

ff808d0a12676bfac88fd26f955154f8884f2bb7c534b9...


malicious

This report is generated from a file or URL submitted to this webservice on February 3rd 2018 14:25:47 Threat Score: 100/100 (UTC) and action script *Heavy Anti-Evasion* AV Detection: 96% Guest System: Windows 7 32 bit, Professional, 6.1 (build 7601), Service Pack 1 Labeled as: Trojan.Sofacy Report generated by Falcon Sandbox © Hybrid Analysis

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

- ✂️ Post
- 🔗 Link
- 📧 E-Mail

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 Indicators5

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

General

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 Indicators14

Anti-Detection/Stealthyness

Queries kernel debugger information

Queries process information

Incident Response

Indicators

- Malicious (5)
- Suspicious (14)
- Informative (23)

File Details

Screenshots (1)

Hybrid Analysis (2)

Network Analysis

Extracted Strings

Extracted Files (6)

Notifications

Community (0)

Back to top































À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. Politique d'utilisation des cookies

Paramètres des cookies

Tout refuser

Autoriser tous les cookies

 <div>HYBRID ANALYSIS</div>	   	 Request Info 	<div></div> <div> </div>
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/Persistence			
Drops executable files			
Spyware/Information Retrieval			
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			
Detected Suricata Alert			
General			
Accesses Software Policy Settings			

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

HYBRID ANALYSIS

Request Info

Creates mutants

Reads Windows Trust Settings

Spawns new processes

Installation/Persistence

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


Opens the Kernel Security Device Driver (KsecDD) of Windows


Unusual Characteristics

Matched Compiler/Packer signature

File Details


All Details: ☐ Off

 ff808d0a12676bfac88fd26f955154f8884f2bb7c534b9936510fd6296c543e8

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

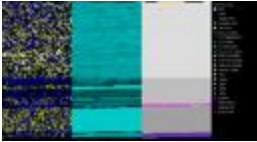
Resources

Icon



Visualization

Input File (PortEx)



À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

File Sections

Name	Entropy	Virtual Address	Virtual Size	Raw Size	MD5	Characteristics
.text	6.66861255711	0x1000	0x121b9	0x12200	1e6061f4d4535374e68e83c19f18f807	-
.rdata	5.24761474655	0x14000	0x6984	0x6a00	0a7b4d817733b96f078fbffb36f61d7f	-
.data	7.73823276185	0x1b000	0x6e58	0x6600	b70fd6a5b034bac4ea8385ee7fa1ac3a	-
.gfids	1.66107032726	0x22000	0xdc	0x200	db95ef5847e56c561d0b6fa30f0d3af0	-
.reloc	6.43882540846	0x23000	0x1108	0x1200	fef4a253ec8067637653825cb5299e40	-


File Imports

ADVAPI32.dll	KERNEL32.dll	SHELL32.dll
AdjustTokenPrivileges		
GetSidSubAuthority		
GetSidSubAuthorityCount		
GetTokenInformation		
OpenProcessToken		

Screenshots







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	151.80.74.167	PDR Ltd. d/b/a PublicDomainRegistry.com	 Italy




À PROPOS DES COOKIES SUR CE SITE


En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)





