PICUS_ee5eca8648e45e2fea9dac0d920ef1a1792d869...

malicious

This report is generated from a file or URL submitted to this webservice on July 16th 2018 00:13:49 (UTC)
Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1
Report generated by Falcon Sandbox © Hybrid Analysis

Threat Score: 100/100
AV Detection: 77%
Labeled as: Trojan.Swrort

Post Link E-Mail

Overview | Sample not shared | Downloads | External Reports
Re-analyze | 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

Multiple malicious artifacts seen in the context of different hosts

Hiding 1 Malicious Indicators

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

Suspicious Indicators 13

Anti-Reverse Engineering

PE file has unusual entropy sections

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/Persistance

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 webservice or standalone version

Informative 28

Anti-Detection/Stealthyness

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 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/Persistance

- Connects to LPC ports
- 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

PICUS_ee5eca8648e45e2fea9dac0d920ef1a1792d8690c41ee7f20343de1927cc88b9.exe

Filename	PICUS_ee5eca8648e45e2fea9dac0d920ef1a1792d8690c41ee7f20343de1927cc88b9.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

Name	Entropy	Virtual Address	Virtual Size	Raw Size	MD5	Characteristics
UPX0	0	0x1000	0x32000	0x0	d41d8cd98f00b204e9800998ecf8427e	-
UPX1	7.85766529255	0x33000	0x1c000	0x1c000	7cb6dac2dfb51aaf4dc15899d45cd751	-
.rsrc	5.10204343895	0x4f000	0x1f000	0x1e400	5ac66730e958194609725c846e661686	-

File Resources

Name	RVA	Size	Type	Language

RT_ICON	0x6545c	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4260130648, next used block 3421270877	Chinese
RT_ICON	0x66508	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 14110783, next used block 14110783	Chinese
RT_ICON	0x68ab4	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40,	Chinese

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)
      - rundll32.exe rundll32 "%LOCALAPPDATA%\Js9mDPd8.dat",Launch (PID: 2428)

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

Network Analysis

DNS Requests

Login to Download DNS Requests (CSV)

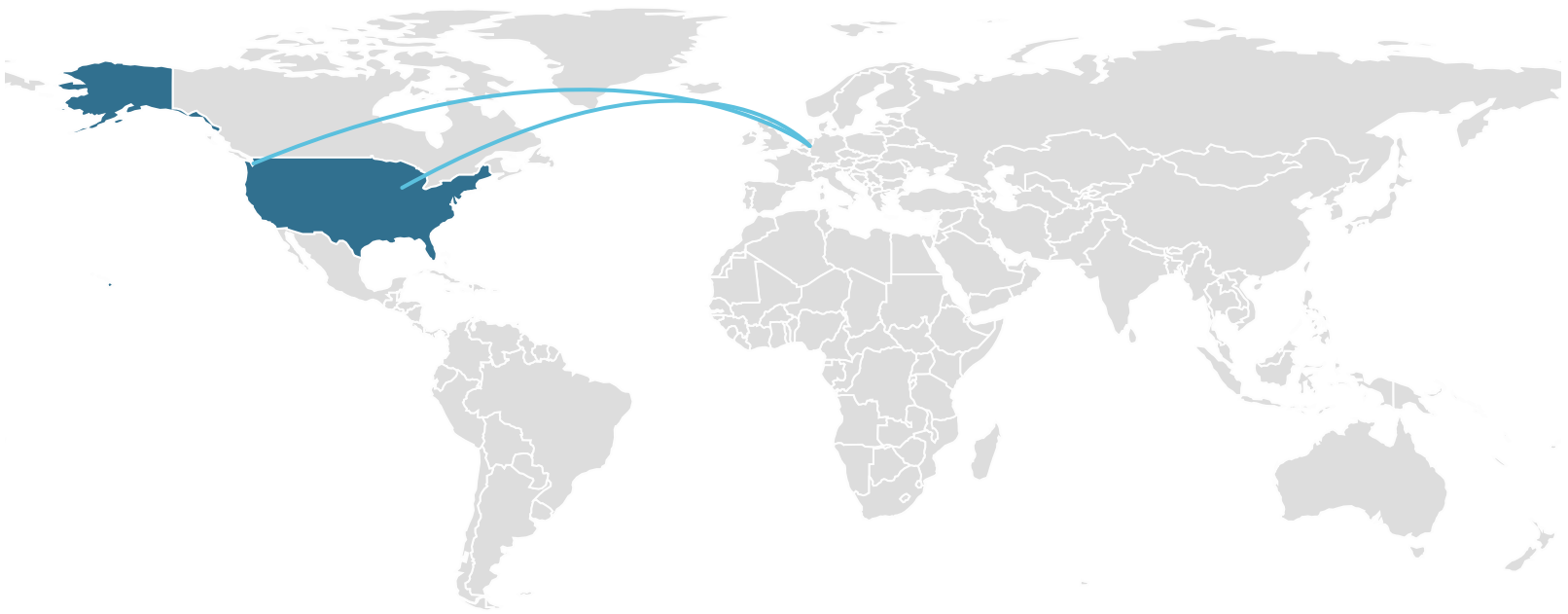
Domain	Address	Registrar	Country
www.amazon.com OSINT	45.76.228.115	MarkMonitor, Inc. Organization: Amazon Technologies, Inc. Name Server: NS1.P31.DYNECT.NET Creation Date: Tue, 01 Nov 1994 00:00:00 GMT	United States
dazqc4f140wtl.cloudfront.n et	13.32.66.49 TTL: 59	MarkMonitor, Inc.	United States

Contacted Hosts

Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
13.32.66.49 OSINT	80 TCP	rundll32.exe PID: 2428	United States
45.76.228.115 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	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-keywords=books	GET /s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books HTTP/1.1 Host: www.amazon.com Accept: */*Cookie: skin=noskin;session-token=AfY9lsIHq2xoFOWlrifFI6shGHsYiDXGdkmUFt9sQTRN8PhYkJD34KB4pYz2ilyM5Wqt/EdlH+BGaVicI62zVg8vwO/3zxNxRfWpPvFrJet3mZI2NLVLtjb6uI1Wn/Q20mVxFVkStqiBgaplCK33KaZulq+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 -> 8.8.8.8:53 (UDP)	A Network Trojan was detected	ETPRO TROJAN Malicious Domain CStrike C2 (blockbitcoin .com in DNS Lookup)	2828268
local ->	A Network Trojan was detected	ETPRO TROJAN Cobalt Strike Malleable C2 Amazon	2826178

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

Search

All Details: Off

Download All Memory Strings (13KiB)

All Strings (1024) | Interesting (311) | network.pcap (558) | PICUS_ee5eca8648e45e... | cmd.exe:1260 (1) | PICUS_ee5eca8648e45e... | 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%08x%08x.%x%x.%s

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

%s.3%08x%08x%08x%08x%08x%08x%08x.%08x%08x%08x%08x%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.%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

Environment 1

Sample was not shared with the community

Community

There are no community comments.

You must be logged in to submit a comment.