

Bye, bye Petya! Decryptor for old versions released. | Malwarebytes Labs

By Malwarebytes Labs

Published: 2017-07-23 · Archived: 2026-04-05 16:02:39 UTC

Following the outbreak of the Petya-based malware in Ukraine, the author of the original version, Janus, decided to release his master key, probably closing the project. You can read the full story [here](#).

Based on the released key, we prepared a decryptor that is capable of unlocking all the legitimate versions of Petya ([read more about identifying Petyas](#)):

- Red Petya
- Green Petya (both versions) + Mischa
- Goldeneye (bootlocker + files)

In case if you have a backup of Petya-encrypted disk, this is the time to take it out from the shelf and kiss your Petya goodbye 😊

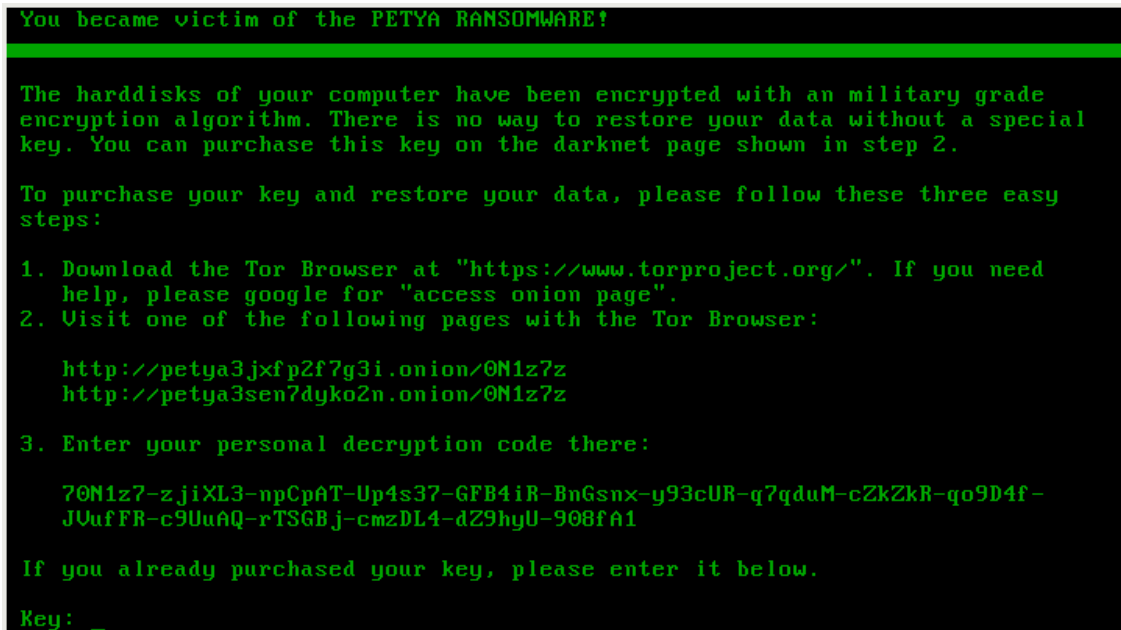
WARNING: During our tests we found that in some cases Petya may hang during decryption, or cause some other problems potentially damaging to your data. That's why, before any decryption attempts, we recommend you to make an additional backup.

// Special thanks to [@Th3PeKo](#) , [@vallejoc](#) and Michael Meyer for all the help in testing!

Variants of the attack

As we know, depending on version Petya may attack your data by two ways:

1 – at a low level, encrypting your Master File Table. For example:



2 – at a high level, encrypting your files one by one (like a typical [ransomware](#)). For example:

Name	Date modified	Type	Size
square1 - Copy - Copy.bmp.7QzX	2016-05-12 18:47	7QZX File	141 KB
square1 - Copy.bmp.7QzX	2016-05-12 18:47	7QZX File	141 KB
square1.bmp.7QzX	2016-05-12 18:47	7QZX File	141 KB
YOUR_FILES_ARE_ENCRYPTED.HTML	2016-05-12 18:47	Firefox HTML Doc...	2 KB
YOUR_FILES_ARE_ENCRYPTED.TXT	2016-05-12 18:47	Text Document	1 KB

Fortunately, the released key allows for recovery in both cases. However the process of decryption will look a bit different.

