Bye, bye Petya! Decryptor for old versions released.

July 24, 2017 by Malwarebytes Labs

Last updated: July 26, 2017

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 😉

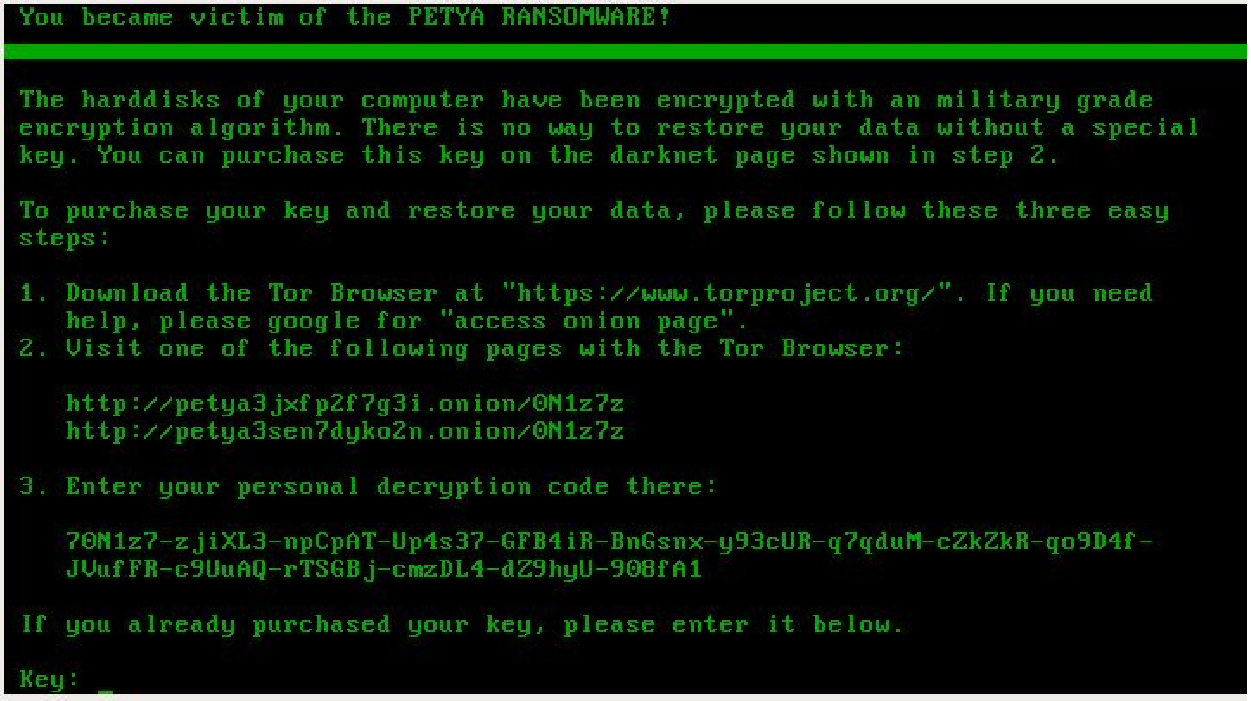
WARNING: During our tests we found that in some cases Petya may hang during decryption, or cause some other problems potentially damaging to your data. That's why, before any decryption attempts, we recommend you to make an additional backup.

// Special thanks to @Th3PeKo , @vallejocc and Michael Meyer for all the help in testing!

Variants of the attack

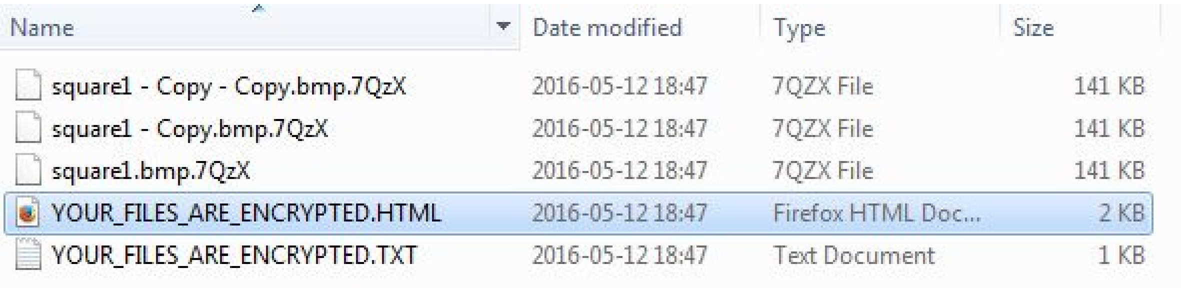
As we know, depending on version Petya may attack your data by two ways:

