



NJCCIC

NJ CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

Ransomware Mitigation Strategies

October 27, 2016

TLP: **WHITE** | While ransomware infections may not be entirely preventable due to the effectiveness of well-crafted phishing emails or drive-by downloads from otherwise legitimate sites, the most effective strategy to mitigate the impact of ransomware is having a comprehensive data backup protocol. In order to increase the likelihood of preventing ransomware infections, organizations must conduct regular training and awareness exercises with all employees to ensure common understanding safe-browsing techniques and how to identify and avoid phishing attempts.

The following is a list of ransomware mitigation recommendations:

Data Protection

- Schedule backups of data often and ensure they are kept offline in a separate and secure location. Consider maintaining multiple backups in different locations for redundancy. Test your backups regularly.
- If an online backup and recovery service is used, contact the service immediately after a ransomware infection is suspected to prevent the malware from overwriting previous file versions with the newly encrypted versions.

System Management

- Ensure anti-virus software is up-to-date with the latest definitions and schedule scans as often as permitted.
 - Enable automated patches for operating systems, software, plugins, and web browsers.
 - Follow the [Principle of Least Privilege](#) for all user accounts; enable User Access Control (UAC) to prevent unauthorized changes.
 - Turn off unused wireless connections.
 - Disable macros on Microsoft Office software.
 - Use ad blocking extensions in browsers to prevent “drive-by” infections from ads 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) on systems and servers if it is not needed in your environment.
 - Use web and email protection to block access to malicious websites and scan all 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. CryptoPrevent is a free tool that can help automate this process and prevent ransomware from executing. Download it [here](#).
 - 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 by any of the leading computer security software 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 Mac OS X users, consider installing the free tool, *RansomWhere?* Information about this tool is available on the Objective-See website [here](#) and the tool itself can be downloaded [here](#).
-

Network Management

- Keep firewall turned on and properly configured.
- Close and monitor unused ports.
- Block known malicious Tor IP addresses. A list of active Tor nodes updated every 30 minutes can be found [here](#).
- Set a network performance baseline for network monitoring prior to an infection to make looking for anomalies and malicious activity easier after the infection.
- 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 users: ensure your data is backed up on iCloud and enable two-factor authentication, only download media and apps from the official iTunes and App Stores, and avoid “jailbreaking” the device.
- For Android users: disable the “unknown sources” option in the Android security settings menu, only install apps from the official Google Play store, and avoid “rooting” the device.

Post-Infection Remediation

- Alert the appropriate information security contact within your organization if unusual activity is seen on networks, computers, or mobile devices.
- Disconnect from networks immediately if an infection is suspected and do not reconnect until the computer or device has been thoroughly scanned and cleaned.
- Depending on the variant, a free decryption tool may be available. To determine which variant infected your system, please see the Appendix of this product or use the [ID Ransomware website](#).
- If an infection occurs, after removing the malware and cleaning the machine, make sure to change all system, network, and online account passwords.

Reporting

If your organization is the victim of a ransomware infection, or would like to learn more about the NJCCIC, please contact a Cyber Liaison at njccic@cyber.nj.gov or visit www.cyber.nj.gov.