HYBRID ANALYSIS

ff808d0a12676bfac88fd26f955154f8884f2bb7c534b99...

malicious

This report is generated from a file or URL submitted to this webservice on February 3rd 2018 14:25:47 (UTC) and action script *Heavy Anti-Evasion*
Guest System: Windows 7 32 bit, Professional, 6.1 (build 7601), Service Pack 1
Report generated by Falcon Sandbox © Hybrid Analysis

Threat Score: 100/100
AV Detection: 96%
Labeled as: Trojan.Sofacy

X Post | Link | E-Mail

Overview | Sample unavailable | Downloads | External Reports | Re-analyze | Hash Seen Before | No similar samples | Report False-Positive | Request Report Deletion

Incident Response

Risk Assessment

Fingerprint	Reads the active computer name
Evasive	Possibly tries to evade analysis by sleeping many times
Network Behavior	Contacts 1 domain and 1 host. View all details

Indicators

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

Malicious Indicators

5

External Systems

Sample was identified as malicious by a large number of Antivirus engines

Sample was identified as malicious by at least one Antivirus engine

The analysis extracted a file that was identified as malicious

Unusual Characteristics

Checks for a resource fork (ADS) file

Hiding 1 Malicious Indicators

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

Suspicious Indicators

14

Anti-Detection/Stealthyness

Queries kernel debugger information

Queries process information

Anti-Reverse Engineering

PE file has unusual entropy sections

Environment Awareness

Contains ability to query CPU information

Possibly tries to evade analysis by sleeping many times

Reads the active computer name

General

Opened the service control manager

Installation/Persistance

Drops executable files

Contains ability to enumerate processes/modules/threads

System Security

Modifies proxy settings

Queries sensitive IE security settings

Unusual Characteristics

Drops cabinet archive files

Imports suspicious APIs

PE file contains unusual section name

Informative 23

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

Queries volume information

Queries volume information of an entire harddrive

Reads the registry for installed applications

External Systems

General

Accesses Software Policy Settings

Accesses System Certificates Settings

Contacts domains

Contacts server

Creates mutants

Reads Windows Trust Settings

Spawns new processes

Installation/Persistance

Connects to LPC ports

Dropped files

Touches files in the Windows directory

Network Related

Found potential URL in binary/memory

Pattern Matching

Code classification distribution is known to appear in malware

Spyware/Information Retrieval

Found a reference to a known community page

System Security

Unusual Characteristics

Matched Compiler/Packer signature

File Details

All Details: Off

ff808d0a12676bfac88fd26f955154f8884f2bb7c534b9936510fd6296c543e8

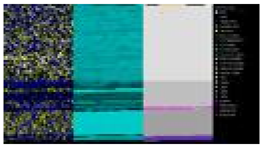
Filename	ff808d0a12676bfac88fd26f955154f8884f2bb7c534b9936510fd6296c543e8
Size	131KiB (133632 bytes)
Type	peexe executable
Description	PE32 executable (GUI) Intel 80386, for MS Windows
Architecture	WINDOWS
SHA256	ff808d0a12676bfac88fd26f955154f8884f2bb7c534b9936510fd6296c543e8
Compiler/Packer	VC8 -> Microsoft Corporation
PDB Pathway	

Resources

Icon

Visualization

Input File (PortEx)



Classification (TrID)

- 43.5% (.DLL) Win32 Dynamic Link Library (generic)
- 29.8% (.EXE) Win32 Executable (generic)
- 13.2% (.EXE) Generic Win/DOS Executable
- 13.2% (.EXE) DOS Executable Generic
- 0.0% (.CEL) Autodesk FLIC Image File (extensions: flc, fli, cel)

File Sections

Name	.text
Entropy	6.66861255711
Virtual Address	0x1000
Virtual Size	0x121b9
Raw Size	0x12200
MD5	1e6061f4d4535374e68e83c19f18f807

Name	.rdata
Entropy	5.24761474655
Virtual Address	0x14000
Virtual Size	0x6984
Raw Size	0x6a00
MD5	0a7b4d817733b96f078fbffb36f61d7f

Name	.data
Entropy	7.73823276185
Virtual Address	0x1b000
Virtual Size	0x6e58
Raw Size	0x6600
MD5	b70fd6a5b034bac4ea8385ee7fa1ac3a

Name	.gfids
Entropy	1.66107032726
Virtual Address	0x22000
Virtual Size	0xdc
Raw Size	0x200
MD5	db95ef5847e56c561d0b6fa30f0d3af0

Name	.reloc
Entropy	6.43882540846
Virtual Address	0x23000
Virtual Size	0x1108
Raw Size	0x1200
MD5	fef4a253ec8067637653825cb5299e40

File Imports

ADVAPI32.dll KERNEL32.dll SHELL32.dll

GetSidSubAuthority

GetSidSubAuthorityCount

GetTokenInformation

OpenProcessToken

Screenshots

ℹ Loading content, please wait...