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



```
You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://petya3jxfp2f7g3i.onion/0N1z7z
   http://petya3sen7dyko2n.onion/0N1z7z

3. Enter your personal decryption code there:

   70N1z7-zjiXL3-npCpAT-Up4s37-GFB4iR-BnGsnx-y93cUR-q7qduM-cZkZkR-qo9D4f-
   JVufFR-c9UuAQ-rTSGBj-cmzDL4-dZ9hyU-908fA1

If you already purchased your key, please enter it below.

Key: _
```

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:

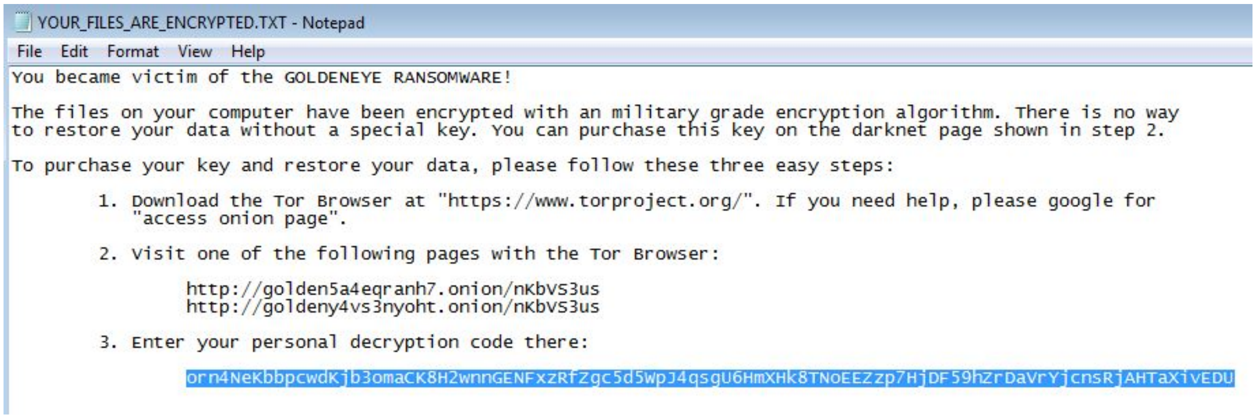
However, victim IDs are very long, and retyping them may be painful and prone to mistakes. That's why, we prepared an alternative: a LiveCD that will automatically read it from the encrypted disk. In order to use it, you need to download the ISO and boot from it your infected machine. Then, follow the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

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

Decrypting files

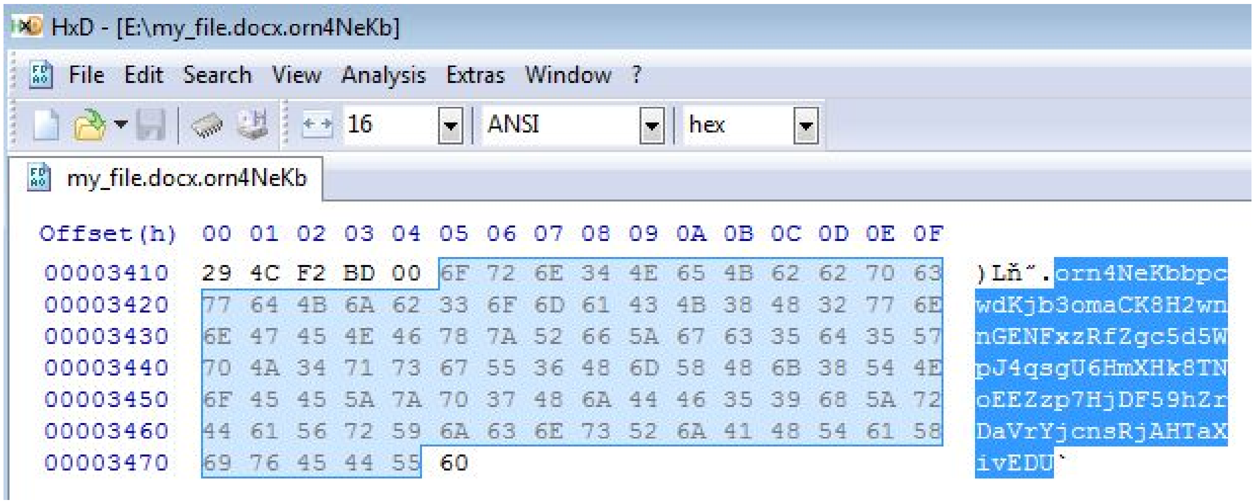
In case if your files has been encrypted, i.e. by Goldeneye or Mischa, you can use the key decryptor released in form of a Windows executable.

