

# SANS ISC: Checking out the new Petya variant - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training SANS ISC InfoSec Forums

 [isc.sans.edu/forums/diary/Checking+out+the+new+Petya+variant/22562/](https://isc.sans.edu/forums/diary/Checking+out+the+new+Petya+variant/22562/)

## Checking out the new Petya variant

This is a follow-up from [our previous diary](#) about today's ransomware attacks using the new Petya variant. So far, we've noted:

- Several hundred more tweets about today's attack can be found on Twitter using [#petya](#).
- The new Petya variant appears to be using the MS17-010 [Eternal Blue](#) exploit to propagate.
- Others claim the new variant [uses WMIC to propagate](#)
- Still no official word on the initial infection vector in today's attacks.
- People everywhere are saying today's activity is similar to last month's WannaCry ransomware attacks.

Brad



433 Posts  
ISC  
Handler  
Jun 27th  
2017

Samples of the new Petya variant are DLL files. So far, we've confirmed the following two SHA256 file hashes are the new variant:

- [027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745](#)
- [64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b1](#)

### ***Examining the new Petya variant***

Petya is a ransomware family that works by modifying the infected Windows system's Master Boot Record (MBR). Using rundll32.exe with #1 as the DLL entry point, I was able to infect hosts in my lab with the above two DLL samples. The reboot didn't occur right away. However, when it did, my infected host did a CHKDSK after rebooting.

```
Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete. It is strongly recommended to let it
complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!

CHKDSK is repairing sector 9920 of 101344 (9%)
```

*Shown above: An infected host immediately after rebooting.*

After CHKDSK finished, the infected Windows host's modified MBR prevented Windows from loading. Instead, the infected host displayed a ransom message.

```
Oops, your important files are encrypted.

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:

[REDACTED]

If you already purchased your key, please enter it below.
Key: _
```

*Shown above: The ransom note from a compromised system.*

Samples of the new Petya variant appear to have WMI command-line (WMIC) functionality. Others have confirmed this variant spreads over Windows SMB and is reportedly using the EternalBlue exploit tool, which exploits CVE-2017-0144 and was originally released by the Shadow Brokers group in April 2017. My infected Windows hosts immediately generated TCP traffic on port 445 and did ARP requests for local network hosts.

