ExPetr/Petya/NotPetya is a Wiper, Not Ransomware

INCIDENTS 28 JUN 2017 1 minute read

// AUTHORS

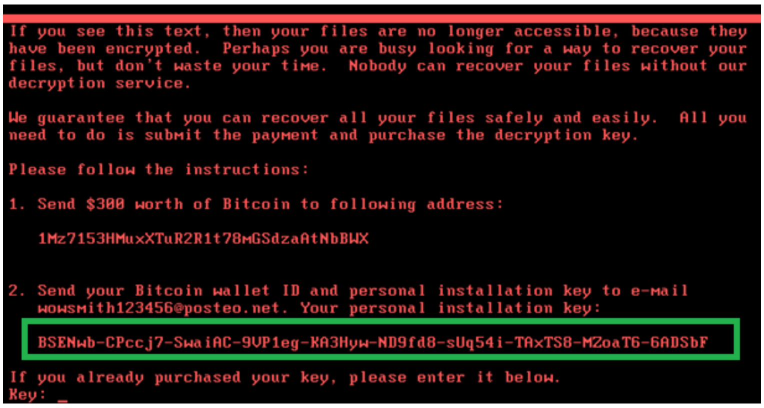
Expert ANTON IVANOV

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.

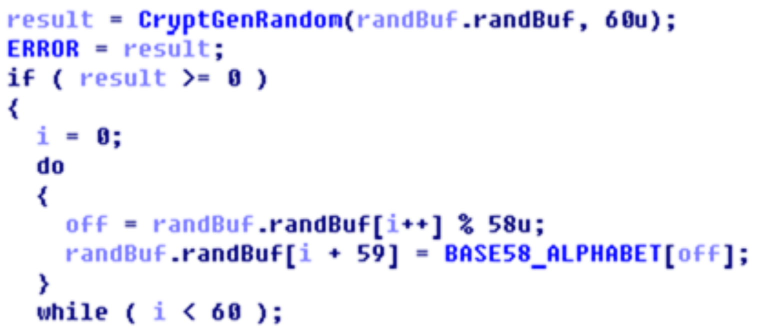
Below the technical details are presented. First, in order to decrypt victim's disk the attackers need the installation ID:



```
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: _
```

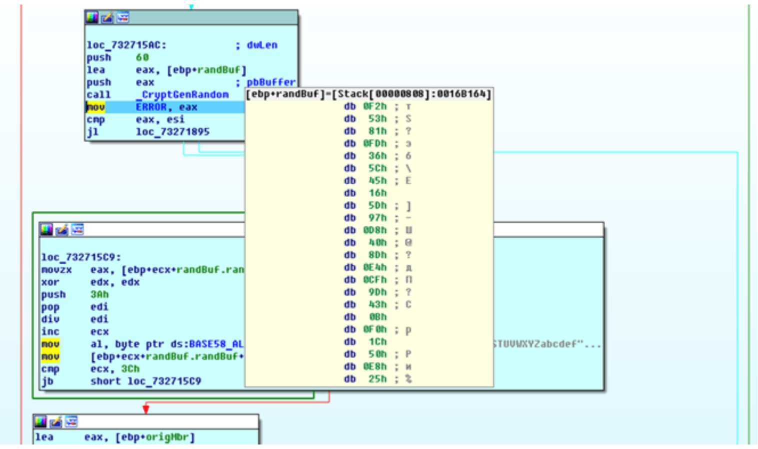
In previous versions of “similar” ransomware like Petya/Mischa/GoldenEye, this installation ID contains crucial information for the key recovery. After sending this information to the attacker they can extract the decryption key using their private key.

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:

FROM THE SAME AUTHORS

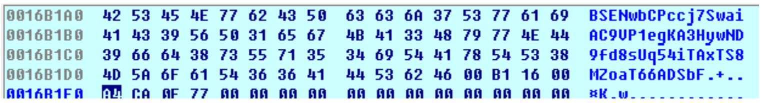
Sodin ransomware exploits Windows vulnerability and processor architecture

KeyPass ransomware

SynAck targeted ransomware uses the Doppelgänging technique

Mining is the new black

Bad Rabbit ransomware



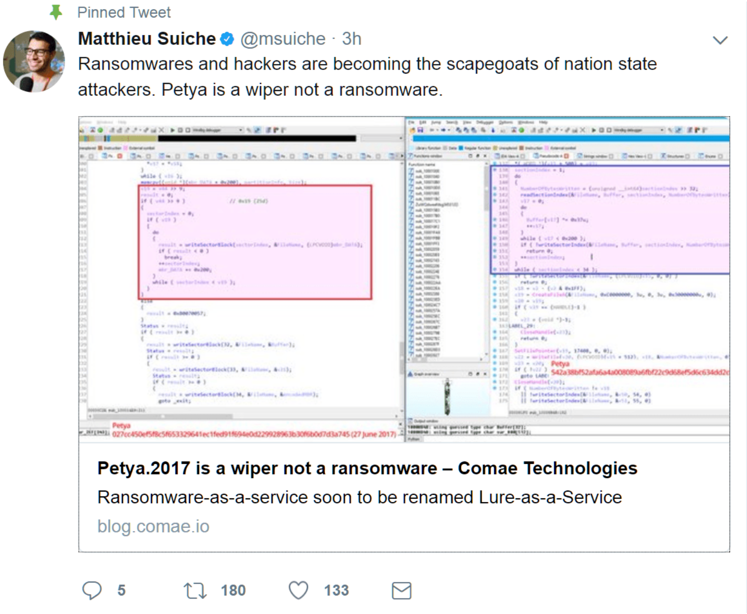
```
0016B1A0  42 53 45 4E 77 62 43 50  63 63 6A 37 53 77 61 69  BSENwbCPccj7Swai
0016B1B0  41 43 39 56 50 31 65 67  4B 41 33 48 79 77 4E 44  AC9VP1egKA3HywND
0016B1C0  39 66 64 38 73 55 71 35  34 69 54 41 78 54 53 38  9fd8sUq54iTAxTS8
0016B1D0  4D 5A 6F 61 54 36 36 41  44 53 62 46 00 B1 16 00  MZoaT66ADSbF.+..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



Pinned Tweet

Matthieu Suiche @msuiche · 3h

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

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

ExPetr/Petya/NotPetya is a Wiper, Not Ransomware

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

Type your comment here

Name *	Email *

Comment

RAMALINGAM
Posted on June 29, 2017. 4:23 am

is the kaspersky update equipped to deal with the ExPetr/Petya/NotPetya wiper/

Reply

> ARASH ZANGENEH
> Posted on June 29, 2017. 9:21 am
>
> Yes, at least our KES 10, managed to block it.
>
> Reply

JO
Posted on June 29, 2017. 8:33 am

I agree that this is a wiper and not a Ransomware however sometimes that actual Malware may not be the main motive behind the attack. This to me is either a currency manipulation on a large scale or simply cyber terrorism.

You can check out the theory below http://www.securityweek.com/latest-wannacry-theory-currency-manipulation

Reply

DIAZOMETHAN
Posted on June 29, 2017. 8:44 am

Weak reason to classify it as a wiper, in my opinion. Wouldn't it be possible that the author stores the key and the ID in a table? In this case, it is nothing more than

IN THE SAME CATEGORY

XZ backdoor: Hook analysis

Assessing the Y, and How, of the XZ Utils incident

XZ backdoor story – Initial analysis

A hack in hand is worth two in the bush

something like a UUID, but it would be still possible for the attacker to decrypt the data.

Matt Suiche gives the better explanation why it is a wiper: Because it destroys some crucial data.

Reply

JANIKO
Posted on June 29, 2017. 1:49 pm

I'd like more info about this : the ID is random, right ? And about the encryption key : is it generated elsewhere ? Is it sent with that random ID to a C&C ? And is it really a wiper or only a bad-written ransomware ?

Reply

ANDREA
Posted on June 29, 2017. 7:59 pm

Hi
we have also this detailed analysis
https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/

We have been able to retrieve most of the files of infected computers. However, as expetya does crypt some of them BEFORE actually being visible, those are encrypted. The TXT are safe, so that means that they're not simply corrupted, but encrypted.

Given the key in the README.TXT file, do you think they can actually be decrypted? NOte that for many files we also have the same exact file BEFORE encryption.