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


YOUR_FILES_ARE_ENCRYPTED.TXT - Notepad
File Edit Format View Help

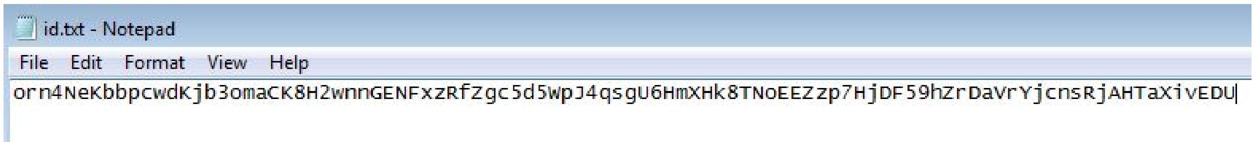
```
You became victim of the GOLDENEYE RANSOMWARE!

The files on your computer have been encrypted with an military grade encryption algorithm. There is no way
to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

        1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for
           "access onion page".

        2. Visit one of the following pages with the Tor Browser:

                http://golden5a4eqranh7.onion/nKbVS3us
                http://goldeny4vs3nyoht.onion/nKbVS3us

        3. Enter your personal decryption code there:

                orn4NeKbbpcwdKjb3omaCK8H2wnnGENFxzRfZgc5d5WpJ4qsgU6HmXHk8TNoEEZzp7HjDF59hZrDaVrYjcnsRjAHTaXivEDU
```

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


HxD - [E:\my_file.docx.orn4NeKb]
File Edit Search View Analysis Extras Window ?
16
ANSI
hex
my_file.docx.orn4NeKb

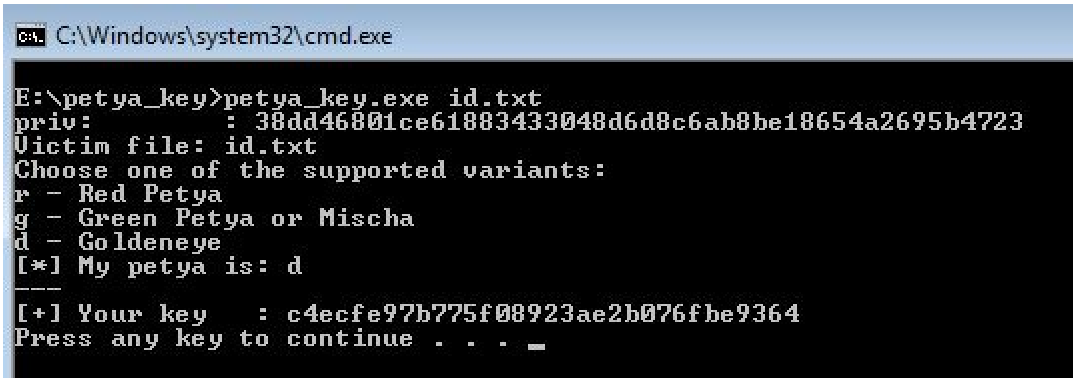
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00003410  29 4C F2 BD 00 6F 72 6E 34 4E 65 4B 62 62 70 63  )Lň˝.orn4NeKbbpc
00003420  77 64 4B 6A 62 33 6F 6D 61 43 4B 38 48 32 77 6E  wdKjb3omaCK8H2wn
00003430  6E 47 45 4E 46 78 7A 52 66 5A 67 63 35 64 35 57  nGENFxzRfZgc5d5W
00003440  70 4A 34 71 73 67 55 36 48 6D 58 48 6B 38 54 4E  pJ4qsgU6HmXHk8TN
00003450  6F 45 45 5A 7A 70 37 48 6A 44 46 35 39 68 5A 72  oEEZzp7HjDF59hZr
00003460  44 61 56 72 59 6A 63 6E 73 52 6A 41 48 54 61 58  DaVrYjcnsRjAHTaX
00003470  69 76 45 44 55 60                                ivEDU`
```

2. Save the ID in a file:



