Three More Ransomware Families Create Sites to Leak Stolen Data

bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/

Lawrence Abrams

By
Lawrence Abrams

- March 24, 2020
- 07:23 PM
- 0

Three more ransomware families have created sites that are being used to leak the stolen data of non-paying victims and further illustrates why all ransomware attacks must be considered data breaches.

Ever since Maze created their "news" site to publish stolen data of their victims who choose not to pay, other ransomware actors such as Sodinokibi/REvil, Nemty, and DoppelPaymer have been swift to follow.

Over the past two days, BleepingComputer has learned of another three ransomware families who have now launched their data leak sites, which are listed below.

While we have been saying it for a long time, with the continued release of data leak sites, ransomware attacks **must** be treated as data breaches now that the personal and private data of employees is being published online.

To make matters worse, other threat actors are taking the data exposed in these leaks and selling it on hacker forums so it can be utilized in other attacks.

Nefilim Ransomware

The Nefilim Ransomware has launched a site called "Corporate Leaks" that is being used to dump the data of victims who do not pay a ransom.

Nefilim is fairly new and is believed to be a new version of the Nemty Ransomware.
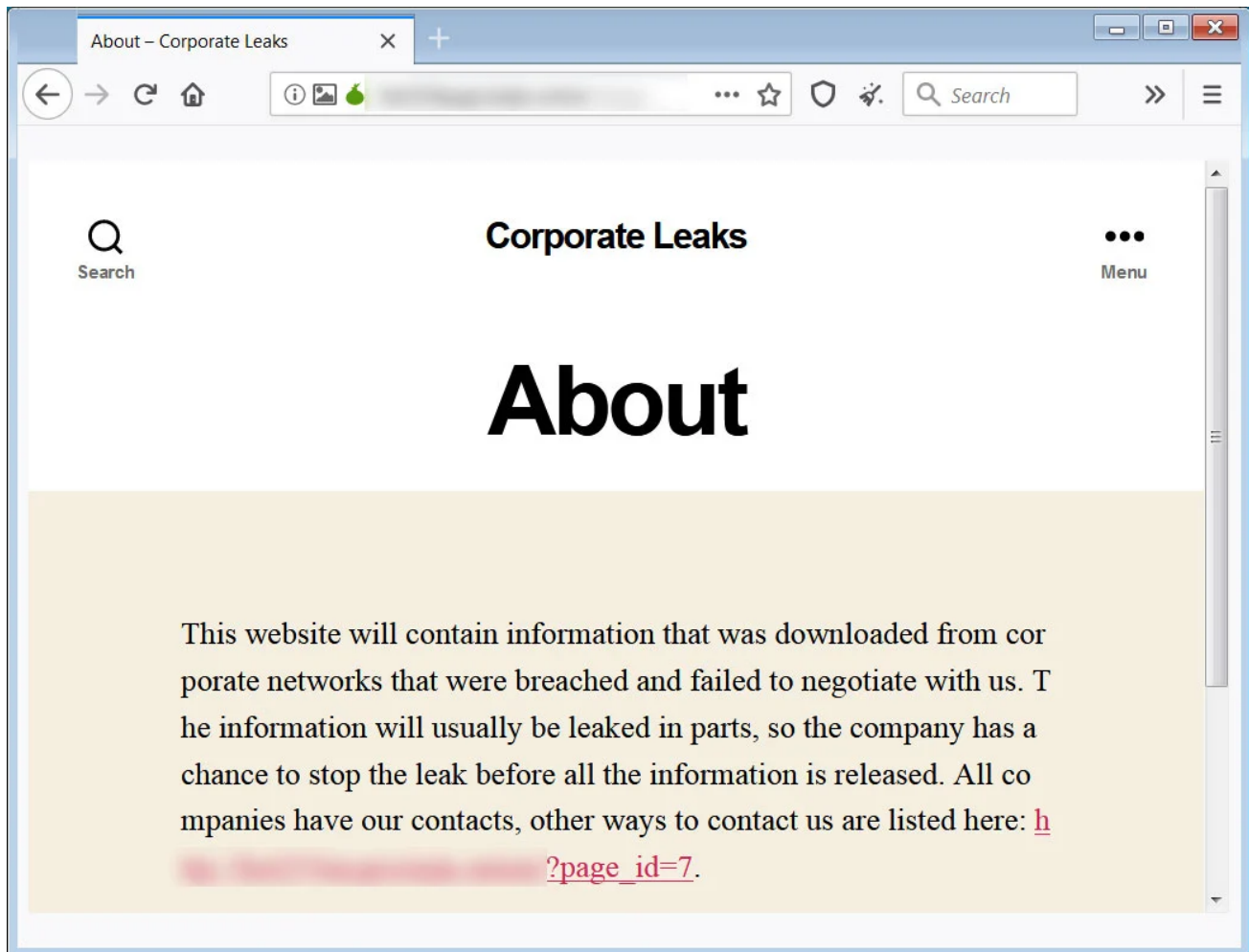
Nefilim Ransomware Leak Site
This leak site currently lists two companies who both are involved with energy or resources.

