyber risk.
- Cyber Security Evaluation Tool (CSET) guides asset owners and operators through a systematic process of evaluating operational technology (OT) and IT. CSET includes the Ransomware Readiness Assessment (RRA), a self-assessment based on a tiered set of practices to help organizations evaluate how well they are equipped to defend and recover from a ransomware incident.

Contacts:

- SLTT and private sector organizations: CISA.JCDC@cisa.dhs.gov

Ransomware Quick References

- StopRansomware.gov—a whole-of-government website that gives ransomware resources and alerts.
- Security Primer – Ransomware (MS-ISAC)—outlines opportunistic and strategic ransomware campaigns, common infection vectors, and best practice recommendations.
- Institute for Security + Technology (IST) Blueprint for Ransomware Defense—an action plan for ransomware mitigation, response, and recovery for small- and medium-sized enterprises.

Additional Resources

- NIST: Zero Trust Architecture
- CISA: Cloud Security Technical Reference Architecture
- CISA: Secure Cloud Business Applications (SCuBA) Project
- CISA: Mitigations and Hardening Guidance for MSPs and Small- and Mid-sized Businesses
- CISA: Protecting Against Cyber Threats to Managed Service Providers and their Customers
- NSA: Mitigating Cloud Vulnerabilities (NSA)

DISCLAIMER OF ENDORSEMENT

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

PURPOSE

This document was developed in furtherance of the authors' cybersecurity missions, including their responsibilities to identify and disseminate threats, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

ACKNOWLEDGEMENTS

Microsoft contributed to this joint guide.