



New Cybersecurity MS Degree

Earn a Master's degree that makes an impact. Enroll in the on-campus Cybersecurity M.S.

cybersecurity.ccny.cuny.edu

[OPEN](#)

[Home](#) > [News](#) > [Security](#) > [New Nefilim Ransomware Threatens to Release Victims' Data](#)

◀ 30

New Nefilim Ransomware Threatens to Release Victims' Data

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





US Commerce Dept Shares Tips On Securing Virtual Meetings

[READ MORE >>](#)

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.



***New* Cybersecurity Degree**

The City College of New York

Earn a Master's degree that makes a difference in the world.
Enroll in the on-campus Cybersecurity Master's program.
cybersecurity.ccny.cuny.edu

OPEN

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.

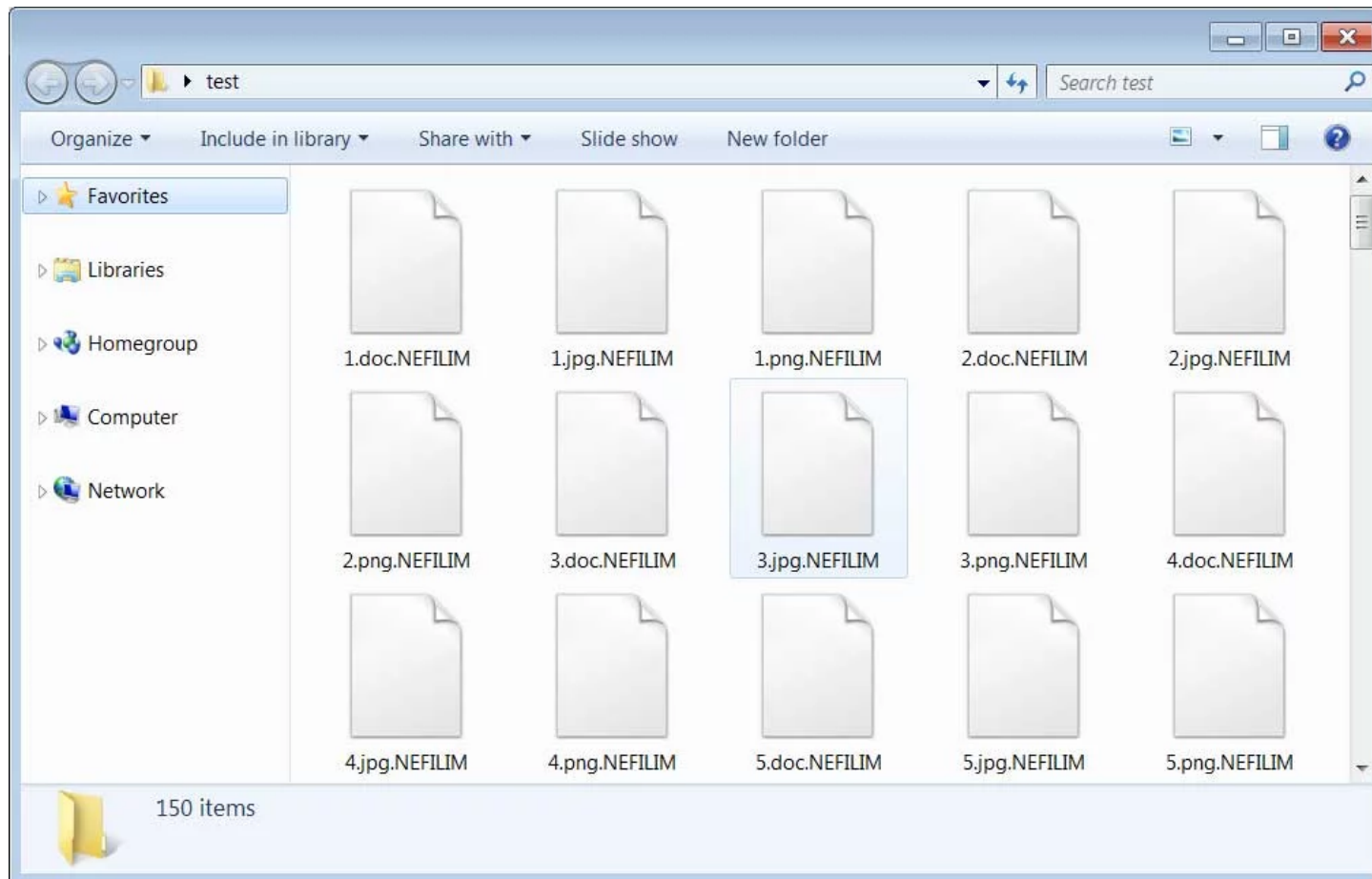
In the past, this would have been seen as an empty threat, but with ransomware infections such as Maze, Sodinokibi, DoppelPaymer, and Nemty all following through with their threats, it should no longer be ignored.