```
orn4NeKbbpcwdKjb3omaCK8H2wnnGENFxzRfZgc5d5WpJ4qsgU6HmXHk8TNoEEZzp7HjDF59hZrDaVrYjcnsRjAHTaXivEDU
```

3. Use our tool to decrypt your key:



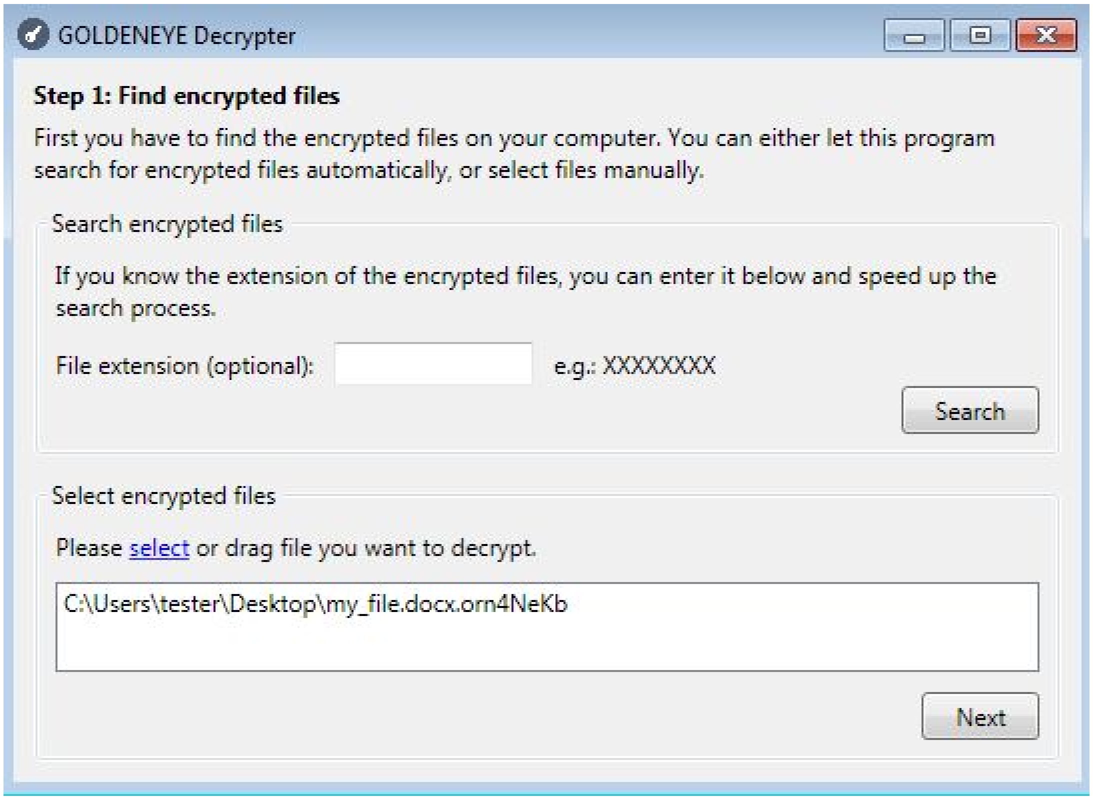
```
E:\petya_key>petya_key.exe id.txt
priv:          : 38dd46801ce61883433048d6d8c6ab8be18654a2695b4723
Victim file: id.txt
Choose one of the supported variants:
r - Red Petya
g - Green Petya or Mischa
d - Goldeneye
[*] My petya is: d
---
[+] Your key    : c4ecfe97b775f08923ae2b076fbe9364
Press any key to continue . . . _
```

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

For **Mischa**: https://drive.google.com/open?id=0Bzb5kQFOXkiSWUZ6dndxZkN1YlE

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

Choose one of your encrypted files:



Step 1: Find encrypted files

