Keeping up with the Petyas: Demystifying the malware family

blog.malwarebytes.com/cybercrime/2017/07/keeping-up-with-the-petyas-demystifying-the-malware-family/

Malwarebytes Labs

July 14, 2017

Last June 27, there was a huge outbreak of a Petya-esque malware with WannaCry-style infector in the Ukraine.

Since there is still confusion about how exactly this malware is linked to the original Petya, we have prepared this small guide on the background of the Petya family.

The origin of Petya

The first Petya ransomware was released around March 2016 by a person/group calling themselves Janus Cybercrime Solutions. This group was advertising their affiliate program, giving other criminals a chance to distribute their malware. Janus Cybercrime Solutions was represented also on Twitter by appropriate accounts, first by @janussec, and then by @JanusSecretary.

The names “Janus” and “Petya” were inspired by the James Bond movie, GoldenEye. The threat actor was consistent with the chosen theme, too—the profile picture of the linked Twitter account was from one of the characters of the movie, a computer programmer/hacker named Boris Grishenko.

JANUS

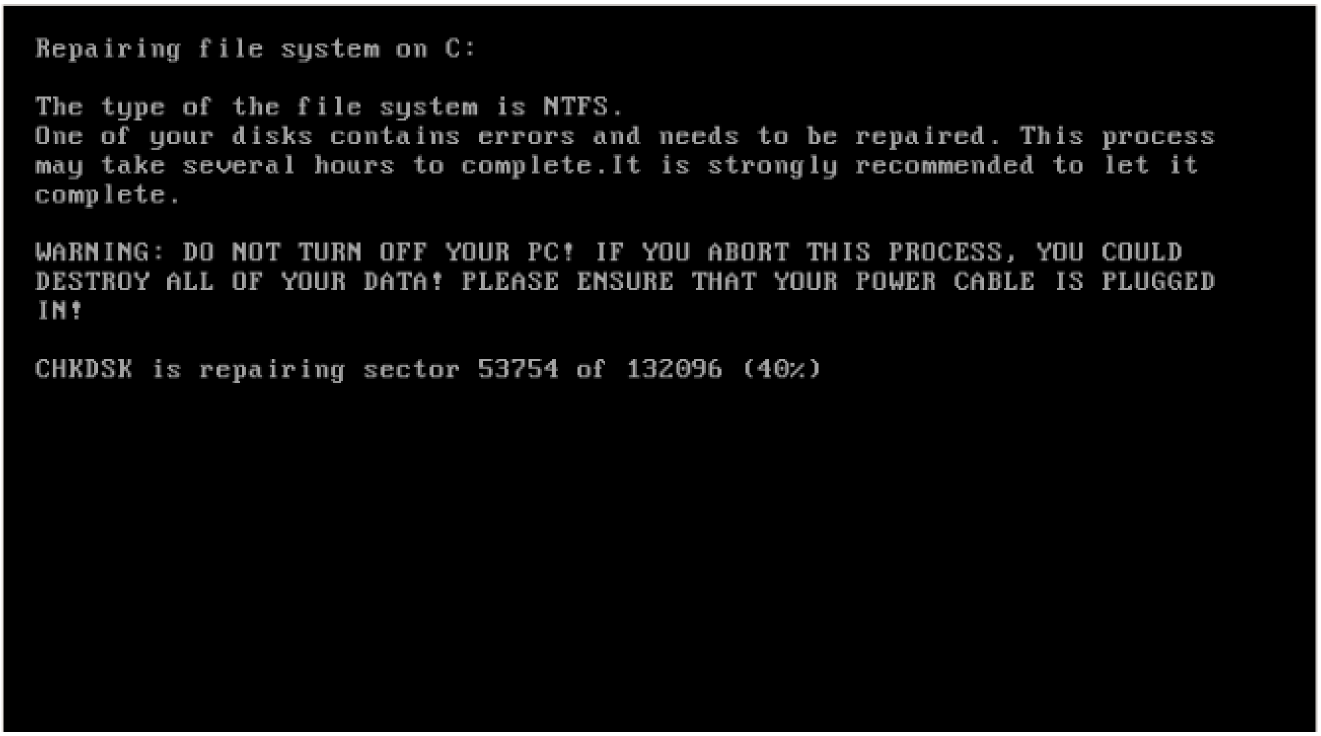
@JanusSecretary Follows you

Unique features

From the very beginning, Petya has been a unique ransomware because it has features that are not common for this type of malware. While most of the ransomware can only encrypt files one by one, Petya denies users access to the full system by attacking low-level structures on the disk.