The Nefilim encryption process

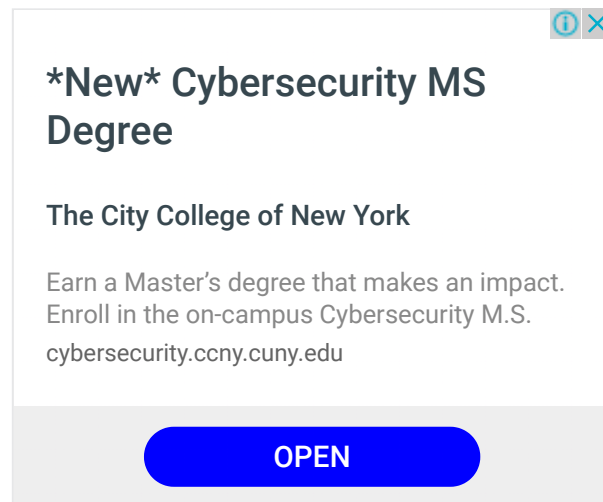
When encrypting files, Nefilim will encrypt a file using AES-128 encryption. This AES encryption key will then be encrypted by an RSA-2048 public key that is embedded in the ransomware executable.

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.

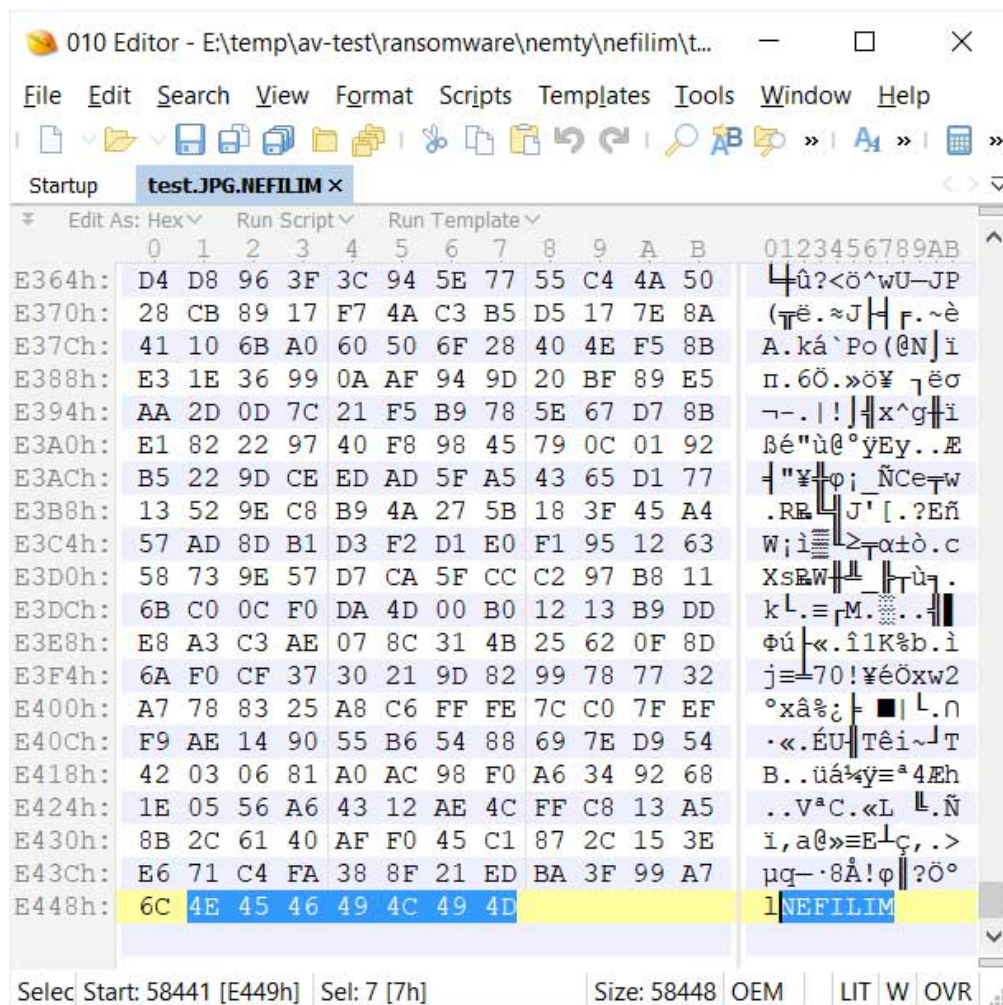
For each encrypted file, Nefilim will append the **.NEFILIM** extension to the file name. For example, a file called 1.doc would be encrypted and named 1.doc.NEFILIM.



