ExPetr/Petya/NotPetya is a Wiper, Not Ransomware

By Anton Ivanov

Published: 2017-06-28 · Archived: 2026-04-06 00:26:32 UTC

Incidents

Incidents

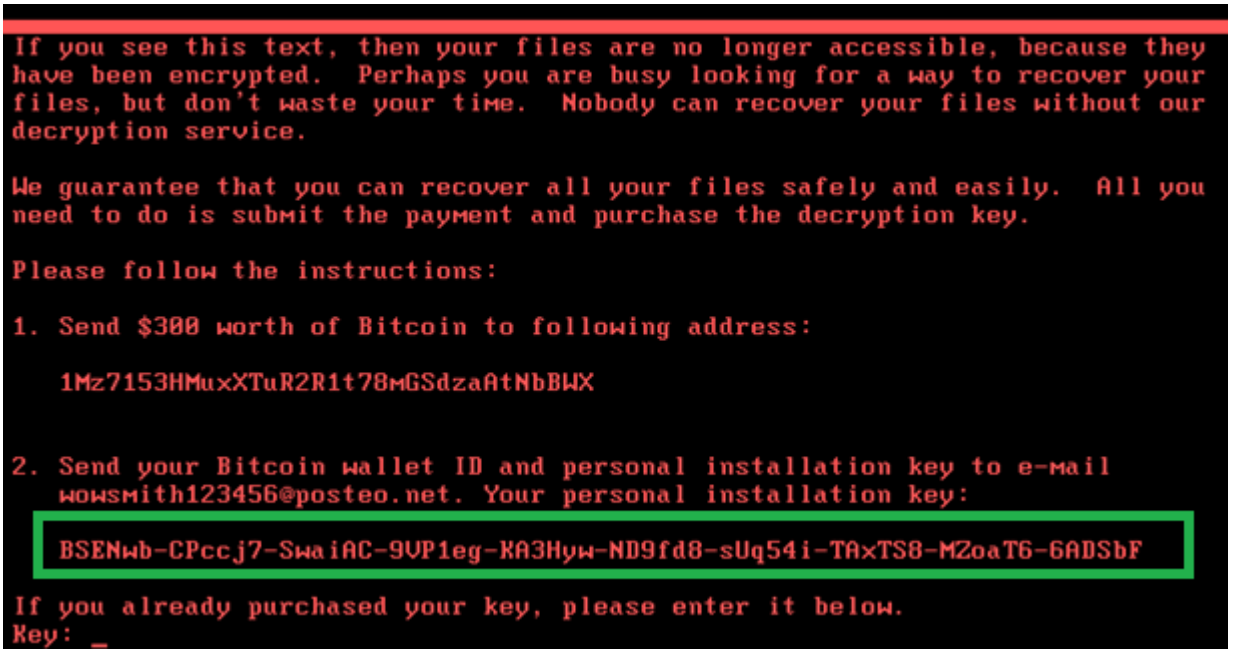
28 Jun 2017

1 minute read

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:

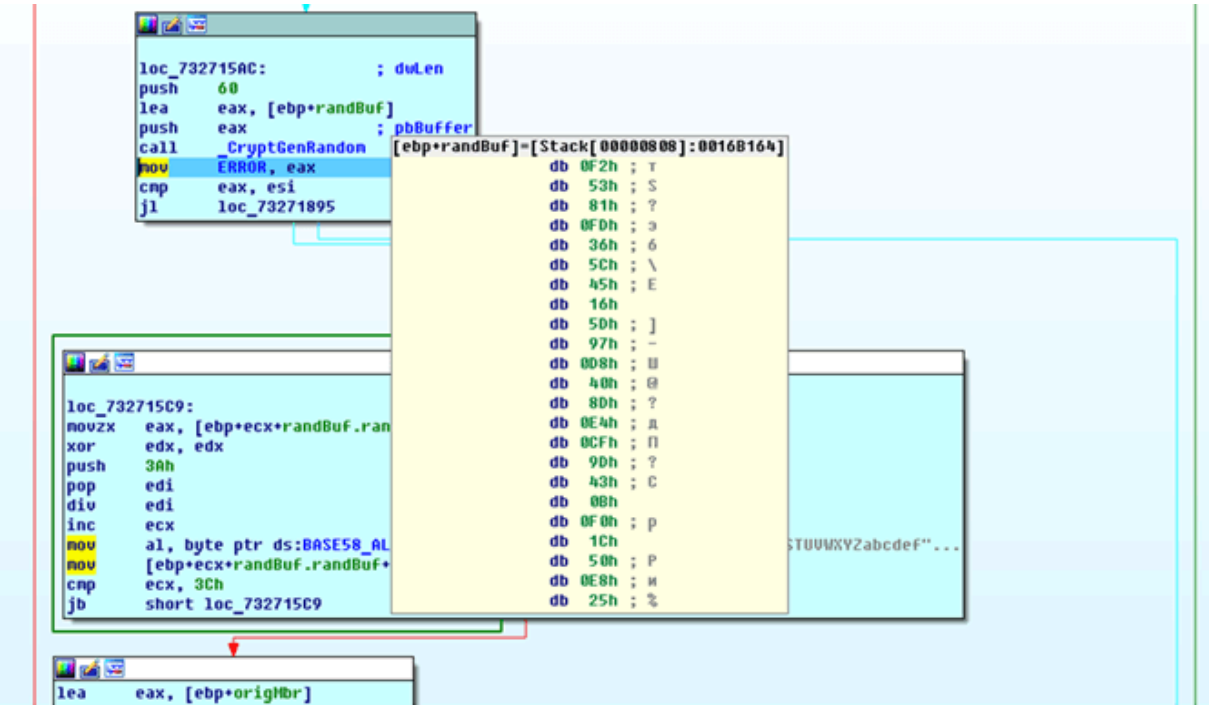


In previous versions of “similar” ransomware like Petya/Mischa/GoldenEye, this installation ID contains crucial information for the key recovery. After sending this information to the attacker they can extract the decryption key using their private key.

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.