HYBRID


ANALYSIS

 ▾


 ▾


 ▾

 ▾

 Request Info

▾







▾

151.80.74.167

443

rundll32.exe

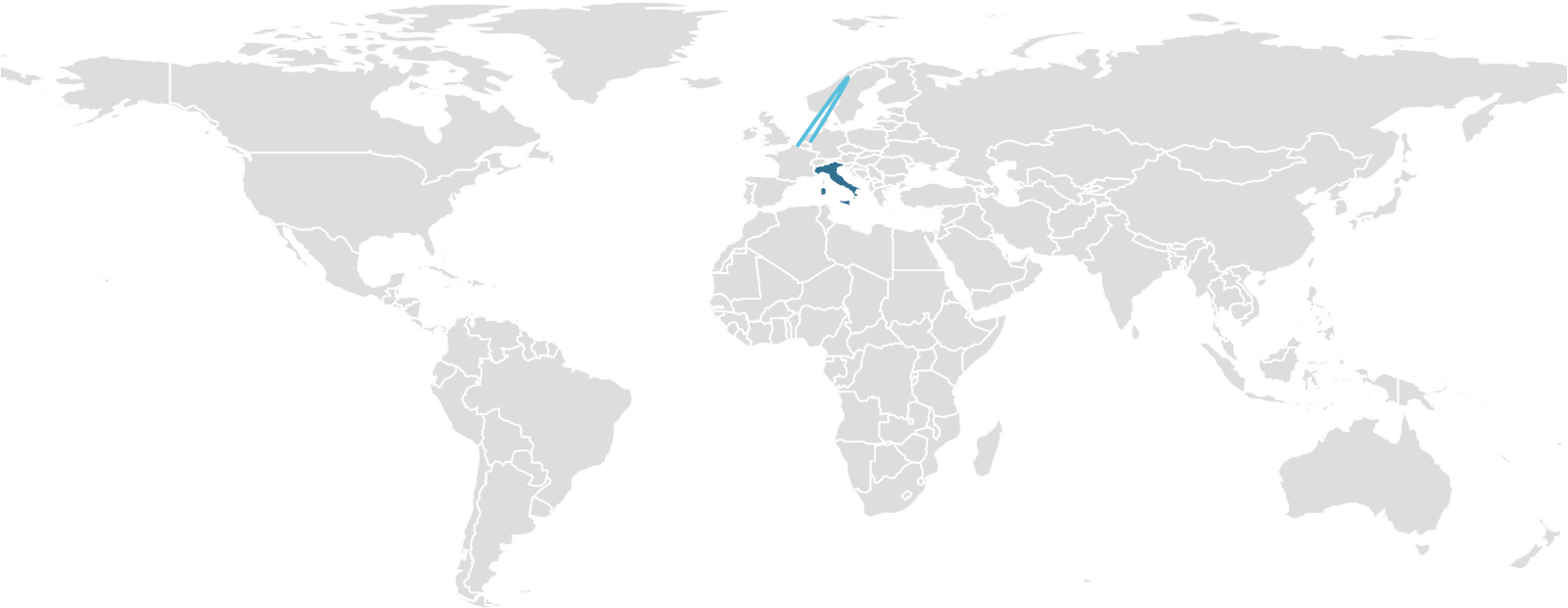
 Italy

 OSINT

TCP

PID: 636

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
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

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)



HYBRID

ANALYSIS

Request Info

Q

×

^appengine.google.com

*.cloud.google.com

*.db833953.google.cn

*.gcp.gvt2.com


*.google-analytics.com

*google.ca

Extracted Files

i Displaying 5 extracted file(s). The remaining 1 file(s) are available in the full version and XML/JSON reports.

Malicious1

 cdnver.dll

Overview

Download Disabled

Extended File Details


VirusTotal Report

Extracted Streams

Hash Seen Before

Size	31KiB (31744 bytes)
Type	peDllexecutable
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 Selection1

 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

Informative3

 cdnver.bat

Download Disabled

Hash Not Seen Before

Size	65B (65 bytes)
Type	text
Description	ASCII text, with no line terminators

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

HYBRID ANALYSIS

Request Info

OverviewDownload DisabledHash 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 DisabledHash Seen Before

Size

127KiB (129994 bytes)

Type

data

Runtime Process

rundll32.exe (PID: 636)

MD5

1dfe86c61a543b557903b5eef1e4fffd

SHA1

a67a046cbacff99f557462256a34b7672be70c0e

SHA256

96e552c153dcfccf832a868a03390597606401829f96c64108df9d5874075355

Notifications

Runtime

Community

There are no community comments.

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

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

Page 7 of 7