certin
Handling Computer Security Incidents

Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

VIRUS ALERTS

Sarbloh Ransomware

Original Issue Date:March 12, 2021

Virus Type: Ransomware

It has been reported that a new ransomware named "Sarbloh" is spreading via specially crafted malicious documents sent as spear phishing email attachments. Malicious document is embedded with Marco with a heavily obfuscated VBA code, which downloads original payload (Sarbloh Ransomware) from an AWS URL silently. Once executed, it encrypts files on affected system (Audio, images, video, databases, and other document files) and renames the encrypted files with the ".sarbloh" extension to make them unusable. The ransom note ("README_SARBLOH.txt") states that the user's files are encrypted and will not be recovered until Sarbloh's creator's demands are fulfilled.

Best Practices and remedial measures:

Users and administrators are advised to take the following preventive measures to protect their computer networks from ransomware infection/attacks:

- Maintain updated Antivirus software on all systems
- Keep the operating system third party applications (MS office, browsers, browser Plugins) up-to-date with the latest patches.
- Do not 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
- Do not enable Macros if prompted by document received from untrusted sources.
- Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.
- 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.
- Check regularly for the integrity of the information stored in the databases.
- Regularly check the contents of backup files of databases for any unauthorized encrypted contents of data records or external elements, (backdoors /malicious scripts.)
- If not required consider disabling, PowerShell / windows script hosting.
- Restrict users' abilities (permissions) to install and run unwanted software applications.
- Enable personal firewalls on workstations.
- Enabled Windows Defender Application Guard with designated the trusted sites as whitelisted, so that rest all sites will be open in container to block the access to memory, local storage, other installed applications or any other resources of interest to the attacker.
- Enable Exploit Protection [Successor to EMET] that includes several client side mitigation steps. Detailed configuration steps can be seen in https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/enable-exploit-protection. Turn on attack surface reduction Rules, including rules that block credential theft, ransom ware activity, and suspicious use of PsExec and WMI.
- Implement strict External Device (USB drive) usage policy.
- Employ data-at-rest and data-in-transit encryption.
- Consider installing Enhanced Mitigation Experience Toolkit, or similar host-level anti-exploitation tools.
- Block the attachments of file types, exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf
- Carry out vulnerability Assessment and Penetration Testing (VAPT) and information security audit of critical networks/systems, especially database servers from CERT-IN empaneled auditors. Repeat audits at regular intervals.

- 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
- Refer following advisory for additional best practices to prevent ransomware attacks https://www.csk.gov.in/alerts/ransomware.html

References

https://blogs.quickheal.com/activists-turn-hacktivists-new-ransomware-that-does-not-demand-money/
https://www.csk.gov.in/alerts/ransomware.html