# New Nefilim Ransomware Threatens to Release Victims' Data

bleepingcomputer.com/news/security/new-nefilim-ransomware-threatens-to-release-victims-data/

Lawrence Abrams

By
Lawrence Abrams

- March 17, 2020
- 12:28 PM
- 0

A new ransomware called Nefilim that shares much of the same code as Nemty has started to become active in the wild and threatens to release stolen data.

Nefilim became active at the end of February 2020 and while it not known for sure how the ransomware is being distributed, it is most likely through exposed Remote Desktop Services.

Head of SentinelLabs Vitali Kremez and ID Ransomware's Michael Gillespie both told BleepingComputer that Nefilim and Nemty 2.5 share much of the same code.

The main difference is that Nefilim has removed the Ransomware-as-a-Service (RaaS) component and now relies on email communications for payments rather than a Tor payment site.

It is not known if this is a fork of their ransomware from the original operators or if new threat actors obtained the source code to release a new version.

## Nefilim threatens to release data

In the Nefilim ransom note, the attackers state that if a user does not pay the ransom in seven days they will release data that was stolen from the network.

A large amount of your private files have been extracted and is kept in a secure location.
If you do not contact us in seven working days of the breach we will start leaking the data.
After you contact us we will provide you proof that your files have been extracted.

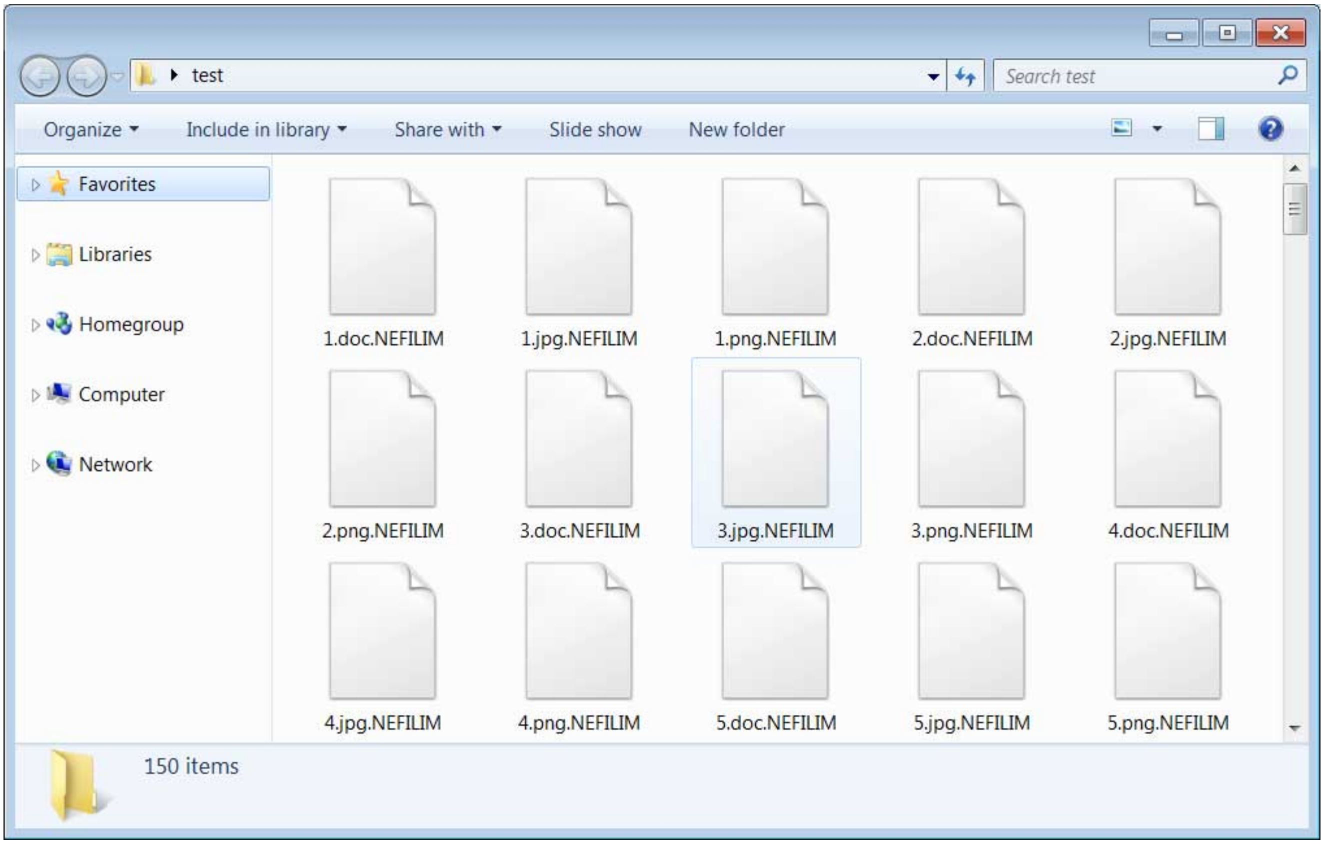
In the past, this would have been seen as an empty threat, but with ransomware infections such as Maze, Sodinokibi, DoppelPaymer, and Nemty all following through with their threats, it should no longer be ignored.

