CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

RANSOMWARE - Cyber Hygiene and Best Practices

The following information is being provided by the Federal Bureau of Investigation (FBI) with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cybersecurity professionals and system administrators guard against the persistent malicious actions of cyber criminals.

The FBI recommends the adoption of a number of best cybersecurity practices to reduce exposure to the threat of ransomware. Key areas on which to focus in combating successful ransomware attacks are prevention, business continuity, and remediation. Below is a list of best practices in those areas for consideration:

- Implementation of a security information and event management (SIEM) solution. SIEM solutions typically provide real-time analysis of security alerts generated by applications and network hardware. Vendors sell SIEM as software, appliances, or as managed services; these products are also used to log security data and generate reports for compliance purposes. A SIEM can not only alert administrators to security issues but may also speed up remediation by providing the ability to collect and review log data in a centralized location.
- Installation of an intrusion detection or intrusion prevention system on the network. An intrusion detection system is a device or software application that monitors a network or systems for malicious activity or policy violations. Any malicious activity or violation is typically reported either to an administrator or collected centrally using a SIEM. An intrusion prevention system has the same functionality as an intrusion detection system with the added feature of response capabilities. Intrusion detection and prevention systems can alert administrators to security issues.
- Patch the operating system, software, and firmware on devices. All endpoints should be patched as vulnerabilities are discovered. This can be made easier through a centralized patch management system.
- Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.
- Manage the use of privileged accounts. Implement the principle of least privilege. No users should be assigned administrative access unless absolutely needed. Those with a need for

administrator accounts should use them only when necessary; and they should operate with standard user accounts at all other times. Limit domain administration to air gapped devices.

- Implement least privilege for file, directory, and network share permissions. If a user needs only to read specific files, they should not have write access to those files, directories, or shares. Configure access controls with least privilege in mind.
- Disable macro scripts from Microsoft Office files transmitted via e-mail. Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full Office suite applications.
- Implement software restriction policies or other controls to prevent the execution of programs in common ransomware locations, such as temporary folders supporting popular Internet browsers, or compression/decompression programs, including those located in the AppData/LocalAppData folder.
- Regularly back up data and verify its integrity.
- Secure your backups. Ensure backups are not connected to the computers and networks they are backing up. Backups are critical in ransomware; if you are infected, offline backups may be the best way to recover your critical data.
- Implement application whitelisting. Only allow systems to execute programs known and permitted by security policy. Limit which users or systems can execute network administration commands (e.g., PsExec) or applications.
- Use virtualized environments or sandboxing software to execute operating system environments or specific programs.
- Categorize data based on organizational value, and implement physical/logical separation of networks and data for different organization units. For example, sensitive research or business data should not reside on the same server and/or network segment as an organization's e-mail environment.
- Require user interaction for end user applications communicating with websites uncategorized by the network proxy or firewall. Examples include requiring users to type information or enter a password when their system communicates with a website uncategorized by the proxy or firewall.
- Require multifactor authentication and regular patching for remote desktop software packages. Restrict the number of users or accounts utilizing remote desktop software packages.
- Test restoration system files from backups regularly.
- Draft a remediation/recovery plan and test the remediation/recovery plan regularly. Coordinate remediation plans with other stakeholders (e.g., legal counsel) so everyone can make informed decisions when an actual ransomware incident occurs.
- Block e-mail messages with attachments from unknown or blacklisted sources.
- Conduct regular red team assessments of network security controls.
- Implement password controls, including minimum strength requirements, account lockouts, password change requirements, and failed log-on logging.

If you are the victim of a ransomware event, please contact the FBI. You may do so by filing a detailed complaint with the Internet Crime Complaint Center (http://www.ic3.gov) or contacting your local Cyber Task Force (http://www.fbi.gov/contact-us/field).