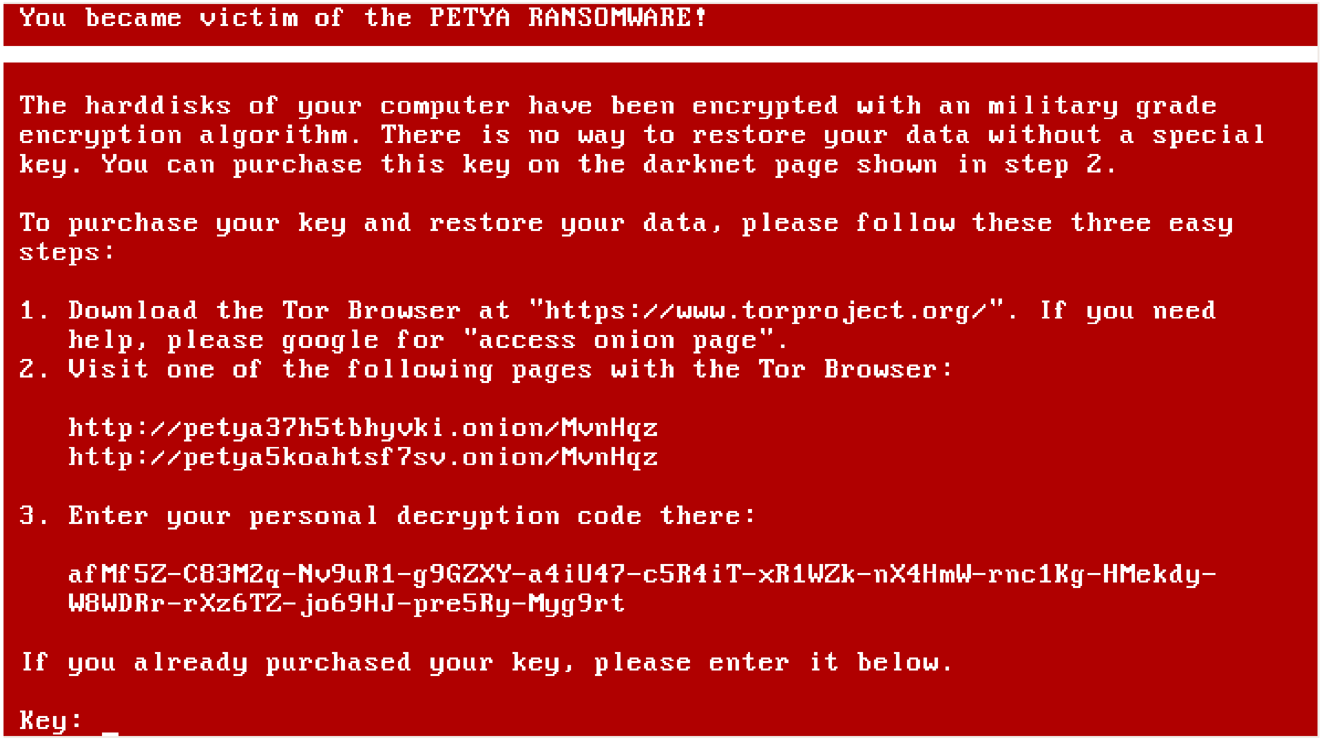
Petya is always installed by some dropper, which is a Windows executable (on each version of Petya the dropper is replaced with a new one).

During installation, the Petya installer overwrites the disk with Petya’s kernel and boot loader. Because of this, the affected machine boots the malicious kernel instead of the legitimate OS. On the first run, it displays a fake CHKDSK screen:



```
Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete.It is strongly recommended to let it
complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!

CHKDSK is repairing sector 53754 of 132096 (40%)
```

Instead of checking the disk, in reality, it encrypts the Master File Table (MFT) with Salsa20. This way, the ransomware makes the disk inaccessible. When encryption is finished, two screens are displayed: a blinking skull followed by the ransom demand. This is how affected system screens look like in the first version of Petya:



```
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://petya37h5tbhyvki.onion/MvnHqz
   http://petya5koahtsf7sv.onion/MvnHqz

3. Enter your personal decryption code there:

   afMf5Z-C83M2q-Nv9uR1-g9GZXY-a4iU47-c5R4iT-xR1WZk-nX4HmW-rnc1Kg-HMekdy-
   W8WDRr-rXz6TZ-jo69HJ-pre5Ry-Myg9rt

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

Key: _
```

Official releases

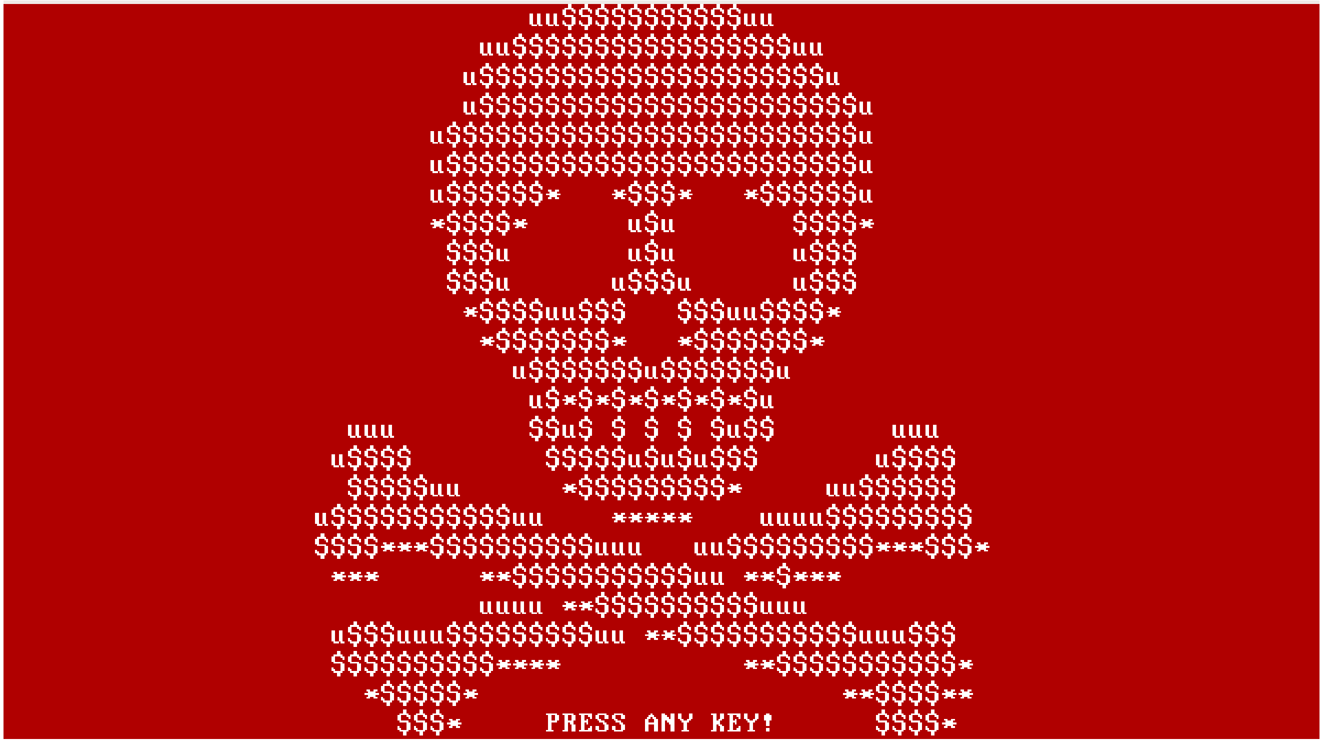
So far, there are 4 releases of Petya ransomware by its original author, Janus:

- 1.0 (Red Petya) – Attacks only MFT
- 2.0 (Green Petya + Mischa) – Attacks either the MFT or files (a variant of the attack depends on the privileges with which the sample was deployed)
- 2.5 (Green Petya + Mischa) – Same as 2.0 but with improvements
- 3.0 (Goldeneye) – Attacks both the MFT and files, using UAC bypass to auto-elevate its privileges

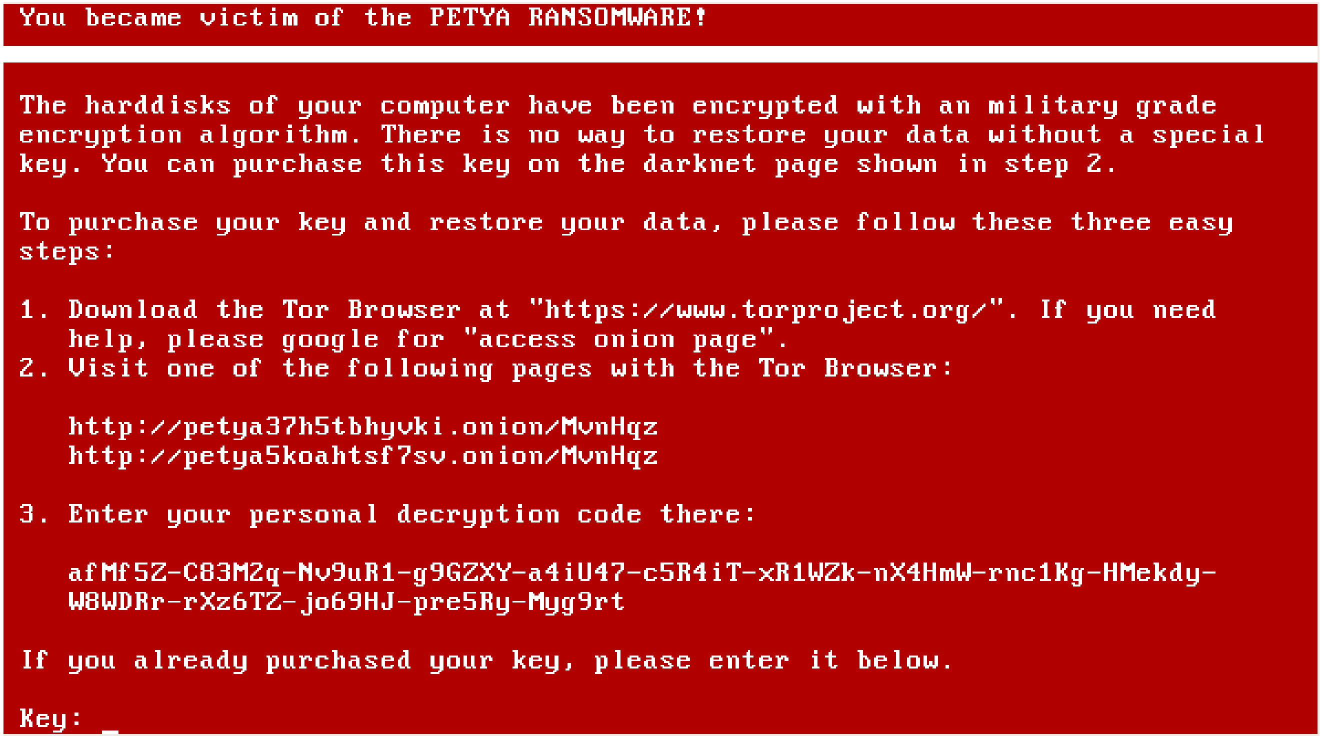
Recently, Janus released the master key that can unlock all official versions described above. You can read more about it in this blog post.

These Petya releases can be identified by the theme colors. We've put together a small gallery below:

