



♦ E-Mail

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

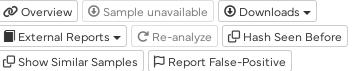
Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1

AV Detection: 98%

Report generated by Falcon Sandbox © Hybrid Analysis

Labeled as: Trojan.Generic

Report generated by Falcon Sandbox © Hybrid Analysis

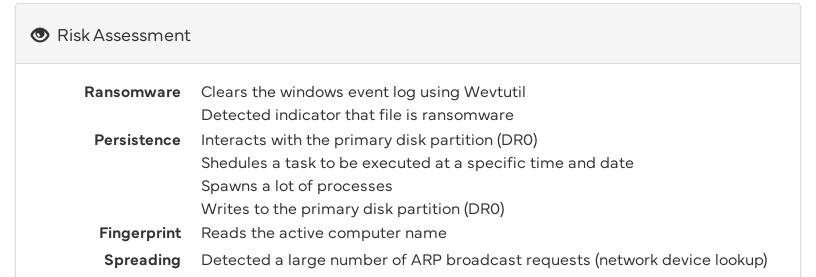




X Post

@ Link

Incident Response



Additional Context



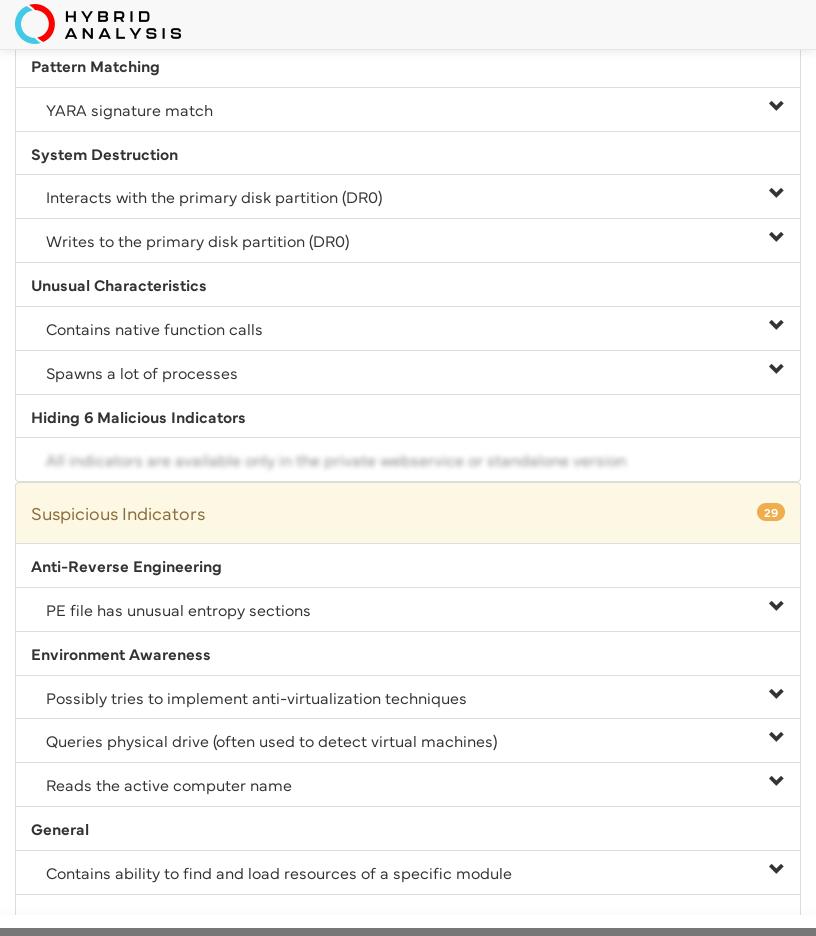


Indicators

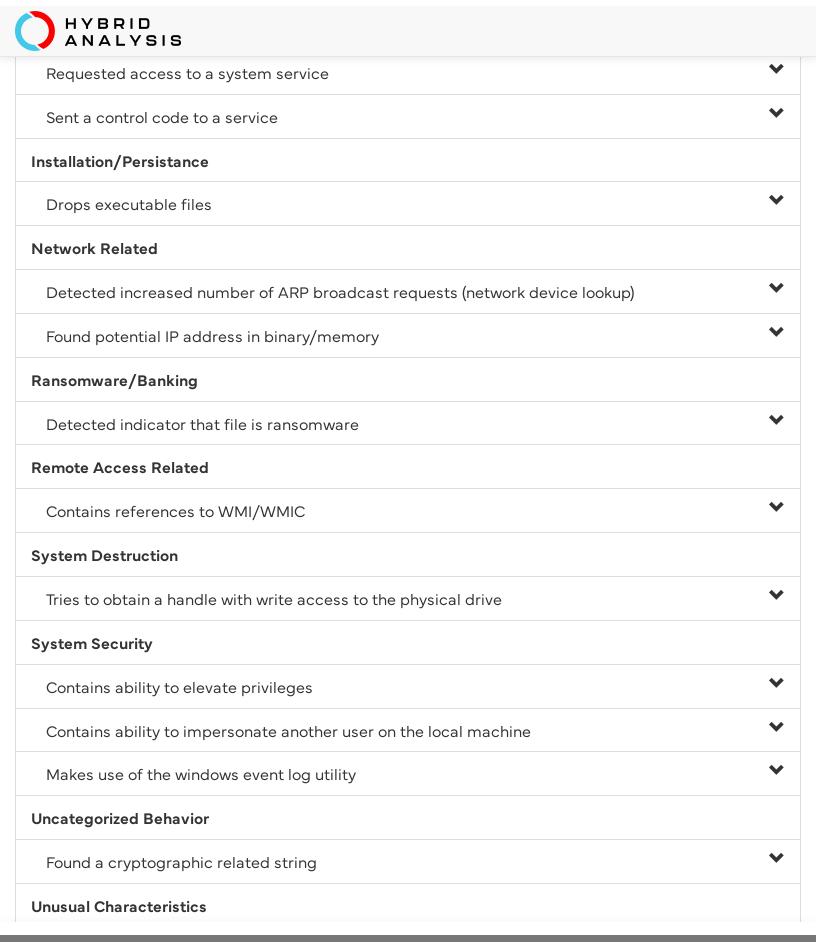