## The Nefilim encryption process

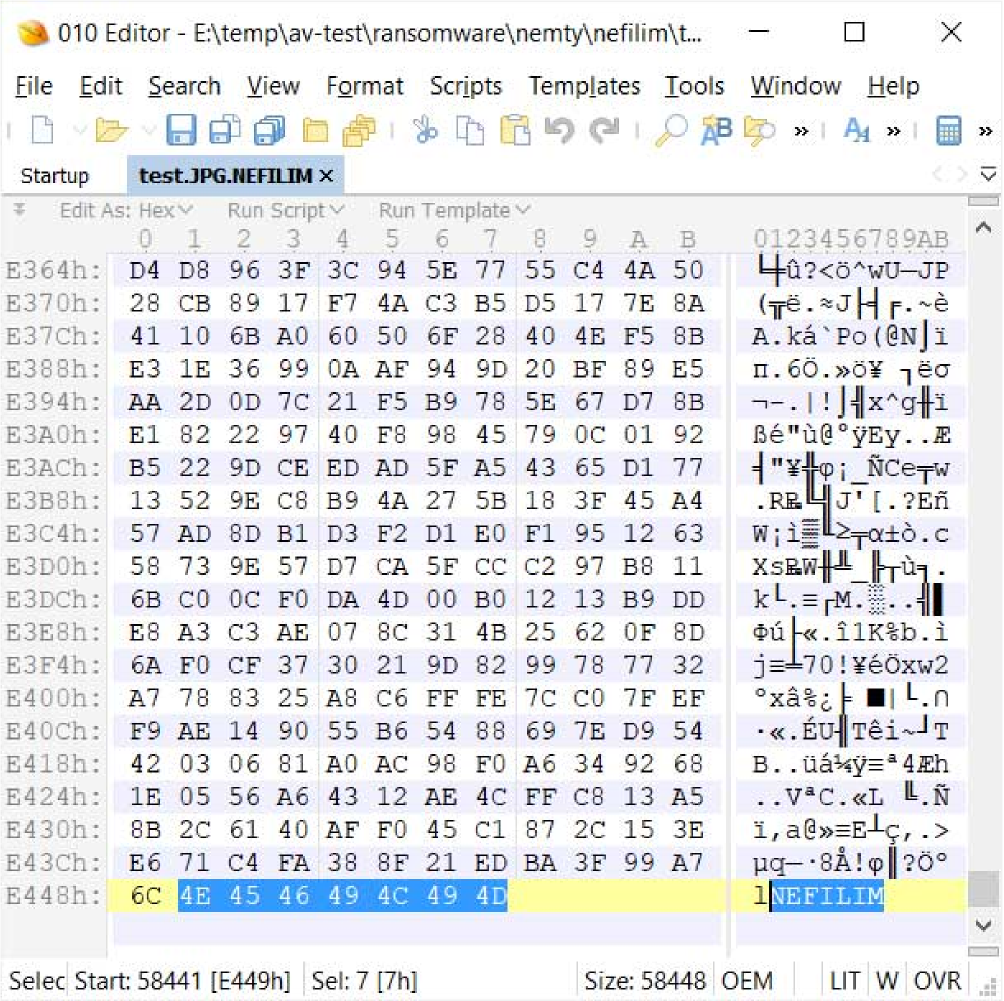
When encrypting files, Nefilim will encrypt a file using AES-128 encryption. This AES encryption key will then be encrypted by an RSA-2048 public key that is embedded in the ransomware executable.

