Booz Allen | CYBER4SIGHT

THE PETYA RANSOMWARE OUTBREAK

Any conclusion or recommendation by Booz Allen as contained in this report should not be viewed as any guarantee or opinion of any future events or future outcomes. Booz Allen undertakes no obligation to update any conclusions or recommendations to reflect anticipated or unanticipated events or circumstances in this report. Booz Allen does not guarantee that this report has identified all cyber threats, or that a security incident or security breach will not occur. Booz Allen takes no responsibility and is not liable for reliance by anyone on the information contained in this report, and any reliance is at the sole risk and discretion of the recipient of this report.

Executive Summary: A ransomware outbreak has infected thousands or tens of thousands of computers around the world with a threat known as Petya (aka Petrwrap, NotPetya, exPetr, Goldeneye, Nyetya). Much is known about the post-infection behaviors of the threat, but a lack of clarity remains regarding the initial infection vector. Ironically, emerging information suggests that the threat may not be ransomware at all but rather a destructive wiper malware.

SUMMARY

A new outbreak of malware—which sources identify as a variant of "Petya"—is affecting a growing list of organizations across the world.[1] Petya is designed to infect victims' computers, spread to other computers on the same network, and encrypt data on the computers, rendering them useless. A "ransom note" presented to victims demands a payment of USD 300 (to be paid in Bitcoin) to decrypt the data. The latest reporting suggests that the ransomware aspects of Petya are a ruse: the malware may simply wipe and destroy data versus reversibly encrypting it for profit.[2]

Once Petya infects a computer, it spreads by using local administrator credentials, abusing the legitimate Windows administrative utilities WMI and PSEXEC, or by using ETERNALBLUE and/or ETERNALROMANCE—government-caliber hacking tools leaked by the infamous ShadowBrokers group—to exploit the server message block (SMB). Microsoft initially patched the underlying ETERNALBLUE/ETERNALROMANCE vulnerabilities in March 2017.[3]

The outbreak may have started in Ukraine, the result of a malicious software update for M.E.Doc, an otherwise legitimate tax and accounting application used almost exclusively in and around Ukraine. It is possible that organizations that conduct business with Ukrainian organizations may also use the software to prepare tax and other financial information for their Ukraine business operations.

So far, the malicious software update for M.E.Doc is the only confirmed delivery vector for Petya. For its part, the makers of M.E.Doc are denying that their software played any role in the infections. However, both Microsoft and the Ukrainian Cyber Police, among others, have reported this as the initial infection vector.[4] Microsoft states that its telemetry data documented the M.E.Doc software

updater process "EzVit.exe" executing malicious command line instructions that installed the Petya variant.

However, unsubstantiated reports state that Petya is arriving via phishing messages and malicious email attachments. Early reports supported this possibility, stating that certain machines became infected through malicious emails containing documents with exploits for CVE-2017-0199, although certain research outlets are refuting this.[5] We've also seen credible sources stating that the certain individuals became infected after visiting the website of the Ukrainian city of Bahmut (bahmut[.]com[.]ua/news), which was reportedly compromised as part of a watering-hole attack.[6] The extensiveness of the infections supports the notion that M.E.Doc , an obscure tax software, might not have been the only infection vector.

The velocity and scope of the current outbreak mirror that of the WannaCry ransomware outbreak, which occurred in mid-May and also leveraged ETERNALBLUE to self-propagate across the Internet. Unlike WannaCry however, Petya does not appear to use ETERNALBLUE to initially infect victims, although some early reports suggested otherwise. Analysis to date indicates that Petya only uses ETERNALBLUE to spread itself once on a victim's network. Barring information that corroborates the rumors of a phishing vector, the malicious M.E.Doc software update may be the only means by which Petya initially ensnares victims.

REPORTED VICTIMS

Victims of the ransomware outbreak have included multiple entities in the following sectors: finance, retail, media and telecommunications, transportation infrastructure, and healthcare. Other known victims include a law firm, delivery companies, a construction company, and various Ukrainian government organizations.

TECHNICAL DETAILS

An analysis performed by a cross section of Booz Allen teams has provided the below technical information with **moderate levels of confidence**. We are still conducting independent analysis of the malware. We are continuing to process, cross-reference, and independently confirm or deny new information as it emerges.

Confirmed and possible initial infection vectors include:

- [Confirmed] According Microsoft, private sources, and other security firms, a compromised version of "M.E.Doc " delivered the ransomware. M.E.Doc is tax and accounting software used by the Ukrainian government. The process EzVit.exe (the legitimate M.E.Doc process) periodically updates itself by beaconing to udp.me-doc.com.ua with the User Agent M.E.Doc 1001189. According to multiple sources, an update to M.E.Doc pushed out on the morning of 27 June contained the Petya malware. The malicious version of the software launches a command that runs rundll32.exe and UniCryptC.exe, both of which are responsible for initiating the Petya infection. rundell32.exe installs perfc.dat. Petya uses perfc.dat to obtain administrator privileges; UniCryptC.exe installs the Petya binary.
- [Unconfirmed] We have unsubstantiated reports from multiple organizations that they were infected with Petya via a malicious email attachment.
- [Unconfirmed] A credible source claims that some infections occurred due to a watering-hole attack that targeted the website of the city of Bahmut (bahmut[.]com[.]ua/news), which is in

the separatist-controlled area of Donetsk, in eastern Ukraine. There is some question now about whether this watering hole delivered the same or a different strain of Petya.

Once on the network, the ransomware:

- Drops a credential-harvesting tool in %TEMP% that our independent analysis identifies as Mimikatz. Petya uses Mimikatz to collect Windows credentials from the local system and uses those passwords to authenticate to other machines on the network.
- Uses the WindowsCredEnumerateW function to enumerate the credentials from the user's credential set associated with the logon session of the current token.
- Uses the Windows DhcpEnumSubnets function to return an enumerated list of subnets defined on the DHCP server. It takes several parameters that allow for the retrieval of all subnets the DHCP server is aware of. This technique allows Petya to list all clients available on the network.
- Checks for open ports 445 and 139.
- Drops and runs PSEXEC to distribute the Petya DLL using harvested credentials.
- Uses WMIC to list remote shares and to pass stolen credentials, and further propagates the Petya DLL to other systems.
- Clears application/event logs using wevtutil.exe.
- Uses ETERNALBLUE to exploit SMB and further spread. ETERNALBLUE (CVE-2017-0144) allows an attacker to send specially crafted shellcode that installs a kernel-level backdoor called DOUBLEPULSAR. Using shellcode DOUBLEPULSAR generates, the attacker can inject a malicious DLL of their choice, in this case, Petya.
- Reboots the system by setting a scheduled task. After reboot, the ransomware encrypts the system's MFT and NTFS partitions and overwrites the MBR with a customized loader.

The SMB exploit appears to be a slightly modified version of EternalBlue. For the sample 027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745, the SMB exploit starts at the offset 0x10005A7E. The shellcode is encoded with a single byte XOR using the key 0xcc. The encoding may allow the ransomware to effectively avoid antivirus scanners.

The Petya variant performs several system process checks before proceeding with file encryption and lateral movement. The ransomware searches for XOR-based hashes of process names, which, if found, either lead the ransomware to not infect the system’s MBR (if a hashed process name of 0x2E214B44 is found), or not attempt exploits of ETERNALBLUE and/or ETERNALROMANCE (if hashed process names of 0x6403527E or 0x651B3005 are found).

The ransomware uses Windows file mapping APIs to identify and encrypt more than 60 different filetypes. Encryption is performed with a unique AES encryption key that is encrypted with an 800-bit RSA public key, and then added to a README.TXT file that displays the ransomware’s ransom note.

CONFIRMED PETYA RANSOMWARE SAMPLE A

- **Filename** petwrap.exe
- **TimeStamp** 2017:06:18 07:14:36+00:00
- **Size** 354KiB (362360 bytes)
- **Type** pedll
- **Description** PE32 executable (DLL) (console) Intel 80386, for MS Windows
- **Architecture** 32 Bit
- **SHA256** 027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745

The malware is signed with the following fake certificate.

```
CN=Microsoft Code Signing PCA, O=Microsoft Corporation, L=Redmond, ST=Washington,
C=US

Serial: 6101cf3e00000000000f



E3:FE:DB:37:F4:87:4E:84:CD:B8:2A:78:9F:FD:CD:67

96:17:09:4A:1C:FB:59:AE:7C:1F:7D:FD:B6:73:9E:4E:7C:40:50:8F
```

EXECUTION SUMMARY

```
 rundll32.exe C:\027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745.
bin.dll",#1" (PID: 2880)

 \_ cmd.exe " /TR "%WINDIR%\system32\shutdown.exe /r /f" /ST 07:45" (PID: 2724)


\_ schtasks.exe " /TR "%WINDIR%\system32\shutdown.exe /r /f" /ST 07:45" (PID: 2720
)

 \_ cmd.exe /c wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wev
tutil cl Application & fsutil usn deletejournal /D C: (PID: 2072)

  \_ wevtutil.exe wevtutil cl Setup (PID: 2204)

  \_ wevtutil.exe wevtutil cl System (PID: 2128)

  \_ wevtutil.exe wevtutil cl Security (PID: 4016)

  \_ wevtutil.exe wevtutil cl Application (PID: 3988)

  \_ fsutil.exe fsutil usn deletejournal /D C: (PID: 1368)

 \_ shutdown.exe %WINDIR%\system32\shutdown.exe" /r /f" (PID: 2796)
```

EXECUTION DETAILS

The trojanized M.E.Doc process EzVit.exe executes rundll32.exe using the following command-line:

```
C:\\Windows\\system32\\rundll32.exe\" \"C:\\ProgramData\\perfc.dat\",#1
```

The malware creates a scheduled task via the command line. The timeframe under which the reboot occurs is randomly set using GetTickCount(). Using this technique, the reboot will occur within 10 to 60 minutes.

```
/TR "%WINDIR%\system32\shutdown.exe /r /f" /ST 07:45
```

The malware also uses Wevtutil to clear logs from various system directories.

```
\cmd.exe wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil
cl Application & fsutil usn deletejournal /D %c:
```

Petya will use WMIC to scan admin$ shares and pass stolen credentials to propagate itself (perfc.dat) to remote systems.

```
-d C:\Windows\System32\rundll32.exe "C:\Windows\%s",#1

wbem\wmic.exe

%s /node:"%ws" /user:"%ws" /password:"%ws"

process call create "C:\Windows\System32\rundll32.exe \"C:\Windows\%s\" #1

\\%s\admin$

\\%ws\admin$\%ws

c:\Windows\
```

MALWARE "KILL SWITCH"

Open sources and our independent analysis confirms that the malware will exit its encryption routine if it determines that a specific local file already exists on the disk.

Users can create a read-only version of the file perfc.dat in the C:\Windows directory that prevents the malware from executing. This method does not prevent the infected machine from further propagating the malware—it only prevents local encryption. This method will not disable the malware across a network. It is not clear if this technique works by adding a different file extension, something other than .dat, to the perfc file.

We do not consider this method to be a comprehensive solution for eliminating exposure to the malware. In fact, this protective measure doesn't seem any more effective than those listed below.

RANSOM PAYMENT

Attackers are using the Bitcoin wallet 1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX for ransomware payments. As of this writing, the address has received 45 payments totaling BTC 3.99. Some of the payments may be from security researchers. Victims were told to send their Bitcoin wallet ID and "personal installation key" to a dedicated email address; the German operator of the email address blocked access to it, and neither victims nor the attacker can process ransom payments.

DETECTION & COUNTERMEASURES OPTIONS

- **[Updated]** Identify running instances of the M.E.Doc process `EzVit.exe`; Identify beacons from `EzVit.exe` to `udp.me-doc.com.ua` with the User Agent `medoc1001189`.
- **[Updated]** Immediately shut down or otherwise "unplug" machines that display the Petya ransom note.
- **[Updated]** Block inbound SMB connections to local machines on TCP port 445 and 139 (NetBIOS, SMB). The effect this might have on normal business operations will vary widely from network to network.
- **[Updated]** Inspect command-line events and process executions that spawn `schtasks.exe` and `wevtutil.exe`. Search for the command lines `schtasks /Create /SC once /TN "" /TR "<system folder>\shutdown.exe /r /f" /ST <time>` and `cmd.exe /c schtasks /RU "SYSTEM" /Create /SC once /TN "" /TR "C:\Windows\system32\shutdown.exe /r /f" /ST <time>`.
- **[Updated]** Audit Windows Event logs with ID 106 to identify lateral movement using WMI, `process call create \"C:\\Windows\\System32\\rundll32.exe \\\"C:\\Windows\\perfc.dat\\\" #1`.
- **[Updated]** Possibly disable PSEXEC and WMI. The effect this might have on normal business operations will vary widely from network to network.
- Identify binaries signed with a fake Microsoft certificate bearing the serial number `6101cf3e00000000000f`.
- Apply SNORT ETERNALBLUE rules (see, **SNORT** section below).
- Monitor for traffic to/from suspected malicious domains and IP addresses (see, **Indicators of Compromise** section below).