First you have to find the encrypted files on your computer. You can either let this program search for encrypted files automatically, or select files manually.

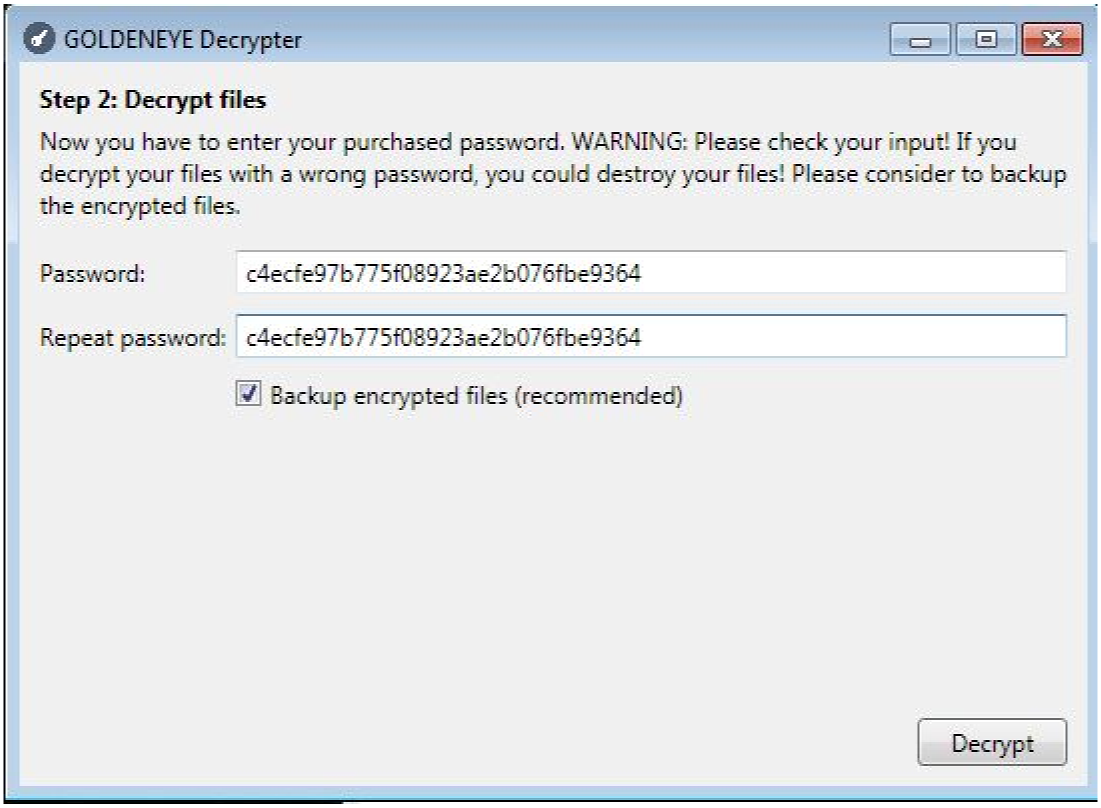
If you know the extension of the encrypted files, you can enter it below and speed up the search process.

File extension (optional): e.g.: XXXXXXXX

Please select or drag file you want to decrypt.

C:\Users\tester\Desktop\my_file.docx.orn4NeKb

Supply the key obtained from the key decoder:



Step 2: Decrypt files

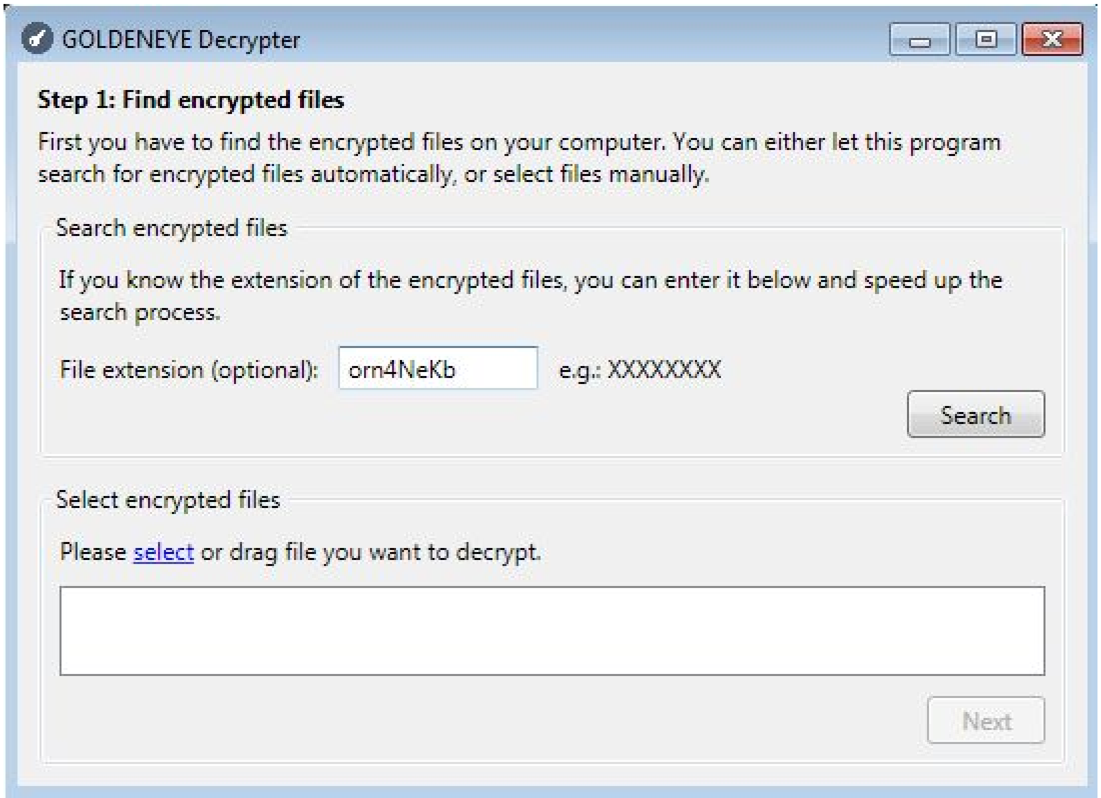
Now you have to enter your purchased password. WARNING: Please check your input! If you decrypt your files with a wrong password, you could destroy your files! Please consider to backup the encrypted files.

Password: c4ecfe97b775f08923ae2b076fbe9364