1 Not all malicious and suspicious indicators are displayed. Get your own cloud service or the full version to view all details.

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/Persistance			
Drops executable files to the Windows system directory	~		
Loads the task scheduler COM API	~		
Shedules a task to be executed at a specific time and date	~		
Writes to the primary disk partition (DR0)	~		
Network Related			

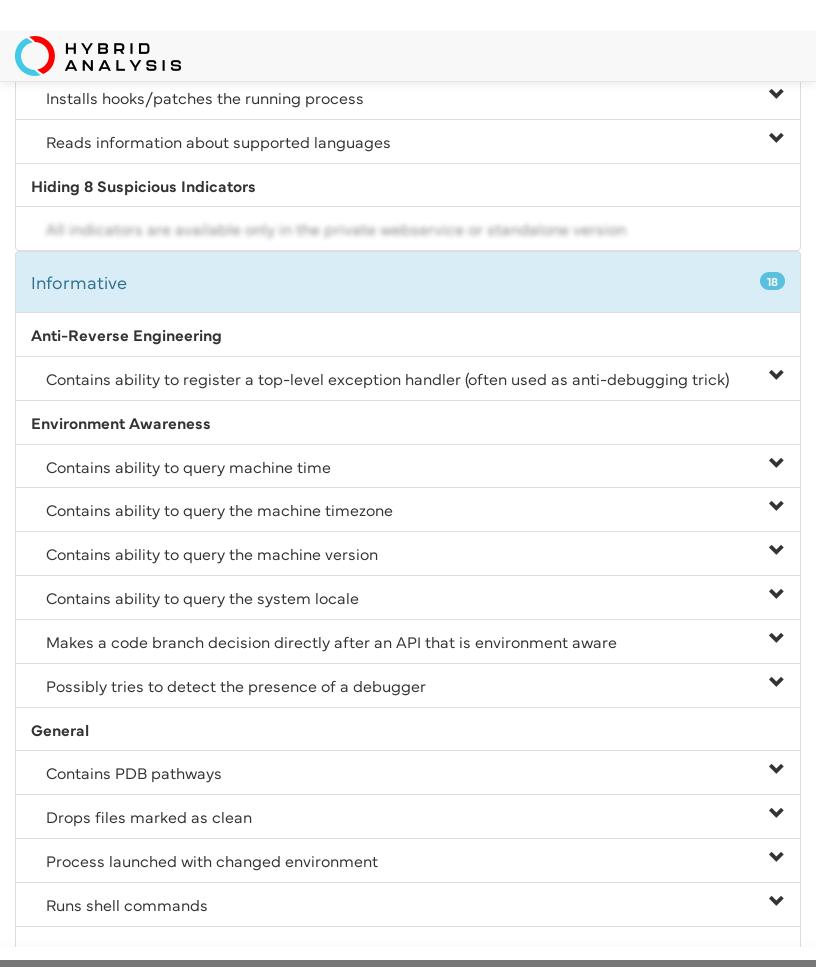
analysis.com/sample/027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745?environmentId=100

