


petwrap.exe

malicious

This report is generated from a file or URL submitted to this webservice on June 27th 2017 15:39:11 (UTC)

Threat Score: 100/100

AV Detection: 98%

Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1

Labeled as: Trojan.Generic

#Petya\_NSA\_EE\_Ransomware


#Petna


#tag


#ransomware


#petya


#eternalblue


-  Overview


 Sample unavailable


 Downloads ▼

 External Reports ▼

 Re-analyze


 Hash Seen Before

 Show Similar Samples

 Report False-Positive

-  Post
-  Link
-  E-Mail

## Incident Response

 Risk Assessment

Ransomware

Clears the windows event log using Wevtutil  
Detected indicator that file is ransomware

Persistence

Interacts with the primary disk partition (DR0)  
Shedules a task to be executed at a specific time and date  
Spawns a lot of processes  
Writes to the primary disk partition (DR0)


Fingerprint

Reads the active computer name

Spreading

Detected a large number of ARP broadcast requests (network device looku p)

## Additional Context

 Related Sandbox Artifacts


Associated SHA25...

3419e0d470f83569be0927128b3e5f992800ceb8f9019fc44763876ed6d8000c

Associated URLs

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

## Indicators



Not all malicious and suspicious indicators are displayed. Get your own cloud service or the full version to view all details.

Malicious Indicators21

Anti-Detection/Stealthyness

Creates a resource fork (ADS) file (often used to hide data)▼

External Systems

Sample was identified as malicious by a trusted Antivirus engine▼

### À PROPOS DES COOKIES SUR CE SITE
























En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

[Paramètres des cookies](#)

Tout refuser

Autoriser tous les cookies

Page 1 of 8

|   |  |   |  |                                     |   |
|---|--|---|--|-------------------------------------|---|
|  HYBRID ANALYSIS |  |    |  Request Info | <input type="text" value="Search"/> |  |
| The analysis spawned a process that was identified as malicious                                   |  |  |  |                                     |   |
| Installation/Persistence  |  |   |  |                                     |   |
| Drops executable files to the Windows system directory  |  |  |  |                                     |   |
| Loads the task scheduler COM API  |  |  |  |                                     |   |
| Schedules a task to be executed at a specific time and date                                       |  |  |  |                                     |   |
| Writes to the primary disk partition (DR0)  |  |    |  |                                     |   |
| Network Related   |  |   |  |                                     |   |
| Detected a large number of ARP broadcast requests (network device lookup)                         |  |    |  |                                     |   |
| Pattern Matching  |  |   |  |                                     |   |
| YARA signature match  |  |    |  |                                     |   |
| System Destruction  |  |   |  |                                     |   |
| Interacts with the primary disk partition (DR0)   |  |  |  |                                     |   |
| Writes to the primary disk partition (DR0)  |  |    |  |                                     |   |
| Unusual Characteristics   |  |   |  |                                     |   |
| Contains native function calls  |  |    |  |                                     |   |
| Spawns a lot of processes   |  |    |  |                                     |   |
| Hiding 6 Malicious Indicators   |  |   |  |                                     |   |
| All indicators are available only in the private webinterface or standalone version               |  |   |  |                                     |   |
| Suspicious Indicators   |  | 29  |  |                                     |   |
| Anti-Reverse Engineering  |  |   |  |                                     |   |
| PE file has unusual entropy sections  |  |  |  |                                     |   |
| Environment Awareness   |  |   |  |                                     |   |
| Possibly tries to implement anti-virtualization techniques  |  |  |  |                                     |   |
| Queries physical drive (often used to detect virtual machines)                                    |  |  |  |                                     |   |
| Reads the active computer name  |  |  |  |                                     |   |
| General   |  |   |  |                                     |   |
| Contains ability to find and load resources of a specific module                                  |  |    |  |                                     |   |
| Opened the service control manager  |  |    |  |                                     |   |
| Requested access to a system service  |  |    |  |                                     |   |
| Sent a control code to a service  |  |    |  |                                     |   |

