NJCCIC

NJ Cybersecurity and Communications Integration Cell

Ransomware: Risk Mitigation Strategies

TLP: **WHITE** | While ransomware infections are not entirely preventable due to the effectiveness of well-crafted phishing emails and drive-by downloads from otherwise legitimate sites, organizations can drastically reduce this risk by implementing cybersecurity strategies and improving cybersecurity awareness and practices of all employees. The most effective strategy to mitigate the risk of data loss resulting from a successful ransomware attack is having a comprehensive data backup process in place; however, backups must be stored off the network and tested regularly to ensure integrity. To increase the likelihood of preventing ransomware infections, organizations must conduct regular training exercises and awareness briefings with all employees to ensure understanding of safe-browsing techniques and how to avoid phishing attempts. The following is a comprehensive list of recommendations, though not exhaustive, to reduce the risk posed by ransomware infections:

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 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.
- Implement application whitelisting to prevent unauthorized or malicious software from executing.
- 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), 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, ensure that login credentials are complex, and implement a 2FA solution to prevent unauthorized access.
- 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. It can be downloaded 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 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 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

- 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.
- 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 devices: ensure data is backed up on iCloud and two-factor authentication is enabled, only download media and apps from the official iTunes and App Stores, and avoid “jailbreaking” the device.
- For Android devices: 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.

How to limit the impact of ransomware infections:

1. All employees should be instructed to immediately unplug the Ethernet network cable or disable Wi-Fi on the system if they suspect a ransomware infection has initiated. This will prevent the ransomware from spreading to other devices on the network or infecting backups that are stored on the network or in a cloud environment. Do not reconnect until the computer or device has been thoroughly scanned and cleaned.
2. Alternatively, instruct employees to turn off the power or unplug the power cord from the system. Although doing so inhibits complete forensic analysis of the infected device, it stops the encryption process and may limit data loss.
3. Employees should notify the appropriate information security contact within your organization as quickly as possible.

How to recover after a ransomware infection has occurred:

1. Are there complete backups for the affected data or system that predate the infection (to avoid restoring an infected instance)? If so, restore from backups and take steps to prevent future infections.
2. If not, is there a publicly available decryption tool or remediation method? Refer to the NJCCIC’s Ransomware Threat Profile for a comprehensive list of ransomware variants and those with known decryption tools.
3. If no decryption tool is available, the only remaining options are to accept the loss or pay the ransom. The NJCCIC discourages paying ransoms of any kind, as this perpetuates the crime and does not guarantee recovery of data.
4. After removing the malware or restoring the machine, make sure to change all system, network, and online account passwords and implement the mitigation recommendations provided in this document.

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.