ID: 509307
Sample Name: 1ca07290000.dll
Cookbook: default.jbs
Time: 11:46:07
Date: 26/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report 1ca07290000.dll 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Threatname: Ursnif 3
Yara Overview 4
Initial Sample 4
Sigma Overview 4
Jbx Signature Overview 4
AV Detection: 4
Key, Mouse, Clipboard, Microphone and Screen Capturing: 4
E-Banking Fraud: 4
Hooking and other Techniques for Hiding and Protection: 5
Stealing of Sensitive Information: 5
Remote Access Functionality: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 7
Contacted Domains 8
Contacted IPs 8
General Information 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 8
IPs 8
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
General 9
File Icon 9
Static PE Info 9
General 9
Entrypoint Preview 10
Data Directories 10
Sections 10
Network Behavior 10
Code Manipulations 10
Statistics 10
Behavior 10
System Behavior 10
Analysis Process: loaddll64.exe PID: 5912 Parent PID: 5740 10
General 10
File Activities 11
Analysis Process: cmd.exe PID: 6672 Parent PID: 5912 11
General 11
File Activities 11
Analysis Process: rundll32.exe PID: 4668 Parent PID: 5912 11
General 11
File Activities 11
Analysis Process: rundll32.exe PID: 4536 Parent PID: 6672 11
General 11
File Activities 12
Disassembly 12
Code Analysis 12

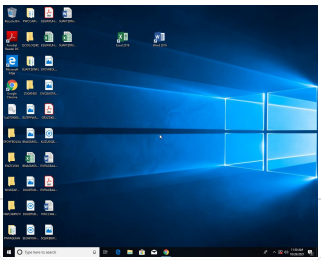
Windows Analysis Report 1ca07290000.dll

Overview

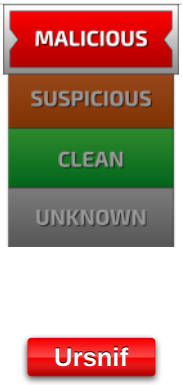
General Information

Sample Name:	1ca07290000.dll
Analysis ID:	509307
MD5:	db1debd01a99ae..
SHA1:	d8dae1e45d0e73..
SHA256:	c838678b643d9d..
Tags:	exe gozi
Infos:	

Most interesting Screenshot:



Detection

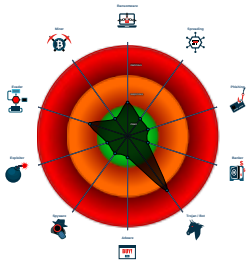


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Ursnif
- PE file does not import any functions
- Tries to load missing DLLs
- Program does not show much activi…
- Creates a process in suspended mo…
- Checks if the current process is bein…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 5912 cmdline: loaddll64.exe 'C:\Users\user\Desktop\1ca07290000.dll' MD5: E0CC9D126C39A9D2FA1CAD5027EBBD18)
  - cmd.exe (PID: 6672 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\1ca07290000.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 4536 cmdline: rundll32.exe 'C:\Users\user\Desktop\1ca07290000.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 4668 cmdline: rundll32.exe C:\Users\user\Desktop\1ca07290000.dll,#1 MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"zwBhS9EXG4wSzAPHZIrWB6YHrz9PLQzX8GBJoOHTrNVk5RNm3SNJGHZOtL3P+FOPmytupVYlNLxqIsCPxVGg0S7BHBxVPc+c9XCYMN0GU4mStoXt11C2neZnN/s4N9D0KHruBdqEWlUxoG1xZu3/l3GA6g+z6sOyfECBKCmsR7vBQJoX
YxCKYgil/TDhyyBMlmgdL+x5SnxnQC9fvRzaaqMl9gg0WC3n7bBorLCbZnrez2Ru1vgSTuycXovATnjqwPRfzz5ZhOhgTK35VFb6fXEvfMqtJdb27F2Zjdu3Us+MOfpJZa4I8yaUTnwgXADo1ukJmJpQ5nvljHcvz3E+qUS2SBIAqLUyM
E73bXxMiww=",
  "c2_domain": [
    "art.microsoftsofymicrosoftsoft.at",
    "r23cirt55ysvtdvl.onion",
    "fop.langoonik.com",
    "poi.redhatbabby.at",
    "pop.biopiof.at",
    "l46t3vgvmtx5wxe6.onion",
    "v10.avyanok.com",
    "apr.intoolkom.at",
    "fgx.dangerboy.at"
  ],
  "ip_check_url": [
    "curlmyip.net",
    "ident.me",
    "l2.io/ip",
    "whatismyip.akamai.com"
  ],
  "serpent_key": "kTOVYpceZWWByuJ0",
  "server": "580",
  "sleep_time": "5",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "600",
  "time_value": "600",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "240",
  "SetWaitableTimer_value(CRC_SENDTIMEOUT)": "300",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "240",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "3500",
  "SetWaitableTimer_value": "60"
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
1ca07290000.dll	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

