

## Three More Ransomware Families Create Sites to Leak Stolen Data

By Lawrence Abrams

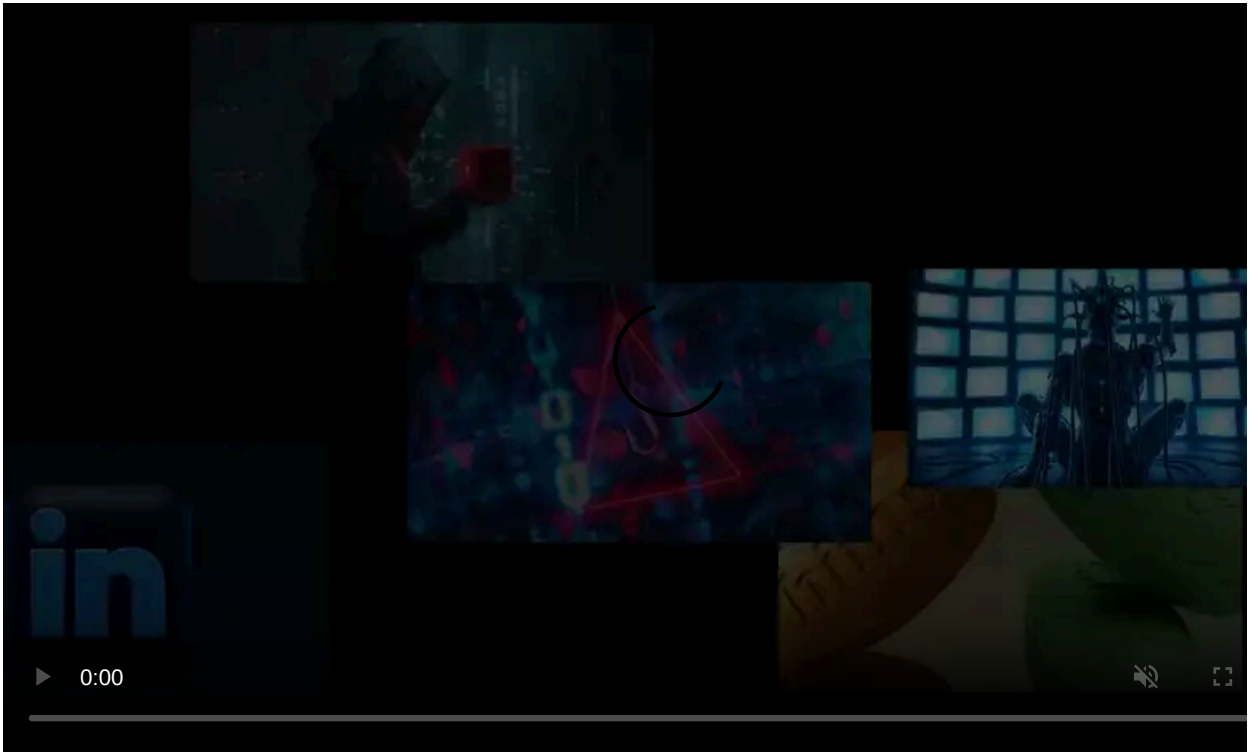
Published: 2020-03-24 · Archived: 2026-04-05 17:27:20 UTC



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.



Visit Advertiser website [GO TO PAGE](#)

