STOP RANSOMWARE </stopransomware>

#StopRansomware Guide

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 Joint Ransomware Task Force </joint-ransomware-task-force>. This guide includes two primary resources:

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

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 <https://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 <https://learn.cisecurity.org/ei-isac-registration>.
  - See the National Council of ISACs <https://www.nationalisacs.org/member-isacs-3> 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 <https://www.fbi.gov/contact-us/field-offices> 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:

- Added FBI and NSA as co-authors based on their contributions and operational insight.
- Incorporated the #StopRansomware <https://www.cisa.gov/stopransomware> effort into the title.
- Added recommendations for preventing common initial infection vectors, including compromised credentials and advanced forms of social engineering.
- Updated recommendations to address cloud backups and zero trust architecture (ZTA).
- Expanded the ransomware response checklist with threat hunting tips for detection and analysis.
- Mapped recommendations to CISA's Cross-Sector Cybersecurity Performance Goals (CPGs) <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>.

Read the full #StopRansomware Guide (May 2023 </resources-tools/resources/stopransomware-guide>).

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 <https://www.cisa.gov/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 <https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>]. Test backup procedures on a regular basis. It is important that backups are maintained offline, as many ransomware variants attempt to find and subsequently delete or encrypt accessible backups to make restoration impossible unless the ransom is paid.

  - 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 <https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].

    - 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 <https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>]. Ensure a hard copy of the plan and an offline version is available.

  - Ensure that data breach notification procedures adhere to applicable state laws. Refer to the National Conference of State Legislatures: Security Breach Notification Laws <https://www.ncsl.org/technology-and-communication/security-breach-notification-laws> for information on each state's data breach notification laws and consult legal counsel when necessary.

  - For breaches involving electronic health information, you may need to notify the Federal Trade Commission (FTC) or the U.S. Department of Health and Human Services (HHS), and—in some cases—the media. Refer to the FTC's Health Breach Notification Rule <https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule> and the HHS Breach Notification Rule <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> for more information.

  - For breaches involving personally identifiable information (PII), notify affected individuals so they can take steps to reduce the chance that their information will be misused. Provide the type of information exposed, recommend remediation actions, and relevant contact information.

  - Notify businesses of a breach if PII stored on behalf of other businesses is stolen.

- 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 <https://www.publicpower.org/system/files/documents/public-power-cyber-incident-response-playbook.pdf> 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** <https://www.cisa.gov/zero-trust-maturity-model> 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

- **Conduct regular vulnerability scanning to identify and address vulnerabilities,** especially those on internet-facing devices, to limit the attack surface [CPG 1.E <https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].
    - CISA offers a no-cost Vulnerability Scanning service and other no-cost assessments: cisa.gov/cyber-resource-hub <https://www.cisa.gov/cyber-resource-hub> [CPG 1.F <https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].

- **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 <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>.

  - 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 <https://media.defense.gov/2020/jan/22/2002237484/-1/-1/0/csi-mitigating-cloud-vulnerabilities_20200121.pdf>.

- **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 <https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].

  - 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 <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-073a>.

  - 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 versions 1 and 2** and upgrade to version 3 (SMBv3) after mitigating existing dependencies (on the part of existing systems or applications) that may break when disabled. Malicious actors use SMB to propagate malware across organizations, so then harden SMBv3:

  - Block or limit internal SMB traffic to systems that require access. This should limit intrusions from moving laterally across your network.

  - Implement SMB signing. This should prevent certain adversary-in-the-middle and pass-the-hash attacks. For more information, refer to Microsoft Mitigating New Technology Local Area Network (LAN) Manager (NTLM) Relay Attacks on Active Directory Certificate Services (AD CS) <https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429> and Microsoft Overview of Server Message Block Signing <https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing>.

  - Block external access of SMB to your network by blocking TCP port 445 with related protocols on User Datagram Protocol (UDP) ports 137–138 and TCP port 139.

  - Implement SMB encryption with Universal Naming Convention (UNC) hardening for systems that support the feature. This should limit the possibility of eavesdropping and interception attacks.

  - Log and monitor SMB traffic to help flag potentially abnormal behaviors.

Initial Access Vector: Compromised Credentials

- **Implement phishing-resistant MFA** <https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf> **for all services**, particularly for email, VPNs, and accounts that access critical systems [CPG 2.H <https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>]. 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 <https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].

- **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 <https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>] [CPG 2.C <https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].

  - 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 <https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].

- **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 <https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage> 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 <https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>]. 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 <https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].

- **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 <https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].

- **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 <https://www.cisa.gov/sites/default/files/publications/cisainsights-cyber-enhanceemailandwebsecurity_s508c-a.pdf> and the Center for Internet Security's blog How DMARC Advances Email Security <https://www.cisecurity.org/insights/blog/how-dmarc-advances-email-security>.

- **Ensure macro scripts are disabled for Microsoft Office files transmitted via email.** These macros can be used to deliver ransomware [CPG 2.N <https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>]. **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 <https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked>. See Microsoft's Block macros from running in Office files from the Internet <https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked#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).

- **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 <https://media.defense.gov/2021/mar/03/2002593055/-1/-1/1/csi_selecting%20a%20protective%20dns%20service_u00117652-21.pdf>.

- **Consider implementing sandboxed browsers** to protect systems from malware originating from web browsing. Sandboxed browsers isolate the host machine from malicious code.

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 <https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_report_v1.0.1_final.pdf>].

  - 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.

- **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.