

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

 Overview

 Sample not shared

 Downloads ▾

 External Reports ▾

 Re-analyze

 Post

 Link

 E-Mail


 Hash Not Seen Before

 No similar samples

 Report False-Positive

 Request Report Deletion

Incident Response

 Risk Assessment

Network Behavior Contacts 3 domains and 2 hosts.  View all details

 MITRE ATT&CK™ Techniques Detection


This report has 14 indicators that were mapped to 9 attack techniques and 5 tactics.  View all details

Additional Context

 OSINT

External References <https://www.intezer.com/iron-cybercrime-group-under-the-scope-2/>

Indicators

 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

All indicators are available only in the private webinterface or standalone version

Suspicious Indicators

13

Anti-Reverse Engineering



PE file is packed with UPX	▼
Environment Awareness	
Contains ability to query CPU information	▼
External Systems	
Found an IP/URL artifact that was identified as malicious by at least one reputation engine	▼
Installation/Persistence	
Drops executable files	▼
Writes data to a remote process	▼
Network Related	
Found potential IP address in binary/memory	▼
Uses a User Agent typical for browsers, although no browser was ever launched	▼
Uncategorized Behavior	
PE file has a section name known to be used by a packer/protector	▼
Unusual Characteristics	
Entrypoint in PE header is within an uncommon section	▼
Imports suspicious APIs	▼
Hiding 2 Suspicious Indicators	
All indicators are available only in the private webinterface or standalone version	



Queries kernel debugger information



Queries the internet cache settings (often used to hide footprints in index.dat or internet cache)



Anti-Reverse Engineering

Contains ability to register a top-level exception handler (often used as anti-debugging trick)



PE file contains zero-size sections



Environment Awareness

Contains ability to query machine time



Possibly tries to detect the presence of a debugger



Reads the active computer name



Reads the cryptographic machine GUID



General

Contacts domains



Contacts server



Creates mutants



GETs files from a webserver



Opened the service control manager



Runs shell commands




Spawns new processes



Spawns new processes that are not known child processes




Installation/Persistence

	
Dropped files	▼
Monitors specific registry key for changes	▼
Touches files in the Windows directory	▼
Network Related	
Found potential URL in binary/memory	▼
Pattern Matching	
Detected EICAR test file artifact	▼
Spyware/Information Retrieval	
Accesses potentially sensitive information from local browsers	▼
System Security	
Creates or modifies windows services	▼
Modifies proxy settings	▼
Opens the Kernel Security Device Driver (KsecDD) of Windows	▼
Queries sensitive IE security settings	▼
Unusual Characteristics	
Matched Compiler/Packer signature	▼

File Details

All Details: ☐ Off

 PICUS_ee5eca8648e45e2fea9dac0d920ef1a1792d8690c41ee7f20343de1927cc88b9.exe



009.exe

Size

234KiB (239616 bytes)

Type

peexe

executable

Description

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

Architecture

WINDOWS

SHA256

ee5eca8648e45e2fea9dac0d920ef1a1792d8690c41ee7f20343de1927cc88b9

Compiler/Packer

Netopsystems FEAD Optimizer 1

Resources

Language

CHINESE

Icon

Visualization

Input File (PortEx)

Version Info

LegalCopyright

Copyright (C) 2017 Mozilla Corporation All rights reserved.

InternalName

Kingsoft Install Tool

FileVersion

2.1.4.4

CompanyName

Mozilla Corporation

ProductName

Kingsoft Install Tool

ProductVersion

2.1.4.4

FileDescription

Kingsoft Install Tool

OriginalFilename

Kingsoft Install Tool

Translation

0x0409 0x04b0

Classification (TrID)

- 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	7cb6dac2dfb51aaf4dc15899d45cd751

Name	.rsrc
Entropy	5.10204343895
Virtual Address	0x4f000
Virtual Size	0x1f000
Raw Size	0x1e400
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)
- cmd.exe** cmd /c rundll32 "%LOCALAPPDATA%\Js9mDPd8.dat",Launch (PID: 1260)
- rundll32.exe** rundll32 "%LOCALAPPDATA%\Js9mDPd8.dat",Launch (PID: 2428)



Network Analysis

DNS Requests

Login to Download DNS Requests (CSV)

Domain	Address	Registrar	Country
www.amazon.com 	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 	80 TCP	rundll32.exe PID: 2428	United States
45.76.228.115 	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	dazqc4f140wtl.cloudfront.net/ZZYO	GET /ZZYO HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: dazqc4f140wtl.cloudfront.net Connection: Keep-Alive Cache-Control: no-cache 200 OK More Details
45.76.228.115:80 (www.amazon.com)	GET	www.amazon.com/s/ref=nb_sb_noss_1/167-3294888-0262949/field-keyword=s=books	GET /s/ref=nb_sb_noss_1/167-3294888-0262949/field-keyword=s=books HTTP/1.1 Host: www.amazon.com Accept: */*Cookie: skin=noskin;session-token=AfY9lslHq2xoFOWlrifFI6shGHsYiDXGdkmUFt9sQTRN8PhYkJD34KB4pYz2ilyM5Wqt/EdlH+BGaVicl62zv g8vwO/3zxNxRfWpPvFrJet3mZI2NLVLTjb6ul1Wn/Q20mVxFVks tqiBgaplCK33KaZulq+a850yb04WnF/mq1Y=csm-hit=s-24KU11BB82RZSYGJ3BDK 1419899012996 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Connection: Keep-Alive Cache-Control: no-cache 200 OK More Details

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 (TCP)	A Network Trojan was detected	ETPRO TROJAN Cobalt Strike Trial HTTP Response Header (EICAR)	2826143

ET rules applied using Suricata. Find out more about proofpoint ET Intelligence [here](#).

Extracted Strings

Q

Search

All Details:

Off

Download All Memory Strings (13KiB)

All Strings (1024)

Interesting (311)

network.pcap (558)

PICUS_ee5eca8648e45e... (1)

cmd.exe:1260 (1)

PICUS_ee5eca8648e45e... (1)

PCAP (5)

rundll32.exe:2428 (206)

screen_0.png (3)

cmd.exe (1)

rundll32.exe (1)

!"#\$%&'()*+,-./0123

!"#\$%&'()*+,-./0123456789;<=>?@

%%IMPORT%%

%d is an x64 process (can't inject x86 content)

%d is an x86 process (can't inject x64 content)

%s.2%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x.%x%x.%s

%s.2%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x.%x%x.%s

%s.4%08x%08x%08x%08x%08x.%08x%08x%08x%08x%08x%08x%08x.%08x%08x%08x%08x%08x%08x.%08x%08x%08x%08x%08x%08x.%08x%08x%08x%08x%08x%08x.%x%x.%s

Extracted Files

Malicious

1

Js9mDPd8.dat

Overview

User Did Not Share

Extended File Details

VirusTotal Report

Extracted Streams

Hash Not Seen Before

Size

57KiB (57856 bytes)

Type

peDll

executable

Description

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


AV Scan Result

Labeled as "Trojan.Generic" (31/66)


Runtime Process

PICUS_ee5eca8648e45e2fea9dac0d920ef1a1792d8690c41ee7f20343de1927cc88b9.exe (PID: 984)


MD5

ab4febc09e14e61eb7537da718e1571c 


SHA1

64a43de008ae3f202358ecbd9309fb3e05badbab 

SHA256

e5de6043274b46df45c51a9aba7e6c71a053f09877d50448d15ea72dbe4487eb 

Notifications

Runtime	
Environment	1
Sample was not shared with the community	



Community

! There are no community comments.

! You must be logged in to submit a comment.