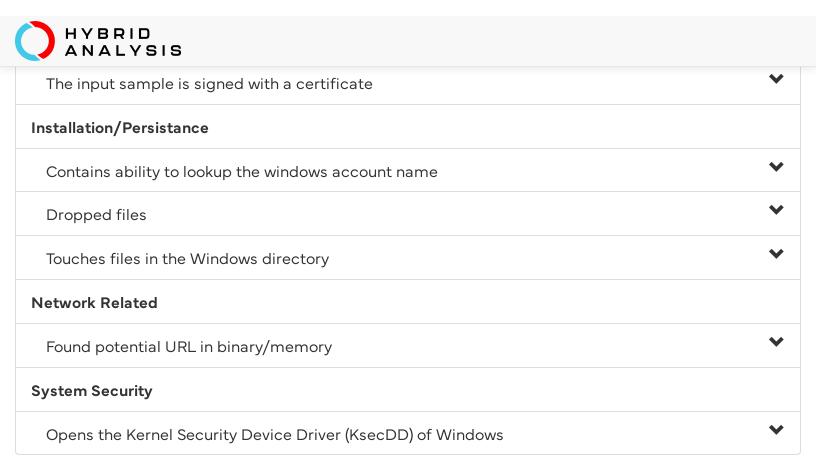


analysis.com/sample/027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745?environmentId=100



analysis.com/sample/027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745?environmentId=100





File Details

All Details: Off petwrap.exe Filename petwrap.exe Size 354KiB (362360 bytes) Type pedll executable Description PE32 executable (DLL) (console) Intel 80386, for MS Windows Architecture **WINDOWS** 027cc450ef5f8c5f65332964lec1fed9lf694e0d229928963b30f6b0d7d3a745 食 **SHA256** PDB Pathway Resources Visualization Input File (PortEx) **ENGLISH** Language



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

PT32.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



CryptAcquireContextA

C= 1=+ 1 - = 1:= C - = + = 1+1 1/

File Certificates

Error validating certificate: Not implemented (0x80004001)

① Download Certificate File (5.9KiB)

Owner	Issuer	Validity	Hashes (MD5, SHA1)
CN=Microsoft Code	CN=Microsoft Root Authority,	08/23/2007	33:14:0F:BB:D4:F7:8B:32:64:BD:AF:83:99:4C:67:90
Signing PCA,	OU=Microsoft Corporation,	00:31:02	30:36:E3:B2:5B:88:A5:5B:86:FC:90:E6:E9:EA:AD:50:81:44:51:66
O=Microsoft	OU=Copyright c 1997 Microsoft Corp.	08/25/2012	
Corporation,	Serial: 2eab11dc50ff5c9dcbc0	09:00:00	
L=Redmond,			
ST=Washington,			
C=US			
CN=Microsoft	CN=Microsoft Code Signing PCA,	12/07/2009	E3:FE:DB:37:F4:87:4E:84:CD:B8:2A:78:9F:FD:CD:67
Corporation,	O=Microsoft Corporation, L=Redmond,	23:40:29	96:17:09:4A:1C:FB:59:AE:7C:1F:7D:FD:B6:73:9E:4E:7C:40:50:8F
OU=MOPR,	ST=Washington, C=US	03/07/2011	
O=Microsoft	Serial: 6101cf3e00000000000f	23:40:29	
Corporation,			
L=Redmond,			
ST=Washington,			
C=US			
CN=Microsoft	CN=Microsoft Root Authority,	09/16/2006	B9:56:D5:DA:60:80:B3:42:72:D1:9D:08:03:A4:E7:AA
T:	O1 1-44:	00.04.47	0F. 4 O.O 4 .CO.OF.00.7F.FO.FD.00.D0.00. 4 O.OO. 4 4.OF.0 O.00.D0.4F

Screenshots



Hybrid Analysis



Analysed 12 processes in total (System Resource Monitor).

<lgnored Process> rundll32.exe C:\027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745.bi n.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) \mathcal{G} FE04.tmp %TEMP%\FE04.tmp" \\.\pipe\{E532AB34-D5C5-4AA8-9511-A05572AE75BC}" (PID: 1968) 🔳 🗗 Hash Seen Before dllhost.dat %WINDIR%\027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b 0d7d3a745.bin.dll",#1 10 "%OSUSER%-PC\%OSUSER%:123456"" (PID: 2512) >_ III 6/1/59 ☐ Hash Seen Before mcmd.exe /c wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Appl ication & 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 Activityy ▲ 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