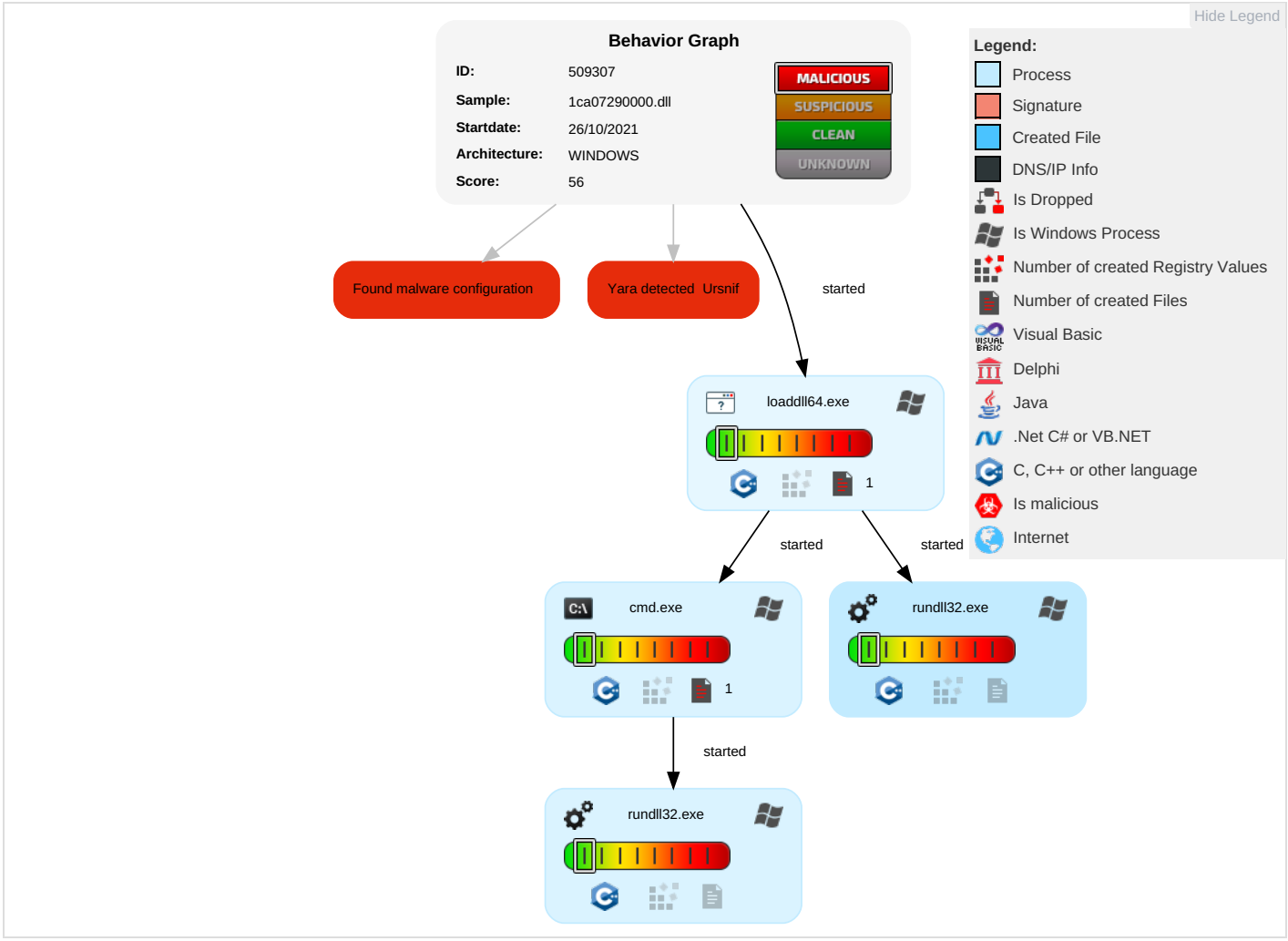
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1 1	Virtualization/Sandbox Evasion 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Rundll32 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	System Information Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