## À PROPOS DES COOKIES SUR CE SITE


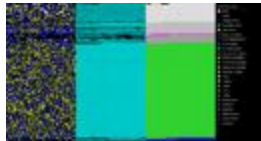
En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)



| HYBRID ANALYSIS   |   | Request Info |  | Search |
|---|---|--------------|--|--------|
| Process launched with changed environment                   | ▼ |              |  |        |
| Runs shell commands   | ▼ |              |  |        |
| Spawns new processes  | ▼ |              |  |        |
| The input sample is signed with a certificate               | ▼ |              |  |        |
| <b>Installation/Persistence</b>                             |   |              |  |        |
| Contains ability to lookup the windows account name         | ▼ |              |  |        |
| Dropped files   | ▼ |              |  |        |
| Touches files in the Windows directory                      | ▼ |              |  |        |
| <b>Network Related</b>                                      |   |              |  |        |
| Found potential URL in binary/memory                        | ▼ |              |  |        |
| <b>System Security</b>                                      |   |              |  |        |
| Opens the Kernel Security Device Driver (KsecDD) of Windows | ▼ |              |  |        |

## File Details

All Details: 







|   |  |
|---|--|
| <div> <div></div> <div>petwrap.exe</div> </div>   |  |
| Filename  | petwrap.exe  |
| Size  | 354KiB (362360 bytes)  |
| Type  | <div> <div>pedll</div> <div>executable</div> </div>              |
| Description   | PE32 executable (DLL) (console) Intel 80386, for MS Windows      |
| Architecture  | WINDOWS  |
| SHA256  | 027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745 |
|   | <div></div>  |
| PDB Pathway   |  |
| <div> <div>Resources</div> <div> <div>Language</div> <div>ENGLISH</div> </div> <div> <div>Icon</div> <div>  </div> </div> </div>   |  |
| <div> <div>Visualization</div> <div> <div>Input File (PortEx)</div> <div>  </div> </div> </div>  |  |
| <div> <div>Classification (TrID)</div> <div> <ul style="list-style-type: none"> <li>67.4% (.EXE) Win32 Executable MS Visual C++ (generic)</li> <li>14.2% (.DLL) Win32 Dynamic Link Library (generic)</li> <li>9.7% (.EXE) Win32 Executable (generic)</li> <li>4.3% (.EXE) Generic Win/DOS Executable</li> <li>4.3% (.EXE) DOS Executable Generic</li> </ul> </div> </div> |  |

## File Sections

| Virtual | Virtual | Raw |
|---------|---------|-----|
|---------|---------|-----|

## À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

|  |   |   |   |   |  |  |
|--|---|---|---|---|--|--|
|  |  ▾ |  ▾ |  |  ▾ |  Request Info ▾ | <div><div>Q</div><div>×</div></div> <div>▾</div> |
| .rsrc  | 7.9982879669  | 0x20000   | 0x3c738   | 0x3c800   | f07e68575f50a62382d99e182baa05d5   | -  |
| .reloc   | 4.77168126134   | 0x5d000   | 0xc02   | 0xe00   | c5d1d4cdade7dcfbe14ec10dcf66cfb1   | -  |

File Resources

| Name      | RVA     | Size    | Type | Language |
|-----------|---------|---------|------|----------|
| RT_RCDATA | 0x200e8 | 0x617e  | data | English  |
| RT_RCDATA | 0x26268 | 0x6b22  | data | English  |
| RT_RCDATA | 0x2cd8c | 0x2ec75 | data | English  |
| RT_RCDATA | 0x5ba04 | 0xd33   | data | English  |

File Imports

|                       |             |              |              |              |            |            |
|-----------------------|-------------|--------------|--------------|--------------|------------|------------|
| ADVAPI32.dll          | CRYPT32.dll | DHCPSAPI.DLL | IPHLPAPI.DLL | KERNEL32.dll | MPR.dll    | msvcrt.dll |
| NETAPI32.dll          | ole32.dll   | SHELL32.dll  | SHLWAPI.dll  | USER32.dll   | WS2_32.dll |            |
| AdjustTokenPrivileges |             |              |              |              |            |            |
| CreateProcessAsUserW  |             |              |              |              |            |            |
| CredEnumerateW        |             |              |              |              |            |            |
| CredFree              |             |              |              |              |            |            |
| CryptAcquireContextA  |             |              |              |              |            |            |
| CryptAcquireContextW  |             |              |              |              |            |            |

File Certificates


❗ Error validating certificate: Not implemented (0x80004001)