Red Petya

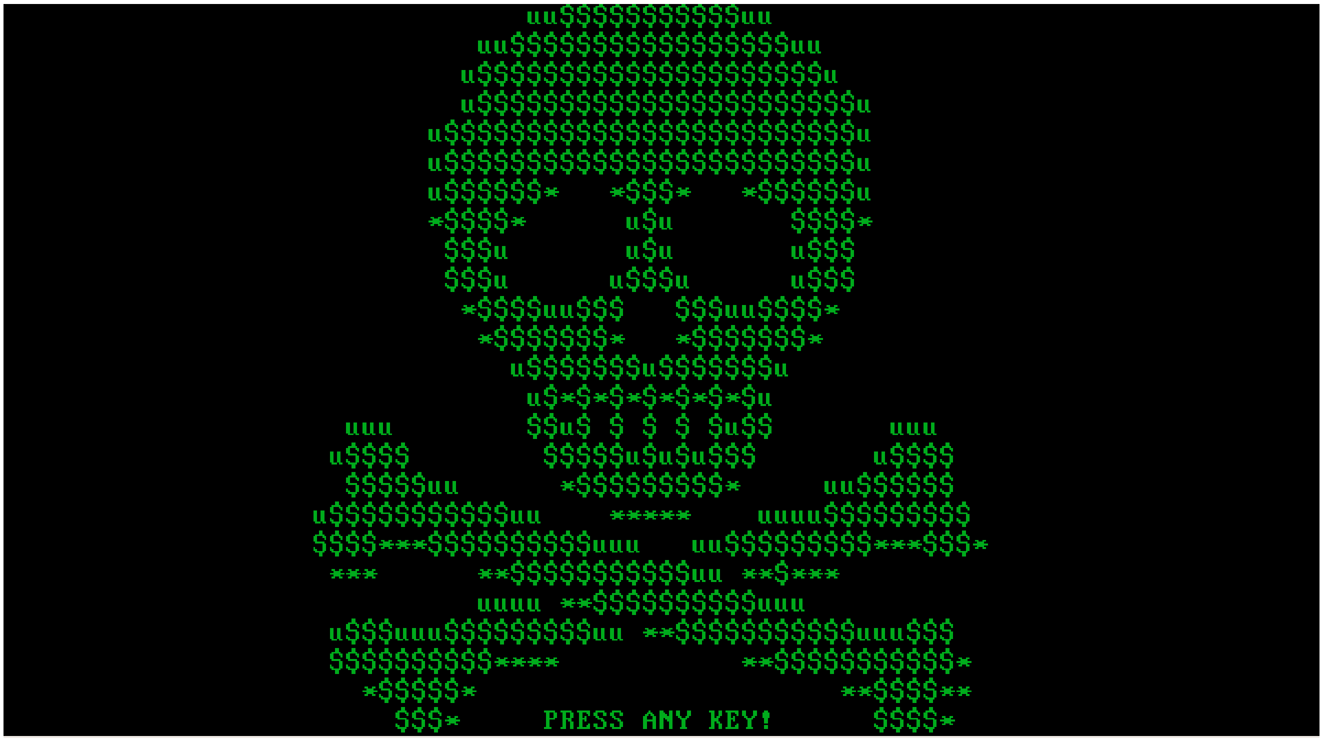


```
             uu$$$$$$$$$$$uu
          uu$$$$$$$$$$$$$$$$$uu
         u$$$$$$$$$$$$$$$$$$$$$u
         u$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$*   *$$$*   *$$$$$$u
       *$$$$*      u$u       $$$$*
        $$$u       u$u       u$$$
        $$$u      u$$$u      u$$$
         *$$$$uu$$$   $$$uu$$$$*
          *$$$$$$$*   *$$$$$$$*
            u$$$$$$$u$$$$$$$u
             u$*$*$*$*$*$*$u
  uuu        $$u$ $ $ $ $u$$       uuu
 u$$$$        $$$$$u$u$u$$$       u$$$$
  $$$$$uu      *$$$$$$$$$$*    uu$$$$$$
u$$$$$$$$$$$uu    *****    uuuu$$$$$$$$$
$$$$***$$$$$$$$$$uuu   uu$$$$$$$$$***$$$*
 ***      **$$$$$$$$$$$uu **$***
          uuuu **$$$$$$$$$$uuu
 u$$$uuu$$$$$$$$$uu **$$$$$$$$$$$uuu$$$
 $$$$$$$$$$****           **$$$$$$$$$$$*
   *$$$$$*                      **$$$$**
     $$$*     PRESS ANY KEY!      $$$$*
```

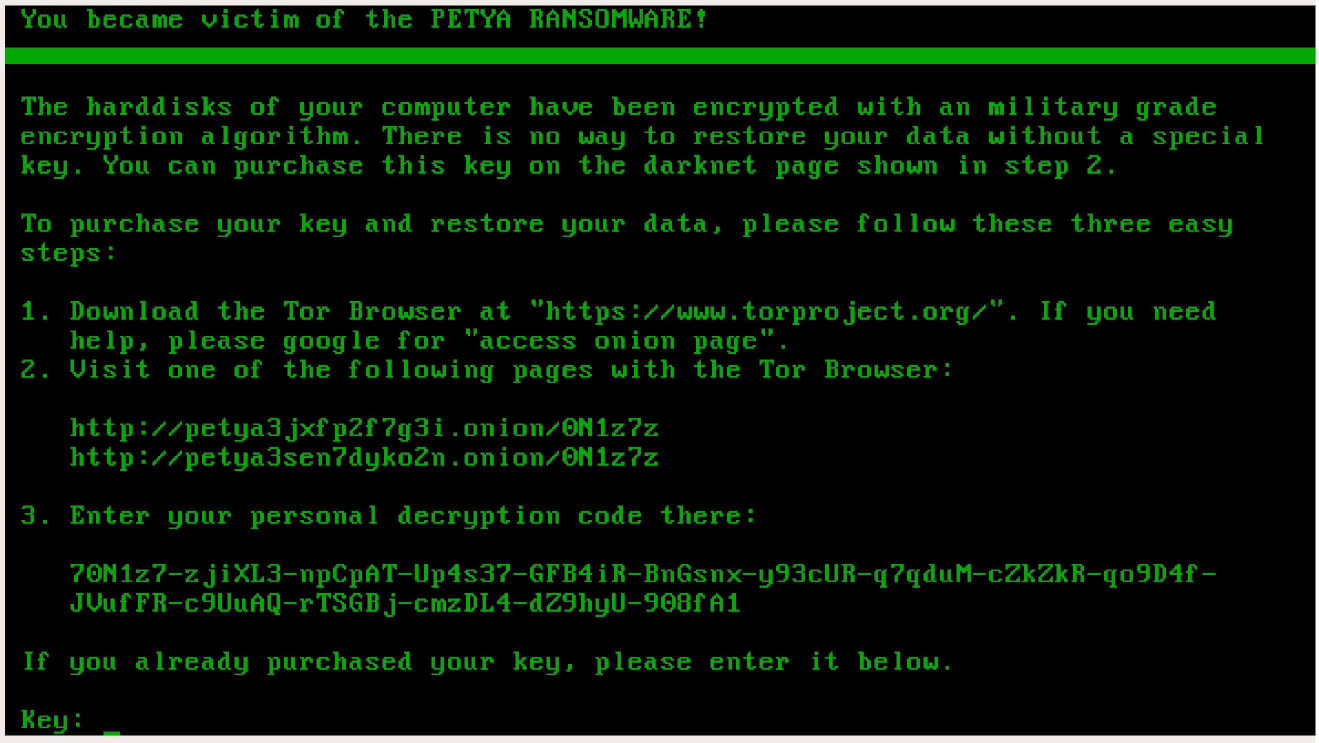


```
You became victim of the PETYA RANSOMWARE!

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://petya37h5tbhyvki.onion/MvnHqz
   http://petya5koahtsf7sv.onion/MvnHqz

3. Enter your personal decryption code there:

   afMf5Z-C83M2q-Nv9uR1-g9GZXY-a4iU47-c5R4iT-xR1WZk-nX4HmW-rnc1Kg-HMekdy-
   W8WDRr-rXz6TZ-jo69HJ-pre5Ry-Myg9rt

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

Key: _
```