Date/Time	Src	port	Dst	port	Info
2017-06-27 16:37:51	10.6.27.101	138	10.6.27.255	138	Get Backup List Request
2017-06-27 16:37:51	10.6.27.101	137	10.6.27.2	137	Name query NB WORKGROUP<lb>
2017-06-27 16:37:51	00:08:02:1c:47		ff:ff:ff:ff:ff:f		Who has 10.6.27.0? Tell 10.6.27.101
2017-06-27 16:37:51	00:08:02:1c:47		ff:ff:ff:ff:ff:f		Who has 10.6.27.254? Tell 10.6.27.101
2017-06-27 16:37:51	20:e5:2a:b6:93		00:08:02:1c:47:a		10.6.27.254 is at 20:e5:2a:b6:93:f1
2017-06-27 16:37:51	10.6.27.101	49159	10.6.27.254	445	49159-microsoft-ds [SYN] Seq=0 Win=8192 Len=0 M
2017-06-27 16:37:51	10.6.27.101	49160	10.6.27.2	445	49160-microsoft-ds [SYN] Seq=0 Win=8192 Len=0 M
2017-06-27 16:37:51	10.6.27.2	445	10.6.27.101	49160	microsoft-ds-49160 [RST, ACK] Seq=1 Ack=1 Win=3
2017-06-27 16:37:52	10.6.27.101	49160	10.6.27.2	445	[TCP Spurious Retransmission] 49160-microsoft-d
2017-06-27 16:37:52	10.6.27.2	445	10.6.27.101	49160	microsoft-ds-49160 [RST, ACK] Seq=1 Ack=1 Win=3
2017-06-27 16:37:52	00:08:02:1c:47		ff:ff:ff:ff:ff:f		Who has 10.6.27.0? Tell 10.6.27.101
2017-06-27 16:37:52	10.6.27.101	49160	10.6.27.2	445	[TCP Spurious Retransmission] 49160-microsoft-d
2017-06-27 16:37:52	10.6.27.2	445	10.6.27.101	49160	microsoft-ds-49160 [RST, ACK] Seq=1 Ack=1 Win=3
2017-06-27 16:37:52	10.6.27.101	49161	10.6.27.2	139	49161-netbios-ssn [SYN] Seq=0 Win=8192 Len=0 MS
2017-06-27 16:37:52	10.6.27.2	139	10.6.27.101	49161	netbios-ssn-49161 [RST, ACK] Seq=1 Ack=1 Win=32
2017-06-27 16:37:52	10.6.27.101	49162	10.6.27.254	445	49162-microsoft-ds [SYN] Seq=0 Win=8192 Len=0 M
2017-06-27 16:37:52	10.6.27.101	49163	10.6.27.2	445	49163-microsoft-ds [SYN] Seq=0 Win=8192 Len=0 M
2017-06-27 16:37:52	10.6.27.2	445	10.6.27.101	49163	microsoft-ds-49163 [RST, ACK] Seq=1 Ack=1 Win=3
2017-06-27 16:37:52	10.6.27.101	49164	10.6.27.254	139	49164-netbios-ssn [SYN] Seq=0 Win=8192 Len=0 MS
2017-06-27 16:37:53	10.6.27.101	137	10.6.27.2	137	Name query NB WORKGROUP<lb>
2017-06-27 16:37:53	10.6.27.101	49161	10.6.27.2	139	[TCP Spurious Retransmission] 49161-netbios-ssn
2017-06-27 16:37:53	10.6.27.2	139	10.6.27.101	49161	netbios-ssn-49161 [RST, ACK] Seq=1 Ack=1 Win=32
2017-06-27 16:39:00	00:08:02:1c:47		ff:ff:ff:ff:ff:f		Who has 10.6.27.17? Tell 10.6.27.101
2017-06-27 16:39:00	00:08:02:1c:47		ff:ff:ff:ff:ff:f		Who has 10.6.27.17? Tell 10.6.27.101
2017-06-27 16:39:01	00:08:02:1c:47		ff:ff:ff:ff:ff:f		Who has 10.6.27.17? Tell 10.6.27.101
2017-06-27 16:39:04	00:08:02:1c:47		ff:ff:ff:ff:ff:f		Who has 10.6.27.18? Tell 10.6.27.101
2017-06-27 16:39:04	00:08:02:1c:47		ff:ff:ff:ff:ff:f		Who has 10.6.27.18? Tell 10.6.27.101
2017-06-27 16:39:05	00:08:02:1c:47		ff:ff:ff:ff:ff:f		Who has 10.6.27.18? Tell 10.6.27.101
2017-06-27 16:39:08	00:08:02:1c:47		ff:ff:ff:ff:ff:f		Who has 10.6.27.19? Tell 10.6.27.101
2017-06-27 16:39:08	00:08:02:1c:47		ff:ff:ff:ff:ff:f		Who has 10.6.27.19? Tell 10.6.27.101
2017-06-27 16:39:09	00:08:02:1c:47		ff:ff:ff:ff:ff:f		Who has 10.6.27.19? Tell 10.6.27.101
2017-06-27 16:39:12	00:08:02:1c:47		ff:ff:ff:ff:ff:f		Who has 10.6.27.20? Tell 10.6.27.101
2017-06-27 16:39:12	00:08:02:1c:47		ff:ff:ff:ff:ff:f		Who has 10.6.27.20? Tell 10.6.27.101
2017-06-27 16:39:13	00:08:02:1c:47		ff:ff:ff:ff:ff:f		Who has 10.6.27.20? Tell 10.6.27.101
2017-06-27 16:39:16	00:08:02:1c:47		ff:ff:ff:ff:ff:f		Who has 10.6.27.21? Tell 10.6.27.101
2017-06-27 16:39:16	00:08:02:1c:47		ff:ff:ff:ff:ff:f		Who has 10.6.27.21? Tell 10.6.27.101
2017-06-27 16:39:17	00:08:02:1c:47		ff:ff:ff:ff:ff:f		Who has 10.6.27.21? Tell 10.6.27.101
2017-06-27 16:39:20	00:08:02:1c:47		ff:ff:ff:ff:ff:f		Who has 10.6.27.22? Tell 10.6.27.101
2017-06-27 16:39:20	00:08:02:1c:47		ff:ff:ff:ff:ff:f		Who has 10.6.27.22? Tell 10.6.27.101

Shown above: Some of the traffic noted in my lab environment.