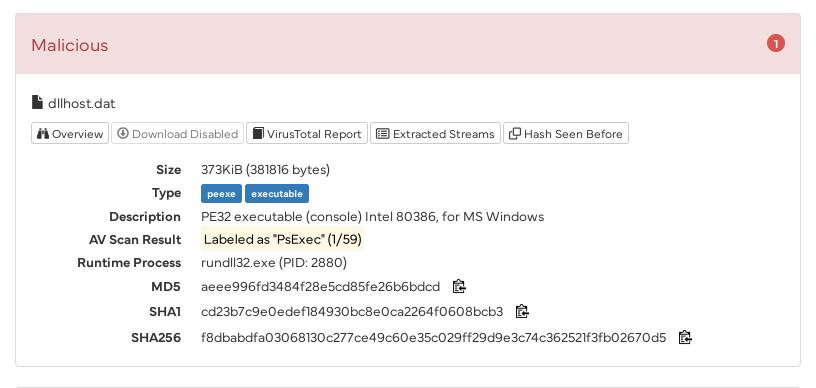
String	Context	Stream UID
192.168.56.11	Domain/IP reference	00026671-00002512-16111-836-0040375B
127.0.0.1	Domain/IP reference	14041-3-10007D6F

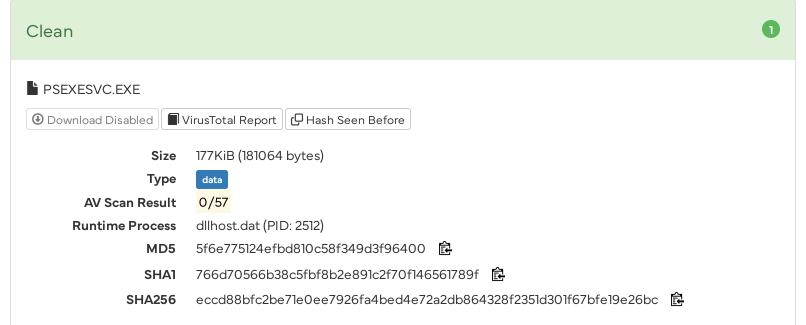
Extracted Strings

Extracted Strings						
Q Search	All Details: Off					
① Download All Memory Strings (17KiB)						
All Strings (1350) Interesting (575) 027cc450ef5f8c5f653329 cmd.exe (2) dllhost.dat:2	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	e (1)					
wevtutil.exe (4)						
"/TR "%WINDIR%\system32\shutdown.exe/r/f"/ST 07:45"						
"%WINDIR%\027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745.bin.dll",#11\PSPUBWS:123456"	0 "PSPUBWS-PC					
%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.						

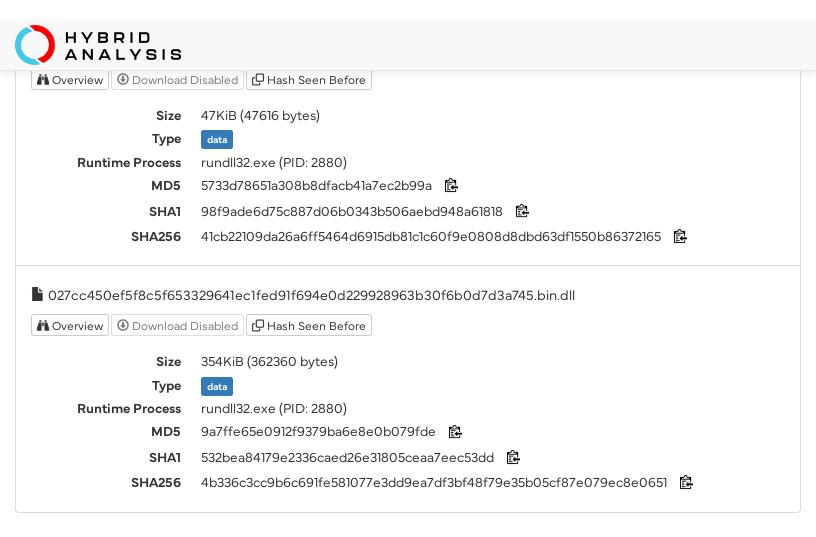


Extracted Files





Informative Selection



Notifications

Runtime



Community

Sandip commented 7 years ago

#Petya

Amigo commented 7 years ago

analysis.com/sample/027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745?environmentId=100



#Fettia (Notretya, Notifetya) Kansoniware hxxps.//lu-ransoniware.blogspot.com/201//00/petya-nsa-ee-ransomware.html

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

1 You must be logged in to submit a comment.

© 2024 Hybrid Analysis — Hybrid Analysis Terms and Conditions of Use — Hybrid Analysis Privacy Notice — Site Notice — Your Privacy Choices 🕖 — Contact Us