TTCSIRT-017.062717: TT-CSIRT Advisory – Petya Ransomware

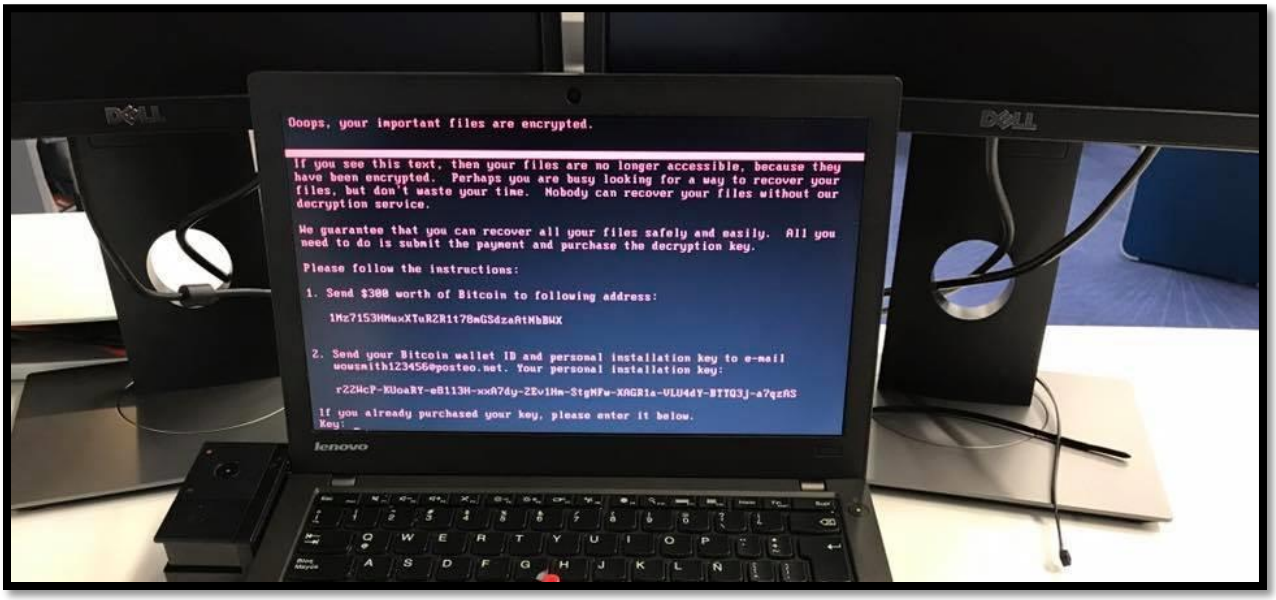
Date first published: 27/6/2017

1.0 Introduction

Discovered:	June 27, 2017
Updated:	June 27, 2017 12:30pm
Type:	Ransomware
Infection Length:	Varies
Systems Affected:	Client Computers, Servers, Websites

This is an alert from TTCSIRT that there are early signs of a new ransomware outbreak currently affecting a large number of countries across the globe such as the United Kingdom, Ukraine, India, Netherlands, Spain, Denmark, and United States along with several others.

The culprit is a new version of Petya, a ransomware that encrypts MFT (Master File Tree) tables for NTFS partitions and overwrites the MBR (Master Boot Record) with a custom bootloader that shows a ransom note and prevents victims from booting their computer.



2.0 Delivery/Exploitation

We have not yet confirmed the initial infection vector for this new Petya variant. Previous variants were spread through e-mail, but we have not identified this latest sample carried in any e-mail related attacks.
Users may be infected through direct exploitation of **CVE-2017-0144** if their host is accessible to the internet on TCP port 445 and has not been updated with the patches included in MS17-010.

Once infected, the virus encrypts each computer to a private key, rendering it unusable until the system is decrypted. The program then instructs the user to pay $300 to a static Bitcoin address, then email the bitcoin wallet and personal ID to a Posteo email address. As of now, block chain records showed eight transactions to the target wallet, totaling roughly $2,300. It's unclear whether any systems have been successfully decrypted after payment.

3.0 Impact

Currently, there are multiple reports from several countries about the ransomware's impact. The most affected country seems to be the Ukraine, where government agencies have reported "cyber-attacks" caused by a mysterious virus that affected the country's largest banks, airports, and utility providers.