Decryptors

We prepared two different builds of the recovery tool, to support the specific needs:

1. a [Live CD](#)
2. a [Windows executable](#)

In both cases, the tool decrypts the individual key from the victim ID.

After obtaining the key, you can use the original decryptors in order to recover your files. You can find the links here:

For **Mischa**: <https://drive.google.com/open?id=0Bzb5kQFOXkiSWUZ6dndxZkN1YIE> For **Goldeneye**: <https://drive.google.com/open?id=0Bzb5kQFOXkiSdTZkUUYxZ0xEeDg>

DISCLAIMER: Those tools are provided as is and you are using them at your own risk. We are not responsible for any damage or lost data.

Defeating the bootlocker

In both cases, you can obtain the key to your Petya by using a Windows Executable and supplying it your victim ID. Detailed instructions has been given [here](#) and on the video below:

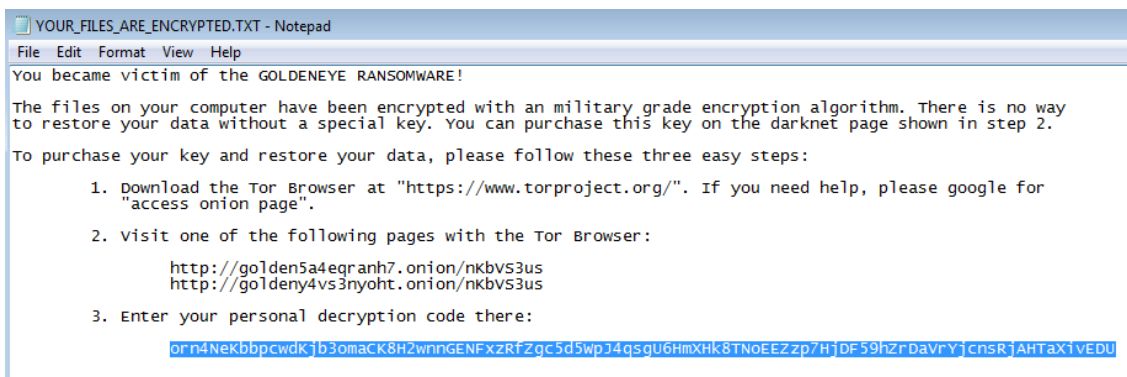
However, victim IDs are very long, and retyping them may be painful and prone to mistakes. That's why, we prepared an alternative: a LiveCD that will automatically read it from the encrypted disk. In order to use it, you need to download the ISO and boot from it your infected machine. Then, follow the displayed instructions:

After obtaining the key, you can use it to decrypt your Master File Table:

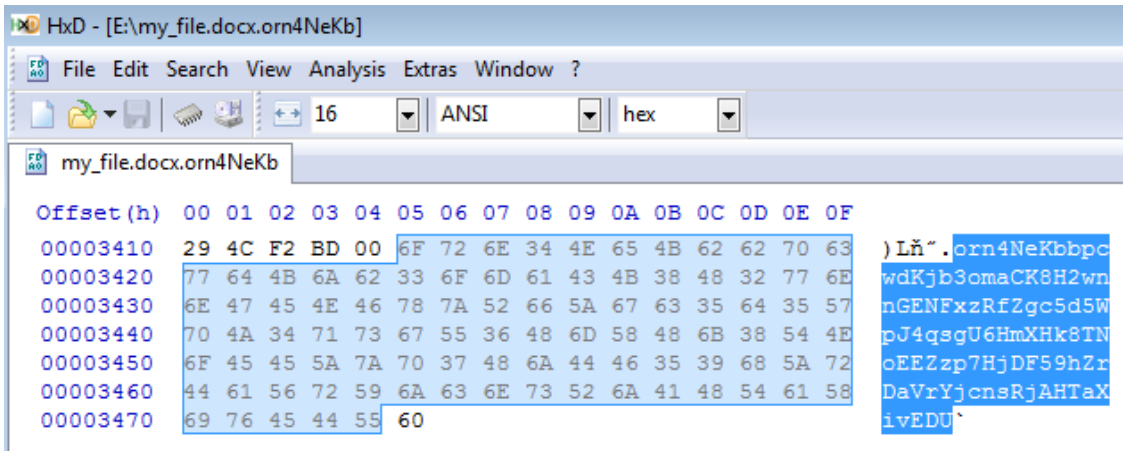
Decrypting files

In case if your files has been encrypted, i.e. by Goldeneye or Mischa, you can use the key decryptor released in form of a [Windows executable](#).

