#REF:105
#Released on:15/04/2020

‘Nefilim’ Ransomware threatens to leak victim’s data

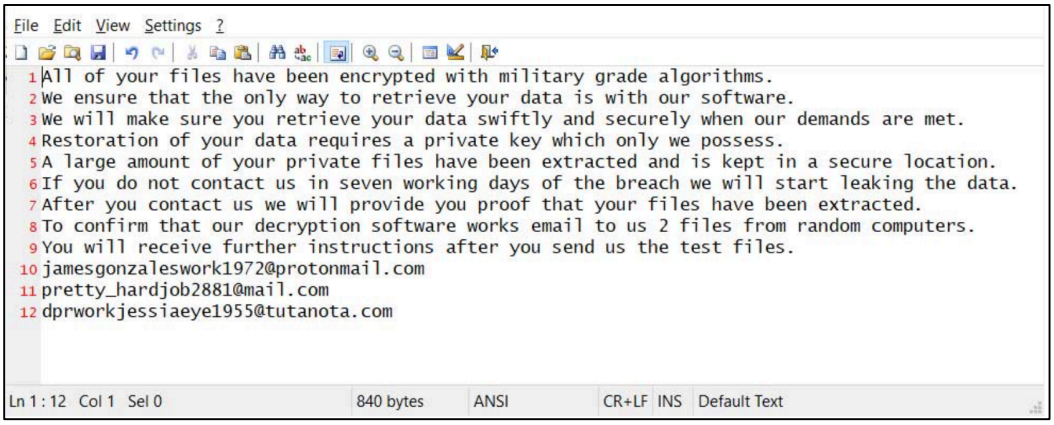
Threat Level
High

Overview
A new ransomware called ‘Nefilim’ threatens to release collected sensitive data of the victims in the public domain if the ransom is not paid.

Description
‘Nefilim’ started to be active at end of February 2020 and the ransomware is most likely to spread through exposed remote desktop services. The ransomware code is similar to the ‘Nemty’ ransomware and the only difference is that ‘Nefilim’ communicates with victims through emails rather than using TOR for the payments. The ransomware note says that, if the victim does not pay the ransom within seven days it will release the stolen data in the public domain.

‘Nefilim’ ransomware is using AES-128 encryption which is impossible to decrypt without the RSA private key. All encrypted files will have the file extension of **‘.NEFILIM’**. As an example a file called a.jpg would be encrypted and named as a.jpg.NEFILIM. After the encryption is completed ransomware note will be displayed on the victim’s computer.

According to the Head of SentinelLabs there is no way to decrypt files without paying the ransom and researchers are still working on a fix.



Impact
- Loss of important files and documents of your company’s data
- May result in complete shutdown of your company’s operations
- Financial loss
- Damaged to your company’s reputation

Solution/ Workarounds
- Implement proper backup policies and adhere to them strictly
- Never pay the ransom
- Have offline backups of important files
- Update and install latest security patches on installed 3 party software
- Keep your virus guard and operating system up to date

#REF:105
#Released on:15/04/2020

Reference

- https://www.bleepingcomputer.com/news/security/new-nefilim-ransomware-threatens-to-release-victims-data/
- https://medium.com/@cyble/nefilim-ransomware-operators-breached-mas-holdings-south-asias-largest-manufacturer-of-lingerie-b19fa3abe82

Disclaimer