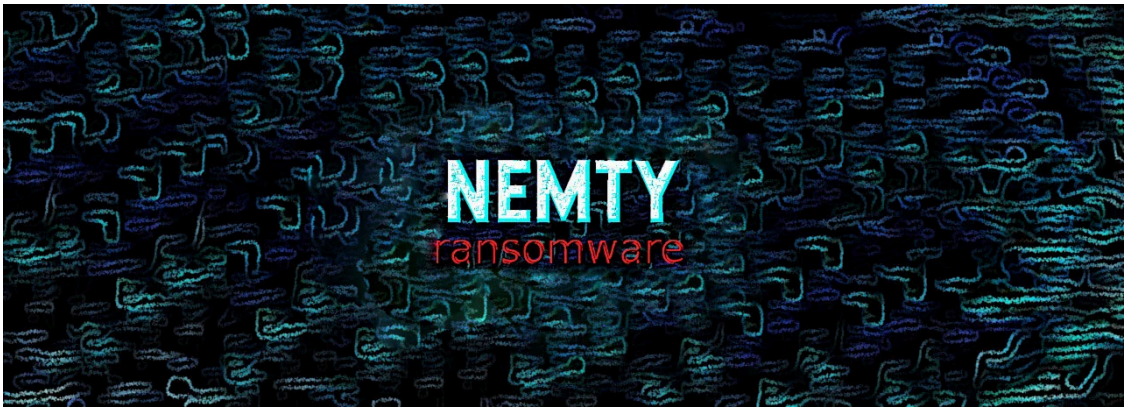
Nemty Ransomware Decryptor Released, Recover Files for Free

By Lawrence Abrams

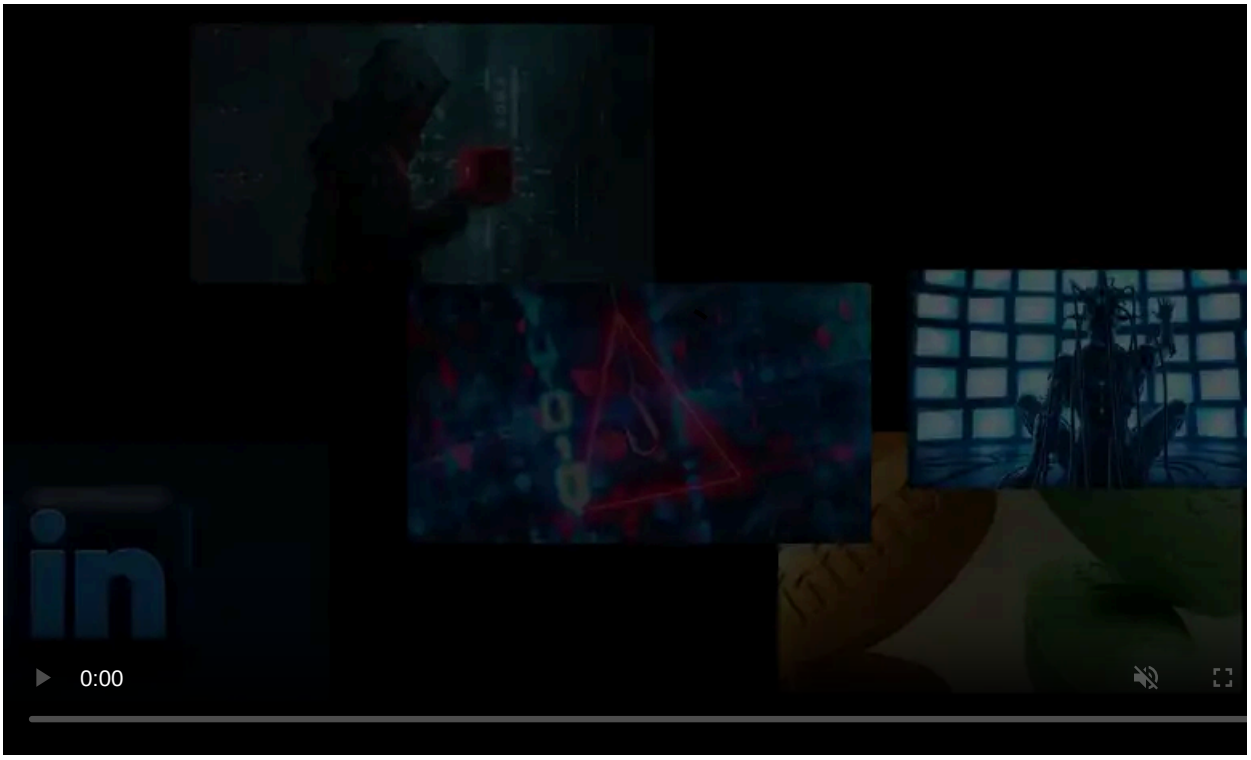
Published: 2019-10-10 · Archived: 2026-04-05 17:07:14 UTC