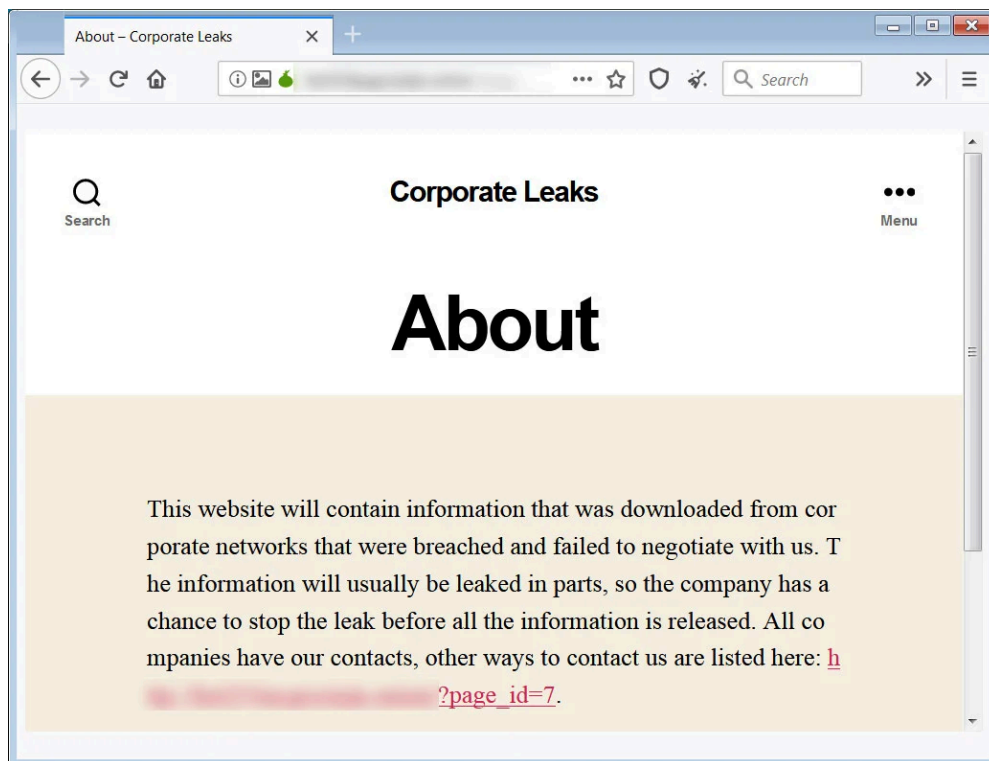
While we have been saying it for a long time, with the continued release of data leak sites, ransomware attacks **must** be treated as data breaches now that the personal and private data of employees is being published online.

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.



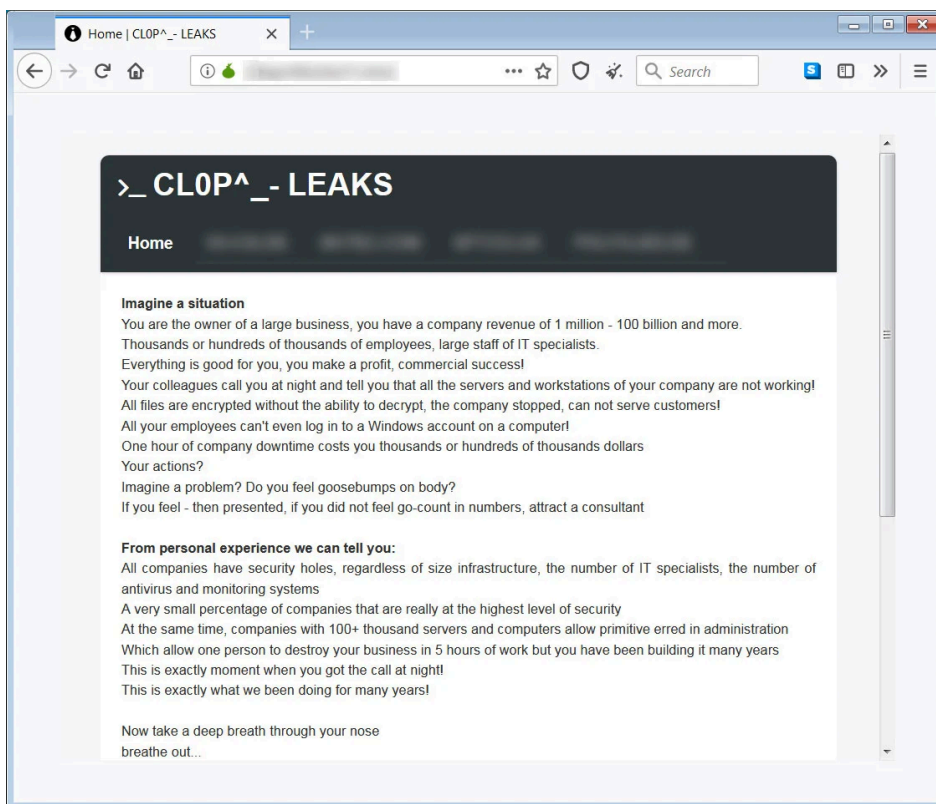
**Nefilim Ransomware Leak Site**

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 "CLOP^\_- 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.