MOTIVATIONAL ASSESSMENTS

Profit may be the clearest motivator here. However, while the attack bears all of the markings of a criminal ransomware campaign, there are certain elements of it that suggest otherwise, if only circumstantially. That the only confirmed infection vector involved hijacking the update process for an obscure Ukrainian tax software suggests that the attack may have been targeted exclusively toward Ukraine. The targeting of a city website in the east of Ukraine also suggests exclusive targeting of individuals in Ukraine.

Emerging research describing this variant of Petya as a wiper rather than a ransomware works against the profit motive as well. Exclusive targeting of individuals in Ukraine, given the rash of suspected Russian state-sponsored attacks against utilities and other entities in that country, and the possibility that the malware in question is a wiper raises the possibility that this could conceivably be a destructive, state-sponsored attack. This theory is further supported by reports that the attackers shut down the email address responsible for facilitating payment reception and key provisioning. We have low confidence in this theory given the information currently available.

INDICATORS OF COMPROMISE

Indicators curated by Booz Allen Hamilton Cyber4Sight intelligence service. Copy the below text into Excel for formatting and to review context/notes.

```
Indicator  Notes

71b6a493388e7d0b40c83ce903bc6b04
MD5 hash of suspected Petya ransomware likely used in recent attacks. 16/61 detect
ion rate on Virus Total as of 27 June 2017. First submitted 27 June 2017. Compilat
ion timestamp 18 June 2017. Reported by Payload Security, Fabian Wosar, and other
sources.

34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d
SHA1 hash of suspected Petya ransomware likely used in recent attacks. 16/61 detec
tion rate on Virus Total as of 27 June 2017. First submitted 27 June 2017. Compila
tion timestamp 18 June 2017. Reported by Payload Security, Fabian Wosar, and other
 sources.

027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745
SHA256 hash of suspected Petya ransomware likely used in recent attacks. 16/61 det
ection rate on Virus Total as of 27 June 2017. First submitted 27 June 2017. Compi
lation timestamp 18 June 2017. Reported by Payload Security, Fabian Wosar, and oth
er sources.

d28801905a63a924996444897d01eb01
MD5 hash of suspected Petya ransomware likely used in recent attacks. 24/61 detect
ion rate on Virus Total as of 3 June 2017. First submitted 31 May 2017. Compilatio
n timestamp April 2015. Reported by ISC SANs on 27 June 2017.

706b152136d15075a0dbe3164bc4231c3e4b0534
SHA1 hash of suspected Petya ransomware likely used in recent attacks. 24/61 detec
tion rate on Virus Total as of 3 June 2017. First submitted 31 May 2017. Compilati
on timestamp April 2015. Reported by ISC SANs on 27 June 2017.

8143d7d370015ccebcdaafce3f399156ffdf045ac8bedcc67bdffb1507be0b58
SHA256 hash of suspected Petya ransomware likely used in recent attacks. 24/61 det
ection rate on Virus Total as of 3 June 2017. First submitted 31 May 2017. Compila
tion timestamp April 2015. Reported by ISC SANs on 27 June 2017.

COFFEINOFFICE[.]XYZ
Domain of suspected Petya C2 sever. Reported byVulnersCom on 27 June 2017

111.90.139.247
IP address of suspected Petya C2 sever. Reported byVulnersCom on 27 June 2017

7ca37b86f4acc702f108449c391dd2485b5ca18c
MD5 hash of suspected Petya dropper. Reported byVulnersCom on 27 June 2017.

2bc182f04b935c7e358ed9c9e6df09ae6af47168
MD5 hash of suspected Petya dropper. Reported byVulnersCom on 27 June 2017.

1b83c00143a1bb2bf16b46c01f36d53fb66f82b5
MD5 hash of suspected Petya dropper. Reported byVulnersCom on 27 June 2017.

82920a2ad0138a2a8efc744ae5849c6dde6b435d
MD5 hash of suspected Petya dropper. Reported byVulnersCom on 27 June 2017.
```

```
415FE69BF32634CA98FA07633F4118E1
MD5 hash of suspected malicious email attachment delivering the Petya ransomware.
Likely exploiting CVE-2017-0199. Reported by VulnersCom on 27 June 2017.

0487382A4DAF8EB9660F1C67E30F8B25
MD5 hash of suspected Petya dropper. Reported byVulnersCom on 27 June 2017

A1D5895F85751DFE67D19CCCB51B051A
MD5 hash associated with Petya ransomware. Reported byVulnersCom on 27 June 2017

hxxp://mischapuk6hyrn72.onion/
C2 payment server associated with Petya ransomware infections. Reported by Bleepin
g Computer on 27 June 2017.

hxxp://petya3jxfp2f7g3i.onion/
C2 payment server associated with Petya ransomware infections. Reported by Bleepin
g Computer on 27 June 2017.

hxxp://petya3sen7dyko2n.onion/
C2 payment server associated with Petya ransomware infections. Reported by Bleepin
g Computer on 27 June 2017.

hxxp://mischa5xyix2mrhd.onion/MZ2MMJ
C2 payment server associated with Petya ransomware infections. Reported by Bleepin
g Computer on 27 June 2017.

hxxp://mischapuk6hyrn72.onion/MZ2MMJ
C2 payment server associated with Petya ransomware infections. Reported by Bleepin
g Computer on 27 June 2017.

hxxp://petya3jxfp2f7g3i.onion/MZ2MMJ
C2 payment server associated with Petya ransomware infections. Reported by Bleepin
g Computer on 27 June 2017.

hxxp://petya3sen7dyko2n.onion/MZ2MMJ
C2 payment server associated with Petya ransomware infections. Reported by Bleepin
g Computer on 27 June 2017.

84.200.16.242
IP address that malicious email attachment connects to download Petya dropper. Rep
orted by VulnsCom on 27 June 2017.

185.165.29.78
IP address associated with Petya ransomware campaign. Reported by VulnsCom on 27 J
une 2017.

a809a63bc5e31670ff117d838522dec433f74bee
MD5 hash associated with Petya ransomware. Reported byVulnersCom on 27 June 2017

bec678164cedea578a7aff4589018fa41551c27f
MD5 hash associated with Petya ransomware. Reported byVulnersCom on 27 June 2017

d5bf3f100e7dbcc434d7c58ebf64052329a60fc2
MD5 hash associated with Petya ransomware. Reported byVulnersCom on 27 June 2017

aba7aa41057c8a6b184ba5776c20f7e8fc97c657
MD5 hash associated with Petya ransomware. Reported byVulnersCom on 27 June 2017
```

```
0ff07caedad54c9b65e5873ac2d81b3126754aac
MD5 hash associated with Petya ransomware. Reported byVulnersCom on 27 June 2017

51eafbb626103765d3aedfd098b94d0e77de1196
MD5 hash associated with Petya ransomware. Reported byVulnersCom on 27 June 2017

078de2dc59ce59f503c63bd61f1ef8353dc7cf5f
MD5 hash associated with Petya ransomware. Reported byVulnersCom on 27 June 2017

e285b6ce047015943e685e6638bd837e
MD5 hash of suspected ransomware dubbed "NotPetya" used in recent attacks. 9/61 de
tection rate on Virus Total as of 27 June 2017. First submitted on 27 June 2017. C
ompilation timestamp 18 June 2017. Reported by Alien Vault on 27 June 2017.

9717cfdc2d023812dbc84a941674eb23a2a8ef06
SHA1 hash of suspected ransomware dubbed "NotPetya" used in recent attacks. 9/61 d
etection rate on Virus Total as of 27 June 2017. First submitted on 27 June 2017.
Compilation timestamp 18 June 2017. Reported by Alien Vault on 27 June 2017.

64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b1
SHA256 hash of suspected ransomware dubbed "NotPetya" used in recent attacks. 9/61
 detection rate on Virus Total as of 27 June 2017. First submitted on 27 June 2017
. Compilation timestamp 18 June 2017. Reported by Alien Vault on 27 June 2017.

hxxp://benkow[.]cc/71b6a493388e7d0b40c83ce903bc6b04[.]bin
URL delivering binary for the ransomware dubbed "NotPetya" attack. Reported by Pay
load Security on 27 June 2017.

169.239.181.127
IP address delivering binary for the ransomware dubbed "NotPetya" attack. Reported
 by Payload Security on 27 June 2017.

h11p://french-cooking[.]com/myguy.exe
URL delivering a suspected dropper for ransomware dubbed "NotPetya." Reported by C
yber4Sight proprietary sources on 27 June 2017.

wowsmith123456[@]posteo.net
Email address associated with the ransomware dubbed "NotPetya" campaign. Reported
by several security researchers on 27 June 2017.

95.141.115.108
IP address possibly associated with the ransomware dubbed "NotPetya." Reported by
VulnsCom on 27 June 2017.

C:\Windows\perfc.dat
File path of malicious document associated with suspected ransomware dubbed "NotPe
tya." Reported by Informzachita(infosec.ru).

C:\myguy.xls.hta
File path of malicious document associated with suspected ransomware dubbed "NotPe
tya." Reported by Informzachita(infosec.ru).

%APPDATA%\10807.exe
File path of malicious document associated with suspected ransomware dubbed "NotPe
tya." Reported by Informzachita(infosec.ru).
```



```
burak.fr
Domain associated with ransomware dubbed "NotPetya." Reported by IBM on 27 June 20
17.

pental.dothome.co.kr
Domain associated with ransomware dubbed "NotPetya." Reported by IBM on 27 June 20
17.

104.155.10.169
IP address associated with ransomware dubbed "NotPetya." Reported by IBM on 27 Jun
e 2017.

df2188e97a57fd60743364c44ffc7289
MD5 hash associated with ransomware dubbed "NotPetya." 12/56 detection rate as of
27 June 2017. First submitted to VirusTotal on 27 June 2017. Reported by IBM on 27
 June 2017.

e614365d97498a6c26be9fd337e3709a1aa0a4fe
SHA1 hash associated with ransomware dubbed "NotPetya." 12/56 detection rate as of
 27 June 2017. First submitted to VirusTotal on 27 June 2017. Reported by IBM on 2
7 June 2017.

5d91f2c2ed8d83739522eb234452f230ebf4b9e1f8cd8d097d99c583e85695aa
SHA256 hash associated with ransomware dubbed "NotPetya." 12/56 detection rate as
of 27 June 2017. First submitted to VirusTotal on 27 June 2017. Reported by IBM on
 27 June 2017.
```

SNORT

```
alert tcp $EXTERNAL_NET any -
> $HOME_NET 445 (msg:"ET NETBIOS Microsoft SRV2.SYS SMB Negotiate ProcessID Functi
on Table Dereference"; flow:to_server,established; content:"|FF 53 4d 42 72|"; off
set:4; depth:5; content:!"|00 00|"; distance:7; within:2; reference:url,www.exploi
t-
db.com/exploits/14674/; reference:url,www.microsoft.com/technet/security/bulletin/
ms09-050.mspx; reference:cve,2009-3103; classtype:attempted-
user; sid:2012063; rev:1;)



alert tcp any any -> any 445 (msg:"ET CURRENT_EVENTS ETERNALBLUE Exploit M2 MS17-
010"; flow:established,to_server; content:"|8000a800000000000000000000000000000000
00ffff000000000000ffff0000000000000000000000000000000000000000000000f1dfff00000000
0000000020f0dfff00f1dfffffffffff600004100000000080efdfff|"; reference:cve,CVE-
2017-0143; classtype:attempted-admin; sid:2024297; rev:1;)



alert smb any any -
> $HOME_NET any (msg:"ET CURRENT_EVENTS Possible ETERNALBLUE Exploit M3 MS17-
010"; flow:to_server,established; content:"|ff|SMB|32 00 00 00 00 18 07 c0|"; offs
et:4; depth:12; content:"|00 00 00 00 00 00 00 00 00 00 00 08 ff fe 00 08|"; dista
nce:2; within:16; fast_pattern; content:"|0f 0c 00 00 10 01 00 00 00 00 00 00 00 f
2 00 00 00 00 00 0c 00 42 00 00 10 4e 00 01 00 0e 00 0d 10 00|"; distance:2; withi
n:34; isdataat:1000,relative; threshold: type both, track by_src, count 10, second
s 1; classtype:trojan-activity; sid:100; rev:1;)
```

YARA

```
rule DoublePulsarXor_Petya


{


  meta:

    description = "Rule to hit on the XORed DoublePulsar shellcode"

    author = "Patrick Jones"

    company = "Booz Allen Hamilton"

    date = "2017-06-28"

    hash = "027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745"

    hash = "64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b1"

  strings:


$DoublePulsarXor_Petya = { FD 0C 8C 5C B8 C4 24 C5 CC CC CC 0E E8 CC 24 6B CC CC C
C 0F 24 CD CC CC CC 27 5C 97 75 BA CD CC CC C3 FE }

  condition:

    $DoublePulsarXor_Petya

}


rule DoublePulsarDllInjection_Petya


{

   meta:

    description = "Rule to hit on the XORed DoublePulsar DLL injection shellcode"

    author = "Patrick Jones"

    company = "Booz Allen Hamilton"

    date = "2017-06-28"

    hash = "027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745"

    hash = "64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b1"
```



```
  strings

$DoublePulsarDllInjection_Petya = { 45 20 8D 93 8D 92 8D 91 8D 90 92 93 91 97 0F 9
F 9E 9D 99 84 45 29 84 4D 20 CC CD CC CC 9B 84 45 03 84 45 14 84 45 49 CC 33 33 33
 24 77 CC CC CC 84 45 49 C4 33 33 33 24 84 CD CC CC 84 45 49 DC 33 33 33 84 47 49
CC 33 33 33 84 47 41 }

  condition:

    $DoublePulsarDllInjection_Petya

}



rule ransomware_PetrWrap {



meta:



copyright = "Kaspersky Lab"

description = "Rule to detect PetrWrap ransomware samples"

last_modified = "2017-06-27"

author = "Kaspersky Lab"

hash = "71B6A493388E7D0B40C83CE903BC6B04"

version = "1.0"



strings:



$a1 = "MIIBCgKCAQEAxP/VqKc0yLe9JhVqFMQGwUITO6WpXWnKSNQAYT0O65Cr8PjIQInTeHkXEjfO2n2
JmURWV/uHB0ZrlQ/wcYJBwLhQ9EqJ3iDqmN19Oo7NtyEUmbYmopcq+YLIBZzQ2ZTK0A2DtX4GRKxEEFLCy
7vP12EYOPXknVy/+mf0JFWixz29QiTf5oLu15wVLONCuEibGaNNpgq+CXsPwfITDbDDmdrRIiUEUw6o3pt
5pNOskfOJbMan2TZu" fullword wide

$a2 = ".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.p
pt.pptx.pst.pvi.py.pyc.rar.rtf.sln.sql.tar.vbox.vbs.vcb.vdi.vfd.vmc.vmdk.vmsd.vmx.
vsdx.vsv.work.xls" fullword wide

$a3 = "DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED" f
ullword ascii

$a4 = "1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX" fullword ascii

$a5 = "wowsmith123456@posteo.net." fullword wide
```

```
condition:


uint16(0) == 0x5A4D and

filesize < 1000000 and any of them }
```

[1] hxxps://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/
[2] hxxps://blog.comae.io/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b
[3] hxxps://technet.microsoft.com/en-us/library/security/ms17-010.aspx
[4] hxxps://twitter.com/CyberpoliceUA/status/879772963658235904?ref_src=twsrc%5Etfw&ref_url=https%3A%2F%2Fmedium.com%2Fmedia%2Fdf1fb804ed0e87b0c25cec520fb6baa0%3FpostId%3D59afd1ee89d4
[5] hxxp://blog.group-ib.com/petya
[6] hxxps://twitter.com/craiu/status/880011103161524224