Green Petya

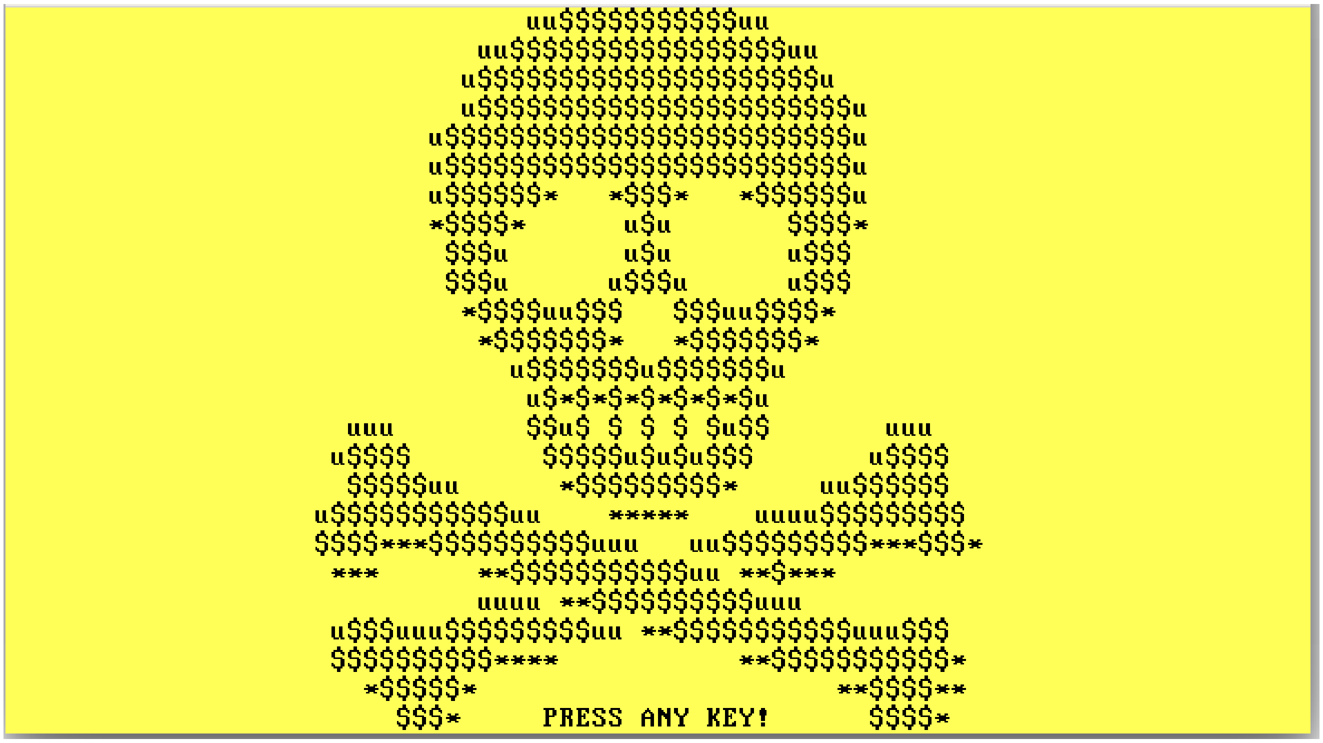


```
             uu$$$$$$$$$$$uu
          uu$$$$$$$$$$$$$$$$$uu
         u$$$$$$$$$$$$$$$$$$$$$u
         u$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$*   *$$$*   *$$$$$$u
       *$$$$*      u$u       $$$$*
        $$$u       u$u       u$$$
        $$$u      u$$$u      u$$$
         *$$$$uu$$$   $$$uu$$$$*
          *$$$$$$$*   *$$$$$$$*
            u$$$$$$$u$$$$$$$u
             u$*$*$*$*$*$*$u
  uuu        $$u$ $ $ $ $u$$       uuu
 u$$$$        $$$$$u$u$u$$$       u$$$$
  $$$$$uu      *$$$$$$$$$*     uu$$$$$$
u$$$$$$$$$$$uu    *****    uuuu$$$$$$$$$
$$$$***$$$$$$$$$$uuu   uu$$$$$$$$$***$$$*
 ***      **$$$$$$$$$$$uu **$***
          uuuu **$$$$$$$$$$uuu
 u$$$uuu$$$$$$$$$uu **$$$$$$$$$$$uuu$$$
 $$$$$$$$$$****           **$$$$$$$$$$$*
   *$$$$$*                      **$$$$**
     $$$*     PRESS ANY KEY!      $$$$*
```

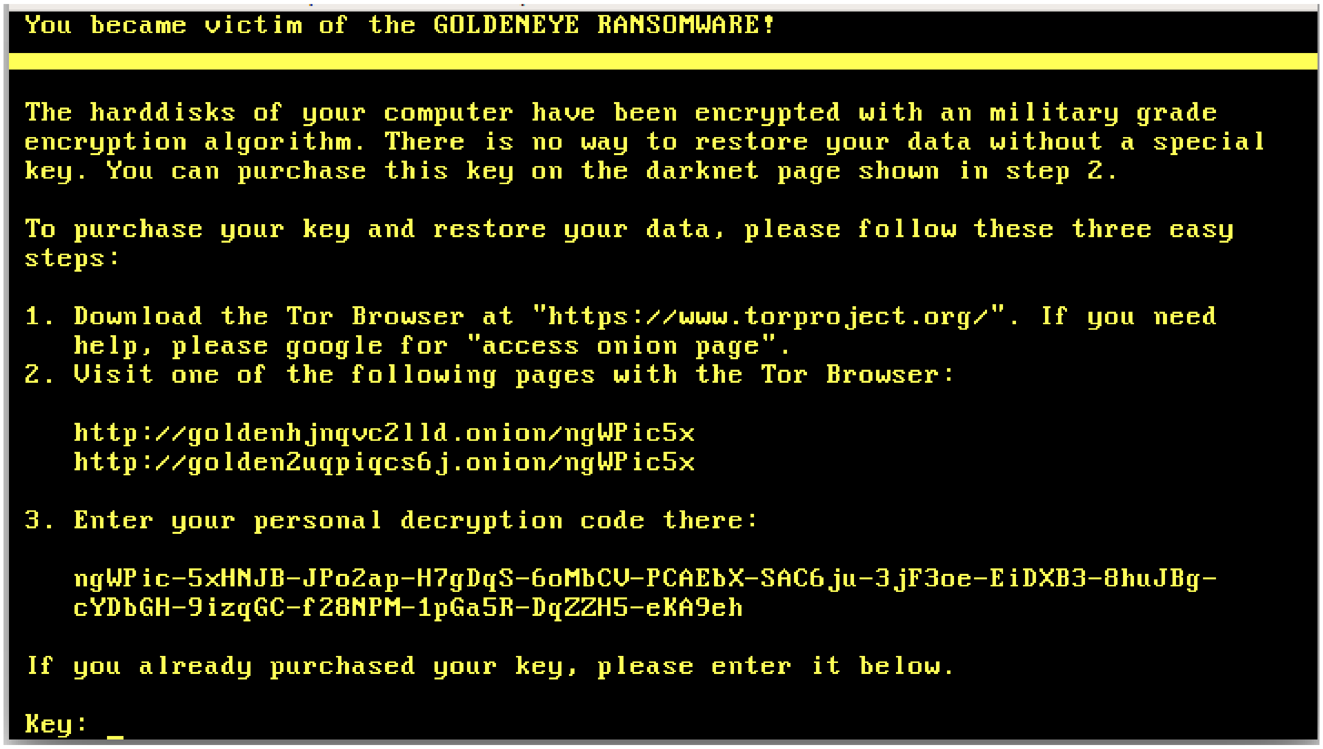


```
You became victim of the PETYA RANSOMWARE!

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: _
```

GoldenEye



```
             uu$$$$$$$$$$$$uu
          uu$$$$$$$$$$$$$$$$$uu
         u$$$$$$$$$$$$$$$$$$$$$u
         u$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$*   *$$$*   *$$$$$$u
       *$$$$*      u$u       $$$$*
        $$$u       u$u       u$$$
        $$$u      u$$$u      u$$$
         *$$$$uu$$$   $$$uu$$$$*
          *$$$$$$$*   *$$$$$$$*
            u$$$$$$$u$$$$$$$u
             u$*$*$*$*$*$*$u
  uuu        $$u$ $ $ $ $u$$       uuu
 u$$$$        $$$$$u$u$u$$$       u$$$$
  $$$$$uu      *$$$$$$$$$$*    uu$$$$$$
u$$$$$$$$$$$uu    *****    uuuu$$$$$$$$$
$$$$***$$$$$$$$$$uuu   uu$$$$$$$$$***$$$*
 ***      **$$$$$$$$$$$uu **$***
          uuuu **$$$$$$$$$$$uuu
 u$$$uuu$$$$$$$$$uu **$$$$$$$$$$$uuu$$$
 $$$$$$$$$$****           **$$$$$$$$$$$*
   *$$$$$*                      **$$$$**
     $$$*     PRESS ANY KEY!      $$$$*
```



```
You became victim of the GOLDENEYE 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://goldenhjnqvc2lld.onion/ngWPic5x
   http://golden2uqpiqcs6j.onion/ngWPic5x

3. Enter your personal decryption code there:

   ngWPic-5xHNJB-JPo2ap-H7gDqS-6oMbCV-PCAEbX-SAC6ju-3jF3oe-EiDXB3-8huJBg-
   cYDbGH-9izqGC-f28NPM-1pGa5R-DqZZH5-eKA9eh

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

Key: _
```

GoldenEye was the latest official release of Petya and was last seen around December 2016.

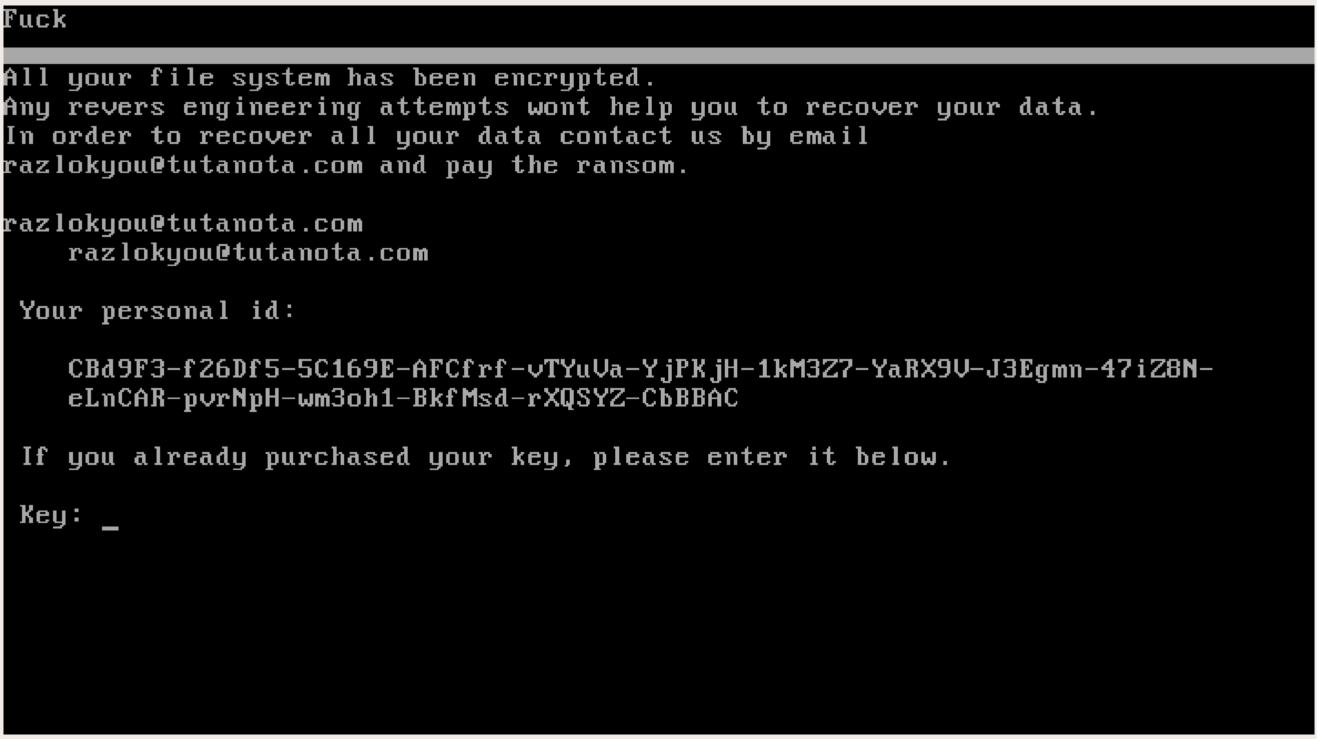
Unofficial releases (pirated versions)

Since Petya is powerful, other cybercriminals have been attracted to use it. However, not all of them want to join the affiliate program and pay its creator. Similar to legitimate software, Petya has pirated versions. So far, we observed two unofficial releases:

- PetrWrap – uses Petya's low-level component as well as patched Petya's DLL, wrapped by a new loader. It's based on Green Petya.
- EternalPetya – also called NotPetya, ExPetr, etc. The malware based on GoldenEye, used in the attack on Ukraine. The high-level layer (PE file) has been rewritten.

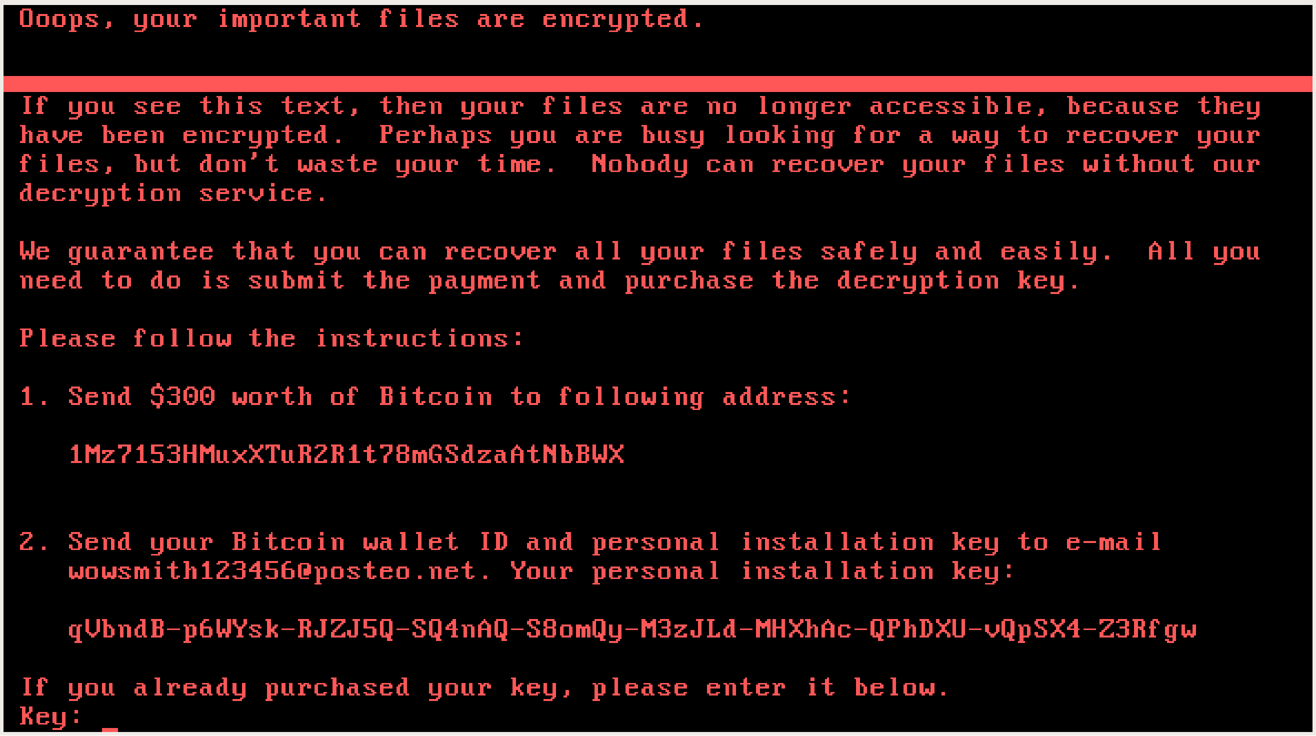
The pirated versions can be identified by the modified look. In both cases, the original Petya's skull has been removed.

PetrWrap



```
Fuck

All your file system has been encrypted.
Any revers engineering attempts wont help you to recover your data.
In order to recover all your data contact us by email
razlokyou@tutanota.com and pay the ransom.

razlokyou@tutanota.com
    razlokyou@tutanota.com

 Your personal id:

    CBd9F3-f26Df5-5C169E-AFCfrf-vTYuVa-YjPKjH-1kM3Z7-YaRX9V-J3Egmn-47iZ8N-
    eLnCAR-pvrNpH-wm3oh1-BkfMsd-rXQSYZ-CbBBAC

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

 Key: _
```

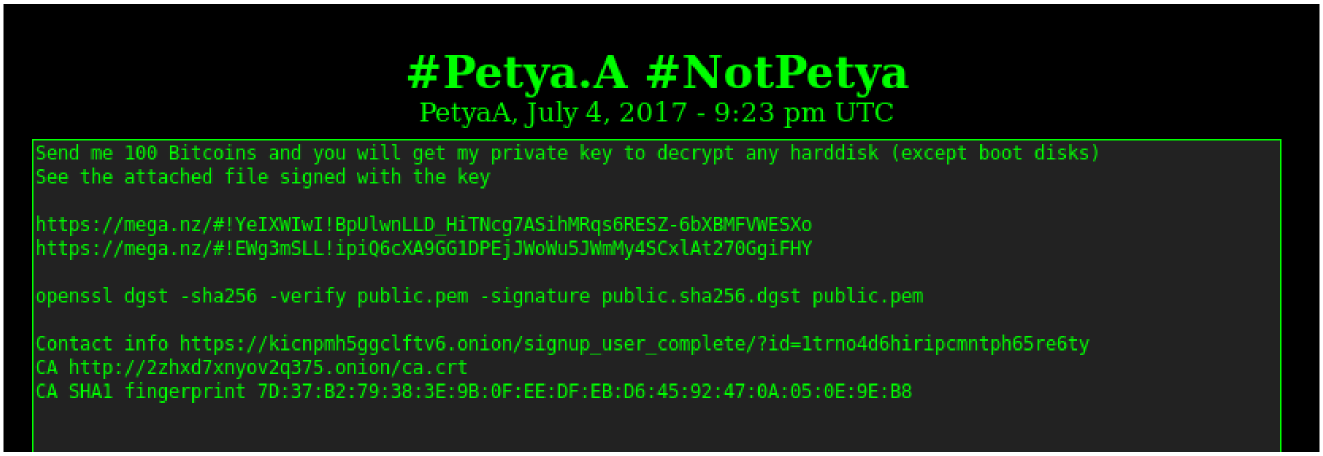
EternalPetya



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   qVbndB-p6WYsk-RJZJ5Q-SQ4nAQ-S8omQy-M3zJLd-MHXhAc-QPhDXU-vQpSX4-Z3Rfgw

If you already purchased your key, please enter it below.
Key: _
```

While PetrWrap was a fully-functional ransomware, EternalPetya seems unfinished or broken on purpose because the Salsa key that used to encrypt the MFT cannot be recovered. Once encrypted, data cannot be decrypted, even by the malware authors.

Same as the original GoldenEye, EternalPetya encrypts also files with the selected extensions before attacking the MFT. Files are encrypted using different algorithms and keys than the MFT (RSA + AES, while the MFT is encrypted using Salsa20). On July 4, the distributors of EternalPetya raised the ransom demand and offered to sell the private RSA key that can potentially help in unlocking encrypted files but not the MFT. Below is the message from the attackers [source]:



#Petya.A #NotPetya

PetyaA, July 4, 2017 - 9:23 pm UTC

```
Send me 100 Bitcoins and you will get my private key to decrypt any harddisk (except boot disks)
See the attached file signed with the key

https://mega.nz/#!YeIXWIwI!BpUlwnLLD_HiTNcg7ASihMRqs6RESZ-6bXBMFVWESXo
https://mega.nz/#!EWg3mSLL!ipiQ6cXA9GG1DPEjJWoWu5JWmMy4SCxlAt270GgiFHY

openssl dgst -sha256 -verify public.pem -signature public.sha256.dgst public.pem

Contact info https://kicnpmh5ggclftv6.onion/signup_user_complete/?id=1trno4d6hiripcmntph65re6ty
CA http://2zhxd7xnyov2q375.onion/ca.crt
CA SHA1 fingerprint 7D:37:B2:79:38:3E:9B:0F:EE:DF:EB:D6:45:92:47:0A:05:0E:9E:B8
```

Copycats

In addition to malware based on the original Petya, copycats also have started to appear. They have nothing in common with Petya's code, they only try to imitate its look or some of its features. Some examples are SatanaRansomware or Petya+, a .NET imitation of Petya discovered by @LawrenceAbrams.

Conclusion

Ransomware piracy is becoming common and this triggers more problems to the victims. Often, the authors of such pirated malware don't care to give the data back. They just use the reputation of known ransomware to scam victims into paying. In addition to the described cases, we have also encountered several versions of pirated DMALocker, wherein some of the variants corrupt the data that make recovery hard or even impossible.

Petya is a powerful malware. And to make things worse, it is also very easy to modify and repurpose. Even if the official line of Petya has been discontinued, we can expect the pirated versions to still be around.

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.