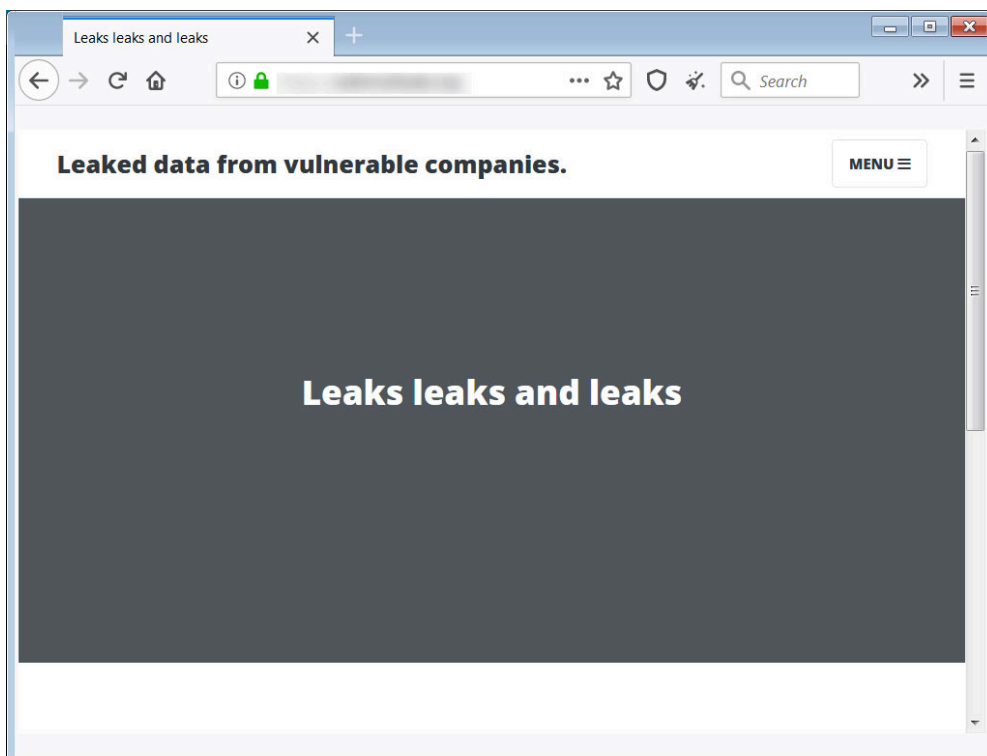
### CL0P Leak Site

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

### Sekhmet Ransomware

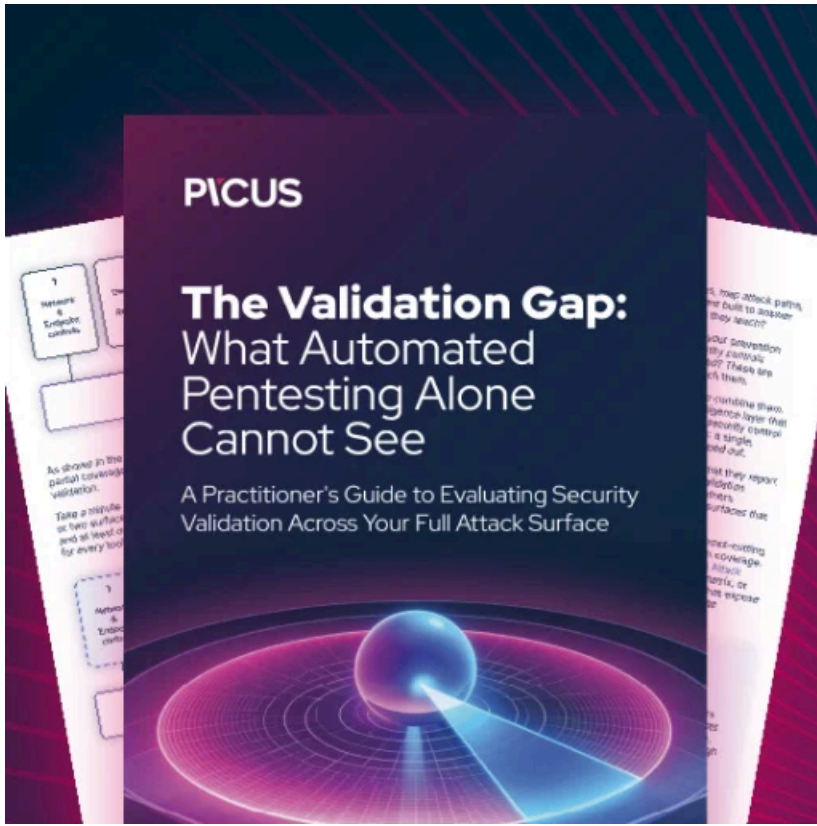
Finally, a relatively new ransomware called Sekhmet has also released a data leak site called "Leaks leaks and leaks".

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.



### [Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---

Source: <https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/>