Reply

PETE
Posted on June 30, 2017. 10:52 am

Ok ID is random – so what?
Did you proove that the random ID has nothing to do with the encryption key?

Reply

QBot banker delivered through business correspondence

// LATEST POSTS

SOC, TI AND IR POSTS

Attackers exploiting a patched FortiClient EMS vulnerability in the wild

ASHLEY MUÑOZ,
FRANCESCO FIGURELLI,
CRISTIAN SOUZA,
EDUARDO OVALLE,
AREG BAGHINYAN

APT REPORTS

Lazarus group evolves its infection chain with old and new malware

VASILY BERDNIKOV, SOJUN RYU

CRIMEWARE REPORTS

Analysis of Cyber Anarchy Squad attacks targeting Russian and Belarusian organizations

KASPERSKY

MALWARE DESCRIPTIONS

Download a banker to track your parcel

DMITRY KALININ

// LATEST WEBINARS

THREAT INTELLIGENCE AND IR

04 SEP 2024, 5:00PM 60 MIN

Inside the Dark Web: exploring the human side of cybercriminals

ANNA PAVLOVSKAYA

TECHNOLOGIES AND SERVICES

13 AUG 2024, 5:00PM 60 MIN

The Cybersecurity Buyer's Dilemma: Hype vs (True) Expertise

OLEG GOROBETS,
ALEXANDER LISKIN

CYBERTHREAT TALKS

16 JUL 2024, 5:00PM 60 MIN

Cybersecurity's human factor – more than an unpatched vulnerability

OLEG GOROBETS

TRAININGS AND WORKSHOPS

09 JUL 2024, 4:00PM 60 MIN

Building and prioritizing detection engineering backlogs with MITRE ATT&CK

ANDREY TAMOYKIN

// REPORTS

BellaCPP: Discovering a new BellaCiao variant written in C++

While investigating an incident involving the BellaCiao .NET malware, Kaspersky researchers discovered a C++ version they dubbed “BellaCPP”.

Lazarus group evolves its infection chain with old and new malware

Lazarus targets employees of a nuclear-related organization with a bunch of malware, such as MISTPEN, LPEClient, RollMid, CookieTime and a new modular backdoor CookiePlus.

Careto is back: what’s new after 10 years of silence?

Kaspersky researchers analyze 2019, 2022 and 2024 attacks attributed to Careto APT with medium to high confidence.

APT trends report Q3 2024

The report features the most significant developments relating to APT groups in Q3 2024, including hacktivist activity, new APT tools and campaigns.

Meet hrtng, Kaspersky GReAT's plugin for IDA Pro
Our secret ingredient for reverse engineering
Read more
k

// SUBSCRIBE TO OUR WEEKLY E-MAILS

The hottest research right in your inbox

Email

Subscribe

□ I agree to provide my email address to “AO Kaspersky Lab” to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the “unsubscribe” link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

THREATS

- APT (Targeted attacks)
- Secure environment (IoT)
- Mobile threats
- Financial threats
- Spam and phishing
- Industrial threats
- Web threats
- Vulnerabilities and exploits
- All threats

CATEGORIES

- APT reports
- Malware descriptions
- Security Bulletin
- Malware reports
- Spam and phishing reports
- Security technologies
- Research
- Publications
- All categories

OTHER SECTIONS

- Archive
- All tags
- Webinars
- APT Logbook
- Statistics
- Encyclopedia
- Threats descriptions
- KSB 2024