This encrypted AES key will then be added to the contents of each encrypted file and can only be decrypted by the RSA private key known to the ransomware developers.

For each encrypted file, Nefilim will append the **.NEFILIM** extension to the file name. For example, a file called 1.doc would be encrypted and named 1.doc.NEFILIM.



**Files encrypted by the Nefilim Ransomware**
In addition to the encrypted AES key, the ransomware will also add the "NEFILIM" string as a file marker to all encrypted files as shown below.

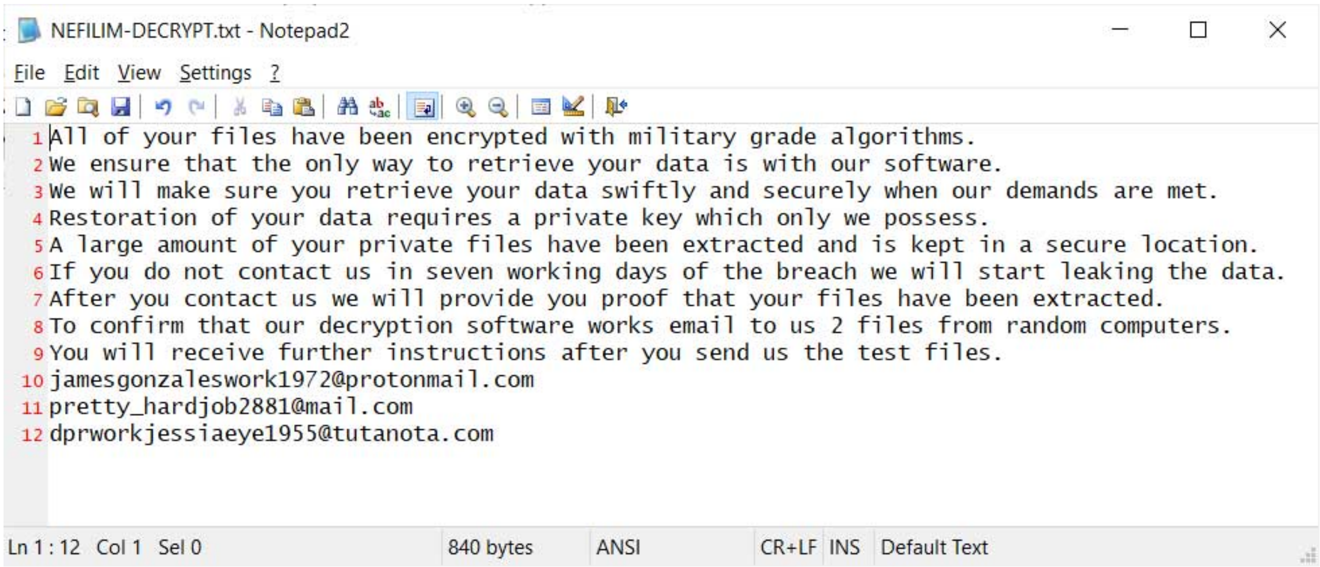

010 Editor - E:\temp\av-test\ransomware\nemty\nefilim\t...
File Edit Search View Format Scripts Templates Tools Window Help
Startup
test.JPG.NEFILIM ×
Edit As: Hex
Run Script
Run Template

```
        0  1  2  3  4  5  6  7  8  9  A  B   0123456789AB
E364h: D4 D8 96 3F 3C 94 5E 77 55 C4 4A 50  ╘╪û?<ö^wU─JP
E370h: 28 CB 89 17 F7 4A C3 B5 D5 17 7E 8A  (╦ë.≈J├╡╒.~è
E37Ch: 41 10 6B A0 60 50 6F 28 40 4E F5 8B  A.ká`Po(@N⌡ï
E388h: E3 1E 36 99 0A AF 94 9D 20 BF 89 E5  π.6Ö.»ö¥ ┐ëσ
E394h: AA 2D 0D 7C 21 F5 B9 78 5E 67 D7 8B  ¬-.|!⌡╣x^g╫ï
E3A0h: E1 82 22 97 40 F8 98 45 79 0C 01 92  ßé"ù@°ÿEy..Æ
E3ACh: B5 22 9D CE ED AD 5F A5 43 65 D1 77  ╡"¥╬φ¡_ÑCe╤w
E3B8h: 13 52 9E C8 B9 4A 27 5B 18 3F 45 A4  .R₧╚╣J'[.?Eñ
E3C4h: 57 AD 8D B1 D3 F2 D1 E0 F1 95 12 63  W¡ì▒╙≥╤α±ò.c
E3D0h: 58 73 9E 57 D7 CA 5F CC C2 97 B8 11  Xs₧W╫╩_╠┬ù╕.
E3DCh: 6B C0 0C F0 DA 4D 00 B0 12 13 B9 DD  k└.≡┌M.░..╣▌
E3E8h: E8 A3 C3 AE 07 8C 31 4B 25 62 0F 8D  Φú├«.î1K%b.ì
E3F4h: 6A F0 CF 37 30 21 9D 82 99 78 77 32  j≡╧70!¥éÖxw2
E400h: A7 78 83 25 A8 C6 FF FE 7C C0 7F EF  ºxâ%¿╞ ■|└.∩
E40Ch: F9 AE 14 90 55 B6 54 88 69 7E D9 54  ∙«.ÉU╢Têi~┘T
E418h: 42 03 06 81 A0 AC 98 F0 A6 34 92 68  B..üá¼ÿ≡ª4Æh