Repeat password: c4ecfe97b775f08923ae2b076fbe9364

☑ Backup encrypted files (recommended)

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:


GOLDENEYE Decrypter

Step 1: Find encrypted files

First you have to find the encrypted files on your computer. You can either let this program search for encrypted files automatically, or select files manually.

Search encrypted files

If you know the extension of the encrypted files, you can enter it below and speed up the search process.

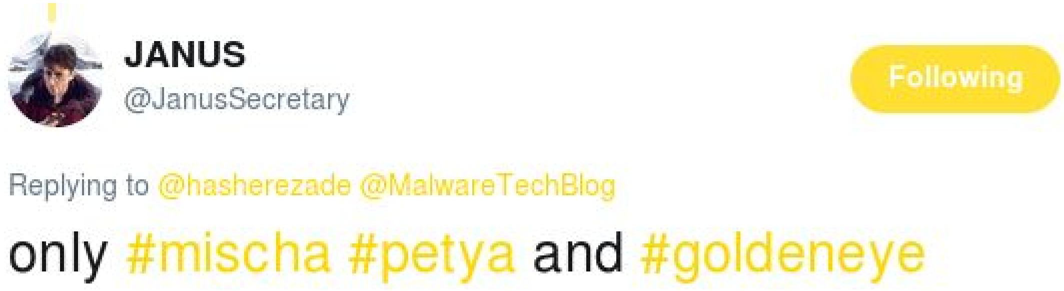
File extension (optional): orn4NeKb e.g.: XXXXXXXX

Select encrypted files

Please select or drag file you want to decrypt.

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

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.*