CLOP Ransomware

The CLOP Ransomware has also released a leak site called "CL0P^_- LEAKS" that they are using to publish stolen data for non-paying victims.

The CLOP Ransomware made news recently after it attacked the Maastricht University and was paid 30 bitcoins to recover their data.
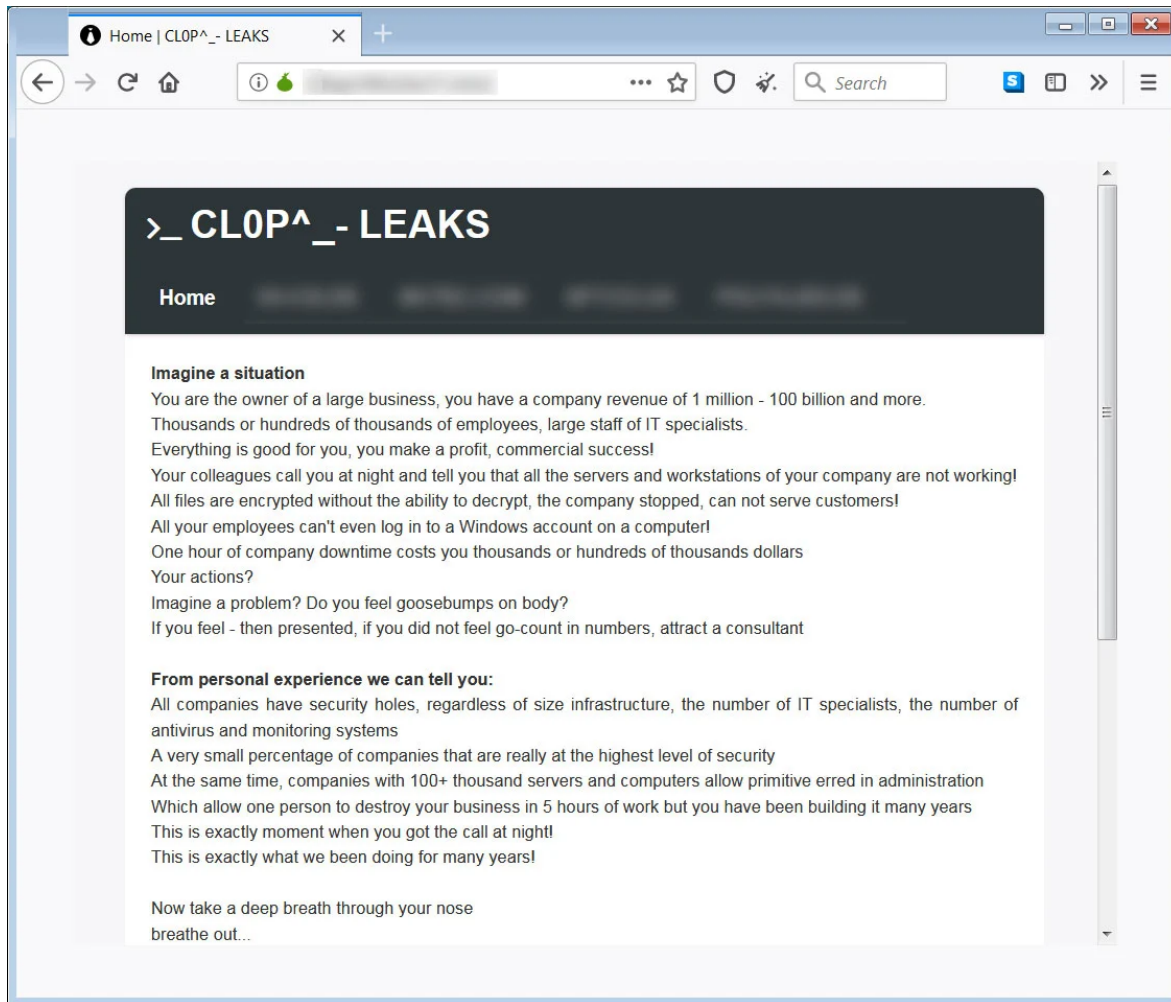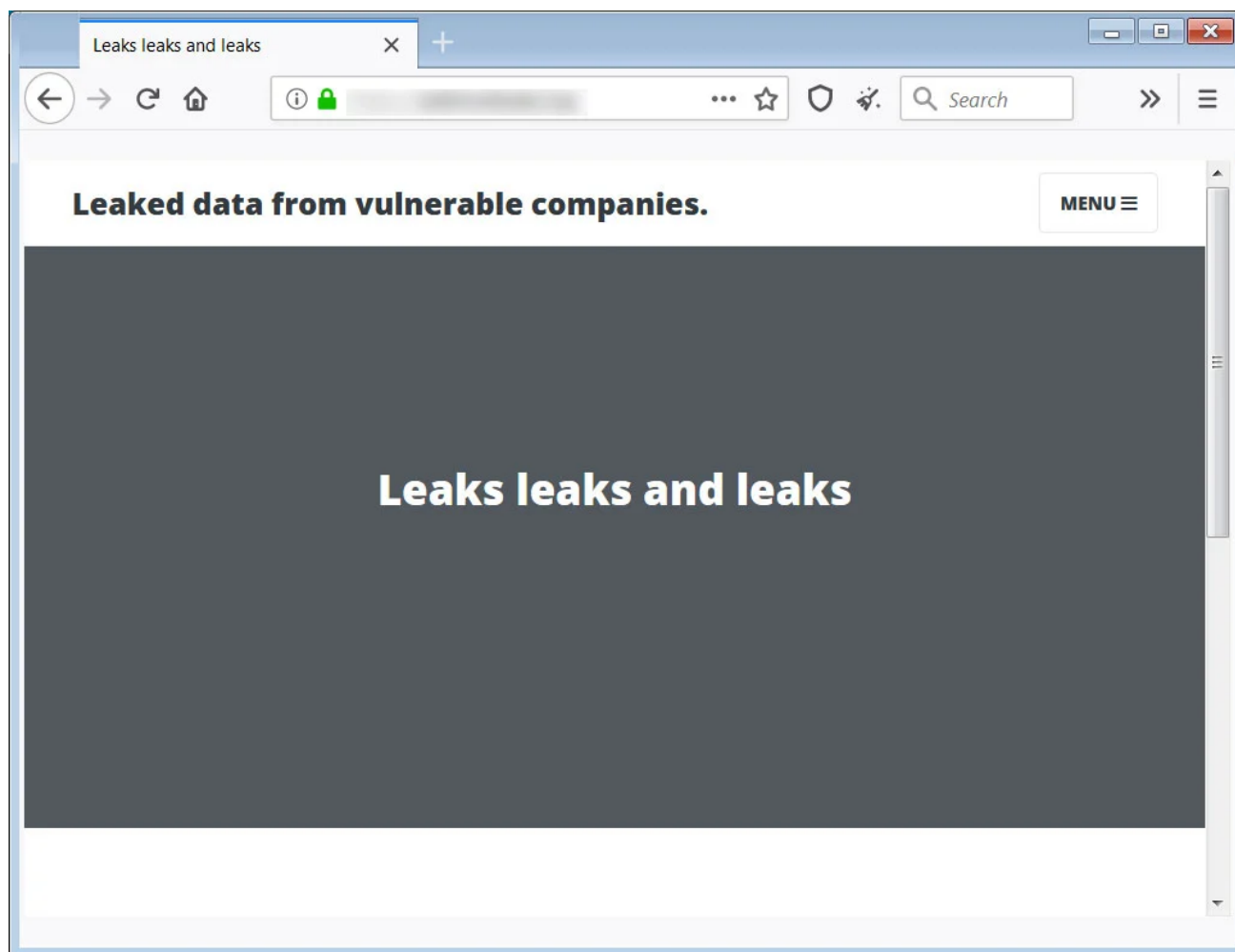
CLOP

Leak Site

The site currently lists four different companies whose data has been released.

Sekhmet Ransomware

Finally, a relatively new ransomware called Sekhmet has also released a data leak site called "Leaks leaks and leaks".

Not much is known about this ransomware other than that their ransom note is named "RECOVER-FILES.txt".

Sekhmet Leak Site
Their leak site only lists one company at this time.

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

Karakurt revealed as data extortion arm of Conti cybercrime syndicate

Snap-on discloses data breach claimed by Conti ransomware gang

- Clop
- Data Exfiltration
- Extortion
- Nefilim
- Ransomware

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.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: