ExPetr/Petya/NotPetya is a Wiper, Not Ransomware

SL securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/

Incidents

Incidents

28 Jun 2017

minute read

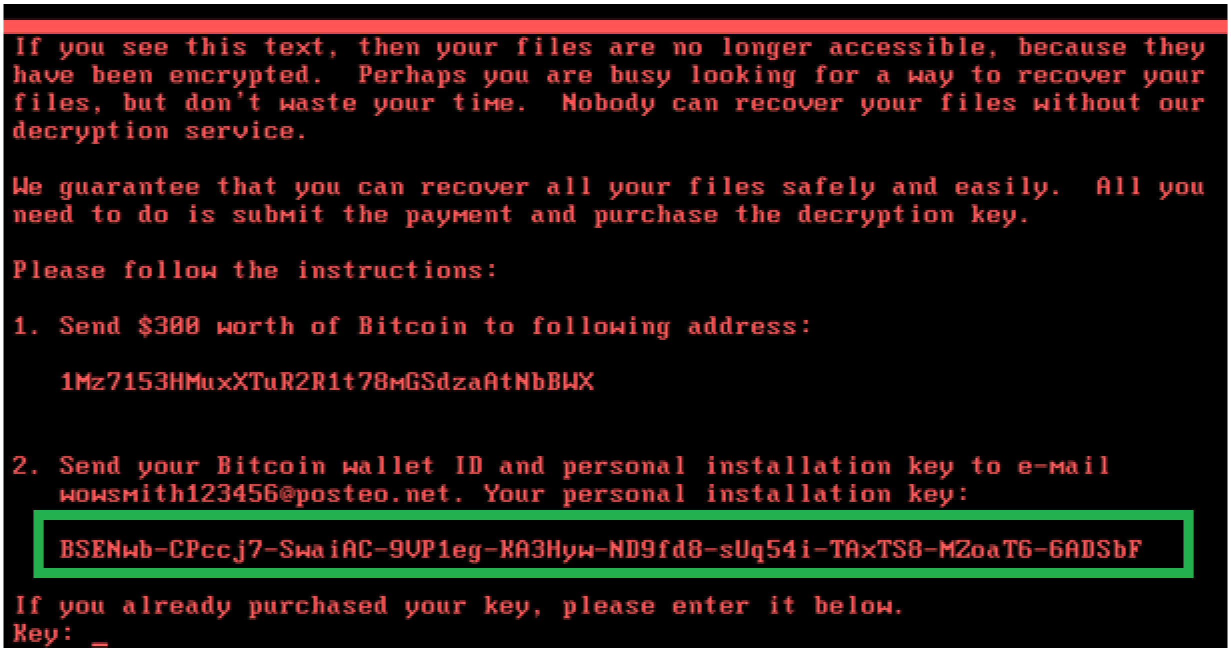
Authors

- Expert Anton Ivanov
- Expert Orkhan Mamedov

After an analysis of the encryption routine of the malware used in the Petya/ExPetr attacks, we have thought that **the threat actor cannot decrypt victims' disk**, even if a payment was made.

This supports the theory that this malware campaign was not designed as a ransomware attack for financial gain. Instead, it appears it was designed as a wiper pretending to be ransomware.

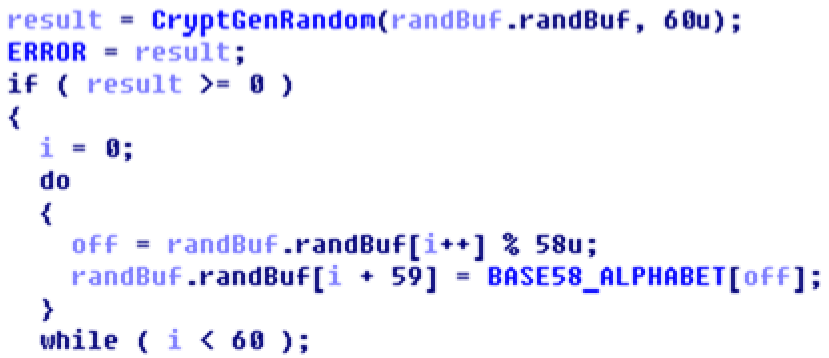
Below the technical details are presented. First, in order to decrypt victim's disk the attackers need the installation ID:



```
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:

   BSENwb-CPccj7-SwaiAC-9VP1eg-KA3Hyw-ND9fd8-sUq54i-TAxTS8-MZoaT6-6ADSbF

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

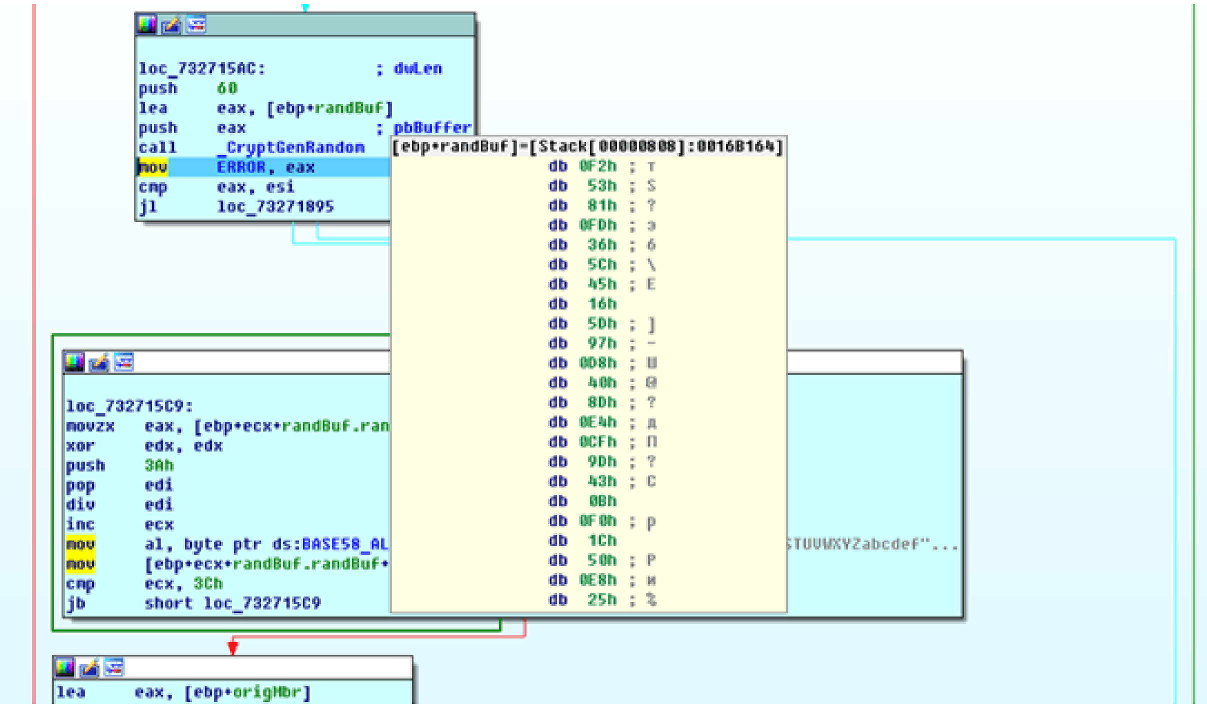
In previous versions of "similar" ransomware like Petya/Mischa/GoldenEye, this installation ID contains crucial information for the key recovery. After sending this information to the attacker they can extract the decryption key using their private key.

Here's how this installation ID is generated in the ExPetr ransomware:



```
result = CryptGenRandom(randBuf.randBuf, 60u);
ERROR = result;
if ( result >= 0 )
{
  i = 0;
  do
  {
    off = randBuf.randBuf[i++] % 58u;
    randBuf.randBuf[i + 59] = BASE58_ALPHABET[off];
  }
  while ( i < 60 );
```

This installation ID in our test case is built using the CryptGenRandom function, which is basically generating random data.



```
loc_732715AC:                 ; dwLen
push    60
lea     eax, [ebp+randBuf]
push    eax                   ; pbBuffer
call    _CryptGenRandom
mov     ERROR, eax
cmp     eax, esi
jl      loc_73271895
```

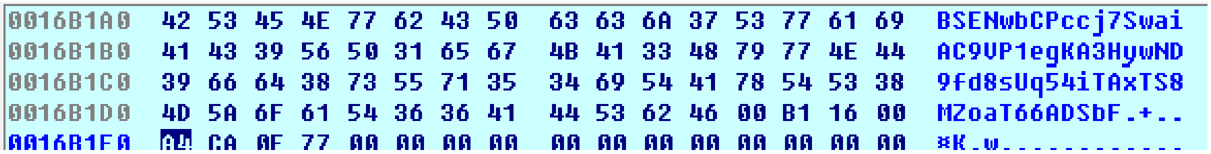
```
[ebp+randBuf]=[Stack[00000808]:0016B164]
                 db 0F2h ; т
                 db  53h ; S
                 db  81h ; ?
                 db 0FDh ; э
                 db  36h ; 6
                 db  5Ch ; \
                 db  45h ; E
                 db  16h
                 db  5Dh ; ]
                 db  97h ; -
                 db 0D8h ; Ш
                 db  40h ; @
                 db  8Dh ; ?
                 db 0E4h ; д
                 db 0CFh ; П
                 db  9Dh ; ?
                 db  43h ; C
                 db  0Bh
                 db 0F0h ; р
                 db  1Ch
                 db  50h ; P
                 db 0E8h ; и
                 db  25h ; %
```

```
loc_732715C9:
movzx   eax, [ebp+ecx+randBuf.ran
xor     edx, edx
push    3Ah
pop     edi
div     edi
inc     ecx
mov     al, byte ptr ds:BASE58_AL
mov     [ebp+ecx+randBuf.randBuf+
cmp     ecx, 3Ch
jb      short loc_732715C9
```

```
STUVWXYZabcdef"...
```

```
lea     eax, [ebp+origMbr]
```

The following buffer contains the randomly generated data in an encoded “BASE58” format:



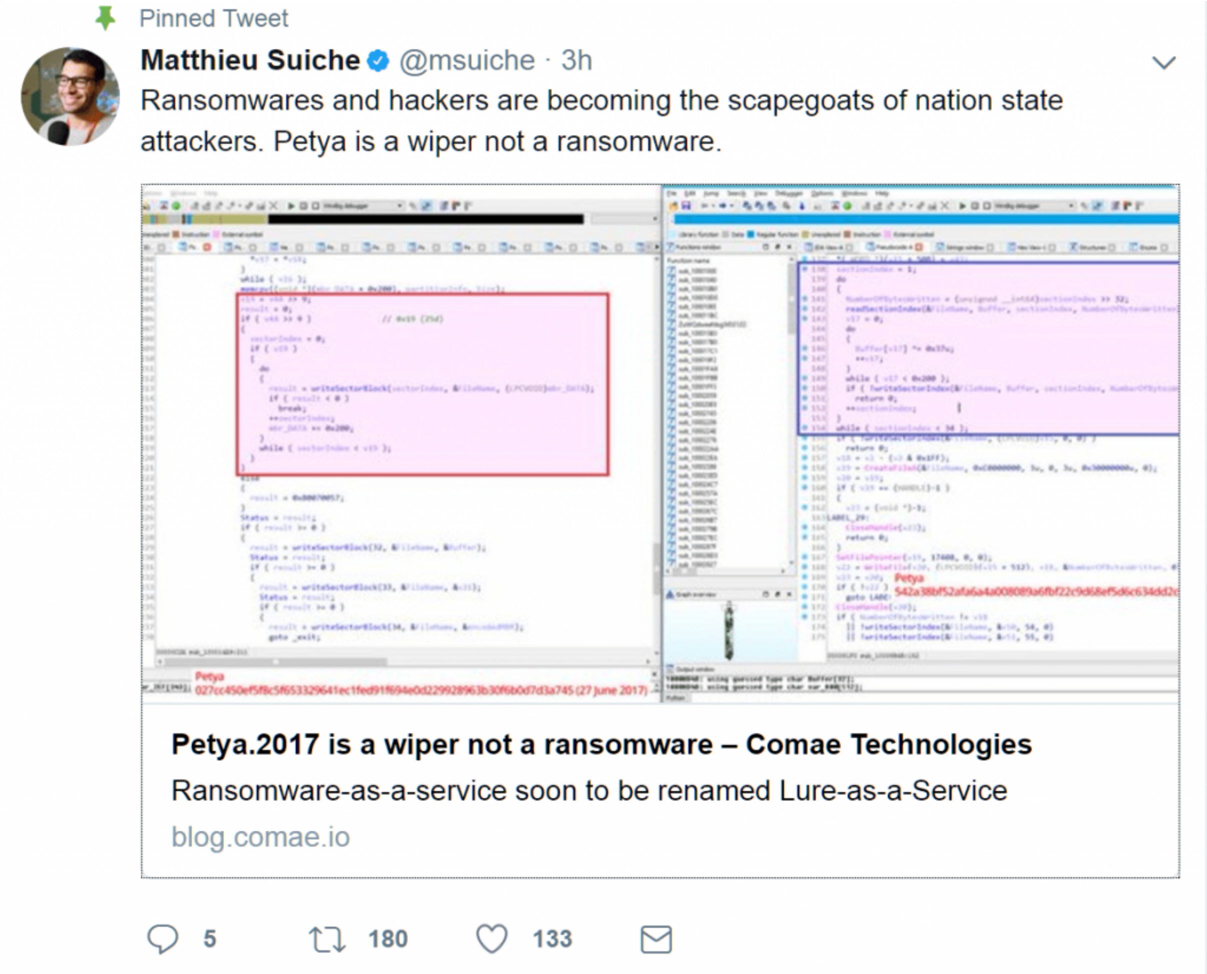
```
0016B1A0  42 53 45 4E 77 62 43 50  63 63 6A 37 53 77 61 69  BSENwbCPccj7Swai
0016B1B0  41 43 39 56 50 31 65 67  4B 41 33 48 79 77 4E 44  AC9VP1egKA3HywND
0016B1C0  39 66 64 38 73 55 71 35  34 69 54 41 78 54 53 38  9fd8sUq54iTAxTS8
0016B1D0  4D 5A 6F 61 54 36 36 41  44 53 62 46 00 B1 16 00  MZoaT66ADSbF.+..
0016B1E0  A4 CA 0F 77 00 00 00 00  00 00 00 00 00 00 00 00  ¤K.w............
```

If we compare this randomly generated data and the final installation ID shown in the first screen, they are the same. In a normal setup, this string should contain encrypted information that will be used to restore the decryption key. For ExPetr, **the ID shown in the ransom screen is just plain random data**.

That means that the attacker cannot extract any decryption information from such a randomly generated string displayed on the victim, and as a result, the victims will not be able to decrypt any of the encrypted disks using the installation ID.

What does it mean? Well, first of all, this is the worst-case news for the victims – even if they pay the ransom they will not get their data back. Secondly, this reinforces the theory that the main goal of the ExPetr attack was not financially motivated, but destructive.

Our friend Matt Suiche from Comae Technologies independently came to the same conclusion.



Matthieu Suiche @msuiche · 3h

Ransomwares and hackers are becoming the scapegoats of nation state attackers. Petya is a wiper not a ransomware.

Petya
027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745 (27 June 2017)
Petya
542a38bf52afa6a4a008089a6fbf22c9d68ef5d6c634dd2

Petya.2017 is a wiper not a ransomware – Comae Technologies

Ransomware-as-a-service soon to be renamed Lure-as-a-Service

blog.comae.io

- Data Encryption
- Malware Descriptions
- Petya
- Ransomware
- Wiper

Authors

- Expert Anton Ivanov
- Expert Orkhan Mamedov

ExPetr/Petya/NotPetya is a Wiper, Not Ransomware

Your email address will not be published. Required fields are marked *

GReAT webinars

13 May 2021, 1:00pm

GReAT Ideas. Balalaika Edition

26 Feb 2021, 12:00pm
17 Jun 2020, 1:00pm
26 Aug 2020, 2:00pm
22 Jul 2020, 2:00pm
From the same authors

Sodin ransomware exploits Windows vulnerability and processor architecture

KeyPass ransomware

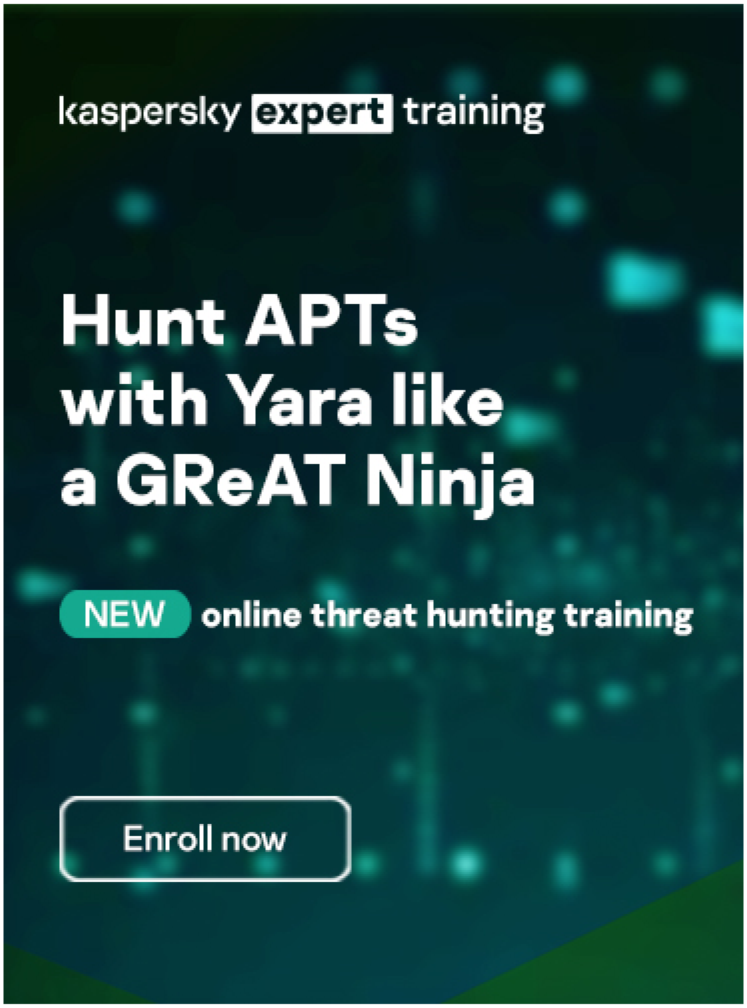
SynAck targeted ransomware uses the Doppelgänging technique

Mining is the new black

Bad Rabbit ransomware

Subscribe to our weekly e-mails

The hottest research right in your inbox


kaspersky expert training
Hunt APTs with Yara like a GReAT Ninja
NEW online threat hunting training
Enroll now

Reports

APT trends report Q1 2022

This is our latest summary of advanced persistent threat (APT) activity, focusing on events that we observed during Q1 2022.

Lazarus Trojanized DeFi app for delivering malware

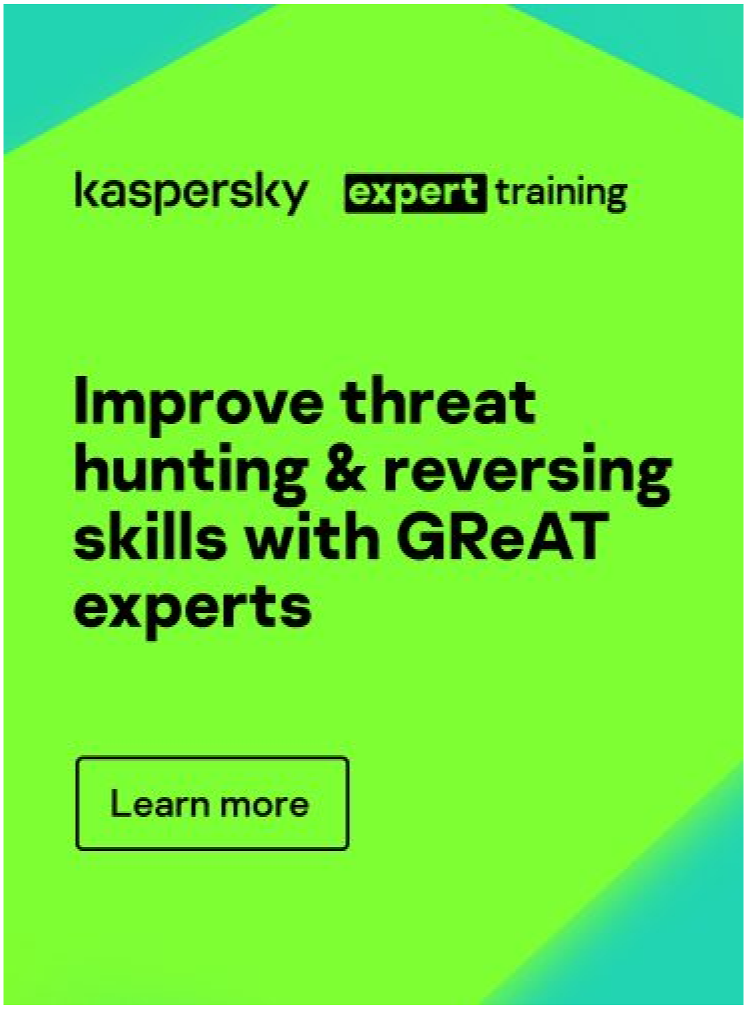
We recently discovered a Trojanized DeFi application that was compiled in November 2021. This application contains a legitimate program called DeFi Wallet that saves and manages a cryptocurrency wallet, but also implants a full-featured backdoor.

MoonBounce: the dark side of UEFI firmware

At the end of 2021, we inspected UEFI firmware that was tampered with to embed a malicious code we dub MoonBounce. In this report we describe how the MoonBounce implant works and how it is connected to APT41.

The BlueNoroff cryptocurrency hunt is still on

It appears that BlueNoroff shifted focus from hitting banks and SWIFT-connected servers to solely cryptocurrency businesses as the main source of the group’s illegal income.


kaspersky expert training
Improve threat hunting & reversing skills with GReAT experts
Learn more

Subscribe to our weekly e-mails

The hottest research right in your inbox

-
-
-