



'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.

A screenshot of a ransomware note displayed in a text editor window. The note is a list of 12 numbered items. The first 9 items are instructions and threats, and the last 3 items are email addresses. The text editor has a menu bar (File, Edit, View, Settings, ?) and a toolbar with various icons. The status bar at the bottom shows 'Ln 1: 12 Col 1 Sel 0', '840 bytes', 'ANSI', 'CR+LF', 'INS', and 'Default Text'.

```
1 All of your files have been encrypted with military grade algorithms.  
2 We ensure that the only way to retrieve your data is with our software.  
3 We will make sure you retrieve your data swiftly and securely when our demands are met.  
4 Restoration of your data requires a private key which only we possess.  
5 A large amount of your private files have been extracted and is kept in a secure location.  
6 If you do not contact us in seven working days of the breach we will start leaking the data.  
7 After you contact us we will provide you proof that your files have been extracted.  
8 To confirm that our decryption software works email to us 2 files from random computers.  
9 You will receive further instructions after you send us the test files.  
10 jamesgonzaleswork1972@protonmail.com  
11 pretty_hardjob2881@mail.com  
12 dprworkjessiaeye1955@tutanota.com
```

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

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

The information provided herein is on "as is" basis, without warranty of any kind.