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

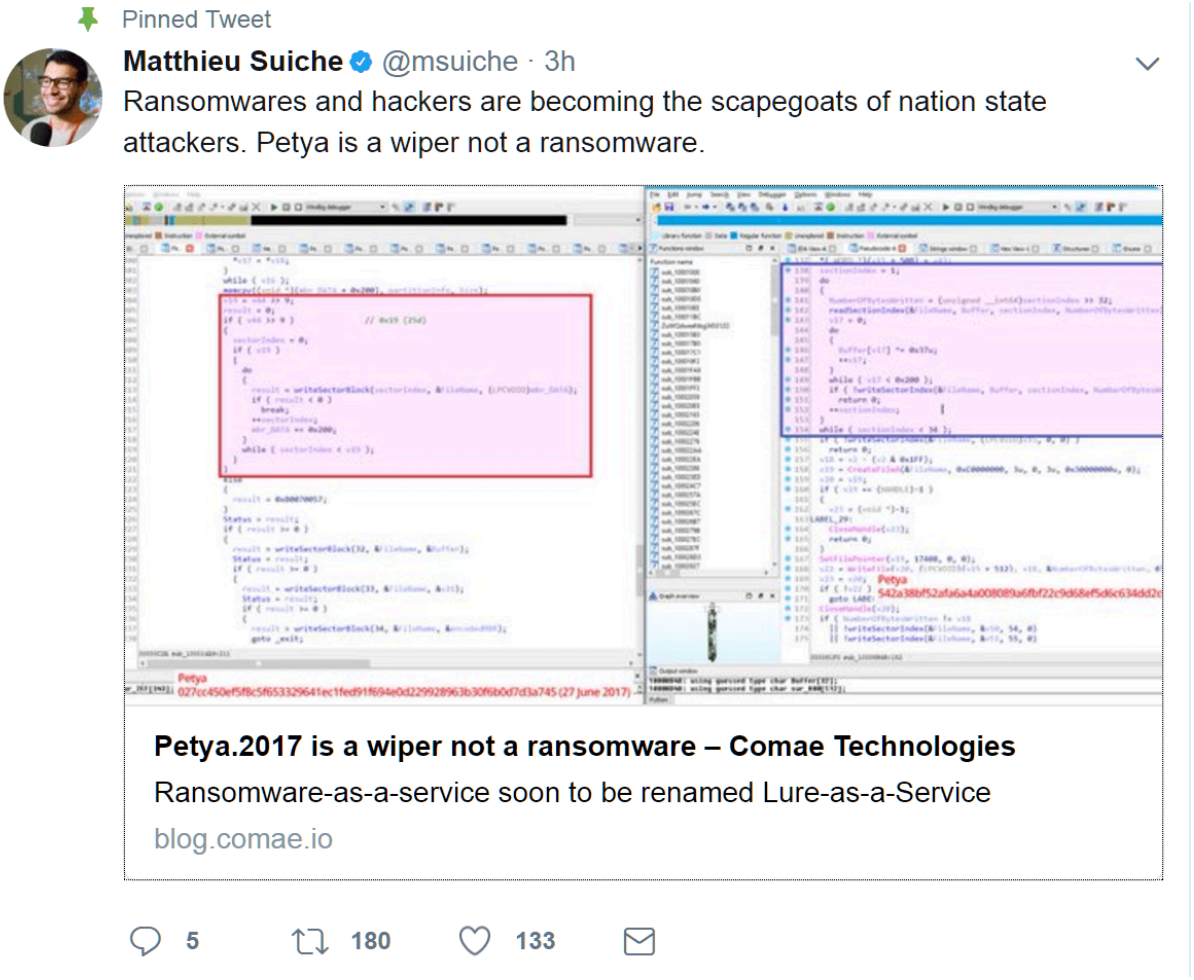
```
0016B1A0  42 53 45 4E 77 62 43 50  63 63 6A 37 53 77 61 69  BSENwbCPccj7Swai
0016B1B0  41 43 39 56 50 31 65 67  4B 41 33 48 79 77 4E 44  AC9VP1egKA3HywND
0016B1C0  39 66 64 38 73 55 71 35  34 69 54 41 78 54 53 38  9fd8sUq54iTAxTS8
0016B1D0  4D 5A 6F 61 54 36 36 41  44 53 62 46 00 B1 16 00  MZoaT66ADSbF.±..
0016B1E0  01 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**.

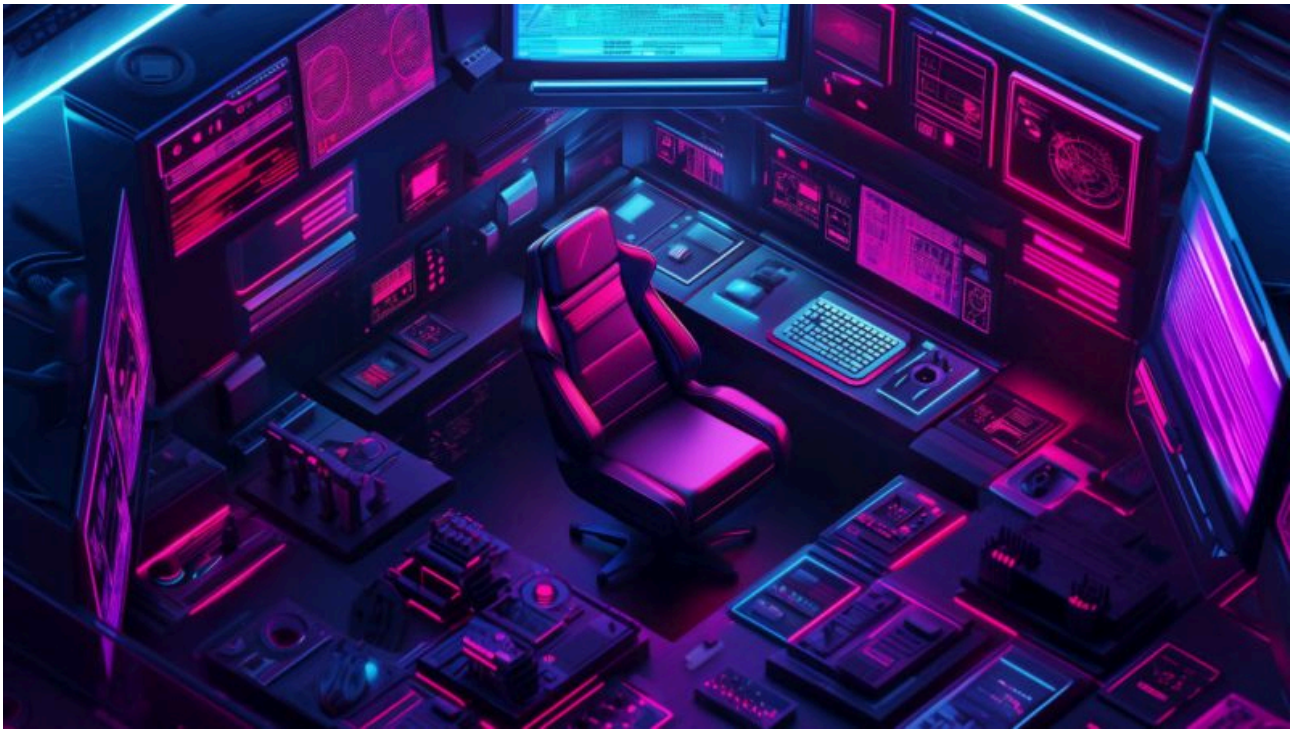
