


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  
Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1 AV Detection: 98%  
Report generated by Falcon Sandbox © Hybrid Analysis

Overview

Sample unavailable

Downloads

External Reports

Re-analyze

Hash Seen Before

Show Similar Samples

Report False-Positive

#Petya\_NSA\_EE\_Ransomware

#Petna

#tag

#ransomware

#petya


#eternalblue

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 lookup)

# Additional Context

 Related Sandbox Artifacts

Associated SHA25...

3419e0d470f83569be0927128b3e5f992800ceb8f9019fc44763876ed6d8000c

Associated URLs

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



# Indicators

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

Malicious Indicators

21

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

Sample was identified as malicious by at least one Antivirus engine

General

The analysis extracted a file that was identified as malicious

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



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	▼



Requested access to a system service	▼
Sent a control code to a service	▼
Installation/Persistence	
Drops executable files	▼
Network Related	
Detected increased number of ARP broadcast requests (network device lookup)	▼
Found potential IP address in binary/memory	▼
Ransomware/Banking	
Detected indicator that file is ransomware	▼
Remote Access Related	
Contains references to WMI/WMIC	▼
System Destruction	
Tries to obtain a handle with write access to the physical drive	▼
System Security	
Contains ability to elevate privileges	▼
Contains ability to impersonate another user on the local machine	▼
Makes use of the windows event log utility	▼
Uncategorized Behavior	
Found a cryptographic related string	▼
Unusual Characteristics	



Installs hooks/patches the running process	▼
Reads information about supported languages	▼
Hiding 8 Suspicious Indicators	
All indicators are available only in the private webinterface or standalone version	
Informative	
18	
Anti-Reverse Engineering	
Contains ability to register a top-level exception handler (often used as anti-debugging trick)	▼
Environment Awareness	
Contains ability to query machine time	▼
Contains ability to query the machine timezone	▼
Contains ability to query the machine version	▼
Contains ability to query the system locale	▼
Makes a code branch decision directly after an API that is environment aware	▼
Possibly tries to detect the presence of a debugger	▼
General	
Contains PDB pathways	▼
Drops files marked as clean	▼
Process launched with changed environment	▼
Runs shell commands	▼



The input sample is signed with a certificate	▼
Installation/Persistence	
Contains ability to lookup the windows account name	▼
Dropped files	▼
Touches files in the Windows directory	▼
Network Related	
Found potential URL in binary/memory	▼
System Security	
Opens the Kernel Security Device Driver (KsecDD) of Windows	▼

## File Details

All Details: ☐ Off

petwrap.exe

Filename	petwrap.exe		
Size	354KiB (362360 bytes)		
Type	<span>peDll</span> <span>executable</span>		
Description	PE32 executable (DLL) (console) Intel 80386, for MS Windows		
Architecture	WINDOWS		
SHA256	027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745		
PDB Pathway			
Resources		Visualization	
Language	ENGLISH	Input File (PortEx)	



Classification (TrID)

- 67.4% (.EXE) Win32 Executable MS Visual C++ (generic)
- 14.2% (.DLL) Win32 Dynamic Link Library (generic)
- 9.7% (.EXE) Win32 Executable (generic)
- 4.3% (.EXE) Generic Win/DOS Executable
- 4.3% (.EXE) DOS Executable Generic

File Sections

Details

Name	.text
Entropy	6.54653060932
Virtual Address	0x1000
Virtual Size	0xbd63
Raw Size	0xbe00
MD5	c5bd3bb710ae377938b17980692b785b

Name	.rdata
Entropy	6.99212929533
Virtual Address	0xd000
Virtual Size	0x8546
Raw Size	0x8600
MD5	46418e52b546c1f696eb8a524f18c56e

Name	.data
Entropy	5.42698913823
Virtual Address	0x16000
Virtual Size	0x9b4a
Raw Size	0x5200
MD5	5216f0c62d1fd41b1d558e129e18d0fe

Name	.rsrc
Entropy	7.9982879669
Virtual Address	0x20000
Virtual Size	0x3c738



Name	.reloc
Entropy	4.77168126134
Virtual Address	0x5d000
Virtual Size	0xc02
Raw Size	0xe00
MD5	c5d1d4cdade7dcfbe14ec10dcf66cfb1

## File Resources

### Details

Name	RT_RCDATA
RVA	0x200e8
Size	0x617e
Type	data
Language	English

Name	RT_RCDATA
RVA	0x26268
Size	0x6b22
Type	data
Language	English

Name	RT_RCDATA
RVA	0x2cd8c
Size	0x2ec75
Type	data

## File Imports

- ADVAPI32.dll
- CRYPT32.dll
- DHCPAPI.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





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 08/25/2012 09:00:00	33:14:0F:BB:D4:F7:8B:32:64:BD:AF:83:99:4C:67:90 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: 6101cf3e00000000000f	12/07/2009 23:40:29 03/07/2011 23:40:29	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
CN=Microsoft Time-stamping PCA	CN=Microsoft Root Authority, OU=Microsoft Corporation	09/16/2006 03:04:17	B9:56:D5:DA:60:80:B3:42:72:D1:9D:08:03:A4:E7:AA 2F:A0:0A:60:05:03:75:50:5D:03:00:03:A0:00:44:05:00:03:03:4F

# Screenshots

i Loading content, please wait...

# Hybrid Analysis



Analysed 12 processes in total (System Resource Monitor).

<Ignored Process>

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)

FE04.tmp %TEMP%\FE04.tmp" \\.pipe\{E532AB34-D5C5-4AA8-9511-A05572AE75BC}" (PID: 1968)

Hash Seen Before

dllhost.dat %WINDIR%\027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745.bin.dll,#1 10 "%OSUSER%-PC\%OSUSER%:123456"" (PID: 2512)

Hash Seen Before

1/59

cmd.exe /c wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil 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)

and some more processes with no relevance.

Logged Script Calls	Logged Stdout	Extracted Streams	Memory Dumps
Reduced Monitoring	Network Activity	Network Error	Multiscan Match

## Network Analysis

### DNS Requests

No relevant DNS requests were made.

### Contacted Hosts

No relevant hosts were contacted.

### HTTP Traffic



# Memory Forensics

String	Context	Stream UID
192.168.56.11	Domain/IP reference	00026671-00002512-16111-836-0040375B
127.0.0.1	Domain/IP reference	14041-3-10007D6F

## Extracted Strings

Q

Search

All Details: 

Off

Download All Memory Strings (17KiB)

- All Strings (1350)Interesting (575)027cc450ef5f8c5f653329...cmd.exe (2)dllhost.dat:2512 (477)
- shutdown.exe:2796 (111)FE04.tmp:1968 (128)dllhost.dat.2738936092 (1...FE04.tmp (1)dllhost.dat (1)
- 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.



# Extracted Files

## Malicious

1

dllhost.dat

- Overview
- Download Disabled
- VirusTotal Report
- Extracted Streams
- Hash Seen Before

**Size** 373KiB (381816 bytes)

**Type** peexe executable

**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

## Clean

1

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

## Informative Selection

2



[Overview](#) [Download Disabled](#) [Hash Seen Before](#)

**Size** 47KiB (47616 bytes)  
**Type** data  
**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** data  
**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 (NotPetya, NonPetya) Ransomware <https://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.