Similarly, in Spain, local media is reporting ransomware attacks at a large number of companies that include food conglomerate Mondelez and law firm giant DLA Piper.

In the UK, marketing firm WPP was affected, along with many other. The US didn't escape the Petya outbreak, and the first major victim to surface was pharma giant Merck.

The attack has even affected operations at the Chernobyl nuclear power plant, which has switched to manual radiation monitoring as a result of the attack. Infections have also been reported in more isolated devices like point-of-sale terminals and ATMs.

4.0 Recommendations

The TT-CSIRT recommends the following:

- Update systems to latest version or patch as reported by manufacturer
- For systems without support or patch it is recommended to isolate from the network or turn off as appropriate.
- Discover which systems, within your network, can be susceptible to attack through the vulnerability of Windows, in which case, can be isolated, updated and / or shut down.

Additionally, take the following action

1. Block source E-mail address

wowsmith123456@posteo.net

2. Block domains:

http://mischapuk6hyrn72.onion/

http://petya3jxfp2f7g3i.onion/

http://petya3sen7dyko2n.onion/

http://mischa5xyix2mrhd.onion/MZ2MMJ

http://mischapuk6hyrn72.onion/MZ2MMJ

http://petya3jxfp2f7g3i.onion/MZ2MMJ

http://petya3sen7dyko2n.onion/MZ2MMJ

http://benkow.cc/71b6a493388e7d0b40c83ce903bc6b04.bin

COFFEINOFFICE.XYZ

http://french-cooking.com/

3. Block IPs:

95.141.115.108

185.165.29.78

84.200.16.242

111.90.139.247

4. Block Ports

Block inbound connections on TCP Port 445

5. Apply patches:

Refer (in Russian): https://habrahabr.ru/post/331762/

6. Disable SMBv1

7. Update Anti-Virus hashes

a809a63bc5e31670ff117d838522dec433f74bee

bec678164cedea578a7aff4589018fa41551c27f

d5bf3f100e7dbcc434d7c58ebf64052329a60fc2

aba7aa41057c8a6b184ba5776c20f7e8fc97c657

0ff07caedad54c9b65e5873ac2d81b3126754aac

51eafbb626103765d3aedfd098b94d0e77de1196

078de2dc59ce59f503c63bd61f1ef8353dc7cf5f

7ca37b86f4acc702f108449c391dd2485b5ca18c

2bc182f04b935c7e358ed9c9e6df09ae6af47168

1b83c00143a1bb2bf16b46c01f36d53fb66f82b5

82920a2ad0138a2a8efc744ae5849c6dde6b435d

myguy.xls EE29B9C01318A1E23836B949942DB14D4811246FDAE2F41DF9F0DCD922C63BC6

BCA9D6.exe 17DACEDB6F0379A65160D73C0AE3AA1F03465AE75CB6AE754C7DCB3017AF1FBD

The TT-CSRT has a Mitigation Guide against ransomware, which includes general guidelines and recommendations, and which details the steps of the disinfection process and the main tools of recovery of the files, in this type of attacks.

As stated in the threat report on ransomware, making the payment for the rescue of the equipment does not guarantee that the attackers send the decryption utility and / or password, only rewards their campaign and motivates them to continue massively distributing this type of harmful code

In the event your system has been affected and you did not have backups, it is recommended to keep the files that had been encrypted by the ransomware before disinfecting the machine, since it is may be possible that in the future a tool may appear, which would allow you to decipher the documents which would have been affected.

If you are a victim of such an attack please contact the TT-CSIRT at 6257937 or via email at incidents@ttcsirt.gov.tt or ttcsirt2@twitter.com

For further enquiries, please contact TT-CSIRT through the following channels:
E-mail: contacts@ttcsirt.gov.tt or incidents@ttcsirt.gov.t t
Phone: 1-868 6235439 (monitored during business hours)
Fax: 1868 624 5831
Business Hours: Mon - Fri 0:800 AM - 6:00 PM. TT TIME
Web: www.ttcsirt.gov.tt

Twitter: http://www.twitter.com/ttcsirt2
Facebook: http://facebook.com/ttcsirt