



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:

GREAT WEBINARS

13 MAY 2021, 1:00PM

GReAT Ideas. Balalaika Edition

[BORIS LARIN](#), [DENIS LEGEZO](#)

26 FEB 2021, 12:00PM

GReAT Ideas. Green Tea Edition

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:

1Mz7153HMuxXTuR2R1t7BmGSdzaAtNbBLX

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: _

JOHN HULTQUIST, BRIAN BARTHOLOMEW, SUGURU ISHIMARU,
VITALY KAMLUK, SEONGSU PARK, YUSUKE NIWA,
MOTOHIKO SATO

17 JUN 2020, 1:00PM

GReAT Ideas. Powered by SAS: malware attribution and next-gen IoT honeypots

MARCO PREUSS, DENIS LEGEZO, COSTIN RAIU,

KURT BAUMGARTNER, DAN DEMETER, YAROSLAV SHMELEV

26 AUG 2020, 2:00PM

GReAT Ideas. Powered by SAS: threat actors advance on new fronts

IVAN KWIATKOWSKI, MAHER YAMOUT, NOUSHIN SHABAB,

PIERRE DELCHER, FÉLIX AIME, GIAMPAOLO DEDOLA,

SANTIAGO PONTIROLI

22 JUL 2020, 2:00PM

GReAT Ideas. Powered by SAS: threat hunting and new techniques

DMITRY BESTUZHEV, COSTIN RAIU, PIERRE DELCHER,

BRIAN BARTHOLOMEW, BORIS LARIN, ARIEL JUNGHEIT,

FABIO ASSOLINI

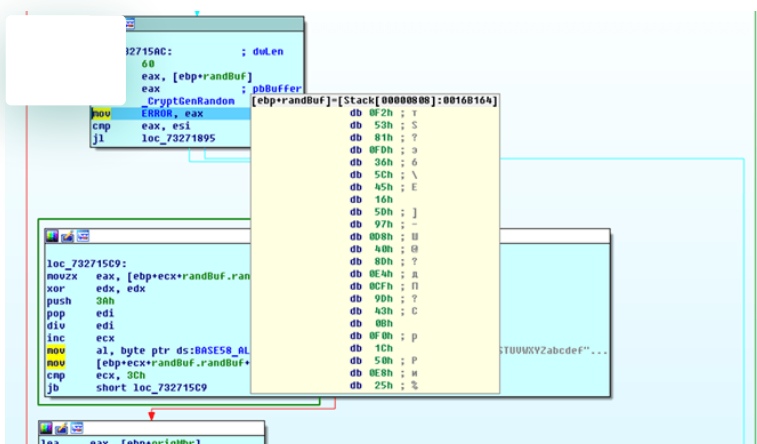
In previous versions of “similar” ransomware like Petya/Mischa/GoldenEye, this installation ID contains crucial information for the key recovery. After sending this information to the attacker they can extract the decryption key using their private key.

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 );
}
```

Search...

Subscribe



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	BSEnwbCPccj7Swa1
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 0A 0F 77 0A 0A 0A 0A	0A 0A 0A 0A 0A 0A 0A 0A	HK.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.



Sodin ransomware exploits Windows vulnerability and processor architecture



KeyPass ransomware



SynAck targeted ransomware uses the Doppelgänger technique



Mining is the new black



Bad Rabbit ransomware

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

5 180 133

Subscribe to our weekly e-mails

The hottest research right in your inbox

Email(Required)

☐ 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.

Subscribe

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

Subscribe

IN THE SAME CATEGORY

XZ backdoor: Hook analysis

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

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](#)

JANI KO

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 prove that the random ID has nothing to do with the encryption key?

[Reply](#)

XZ backdoor story – Initial analysis

A hack in hand is worth two in the bush

QBot banker delivered through business correspondence



// LATEST POSTS

APT REPORTS

APT trends report Q2 2024

GREAT

RESEARCH

Indirect prompt injection in the real world: how people manipulate neural networks

VLADISLAV TUSHKANOV

MALWARE DESCRIPTIONS

LianSpy: new Android spyware targeting Russian users

DMITRY KALININ

CRIMEWARE REPORTS

How “professional” ransomware variants boost cybercrime groups

GREAT

// LATEST WEBINARS

TRAININGS AND
WORKSHOPS

09 JUL 2024, 4:00PM 60 MIN
Building and prioritizing detection engineering backlogs with MITRE ATT&CK

ANDREY TAMOYKIN

CYBERTHREAT TALKS

08 MAY 2024, 5:00PM 60 MIN
Analyzing last year's cyber incident cases

AYMAN SHAABAN

CYBERTHREAT TALKS

19 MAR 2024, 5:00PM 60 MIN
Industrial cybersecurity in 2024: trends and forecasts

EVGENY GONCHAROV

CYBERTHREAT TALKS

24 APR 2024, 5:00PM 60 MIN
MDR report 2023: Analyzing the state of the global threat landscape

SERGEY SOLDATOV

// REPORTS

BlindEagle flying high in Latin America

Kaspersky shares insights into the activity and TTPs of the BlindEagle APT, which targets organizations and individuals in Colombia, Ecuador, Chile, Panama and other Latin American countries.

APT trends report Q2 2024

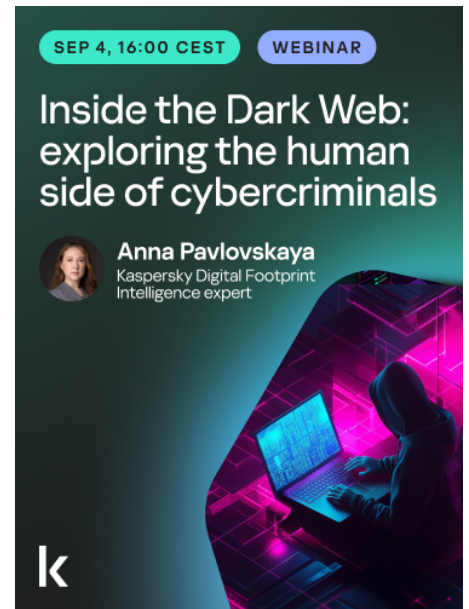
The report features the most significant developments relating to APT groups in Q2 2024, including the new backdoor in Linux utility XZ, a new RAT called SalmonQT, and hacktivist activity.

EastWind campaign: new CloudSorcerer attacks on government organizations in Russia

Kaspersky has identified a new EastWind campaign targeting Russian organizations and using CloudSorcerer as well as APT31 and APT27 tools.

CloudSorcerer – A new APT targeting Russian government entities

Kaspersky discovered a new APT CloudSorcerer targeting Russian government entities and using cloud services as C2, just like the CloudWizard actor.



// SUBSCRIBE TO OUR WEEKLY E- MAILS

The hottest
research right in
your inbox

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

CATEGORIES

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

OTHER SECTIONS

Archive
All tags
Webinars
APT Logbook
Statistics
Encyclopedia
Threats descriptions
KSB 2023

© 2024 AO Kaspersky Lab. All Rights Reserved.

Registered trademarks and service marks are the property of their respective owners.

Privacy Policy
Cookies

License Agreement