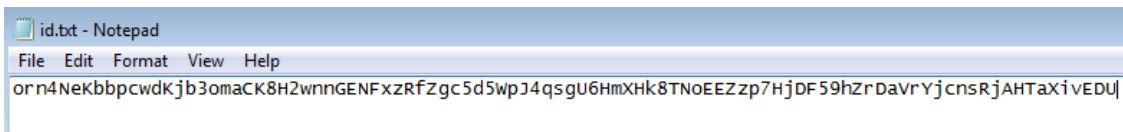
1. Find your victim ID (“personal decryption code”). It will be in your ransom note:



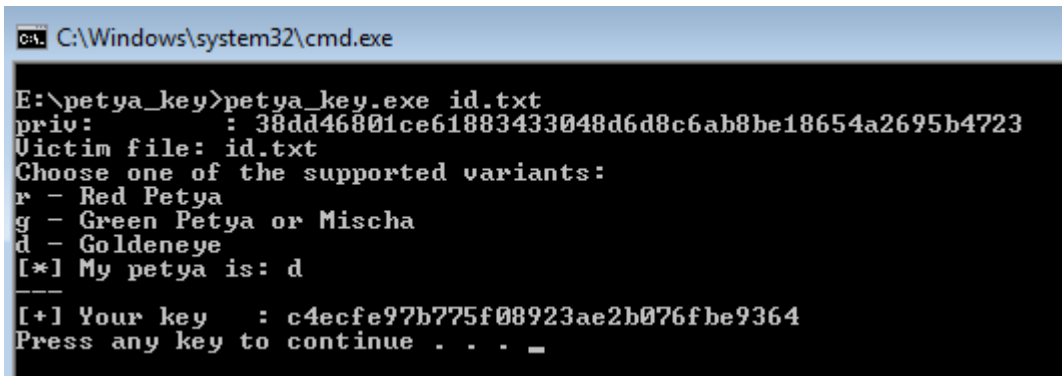
In case if you don't have the note, you can find the ID appended at the end of any of your encrypted files:



2. Save the ID in a file:



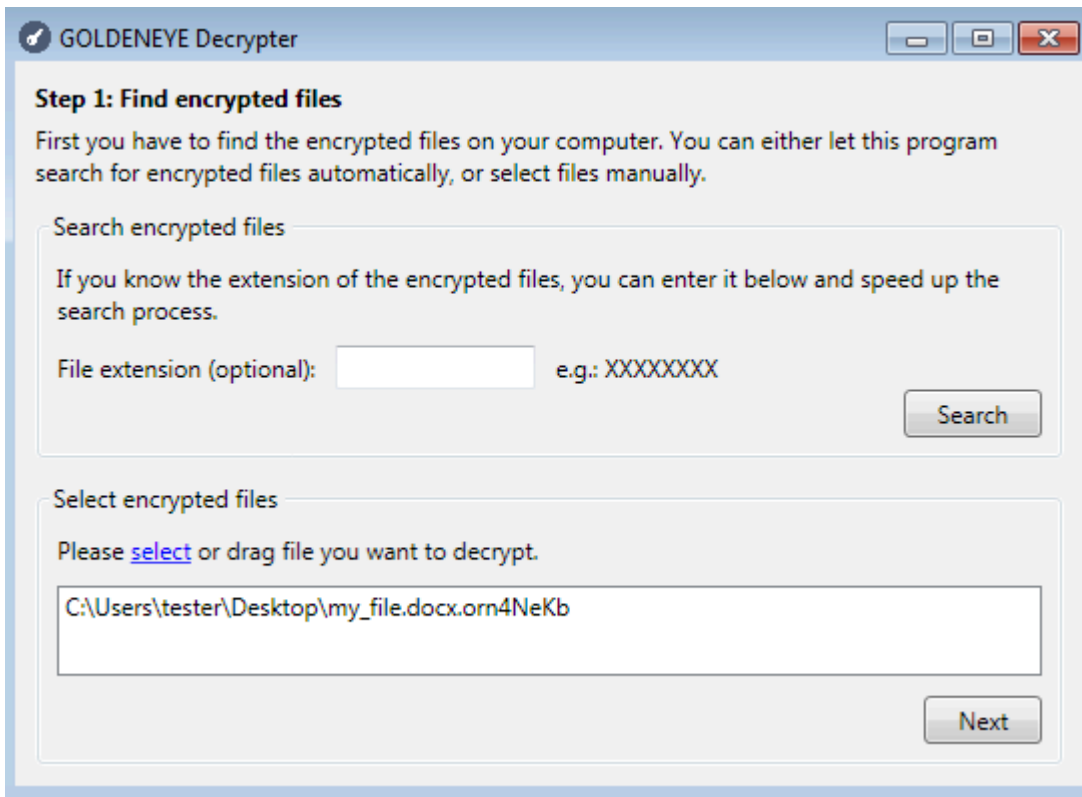
3. Use our tool to decrypt your key:



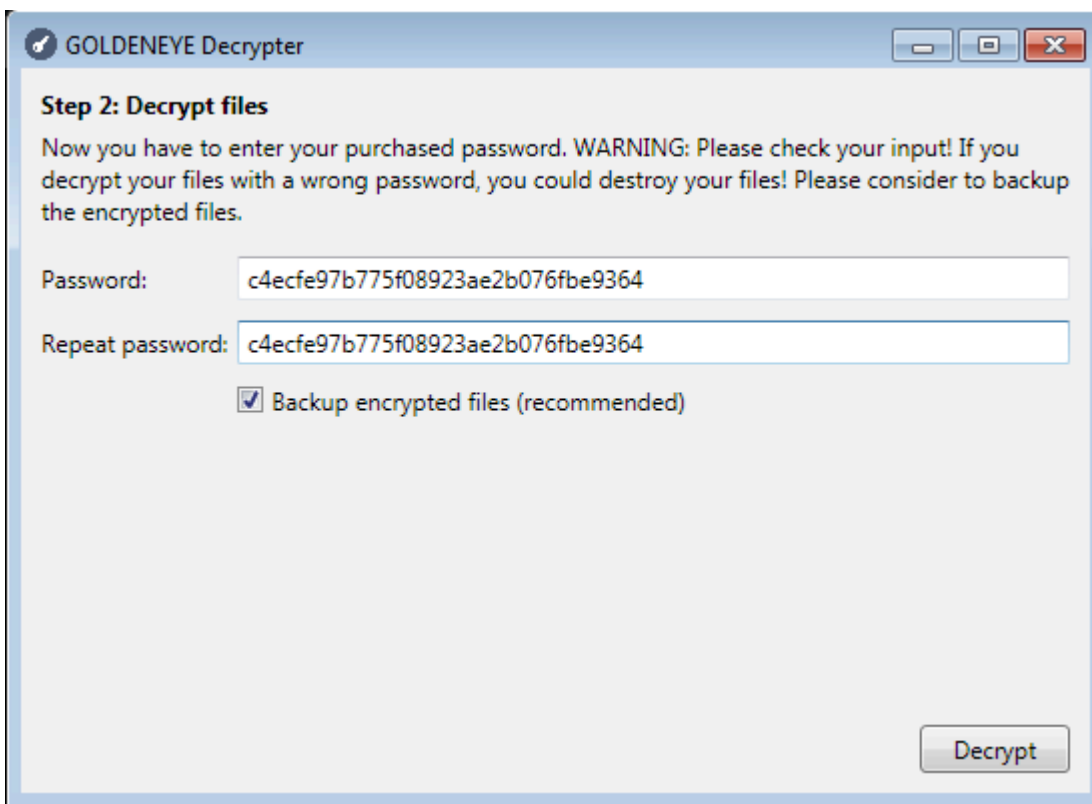
3. Copy the obtained key. Download the original decryptor, appropriate for your version:

For **Mischa**: <https://drive.google.com/open?id=0Bzb5kQFOXkiSWUZ6dndxZkN1YIE> For **Goldeneye**: <https://drive.google.com/open?id=0Bzb5kQFOXkiSdTZkUUYxZ0xEeDg>

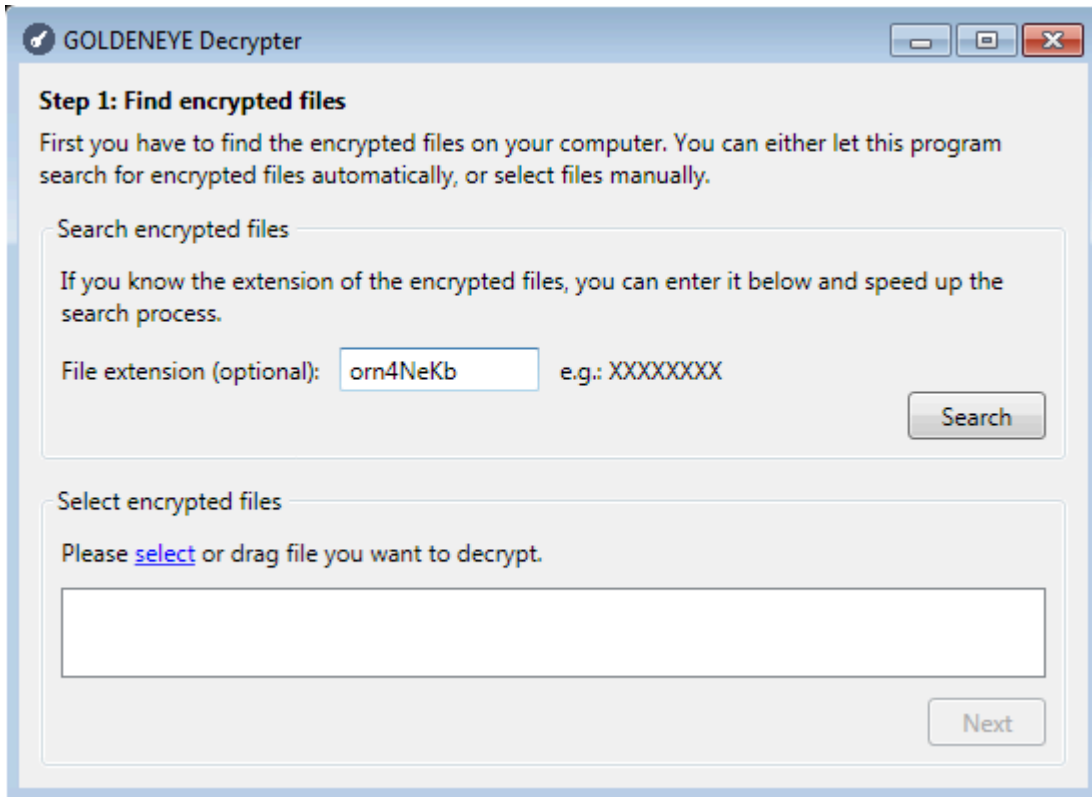
Choose one of your encrypted files:



Supply the key obtained from the key decoder:



Decrypt the file and check if the output is valid. If everything is fine, you can use the same key to decrypt rest of your files. Supply the extension to the decryptor, and it will find them automatically:



Conclusion

The presented tools allow you to unlock all the legitimate versions of Petya that are released up to now by Janus Cybercrime Solutions. It cannot help the victims of pirated Petyas, [like PetrWrap or EternalPetya](#) (aka NotPetya). It matches the announcement made by Janus on twitter:



JANUS
@JanusSecretary

Following

Replying to [@hasherezade](#) [@MalwareTechBlog](#)

only [#mischa](#) [#petya](#) and [#goldeneye](#)

Is it the end of Petya's story? Probably yes, however, the future will learn.

This was a guest post written by Hasherezade, an independent researcher and programmer with a strong interest in InfoSec. She loves going in details about malware and sharing threat information with the community. Check her out on Twitter [@hasherezade](#) and her personal blog: <https://hshrzd.wordpress.com>.

Source: <https://blog.malwarebytes.com/malwarebytes-news/2017/07/bye-bye-petya-decryptor-old-versions-released/>