📎 Download Certificate File (5.9KiB)

| Owner  | Issuer  | Validity                                   | Hashes (MD5, SHA1)   |
|--|---|--|--|
| CN=Microsoft Code Signing PCA, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US     | CN=Microsoft Root Authority, OU=Microsoft Corporation, OU=Copyright c 1997 Microsoft Corp. Serial: 2eab11dc50ff5c9dcbc0 | 08/23/2007 00:31:02<br>08/25/2012 09:00:00 | 33:14:0F:BB:D4:F7:8B:32:64:BD:AF:83:99:4C:67:90<br>30:36:E3:B2:5B:88:A5:5B:86:FC:90:E6:E9:EA:AD:50:81:44:51:66 |
| CN=Microsoft Corporation, OU=MOPR, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US | CN=Microsoft Code Signing PCA, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US Serial: 6101cf3e000000000000f    | 12/07/2009 23:40:29<br>03/07/2011 23:40:29 | E3:FE:DB:37:F4:87:4E:84:CD:B8:2A:78:9F:FD:CD:67<br>96:17:09:4A:1C:FB:59:AE:7C:1F:7D:FD:B6:73:9E:4E:7C:40:50:8F |
| CN=Microsoft   | CN=Microsoft Root Authority   | 08/16/2006                                 | B9:56:D5:DA:60:80:B2:42:73:D1:0D:08:03:A4:E7:AA  |

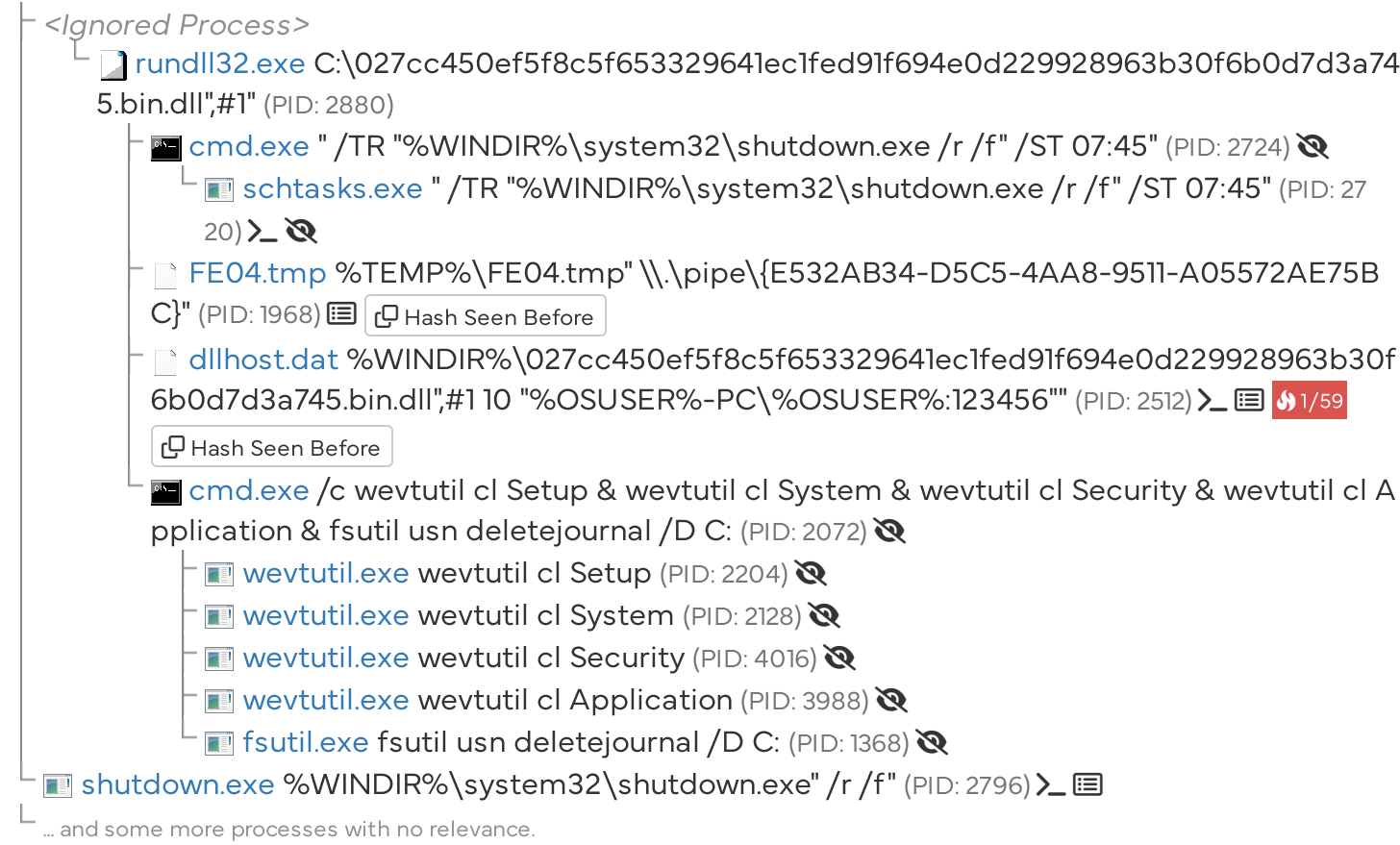
Screenshots


# Hybrid Analysis




Tip: Click an analysed process below to view more details.

