

JoeSandbox Cloud BASIC



ID: 432617

Sample Name: 190ca530000.dll

Cookbook: default.jbs

Time: 15:43:25

Date: 10/06/2021

Version: 32.0.0 Black Diamond


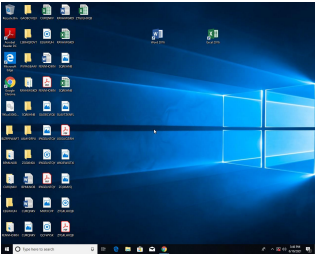
Table of Contents

Table of Contents	2
Analysis Report 190ca530000.dll	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Overview	3
Initial Sample	3
Sigma Overview	3
Signature Overview	3
AV Detection:	4
Key, Mouse, Clipboard, Microphone and Screen Capturing:	4
E-Banking Fraud:	4
Hooking and other Techniques for Hiding and Protection:	4
Stealing of Sensitive Information:	4
Remote Access Functionality:	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	7
Contacted Domains	7
URLs from Memory and Binaries	7
Contacted IPs	7
General Information	7
Simulations	8
Behavior and APIs	8
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	9
Static PE Info	9
General	9
Entrypoint Preview	9
Data Directories	9
Sections	9
Network Behavior	9
Code Manipulations	10
Statistics	10
Behavior	10
System Behavior	10
Analysis Process: loadll64.exe PID: 6544 Parent PID: 6012	10
General	10
File Activities	10
Analysis Process: cmd.exe PID: 6552 Parent PID: 6544	10
General	10
File Activities	10
Analysis Process: rundll32.exe PID: 6560 Parent PID: 6544	10
General	10
File Activities	11
Analysis Process: rundll32.exe PID: 6572 Parent PID: 6552	11
General	11
File Activities	11
Disassembly	11
Code Analysis	11

Analysis Report 190ca530000.dll

Overview

General Information

Sample Name:	190ca530000.dll
Analysis ID:	432617
MD5:	6b8aeadf5f9a3ed..
SHA1:	f76f9c3f90fcb142..
SHA256:	fc988ef7e8247da..
Tags:	exe gozi
Infos:	
Most interesting Screenshot:	
	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

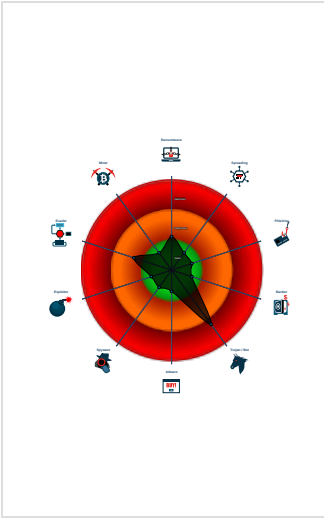
Ursnif

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub...
- Multi AV Scanner detection for subm...
- Yara detected Ursnif
- Machine Learning detection for samp...
- Checks if the current process is bein...
- Creates a process in suspended mo...
- PE file does not import any functions
- Program does not show much activi...
- Tries to load missing DLLs

Classification



Process Tree

- System is w10x64
-  loadaddll64.exe (PID: 6544 cmdline: loadaddll64.exe 'C:\Users\user\Desktop\190ca530000.dll' MD5: A84133CCB118CF35D49A423CD836D0EF)
 -  cmd.exe (PID: 6552 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\190ca530000.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
 -  rundll32.exe (PID: 6572 cmdline: rundll32.exe 'C:\Users\user\Desktop\190ca530000.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
 -  rundll32.exe (PID: 6560 cmdline: rundll32.exe C:\Users\user\Desktop\190ca530000.dll,#1 MD5: 73C519F050C20580F8A62C849D49215A)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
190ca530000.dll	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

AV Detection:



Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

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:

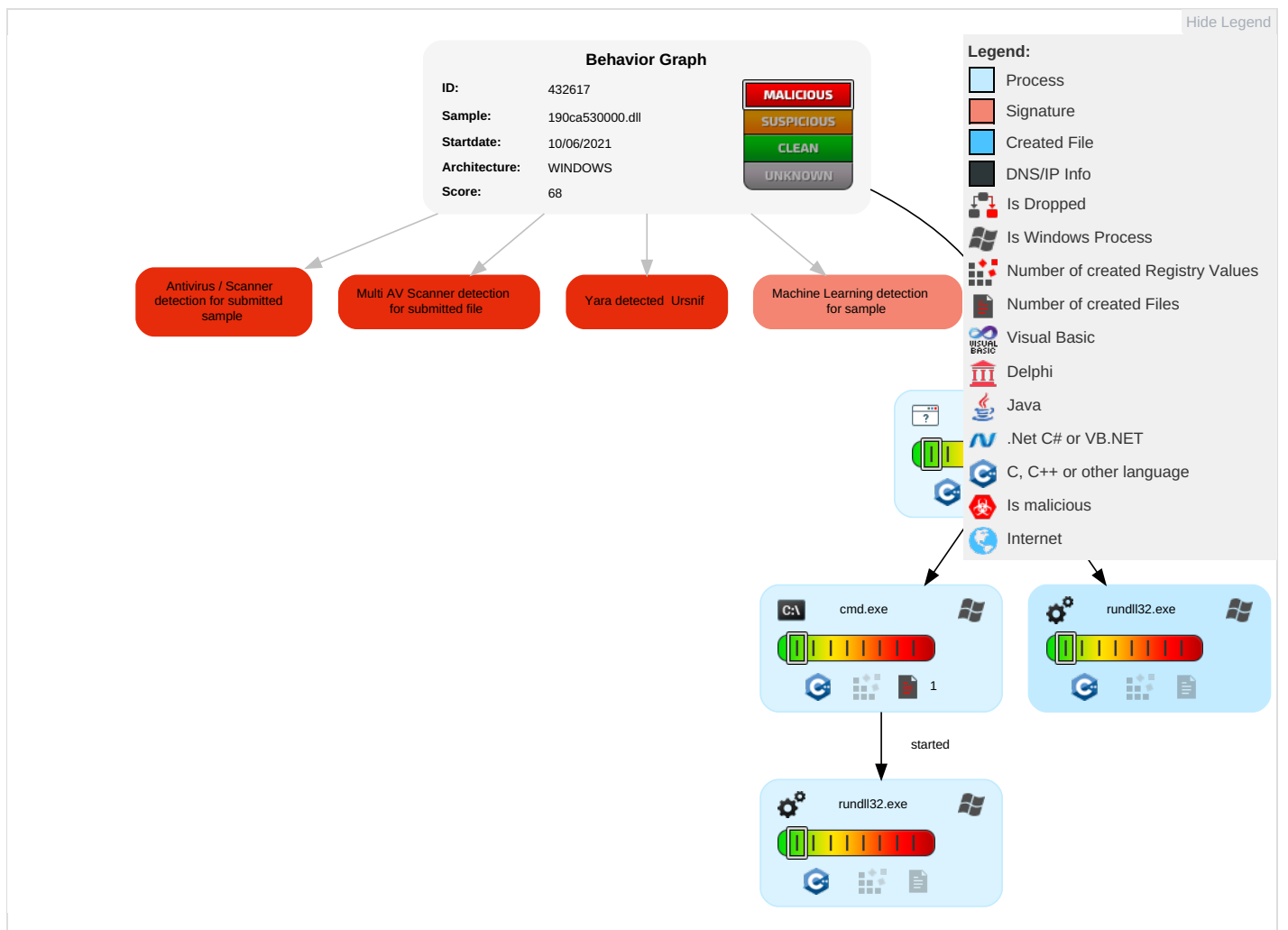


Yara detected Ursnif

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 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

