

# ExPetr/Petya/NotPetya is a Wiper, Not Ransomware

By [Anton Ivanov](#), [Orkhan Mamedov](#) on June 28, 2017.  
6:51 pm

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-9UP1eg-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.

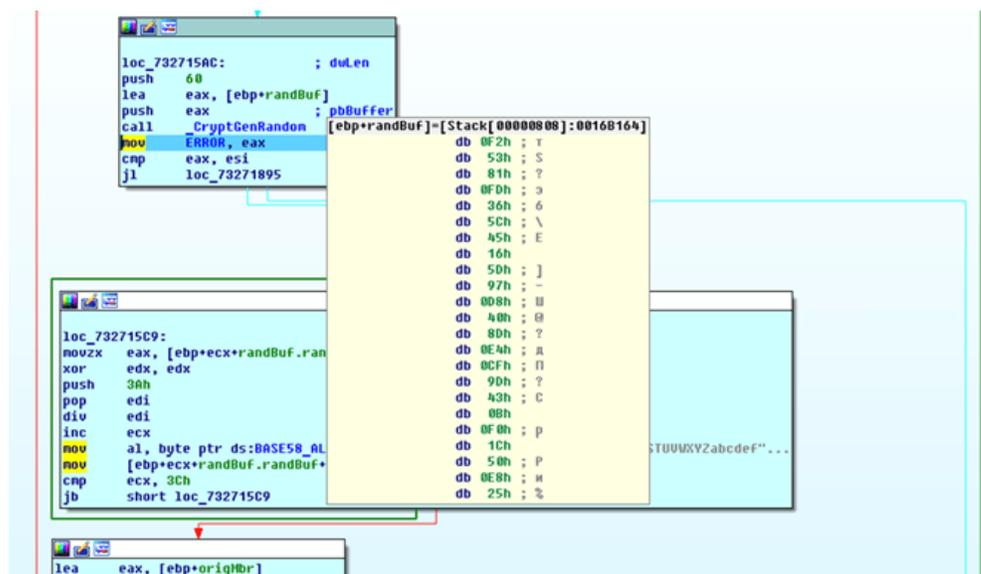
Here's how this installation ID is generated in the ExPetr ransomware:

```

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.



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 AC9UP1egKA3HywND
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 00 00 00 00 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 ExpPetr 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

Ransoms 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](http://blog.comae.io)

5 180 133

## Related Posts



THERE ARE 4 COMMENTS

If you would like to comment on this article you must first [login](#)

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 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

---