Files encrypted by the Nefilim Ransomware



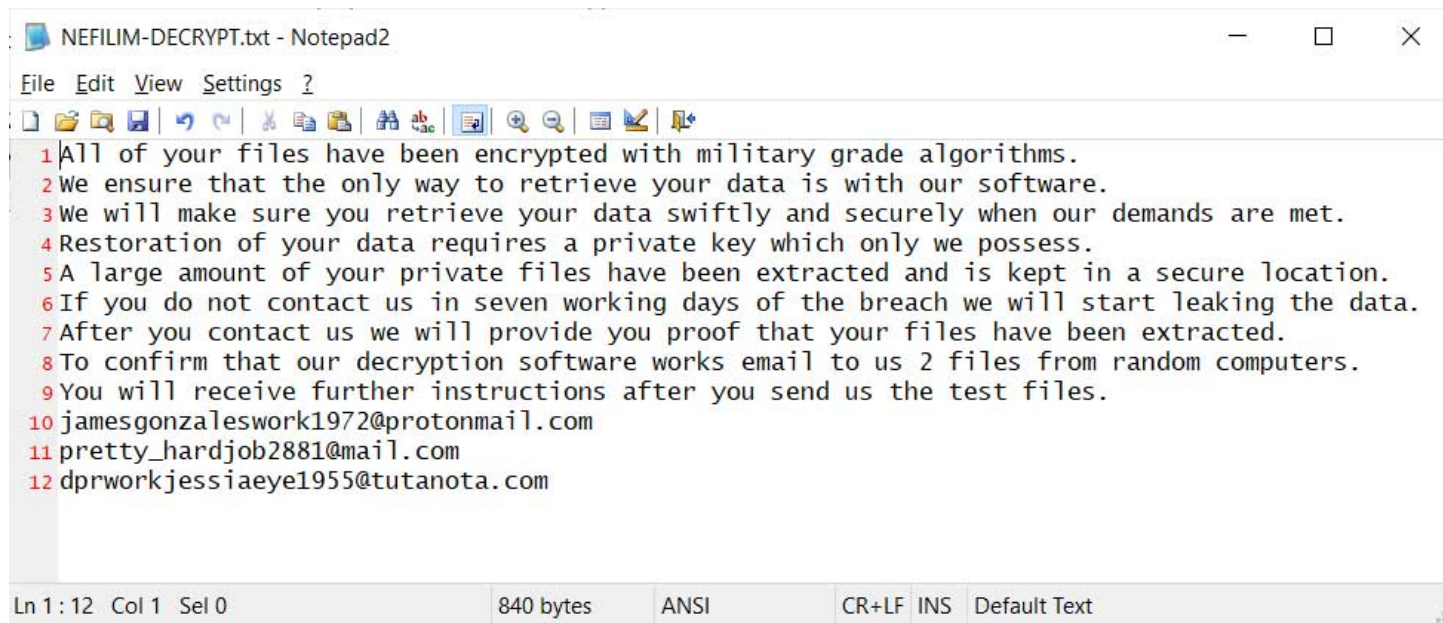
In addition to the encrypted AES key, the ransomware will also add the "NEFILIM" string as a file marker to all encrypted files as shown below.



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".



```
NEFILIM-DECRYPT.txt - Notepad2
File Edit View Settings ?
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 jamesgonzalesswork1972@protonmail.com
11 pretty_hardjob2881@mail.com
12 dprworkjessiaeye1955@tutanota.com
Ln 1: 12 Col 1 Sel 0 840 bytes ANSI CR+LF INS Default Text
```

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:

Ransomware Threatens to Reveal Company's 'Dirty' Secrets

Nemty Ransomware Punishes Victims by Posting Their Stolen Data

Sodinokibi Ransomware May Tip NASDAQ on Attacks to Hurt Stock Prices

DoppelPaymer Ransomware Launches Site to Post Victim's Data

DoppelPaymer Ransomware Sells Victims' Data on Darknet if Not Paid

IOCs

Hashes:

```
5ab834f599c6ad35fcd0a168d93c52c399c6de7d1c20f33e25cb1fdb25aec9c6
```