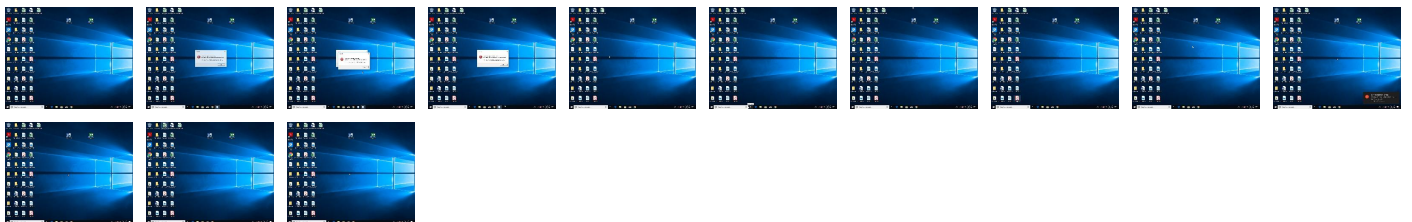
Behavior Graph



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

Source	Detection	Scanner	Label	Link
190ca530000.dll	30%	ReversingLabs	Win64.InfoStealer.Convage nt	
190ca530000.dll	100%	Avira	HEUR/AGEN.1108168	
190ca530000.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432617
Start date:	10.06.2021
Start time:	15:43:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	190ca530000.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:	19
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:	<ul style="list-style-type: none"> • HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.troj.winDLL@7/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	<ul style="list-style-type: none"> • Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none"> • Adjust boot time • Enable AMSI • Found application associated with file extension: .dll

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):	6.339393236609403
TrID:	<ul style="list-style-type: none">Win64 Dynamic Link Library (generic) (102004/3) 84.94%Win64 Executable (generic) (12005/4) 10.00%DOS Executable Borland Pascal 7.0x (2037/25) 1.70%Generic Win/DOS Executable (2004/3) 1.67%DOS Executable Generic (2002/1) 1.67%
File name:	190ca530000.dll
File size:	223744
MD5:	6b8aeadf5f9a3edc608ffba47d7f9c0d
SHA1:	f76f9c3f90fcb14261717d1f3f092811ae796877
SHA256:	fc988ef7e8247da650b64d403308dc2388ee5dd7bd2cd840fc7dd8527baecb7e
SHA512:	9ac7031e77010869542bdfe10023d066fcd0e7467e9fd82a103614ad56e91ded22c397e9d34801f802f860bdc0c40433bd93baf7f4845e879af5b9f6473c64a6

General

SSDEEP:	6144:yDf/CNUv2Qy9Vv/02/R2y7MQVSP5qMW0GpL:yD/CSv29Vv/02/R2y7zVSq/L
File Content Preview:	MZ.....PE..d...0.`...

File Icon

	
Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1800177f0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	
Time Stamp:	0x6092DF30 [Wed May 5 18:08:48 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	2
File Version Major:	5
File Version Minor:	2
Subsystem Version Major:	5
Subsystem Version Minor:	2
Import Hash:	

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2bbc8	0x2bc00	False	0.570217633929	zlib compressed data	6.34324037582	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2d000	0x4b27	0x4c00	False	0.402857730263	data	5.24853115683	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x32000	0x1f88	0x1a00	False	0.323317307692	lif file	3.89787704204	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x34000	0x17ac	0x1800	False	0.539713541667	data	5.31995773629	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bss	0x36000	0x2148	0x2200	False	0.427504595588	data	4.96451183531	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x39000	0x1000	0xa00	False	0.47265625	data	4.40942809294	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: 6544 Parent PID: 6012

General

Start time:	15:44:17
Start date:	10/06/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\190ca530000.dll'
Imagebase:	0x7ff647420000
File size:	140288 bytes
MD5 hash:	A84133CCB118CF35D49A423CD836D0EF
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: 6552 Parent PID: 6544

General

Start time:	15:44:17
Start date:	10/06/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\190ca530000.dll',#1
Imagebase:	0x7ff7180e0000
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: 6560 Parent PID: 6544

General

Start time:	15:44:18
Start date:	10/06/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\190ca530000.dll,#1
Imagebase:	0x7ff78a5b0000
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: 6572 Parent PID: 6552

General

Start time:	15:44:18
Start date:	10/06/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\190ca530000.dll',#1
Imagebase:	0x7ff78a5b0000
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