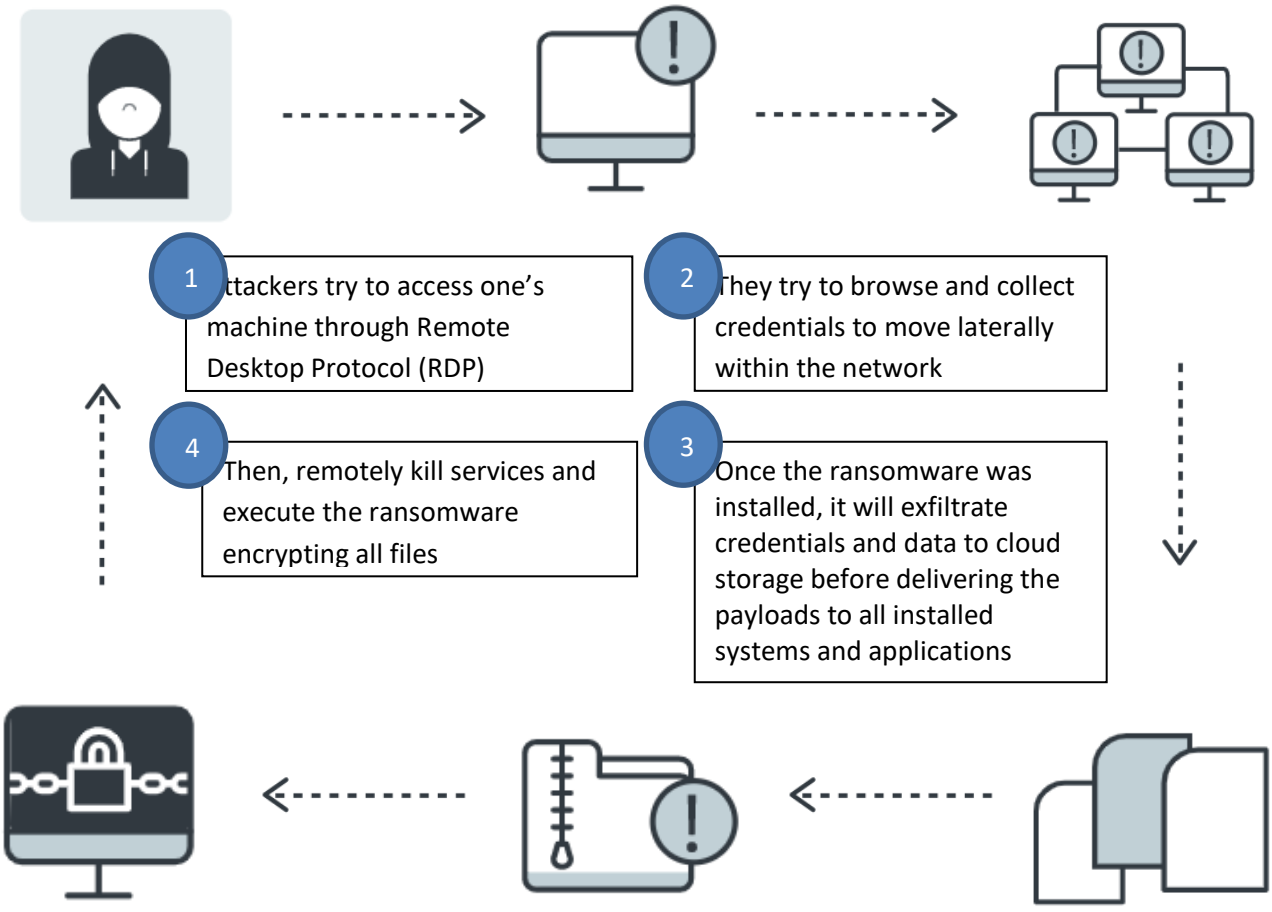
Nefilim Ransomware
(CSB21-02)

Nefilim ransomware emerged in March 2020 targeting businesses worldwide. Nefilim operates by encrypting the files of infected systems and demand payment for decryption tool/key. All compromised files are appended with the ".NEFILIM" extension. Nefilim authors threatens to release their victim's sensitive information on the Dark Web if their victim fails to pay to their demands within seven (7) days.

Nefilim ransomware reportedly shares a similarity in code with Nemty ransomware which was discovered in August 2019. The main difference between the said ransomware is that Nefilim has removed the Ransomware-as-a-Service (RaaS) component, relying on email communications for payment instead of using Tor payment sites.

HOW IT WORKS



IMPACT

- Manipulates, interrupt, or destroy your systems to disrupt availability, compromise integrity.
- Encrypts data and possible leak of sensitive information on the Dark Web.

MITIGATIONS

- Disconnect affected system from the network.
- Use antivirus and anti-malware software to clean the ransomware.
- Perform a full system scan in safe mode to remove any infections.

PREVENTION

- Avoid installing free programs found on the internet.
- Ensure that all systems and software are up-to-date.
- Take inventory of network devices and software. Remove unwanted, unneeded, or unexpected hardware and software from the network.
- Use strong passwords and multi-factor authentication on Remote Desktop connection.
- Always update anti-virus and anti-malware software.
- Always backup your data.
- Regularly conduct anti-virus and anti-malware scans.
- Do not open mails and mail attachment from unknown services.
- Do not download or use illegal software.

REFERENCE

- https://www.bleepingcomputer.com/news/security/new-nefilim-ransomware-threatens-to-release-victims-data/
- https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/updated-analysis-on-nefilim-ransomware-s-behavior
- https://www.sophos.com/en-us/press-office/press-releases/2021/01/sophos-tracks-nefilim-and-other-ransomware-attacks.aspx