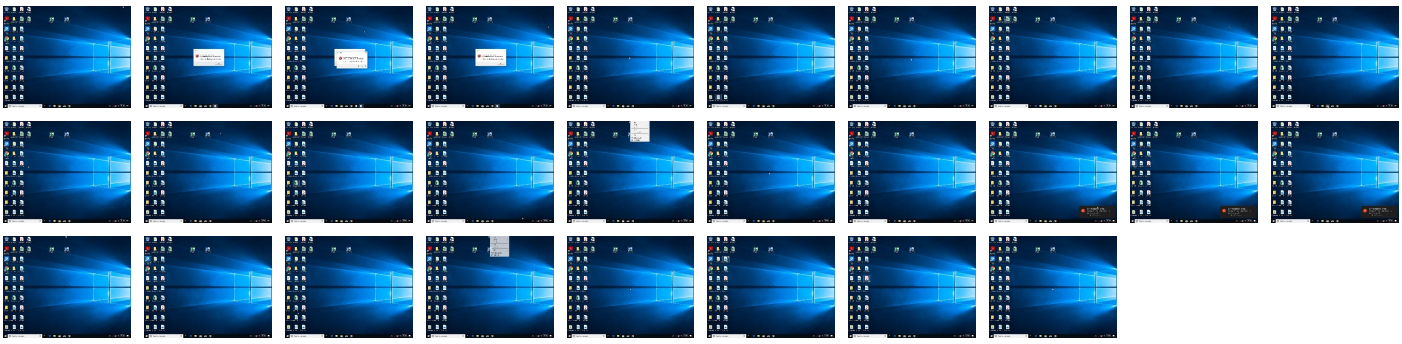
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	509307
Start date:	26.10.2021
Start time:	11:46:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1ca07290000.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.troj.winDLL@7/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	MS-DOS executable
Entropy (8bit):	6.449565836821331
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 84.88% • Win64 Executable (generic) (12005/4) 9.99% • DOS Executable Borland Pascal 7.0x (2037/25) 1.69% • Generic Win/DOS Executable (2004/3) 1.67% • DOS Executable Generic (2002/1) 1.67%
File name:	1ca07290000.dll
File size:	247808
MD5:	db1debd01a99ae5b44a4ea5f8d8643d1
SHA1:	d8dae1e45d0e73d650193304763ecf41390940d3
SHA256:	c838678b643d9d61156280adf5ebee54112496778820a4e93bfcfd72a93ea8d6
SHA512:	40b719ef06245136b8bae6bc035bc97a8f40dcaaca90bccecd8d945b958c890fab0bcd957549a78f1f2454504d2dafe6381e5b7421088bdf811f2bc0b97d6c41
SSDEEP:	6144:2W/TYr/Pbqk2ZFOY/ybb00h2ETEzIwt7WtBk4S2Ui:2W/TYLPbqRul5dQzPt7WtBC2
File Content Preview:	MZ..... ....PE..d..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x18001fa5c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui

General

Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	
Time Stamp:	0x61486E8D [Mon Sep 20 11:20:45 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2fbbc	0x2fc00	False	0.578472676702	data	6.40333341974	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x31000	0x6837	0x6a00	False	0.372383549528	data	5.26054475062	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x38000	0x1e40	0x1800	False	0.334147135417	lif file	3.91809869296	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x3a000	0x1908	0x1a00	False	0.525540865385	data	5.32109686589	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bss	0x3c000	0x1f50	0x2000	False	0.964477539062	data	7.89665470155	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x3e000	0x1000	0xc00	False	0.529947916667	data	4.87572792309	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 5912 Parent PID: 5740

General

Start time:	11:47:00
Start date:	26/10/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\1ca07290000.dll'
Imagebase:	0x7ff6002d0000
File size:	1136128 bytes
MD5 hash:	E0CC9D126C39A9D2FA1CAD5027EBBD18
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 6672 Parent PID: 5912

General

Start time:	11:47:01
Start date:	26/10/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\1ca07290000.dll',#1
Imagebase:	0x7ff6fc100000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 4668 Parent PID: 5912

General

Start time:	11:47:01
Start date:	26/10/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\1ca07290000.dll,#1
Imagebase:	0x7ff64d5d0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 4536 Parent PID: 6672

General

Start time:	11:47:01
Start date:	26/10/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\1ca07290000.dll',#1
Imagebase:	0x7ff64d5d0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Disassembly

Code Analysis