Hybrid Analysis

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

Analysed 2 processes in total (System Resource Monitor).

```
└ Input Sample (PID: 1144) 24/66
    └ rundll32.exe "%LOCALAPPDATA%\cdnver.dll",#1 (PID: 636) ⇄
```

⚙ 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
cdnverify.net OSINT	151.80.74.167	PDR Ltd. d/b/a PublicDomainRegistry.com	Italy

Contacted Hosts

Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
151.80.74.167 OSINT	443 TCP	rundll32.exe PID: 636	Italy

Contacted Countries

HTTP Traffic

No relevant HTTP requests were made.

Suricata Alerts

Event	Category	Description	SID
local -> 52.138.148.159:80 (TCP)	Misc activity	ET INFO Windows OS Submitting USB Metadata to Microsoft	2025275

local -> 52.138.148.159:80 (TCP)	Misc activity	ET INFO Windows OS Submitting USB Metadata to Microsoft	2025275
local -> 52.138.148.159:80 (TCP)	Misc activity	ET INFO Windows OS Submitting USB Metadata to Microsoft	2025275

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

Extracted Strings

Search

All Details: Off

Download All Memory Strings (8.4KiB)

All Strings (818) | Interesting (277) | ff808d0a12676bfac88fd2... | rundll32.exe (1) | network.pcap (163) | cdnver.dll.2569912557 (87) | rundll32.exe:636 (214) | ff808d0a12676bfac88fd2... | screen_0.png (4) | cdnver.bat (1)

```
"%LOCALAPPDATA%\cdnver.dll",#1
$http://g.symcb.com/crls/gtglobal.crl0!
%LOCALAPPDATA%\cdnver.bat
((((( H
)http://crl.geotrust.com/crls/secureca.crl0N
*.android.com
*.appengine.google.com
*.cloud.google.com
*.db833953.google.cn
*.gcp.gvt2.com
*.google-analytics.com
*.google.ca
```

Extracted Files

reports.

Malicious 1

cdnver.dll

Overview | Download Disabled | Extended File Details | VirusTotal Report | Extracted Streams | Hash Seen Before

Size	31KiB (31744 bytes)
Type	pedll executable
Description	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
AV Scan Result	Labeled as "Gen:Variant.Razy" (16/65)
Runtime Process	rundll32.exe (PID: 636)
MD5	aa2cd9d9fc5d196caa6f8fd5979e3f14
SHA1	5bb9f53636efafdd30023d44be1be55bf7c7b7d5
SHA256	12e6642cf6413bdf5388bee663080fa299591b2ba023d069286f3be9647547c8

Informative Selection 1

Cab3270.tmp

Overview | Download Disabled | Hash Seen Before

Size	53KiB (54018 bytes)
Type	data
Description	Microsoft Cabinet archive data, 54018 bytes, 1 file
Runtime Process	rundll32.exe (PID: 636)
MD5	06ed9a39ac55eb00dd78e416e1a804f6
SHA1	270464d1618197d86ff89184ba5ed45708d38bd9
SHA256	298bba62caa0b61a402f715bb5b8d1d28ecd0b58d9a9b6b8ae7947b39da8b1eb

Informative 3

Download Disabled | Hash Not Seen Before

Size	65B (65 bytes)
Type	text
Description	ASCII text, with no line terminators
Runtime Process	ff808d0a12676bfac88fd26f955154f8884f2bb7c534b9936510fd6296c543e8.exe (PID: 1144)
MD5	f9cbf2a3ffb4151e0bfb42d1ea6b0d66
SHA1	98d15100af8a59d3b4c573c867b06afd7062a247
SHA256	34509857a943d1dbdf730ed94413737425c44fc4849c298db82defc6e757d4f8

77EC63BDA74BD0D0E0426DC8F8008506

Overview | Download Disabled | Hash Seen Before

Size	53KiB (54018 bytes)
Type	data
Description	Microsoft Cabinet archive data, 54018 bytes, 1 file
Runtime Process	rundll32.exe (PID: 636)
MD5	06ed9a39ac55eb00dd78e416e1a804f6
SHA1	270464d1618197d86ff89184ba5ed45708d38bd9
SHA256	298bba62caa0b61a402f715bb5b8d1d28ecd0b58d9a9b6b8ae7947b39da8b1eb

Tar3271.tmp

Download Disabled | Hash Seen Before

Size	127KiB (129994 bytes)
Type	data
Runtime Process	rundll32.exe (PID: 636)
MD5	1dfe86c61a543b557903b5eef1e4fffd
SHA1	a67a046cbacff99f557462256a34b7672be70c0e
SHA256	96e552c153dcfccf832a868a03390597606401829f96c64108df9d5874075355

Notifications

Community

There are no community comments.

You must be logged in to submit a comment.