Threat Briefing

Global Ransomware Campaign

Briefing Date	28 June 2017
Priority	High

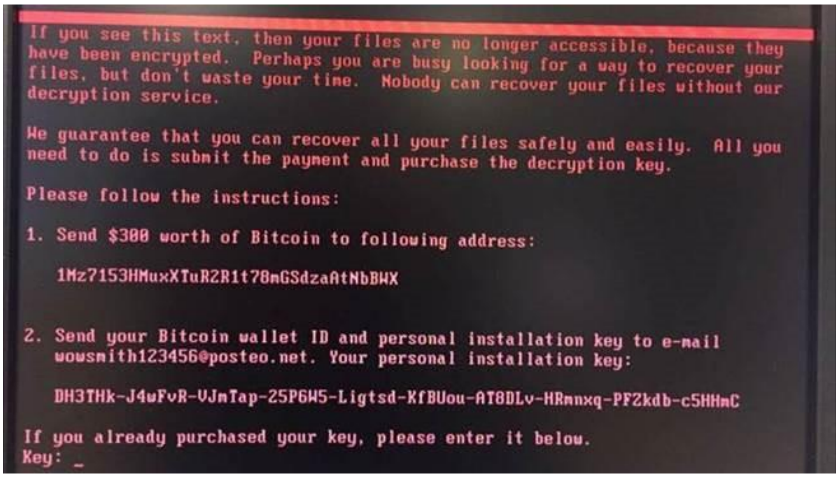
Key Points

- Reports have emerged of an international ransomware campaign which has affected hundreds of organisations
- Organisations affected by the campaign have been infected with ransomware some have described as a variant of Petya, which is demanding that users send a payment of USD 300 in Bitcoin per infected machine
- The ransomware is most likely to be spreading between and within organisations using the Eternal Blue exploit, which was instrumental in enabling the recent WannaCry campaign to reach so many victims
- Unlike with the WannaCry campaign, no associated kill-switch domain has been identified which could lead to a rapid halt in infections
- Organisations are strongly encouraged to make sure that, where possible, systems are patched against the Eternal Blue exploit using MS17-010

Introduction

On 27 June, reports emerged in Ukraine detailing a widespread ‘cyber attack’ affecting organisations from a wide selection of industries. News of this cyber-attack spread incredibly quickly, as organisations in a large number of other countries were affected. As further details have emerged, it has become apparent that this cyber attack relates to a widespread ransomware campaign, which has been using similar methods to the WannaCry campaign to distribute itself to different networks. This suggests that there are still many organisations which have not effectively patched their systems against the Eternal Blue vulnerability.

Rating	4	Version	1.0
Source Reliability	2	Last update	27/06/2017
Information Reliability	2	Next update	N/A



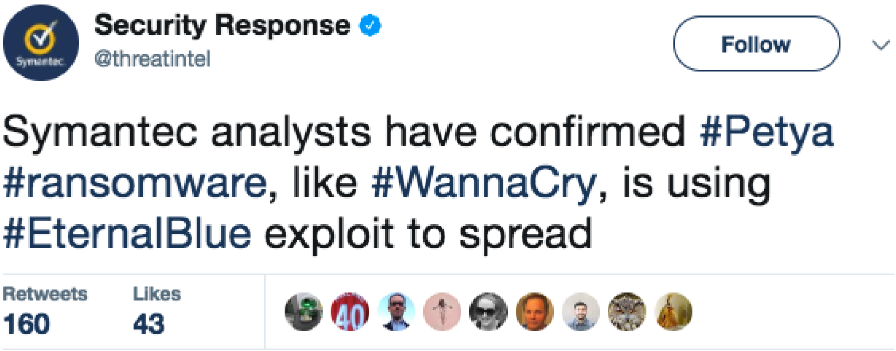
```
If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

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:

   DH3THk-J4wFvR-VJmTap-25P6W5-Ligtsd-KfBUou-AT8DLv-HRmnxq-PF2kdb-c5HHmC

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

Figure 1: Image displayed on machines infected by ransomware associated with this campaign.

Distribution

Open sources currently indicate that the initial infection may have come through a phishing campaign focusing on targets in Ukraine, but that the exploitation of the Eternal Blue vulnerability has allowed it to spread rapidly to different countries and networks. **Currently, there are no samples of any phishing emails, suggesting that the spread of the ransomware was achieved solely through the use of Eternal Blue** vulnerability, much in the same way that the WannaCry ransomware spread. Infected machines are reportedly allowed to remain up for an hour, in order to distribute the malware further, prior to being rebooted and displaying the ransom message.[1]

In addition to the use of the Eternal Blue vulnerability, the ransomware has also been reported as attempting to make use of active directory credentials for latera movement within infected organisations using WMIC and PsExec.[2] **This could potentially allow the ransomware to spread to machines which were not vulnerable to the Eternal Blue vulnerability.**



Security Response
@threatintel

Symantec analysts have confirmed #Petya #ransomware, like #WannaCry, is using #EternalBlue exploit to spread

Retweets 160
Likes 43

Figure 2: Tweet from security researcher identifying code linked to use of Eternal Blue

Payload

The payload has widely reported to be a variant of the Petya ransomware, which encrypts MFT (Master File Tree) tables for NTFS partitions and overwrites the MBR (Master Boot Record) with a custom bootloader displaying a ransom note and preventing the target computer from booting. Analysts at Kasperksy have indicated that this may actually be a completely new ransomware; however, analysis of these claims is ongoing. Analysis of payloads which

[1] twitter.com/rikvduijn/status/879735252339630081
[2] twitter.com/0x09AL/status/879702450038599681

are linked to further infection using the Eternal Blue exploit have indicated that the attackers performed basic obfuscation of the function (using XOR) and that they rewrote the exploit in a 'cleaner' manner.[3]

The ransom demand has so far only been linked to a single email address (Wowsmith123456[@]posteo.net) and Bitcoin address (1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX). Payments to that address, as of BST 17:40, stood at 1.752 Btc (approximately GBP 3,150).[4]

Investigation thus far indicates that the ransomware is not linked to a killswitch domain, meaning that more elaborate actions will be required in order to minimise the spread of the ransomware.

Recommendations

Where possible, organisations should ensure that they have patched their systems to mitigate against the Eternal Blue exploit. This patch, MS17-010, was published in March 2017 and should effectively halt any attacks within this campaign.[5] Those organisations that are unable to install this patch should ensure that they block all incoming traffic on port 445. It appears highly likely that the ransomware has been designed to spread across file shares as well; organisations which have suffered from infections should ensure that infected devices are removed from the internal network as soon as possible.

While a phishing component has not been confirmed in association with this campaign, it is strongly advised that individuals heed the following advice:

- Avoid opening emails that are sent from unknown entities
- Do not open attachments that can be potentially dangerous such as: .exe, .js, .vbs, .bat, .php, .pif, .scr and .dat
- Keep systems updated to defend against known exploits
- Educate users about the dangers of opening attachments or click in links from none trusted sources and take basic actions in order to prevent an infection

Key Victims

Hundreds of organisations have already been hit by the ransomware attack across a wide number of countries. Some of the larger companies infected include:

- Ukraine's central bank, the National Bank of Ukraine
- Ukrainian bank Oschadbank
- Ukrainian telecoms company Ukrtelecom
- Ukrainian delivery service company Nova Poshta
- Russian state oil giant Rosneft
- Kyivenergo, Kiev power company
- Radiation monitoring system at Chernobyl
- Website of Kiev's Boryspil international airport
- Danish sea transport company Maersk's APM Terminals subsidiary

[3] blog.comae.io/byata-enhanced-wannacry-a3ddd6c8dabb
[4] blockchain.info/address/1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
[5] technet.microsoft.com/en-us/library/security/ms17-010.aspx

- British advertising firm WPP
- French industrial group Saint-Gobain
- US pharmaceuticas firm Merck
- Mondelez
- DLA Piper

Infections have been detected in countries including:

- Brazil
- Ukraine
- Russia
- Spain
- Belarus
- Germany
- Italy
- France
- Poland
- India
- Netherlands

It appears highly likely that firms targeted in this campaign have not installed patches which mitigated the Eternal Blue vulnerability. The above represents only a very small number of the overall affected companies.

Further Information

If you are concerned about the threat posed by ransomware campaigns, please contact the Cyber Intelligence Centre (CIC) for further information. The CIC is part of Deloitte's experienced Cyber Risk practice, which can provide information remotely or, if required, can provide an on-site advisory team to assist you in identifying and remediating security vulnerabilities in your IT infrastructure.

This is an ongoing incident, the CIC will provide further information as an when it becomes available.

Rating	4	Version	1.0
Source Reliability	2	Last update	27/06/2017
Information Reliability	2	Next update	N/A

Indicators

File Hashes

sha256: 027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745

sha1: 34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d

md5: 71b6a493388e7d0b40c83ce903bc6b04

ff64f6a948495bb4954422aa190cc5de18acbf5e

36086eb7e20f6e11e62104360b6d6f03370c9cbc

da2f74aa5e2f8bded2a88a4d2bb267676820ba62

IP Address

185.165.29.78

Associated hashes

a809a63bc5e31670ff117d838522dec433f74bee

bec678164cedea578a7aff4589018fa41551c27f

d5bf3f100e7dbcc434d7c58ebf64052329a60fc2

aba7aa41057c8a6b184ba5776c20f7e8fc97c657

0ff07caedad54c9b65e5873ac2d81b3126754aac

51eafbb626103765d3aedfd098b94d0e77de1196

078de2dc59ce59f503c63bd61f1ef8353dc7cf5f

IP Address

84.200.16.242

Associated hashes

7ca37b86f4acc702f108449c391dd2485b5ca18c

2bc182f04b935c7e358ed9c9e6df09ae6af47168

1b83c00143a1bb2bf16b46c01f36d53fb66f82b5

82920a2ad0138a2a8efc744ae5849c6dde6b435d

Other IP Addresses

95.141.115.108

Rating	4	Version	1.0
Source Reliability	2	Last update	27/06/2017
Information Reliability	2	Next update	N/A

111.90.139.247

URLs

French-cooking[.]com

Filenames

myguy.xls

myguy.exe

Payment C&C Servers

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

Targeted File Extensions

.3ds.7z.accdb.ai.asp.aspx.avhd.back.bak.c.cfg.conf.cpp.cs.ctl.dbf.disk.djvu.doc.docx.dwg.eml.fdb.gz.h.hdd.kdbx.mail.mdb.msg.nrg.ora.ost.ova.ovf.pdf.php.pmf.ppt.pptx.pst.pvi.py.pyc.rar.rtf.sln.sql.tar.vbox.vbs.vcb.vdi.vfd.vmc.vmdk.vmsd.vmx.vsdx.vsv.work.xls.xlsx.xvd.zip.

YARA Rules:

```
rule sig_34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d {

   meta:

        hash1 = "027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745"

   strings:

        $s3 = "%s /node:\"%ws\" /user:\"%ws\" /password:\"%ws\" " fullword wide

        $s4 = "One of your disks contains errors and needs to be repaired. This process" fullword ascii

        $s5 = "wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Application & fsutil usn deletejournal /D %c:" fullword wide

        $s6 = "shutdown.exe /r /f" fullword wide

        $s7 = "WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD" fullword ascii

        $s8 = "wowsmith123456@posteo.net. Your personal installation key:" fullword ascii
        $s9 = "schtasks %ws/Create /SC once /TN \"\" /TR \"%ws\" /ST %02d:%02d" fullword wide

        $s10 = "\\\\.\\pipe\\%ws" fullword wide

        $s11 = "u%s \\\\%s -accepteula -s " fullword wide

        $s13 = "they have been encrypted. Perhaps you are busy looking for a way to recover" fullword wide

        $s14 = "All you need to do is submit the payment and purchase the decryption key." fullword wide

        $s15 = "have been encrypted.    Perhaps you are busy looking for a way to recover your" fullword ascii

        $s17 = "Ooops, your important files are encrypted." fullword wide

        $s18 = "need to do is submit the payment and purchase the decryption key." fullword ascii

        $s19 = "If you already purchased your key, please enter it below." fullword ascii

        $s20 = "wbem\\wmic.exe" fullword wide


    condition:

        ( uint16(0) == 0x5a4d and filesize < 1000KB and ( 5 of ($s*)) ) or ( all of them )

}
```

Samples and Ongoing Analysis

https://gist.github.com/vulnersCom/65fe44d27d29d7a5de4c176baba45759

https://www.reverse.it/sample/fe2e5d0543b4c8769e401ec216d78a5a3547dfd426fd47e097df04a5f7d6d206?environmentId=100

https://www.hybrid-analysis.com/sample/027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745?environmentId=100

https://otx.alienvault.com/pulse/5952674095270e2d0f055eaf/

Document Reliability

Source Reliability						
1	7	6	5	4	3	2
2	8	7	6	5	4	3
3	9	8	7	6	5	4
4	10	9	8	7	6	5
5	11	10	9	8	7	6
6	12	11	10	9	8	7
	6	**5**	**4**	**3**	**2**	**1**
	Information Reliability					

Source Reliability

Rating	Rating description	Description
1	Reliable	No doubt about the source's authenticity, trustworthiness, or competency. History of complete reliability.
2	Usually reliable	Minor doubts. History of mostly valid information.
3	Fairly reliable	Doubts. Provided valid information in the past.
4	Not usually reliable	Significant doubts. Provided valid information in the past.
5	Unreliable	Lacks authenticity, trustworthiness and competency. History of invalid information.
6	Cannot be judged	Insufficient information to evaluate reliability. May or may not be reliable.

Information Reliability

Rating	Rating description	Description
1	Confirmed	Logical, consistent with other relevant information, confirmed by independent sources.
2	Probably true	Logical, consistent with other relevant information, not confirmed.
3	Possibly true	Reasonably logical, agrees with some relevant information, not confirmed.
4	Doubtfully true	Not logical but possible, no other information on the subject, not confirmed.
5	Improbable	Not logical, contradicted by other relevant information.
6	Cannot be judged	The validity of the information cannot be determined.

Rating	4	Version	1.0
Source Reliability	2	Last update	27/06/2017
Information Reliability	2	Next update	N/A

Deloitte.

Statement of Responsibility

We take responsibility for this report which is prepared on the basis of the limitations set out below. The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that may exist or all improvements that might be made. Any recommendations made for improvements should be assessed by you for their full impact before they are implemented.

Deloitte LLP

London

27/06/2017

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.co.uk/about for a detailed description of the legal structure of DTTL and its member firms.

Deloitte LLP is the United Kingdom member firm of DTTL.

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication. Deloitte LLP would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. Deloitte LLP accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Registered office: Hill House, 1 Little New Street, London EC4A 3TR, United Kingdom. Registered in England No 3311052

Rating	4	Version	1.0
Source Reliability	2	Last update	27/06/2017
Information Reliability	2	Next update	N/A