That means that the attacker cannot extract any decryption information from such a randomly generated string displayed on the victim, and as a result, the victims will not be able to decrypt any of the encrypted disks using the installation ID.

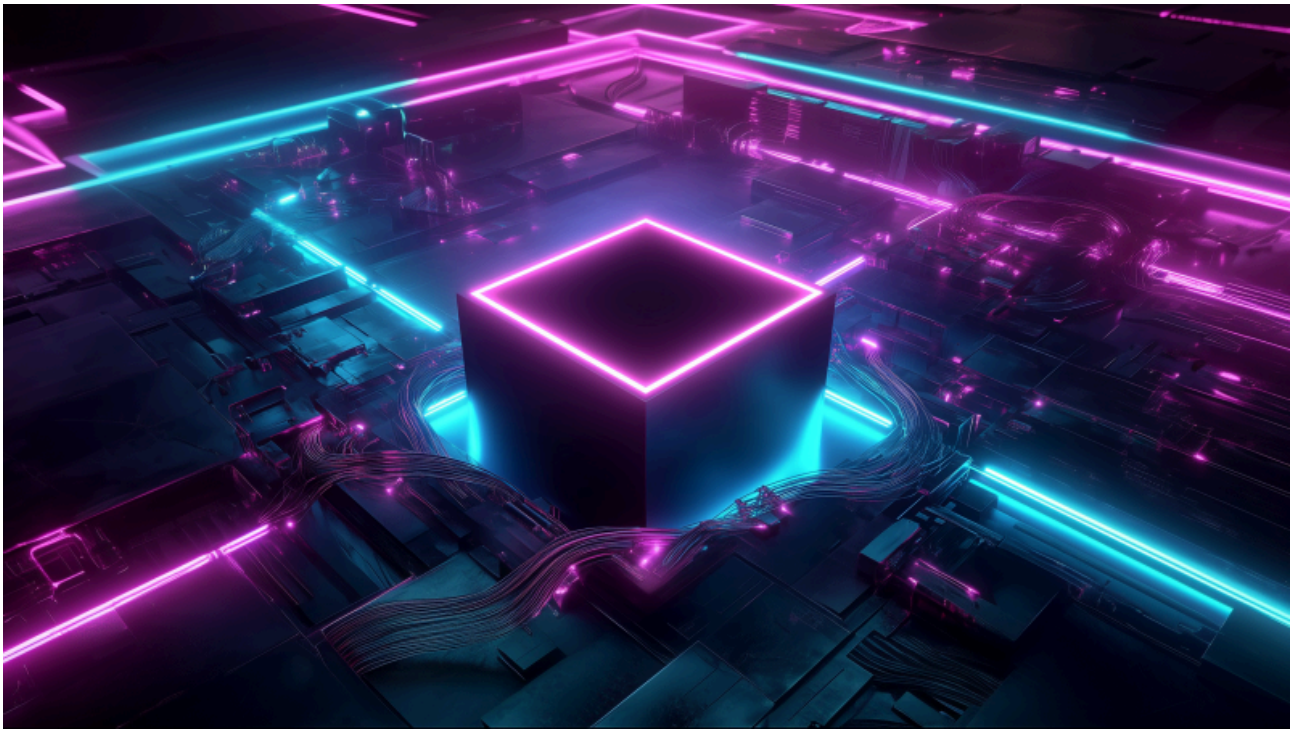
What does it mean? Well, first of all, this is the worst-case news for the victims – even if they pay the ransom they will not get their data back. Secondly, this reinforces the theory that the main goal of the ExPetr attack was not financially motivated, but destructive.

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



Latest Webinars





Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.
