NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
Cyber Center
Cyber Advisory

The NTIC Cyber Center Ransomware Mitigation Guide

TLP: **WHITE** | ***Ransomware is a type of malicious software (malware) designed to extort money from victims by restricting access to a computer, mobile device, or digital files.*** The most common form of this malware is crypto-ransomware, which uses an encryption process to render devices and files unusable until a decryption key is obtained by the victim. Indiscriminate ransomware infections most often occur because an unsuspecting victim opened a malicious email attachment, clicked on a poisoned link in an email, or visited a compromised website. Targeted ransomware attacks are commonly deployed manually by a cyber threat actor after he or she gains unauthorized access to a system or server on a network. While ransomware attacks cannot completely be prevented, the risk and impact of this type of malware infection can be dramatically reduced by implementing the following cybersecurity strategies and improving cybersecurity awareness within your organization. *(The NTIC Cyber Center provides the following list for informational purposes and does not endorse any specific commercial products, processes, or services.)*

Data Management

- Schedule data backups often and ensure they are kept offline in a separate and secure location. Initially perform a full backup and then conduct either incremental, differential, or mirror backups depending on your organization's needs and capabilities. Consider maintaining multiple backups in different locations for redundancy. Test backups regularly to ensure their integrity.
- If an online backup and recovery service is used, contact the service provider immediately after a ransomware infection is suspected to prevent the malware from overwriting previous file versions with the newly encrypted versions.

System Management

- Use reputable antivirus software and ensure that it is activated and updated with the latest malware definitions. Schedule scans as often as permitted.
- Enable automated patching for operating systems, software, plugins, and web browsers.
- Follow the Principle of Least Privilege for all user accounts and enable User Access Control (UAC) to prevent unauthorized changes to user privileges. Regularly audit user accounts and disable or delete those that are no longer in use.
- Implement application whitelisting to prevent unauthorized or malicious software from executing.
- Turn off unused wireless connections.
- Disable macros on Microsoft Office software.
- Use reputable ad blocking extensions in browsers to prevent "drive-by" infections from advertisements containing malicious code.
- Disable the ***vssadmin.exe*** tool by renaming it to prevent ransomware from deleting Shadow Volume Copies. Instructions on how to rename this tool are included here.
- Disable Windows Script Host and Windows PowerShell.
- Disable Remote Desktop Protocol (RDP), Telnet, and SSH connections on systems and servers if it is not needed in your environment. Block inbound traffic to associated ports.
- If remote access is needed, audit access, whitelist authorized IP addresses, ensure that login credentials are complex, and implement a multifactor authentication solution to prevent unauthorized access.

- Use web filtering tools to block access to malicious websites. Scan all incoming emails, attachments, and downloads and configure email servers to proactively block emails containing suspicious attachments such as ***.exe***, ***.vbs***, and ***.scr***.
- Configure systems by modifying the Group Policy Editor to prevent executables (***.exe***, ***.rar***, ***.pdf***, ***.exe***, ***.zip***) from running in ***%appdata%***, ***%localappdata%***, ***%temp%*** and the Recycle Bin.
- *Implement a behavior blocker to prevent ransomware from executing or making any unauthorized changes to systems or files.
- *Consider utilizing a free or commercially available anti-ransomware tool offered by leading computer security vendors.
- *To counteract ransomware variants that modify the Master Boot Record (MRB) and encrypt the Master File Table (MFT), Cisco Talos has released a Windows disk filter driver called MBRFilter, available on GitHub here.
- *For macOS X users, a free tool called *RansomWhere?* is available to monitor for and prevent ransomware infections. Information about this tool is available on the Objective-See website here and the tool itself can be downloaded here.

**The NTIC Cyber Center recommends exercising caution before downloading any software from the internet, scanning associated files for malware prior to installation, and testing them in a staging environment prior to performing a large-scale deployment.*

Network Management

- Set a network performance baseline for network monitoring prior to an infection to improve your ability to detect anomalies and malicious activity.
- Ensure your firewall is enabled and properly configured.
- Close and monitor unused ports.
- Disable SMBv1 on firewall and all systems on the network.
- Block inbound traffic to TCP/UDP ports 139 and TCP port 445.
- Block known malicious Tor IP addresses. A list of active Tor nodes updated every 30 minutes can be found here.
- Perform vulnerability scans against your organization's IP address range(s) regularly to identify poorly configured and vulnerable internet-facing systems and take the appropriate corrective actions as needed.
- Keep network log files for a full year in the event a ransomware or other network intrusion incident leads to a criminal investigation.

Mobile Device Management

- For Apple iOS devices: ensure data is backed up on iCloud and two-factor authentication is enabled, only download media and apps from the official App Store, and avoid "jailbreaking" the device.
- For Android devices: disable the "unknown sources" option in the Android security settings menu, install apps only from the official Google Play store after carefully reading the associated ratings and reviews, and avoid "rooting" the device.

How to quickly contain a ransomware infection:

- Immediately unplug the Ethernet network cable or disable Wi-Fi on the infected system. This will prevent the ransomware from spreading to other systems on the network or infecting backups that are stored on the network or in a cloud environment. Immediately quarantine the infected system and do not reconnect it to the network until it has been thoroughly scanned and cleaned.
- Alternatively, instruct employees to turn off the power or unplug the power cord from the system. Although doing so may hinder a complete forensic analysis of the infected system, it stops the encryption process and may limit data loss.
- Employees should notify the appropriate information security contact within your organization as quickly as possible.

How to recover after a ransomware infection has occurred:

- Locate backups of the affected data or system that predate the infection (to avoid restoring an infected instance), restore the data, and harden the system and network against future infections.
- If no viable backups are available, conduct an online search of the ransomware variant to see if there is a publicly available decryption tool or remediation method. *No More Ransom!* is one online resource that provides guidance to victims and free decryption tools for a number of variants. Victims are also encouraged to submit an incident report to the NTIC Cyber Center at ncrintel.org and an analyst may be able to provide additional assistance.
- If no decryption tool is available, the only remaining options are to accept the data loss or pay the ransom. The NTIC Cyber Center discourages paying ransoms of any kind, as this perpetuates the crime and does not guarantee data recovery. Additionally, organizations that send ransom payments to known sanctioned individuals may be subject to secondary sanctions, fines, or face other legal ramifications according to a November 2018 press release by the US Department of the Treasury's Office of Foreign Assets Control (OFAC).
- After removing the malware and restoring the machine, change all system, network, and online account passwords and implement the mitigation recommendations provided in this document.