Keep in mind this is a new variant of Petya ransomware. I'm still seeing samples of the regular Petya ransomware submitted to places like VirusTotal and other locations. From what we can tell, those previous versions of Petya are not related to today's attacks.

You became victim of the PETYA RANSOMWARE!

The harrddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:


1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:


http://petya37h5tbhyvki.onion/a3KTMU  
http://petya5koahstf7sv.onion/a3KTMU

3. Enter your personal decryption code there:

If you already purchased your key, please enter it below.

Key: \_

Regular Petya ransomware 

 New Petya variant noted in today's attacks

Ooops, your important files are encrypted.

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:

If you already purchased your key, please enter it below.

Key: \_

*Shown above: Difference in ransomware notes between the old and new Petya variants.*

### **New Petya variant ransom message**

Ooops, your important files are encrypted.

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 the following address:

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail [wowsmith123456@posteo.net](mailto:wowsmith123456@posteo.net). Your personal installation key:


012345-6789ab-cdefgh-ijklmn-opqrst-uvwxyz-ABCDEF-GHIJKL-MNOPQR-STUVWX

If you already purchased your key, please enter it below.  
Key:

### ***More reports about the new Petya variant***

- Bleeping Computer: [WannaCry Déjà Vu: Petya Ransomware Outbreak Wreaking Havoc Across the Globe](#)
- The Hacker News: [Petya Ransomware Spreading Rapidly Worldwide, Just Like WannaCry](#)
- Reuters: [Petya ransomware virus is back amid cyber attack: Swiss agency](#)
- Palo Alto Networks Blog: [Threat Brief: Petya ransomware](#)

---

Thread locked <a href="#">Subscribe</a>	Jun 27th 2017 4 years ago
Lots of good IOCs and updated info on Github: <a href="https://gist.github.com/vulnersCom/65fe44d27d29d7a5de4c176baba45759">https://gist.github.com/vulnersCom/65fe44d27d29d7a5de4c176baba45759</a>	Anonymous
<a href="#">Quote</a>	Jun 27th 2017 4 years ago
There are reports that the CHKDSK screen is fake, put up to mask the encryption of files.	Jim  4 Posts
<a href="#">Quote</a>	Jun 27th 2017 4 years ago
Details from Check Point on possible initial attack vector. <a href="http://blog.checkpoint.com/2017/06/27/global-ransomware-attack-spreading-fast/">http://blog.checkpoint.com/2017/06/27/global-ransomware-attack-spreading-fast/</a>	Anonymous

---

---

<u>Quote</u>	Jun 27th 2017 4 years ago
Vaccine, not Killswitch, Found for Petya (NotPetya) Ransomware Outbreak <a href="https://www.bleepingcomputer.com/news/security/vaccine-not-killswitch-found-for-petya-notpetya-ransomware-outbreak/">https://www.bleepingcomputer.com/news/security/vaccine-not-killswitch-found-for-petya-notpetya-ransomware-outbreak/</a>	Brett  19 Posts
<u>Quote</u>	Jun 28th 2017 4 years ago
NAKED SECURITY - Deconstructing Petya: how it spreads and how to fight back <a href="https://nakedsecurity.sophos.com/2017/06/28/deconstructing-petya-how-it-spreads-and-how-to-fight-back/">https://nakedsecurity.sophos.com/2017/06/28/deconstructing-petya-how-it-spreads-and-how-to-fight-back/</a>	Brett  19 Posts
<u>Quote</u>	Jun 28th 2017 4 years ago
Good write up by MSFT --> <a href="https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/">https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/</a>	Anonymous
<u>Quote</u>	Jun 28th 2017 4 years ago

---