E424h: 1E 05 56 A6 43 12 AE 4C FF C8 13 A5  ..VªC.«L ╚.Ñ
E430h: 8B 2C 61 40 AF F0 45 C1 87 2C 15 3E  ï,a@»≡E┴ç,.>
E43Ch: E6 71 C4 FA 38 8F 21 ED BA 3F 99 A7  µq─·8Å!φ║?Öº
E448h: 6C 4E 45 46 49 4C 49 4D              lNEFILIM
```

**NEFILIM file marker**

When done, a ransom note named **NEFILIM-DECRYPT.txt** will be created throughout the system that contains instructions on how to contact the ransomware developers.

This ransom note contains different contact emails and the threat that they will leak data if a ransom is not paid within seven days of the "breach".



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

Caption

Unfortunately, a brief analysis by Gillespie indicates that this ransomware appears to be secure, which means that there is no current way to recover files for free.

The ransomware, though, is still being researched and if new weaknesses we will publish updated information.

### Related Articles:

Industrial Spy data extortion market gets into the ransomware game

New RansomHouse group sets up extortion market, adds first victims

Quantum ransomware seen deployed in rapid network attacks

Ransom payment is roughly 15% of the total cost of ransomware attacks

Karakurt revealed as data extortion arm of Conti cybercrime syndicate

## IOCs

### Hashes:

```
5ab834f599c6ad35fcd0a168d93c52c399c6de7d1c20f33e25cb1fdb25aec9c6
```

### Associated files:

```
NEFILIM-DECRYPT.txt
```

### Associated emails:

```
jamesgonzaleswork1972@protonmail.com
pretty_hardjob2881@mail.com
dprworkjessiaeye1955@tutanota.com
```

### Ransom note text:

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

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.