Associated files:

```
NEFILIM-DECRYPT.txt
```

Associated emails:

```
jamesgonzalesswork1972@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.

jamesgonzalesswork1972@protonmail.com
pretty_hardjob2881@mail.com
dprworkjessiaeye1955@tutanota.com

***New* Cybersecurity MS Degree - The City College of New York**

Earn a Master's degree that makes an impact. Enroll in the on-campus Cybersecurity M.S.
cybersecurity.cuny.edu

OPEN

[DATA EXFILTRATION](#)[EXTORTION](#)[NEFILIM](#)[NEMTY RANSOMWARE](#)[RANSOM](#)[RANSOMWARE](#)

LAWRENCE ABRAMS

Lawrence Abrams is the creator and owner of BleepingComputer.com. Lawrence's area of expertise includes 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.

[◀ PREVIOUS ARTICLE](#)[NEXT ARTICLE ▶](#)

Post a Comment

[Community Rules](#)

You need to login in order to post a comment

[Login](#)

[Not a member yet? Register Now](#)

You may also like:



***New* Cybersecurity
MS Degree - The City
College of New York**

Ad cybersecurity.ccny.cuny.edu

**Bumbling Hacker
"Bitcoin Baron"
Sentenced to 20
Months in Prison**

bleepingcomputer.com

**huawei p30 lite 激安
通販 - ファーウェイP30
Lite本体が安い**

Ad qoo10.jp

**Anonymous Member
Arrested in Ohio**

bleepingcomputer.com

**Secure Embedded
Linux Platform - CVEs
and Bug Fixes**

Ad mvista.com

**CIA Created Toolkit for
Hacking Hundreds of
Routers Models**

bleepingcomputer.com

**Older Versions of
Chrome - Download**

bleepingcomputer.com

**Microsoft Ren
Windows 10 1
Realtek Driver
Block**

bleepingcomputer.com

广告 X

***New* Cybersecurity MS Degree**

The City College of New York

Earn a Master's degree that makes an impact.
Enroll in the on-campus Cybersecurity M.S.
cybersecurity.ccny.cuny.edu

OPEN

POPULAR STORIES



US Democratic Party Symbol Changed to a Rat in Google Search

.....



**Windows 10 KB4551762
Security Update Fails to Install,
Causes Issues**

**NEWSLETTER SIGN
UP**

To receive periodic updates
and news from
BleepingComputer, please
use the form below.

Submit

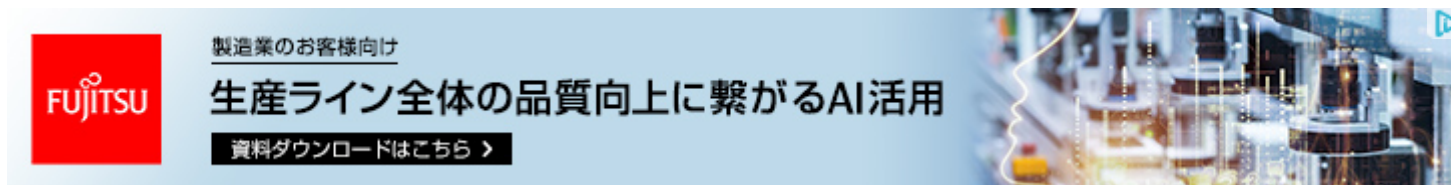
广告 X

***New* Cybersecurity MS Degree**

The City College of New York

Earn a Master's degree that makes an impact.
Enroll in the on-campus Cybersecurity M.S.
cybersecurity.ccny.cuny.edu

OPEN



NEWSLETTER SIGN UP

Email Address...

SUBMIT

Follow us:    

MAIN SECTIONS

[News](#)

[Downloads](#)

[Virus Removal Guides](#)

[Tutorials](#)

[Startup Database](#)

[Uninstall Database](#)

[File Database](#)

[Glossary](#)

COMMUNITY

[Forums](#)

[Forum Rules](#)

[Chat](#)

USEFUL RESOURCES

[Welcome Guide](#)

[Sitemap](#)

COMPANY

[About BleepingComputer](#)

[Contact Us](#)

[Send us a Tip!](#)

[Advertising](#)

[Write for BleepingComputer](#)

[Social & Feeds](#)

[Changelog](#)

[Terms of Use - Privacy Policy](#)

