

Security Advisory: Petya Ransomware Attack

Date: June 28, 2017

Version: 1.0

Recommendations

- In order to prevent infection, users and organizations are advised to apply patches to Windows systems as mentioned in Microsoft Security Bulletin MS17-010. <https://technet.microsoft.com/library/security/MS17-010>
- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
- Block SMB ports on Enterprise Edge/perimeter network devices [UDP 137, 138 and TCP 139, 445] or Disable SMBv1.
- <https://support.microsoft.com/en-us/help/2696547>
- Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser.
- Restrict execution of powershell /WSCRIPT/ PSEXEC / WMIC in enterprise environment Ensure installation and use of the latest version (currently v5.0) of PowerShell, with enhanced logging enabled. script block logging, and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.
- Establish a Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) for your domain, which is an email validation system designed to prevent spam by detecting email spoofing by which most of the ransomware samples successfully reaches the corporate email boxes.
- Application whitelisting/Strict implementation of Software Restriction Policies (SRP) to block binaries running from %APPDATA%, %PROGRAMDATA% and %TEMP% paths. Ransomware sample drops and executes generally from these locations. Enforce application whitelisting on all endpoint workstations.
- Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.
- Disable macros in Microsoft Office products. Some Office products allow for the disabling of macros that originate from outside of an organization and can provide a hybrid approach when the organization depends on the legitimate use of macros. For Windows, specific settings can block macros originating from the Internet from running.
- Configure access controls including file, directory, and network share permissions with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.
- Maintain updated Antivirus software on all systems.
- Consider installing Enhanced Mitigation Experience Toolkit, or similar host-level anti-exploitation tools.
- Block attachments of file-types, exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf
- Regularly check the contents of backup files of databases for any unauthorized encrypted contents of data records or external elements, (backdoors /malicious scripts.)
- Keep the operating system third party applications (MS office, browsers, browser Plugins) up-to-date with the latest patches.
- Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.

- Network segmentation and segregation into security zones - help protect sensitive information and critical services. Separate administrative network from business processes with physical controls and Virtual Local Area Networks.
- Disable remote Desktop Connections, employ least-privileged accounts.
- Ensure integrity of the codes /scripts being used in database, authentication and sensitive systems, Check regularly for the integrity of the information stored in the databases.
- Restrict users' abilities (permissions) to install and run unwanted software applications.
- Employ data-at-rest and data-in-transit encryption.

Individuals or organizations are not encouraged to pay the ransom, as this does not guarantee files will be released. Report such instances of fraud to CERT-In and Law Enforcement agencies.

References

- <https://isc.sans.edu/forums/diary/Checking+out+the+new+Petya+variant/22562/>
- <https://www.symantec.com/connect/blogs/petya-ransomware-outbreak-here-s-what-you-need-know>
- <https://kc.mcafee.com/corporate/index?page=content&id=KB89540>