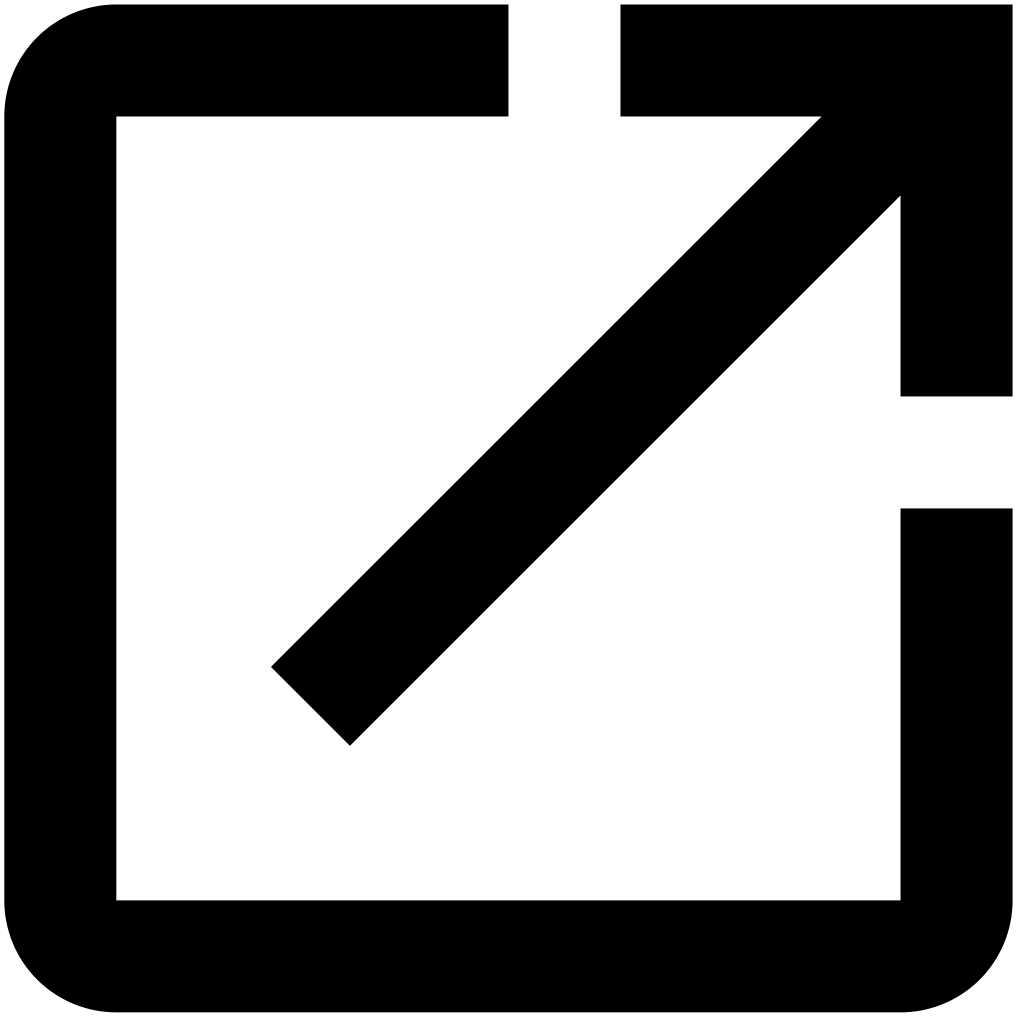


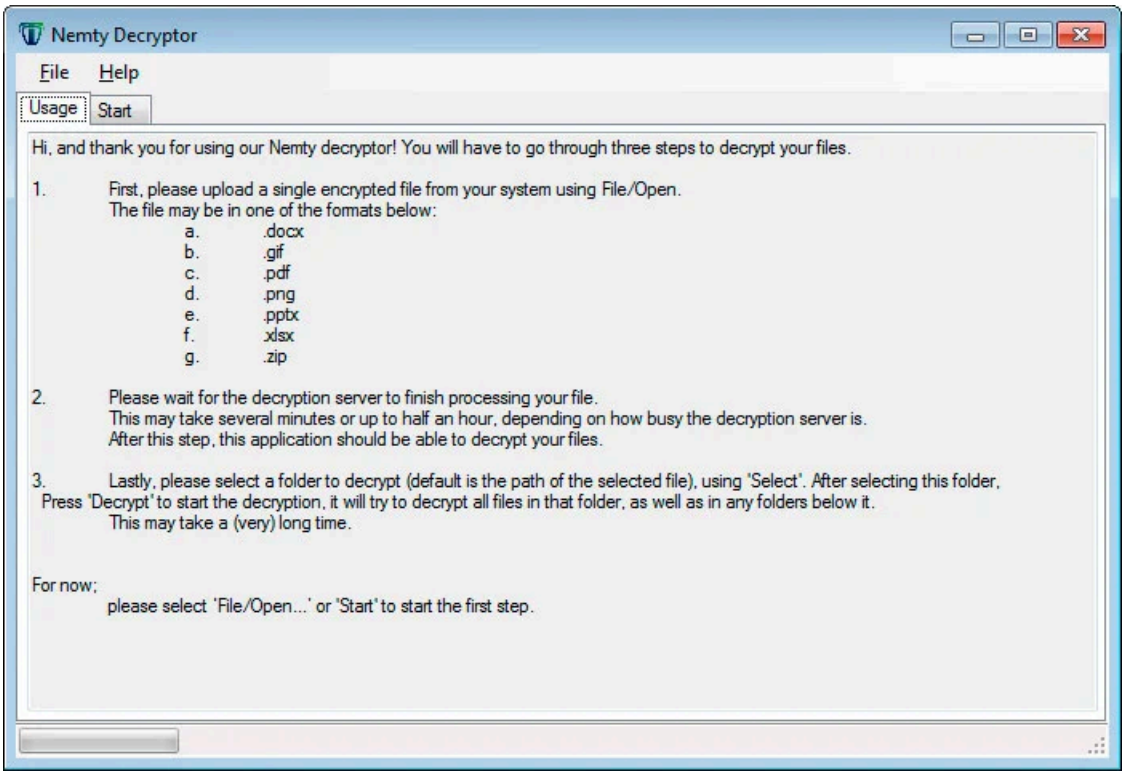
Victims of the Nemty Ransomware finally have something to be happy about as researchers have released a decryptor that allows them to recover files for free.

Since August 2019, the Nemty Ransomware has been utilizing a variety of distribution methods [1, 2, 3] to infect victims and encrypt their files.

The good news is that victims finally get to fight back as researchers from the security firm Tesorion have created a decryptor that works on Nemty versions 1.4 and 1.6, with 1.5 coming soon.


0:00





The decryptor currently supports only a limited amount of file extensions, but Tesorion has told BleepingComputer that they are expanding support for more file types every day.

The file types currently supported by the decryptor are:

```
avi, bmp, gif, mp3, jpeg, jpg, mov, mp4, mov, mp4, qt, 3gp, mpeg, mpg, doc, docb, dot, ole, pot, pps, ppt, wbk, xlm, xls,
```

Instead of offering a decryptor that computes a key on a victim's computer, Tesorion opted to have the decryption key generation done on their own servers.

Tesorion told BleepingComputer they went this route in order to prevent the ransomware developers from analyzing the decryptor and learning the weakness in their algorithm.

The researchers are not wrong, either, as the ransomware developers are definitely watching as shown by the inclusion of the "tesorion thanks for your article" string in the latest Nemty 1.6 executable.