Analysed 12 processes in total ([System Resource Monitor](#)).





HYBRID  
ANALYSIS



Request Info

Q

×


shutdown.exe (1)    schtasks.exe:2720 (3)    rundll32.exe:2880 (96)    rundll32.exe (1)    fsutil.exe (1)

wevtutil.exe (4)

|   |
|---|
| " /TR "%WINDIR%\system32\shutdown.exe /r /f" /ST 07:45"   |
| "%WINDIR%\027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745.bin.dll",#1 10 "PSPUBWS-PC\PSPUBWS:123456" |
| %M!%M!%M!%M!%M!%M!%M!%M!%M!%M!  |
| %s -install to install the service  |
| %s -remove to remove the service  |
| %s /node:"%ws" /user:"%ws" /password:"%ws"  |
| %s error: %d  |
| %s exited on %s with error code %d.   |
| %s exited with error code %d.   |
| %s requires Windows NT/2000/XP/2003.  |
| %s service on %s...   |

## Extracted Files

Malicious1

 dllhost.dat




Overview

Download Disabled


VirusTotal Report

Extracted Streams

Hash Seen Before

|                 |  |
|-----------------|--|
| Size            | 373KiB (381816 bytes)  |
| Type            | peexeexecutable  |
| Description     | PE32 executable (console) Intel 80386, for MS Windows  |
| AV Scan Result  | Labeled as "PsExec" (1/59)   |
| Runtime Process | rundll32.exe (PID: 2880)   |
| MD5             | aeee996fd3484f28e5cd85fe26b6bdcd                                    |
| SHA1            | cd23b7c9e0edef184930bc8e0ca2264f0608bcb3                           |
| SHA256          | f8dbabdfa03068130c277ce49c60e35c029ff29d9e3c74c362521f3fb02670d5  |




Clean1

 PSEXESVC.EXE

Download Disabled

VirusTotal Report

Hash Seen Before


|                 |  |
|-----------------|--|
| Size            | 177KiB (181064 bytes)  |
| Type            | data   |
| AV Scan Result  | 0/57   |
| Runtime Process | dllhost.dat (PID: 2512)  |
| MD5             | 5f6e775124efbd810c58f349d3f96400                                    |
| SHA1            | 766d70566b38c5fbf8b2e891c2f70f146561789f                            |
| SHA256          | eccd88bfc2be71e0ee7926fa4bed4e72a2db864328f2351d301f67bfe19e26bc  |

Log Malicious Objects




### À PROPOS DES COOKIES SUR CE SITE


En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)





HYBRID


ANALYSIS

 ▾


 ▾

 ▾

 ▾




 Request Info


▾





×


▾




|                 |  |   |  |
|-----------------|--|---|--|
| Runtime Process | rundll32.exe (PID: 2880)   |   |  |
| MD5             | 5733d78651a308b8dfacb41a7ec2b99a                                 |    |  |
| SHA1            | 98f9ade6d75c887d06b0343b506aebd948a61818                         |   |  |
| SHA256          | 41cb22109da26a6ff5464d6915db81c1c60f9e0808d8dbd63df1550b86372165 |  |  |

 027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745.bin.dll

 Overview


 Download Disabled

 Hash Seen Before

|                 |  |   |  |
|-----------------|--|---|--|
| Size            | 354KiB (362360 bytes)  |   |  |
| Type            | <div>data</div>  |   |  |
| Runtime Process | rundll32.exe (PID: 2880)   |   |  |
| MD5             | 9a7ffe65e0912f9379ba6e8e0b079fde                                 |    |  |
| SHA1            | 532bea84179e2336caed26e31805ceaa7eec53dd                         |    |  |
| SHA256          | 4b336c3cc9b6c691fe581077e3dd9ea7df3bf48f79e35b05cf87e079ec8e0651 |  |  |

## Notifications

Runtime



## Community


Sandip commented 7 years ago

#Petya

Amigo commented 7 years ago

#Petya\_NSA\_EE\_Ransomware: Full Description or #Petya Ransomware: NSA Exploit Edition or #Petna (NotPetya, NonPetya) Ransomware hxxps://id-ransomware.blogspot.com/2017/06/petya-nsa-ee-ransomware.html

9 comments are hidden. Please click this link to display all.

 You must be logged in to submit a comment.

### À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)