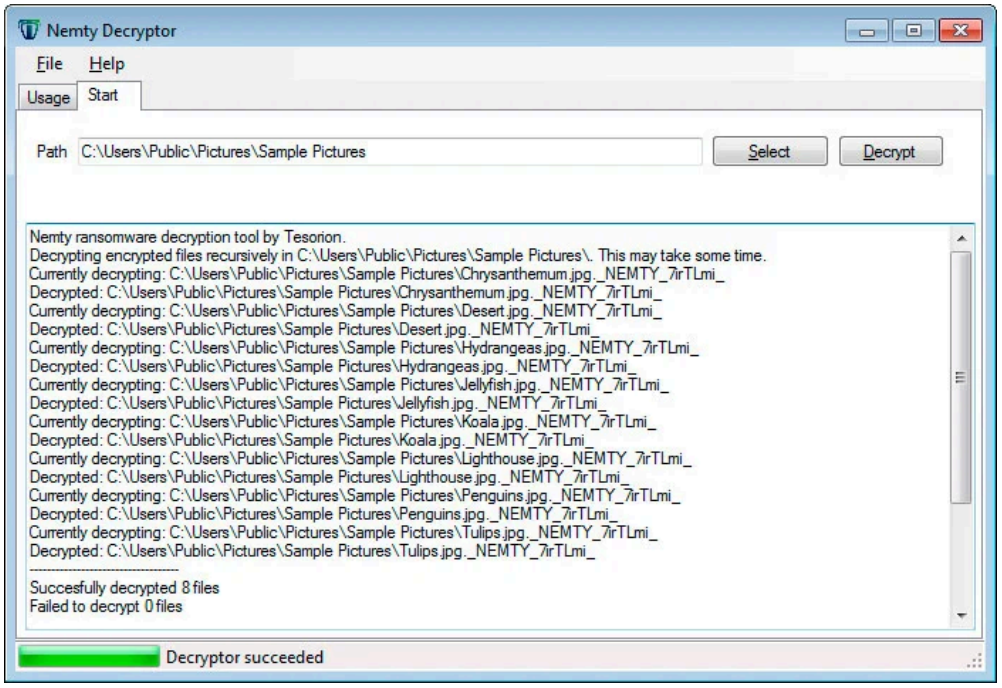
Decrypting Nemty encrypted files

Tesorion provided BleepingComputer with their decryptor so that we would test its ability to decrypt Nemty encrypted files and in our tests it was able to decrypt most of the more common file types that people commonly use such as Office documents, videos, and images.

When using the decryptor, users will upload an encrypted file to Tesorion's server. The supported files that can be uploaded are either a docx, .gif, .pdf, .png, .pptx, .xlsx, or .zip file.

Once a file is uploaded, Tesorian's servers will compute the decryption key for the uploaded file and send it back and load into the decryptor.

Once loaded, victims can then select the folder or drive that they wish to decrypt and begin recovering their files.



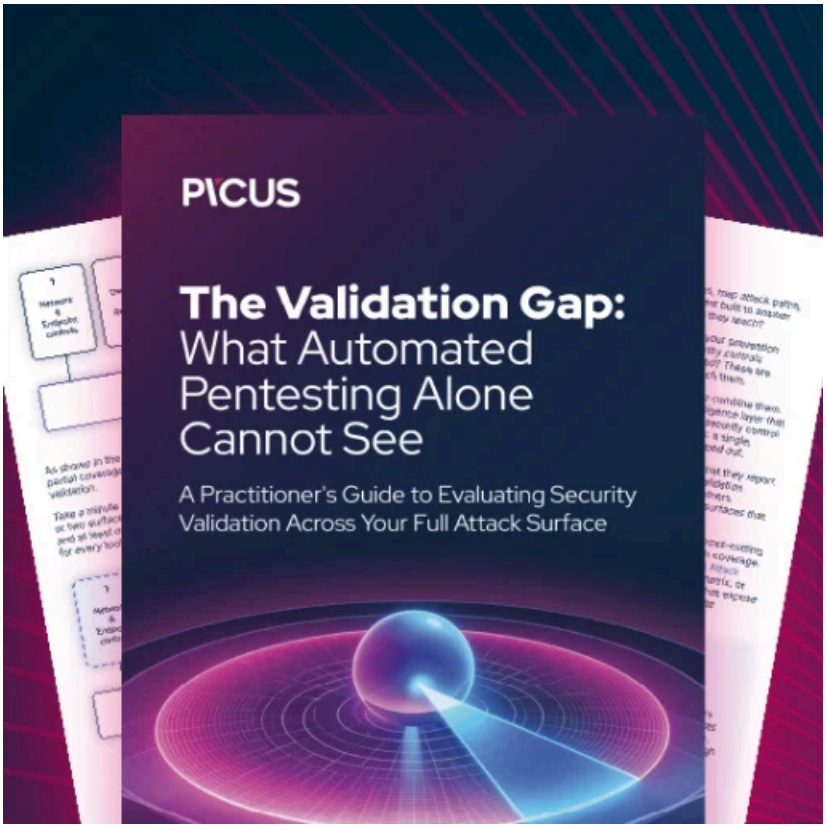
Decrypted Files

In the earlier builds shared with BleepingComputer, we hit some issues on certain file types. With the latest release tested today, the decryptor worked very well and was able to recover most of the encrypted files on my test machine.

The only files it was not able to decrypt were non-standard file formats, but as previously stated, Tesorion continues to support new file types every day.

In order to download the decryptor, users can contact the Tesorion CSIRT and request help with the Nemty Ransomware. Tesorion will then send a link to the decryptor that will allow you to decrypt your files.

Tesorion has told us that they are currently working with Europol to get their decryptor on the NoMoreRansom site so that it will become more widely available to victims.



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/nemty-ransomware-decryptor-released-recover-files-for-free/