

JOESandbox Cloud BASIC



ID: 547692

Sample Name: 202c6770000.dll

Cookbook: default.jbs

Time: 13:44:08

Date: 04/01/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report 202c6770000.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
System Summary:	4
Jbx Signature Overview	4
AV Detection:	4
Key, Mouse, Clipboard, Microphone and Screen Capturing:	4
E-Banking Fraud:	4
System Summary:	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	5
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	6
Contacted Domains	7
Contacted IPs	7
General Information	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	7
IPs	7
Domains	8
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	8
Static PE Info	8
General	8
Entrypoint Preview	9
Data Directories	9
Sections	9
Network Behavior	9
Code Manipulations	9
Statistics	9
Behavior	9
System Behavior	9
Analysis Process: loadll64.exe PID: 6580 Parent PID: 1572	9
General	9
File Activities	10
Analysis Process: cmd.exe PID: 6588 Parent PID: 6580	10
General	10
File Activities	10
Analysis Process: rundll32.exe PID: 5128 Parent PID: 6580	10
General	10
File Activities	10
Analysis Process: rundll32.exe PID: 6108 Parent PID: 6588	10
General	10
File Activities	11
Disassembly	11
Code Analysis	11

Windows Analysis Report 202c6770000.dll

Overview

General Information

Sample Name:	202c6770000.dll
Analysis ID:	547692
MD5:	4b76083e201810..
SHA1:	963f018eb2d3a6a.
SHA256:	8cba0769d25a6c..
Tags:	exe gozi
Infos:	
Most interesting Screenshot:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

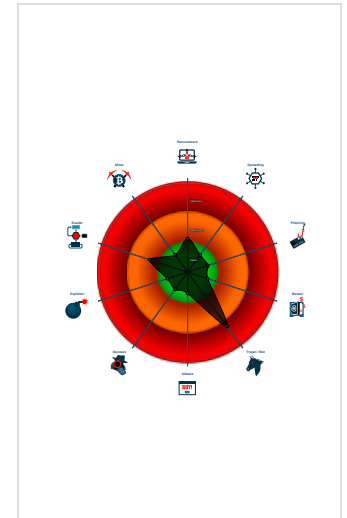
Ursnif

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Ursnif
- Sigma detected: Suspicious Call by ...
- 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: 6580 cmdline: loaddll64.exe "C:\Users\user\Desktop\202c6770000.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
 - cmd.exe (PID: 6588 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\202c6770000.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
 - rundll32.exe (PID: 6108 cmdline: rundll32.exe "C:\Users\user\Desktop\202c6770000.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
 - rundll32.exe (PID: 5128 cmdline: rundll32.exe C:\Users\user\Desktop\202c6770000.dll,#1 MD5: 73C519F050C20580F8A62C849D49215A)
- cleanup

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
  "R+UxqbV/y+ZU1c0seFgwYm43sz1DSnatV8GC7d9ajlQ+vaAx2oxbmrXwev8nSqGGA/bUt2ZkqSt/nxO6+/Ak7RHUIzazuiKwj2CwtI2KIDL8nZs0oHbZTy0zo34t4SghK0mz0ogisuhvhvEfnzRtTwTwtCrGujd4Sa3+qw1BPxaNAN0
  DFEVfIrk201z4jAs",
  "c2_domain": [
    "Lycos.com",
    "mail.yahoo.com",
    "193.56.255.251",
    "193.56.255.250",
    "193.56.255.249",
    "numolerunosell.online",
    "gumolerunosell.online",
    "rumolerunosell.online"
  ],
  "dga_tld": "com ru org",
  "DGA_count": "10",
  "server": "12",
  "serpent_key": "10291029JSJUYNHG",
  "sleep_time": "60",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "600",
  "time_value": "1000",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "122",
  "SetWaitableTimer_value(CRC_SENDDTIMEOUT)": "1000",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "122",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "4474",
  "SetWaitableTimer_value": "200"
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
202c6770000.dll	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	


Sigma Overview

System Summary:



Sigma detected: Suspicious Call by Ordinal

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

System Summary:



Hooking and other Techniques for Hiding and Protection:



Yara detected Ursnif

Stealing of Sensitive Information:



Yara detected Ursnif

Remote Access Functionality:

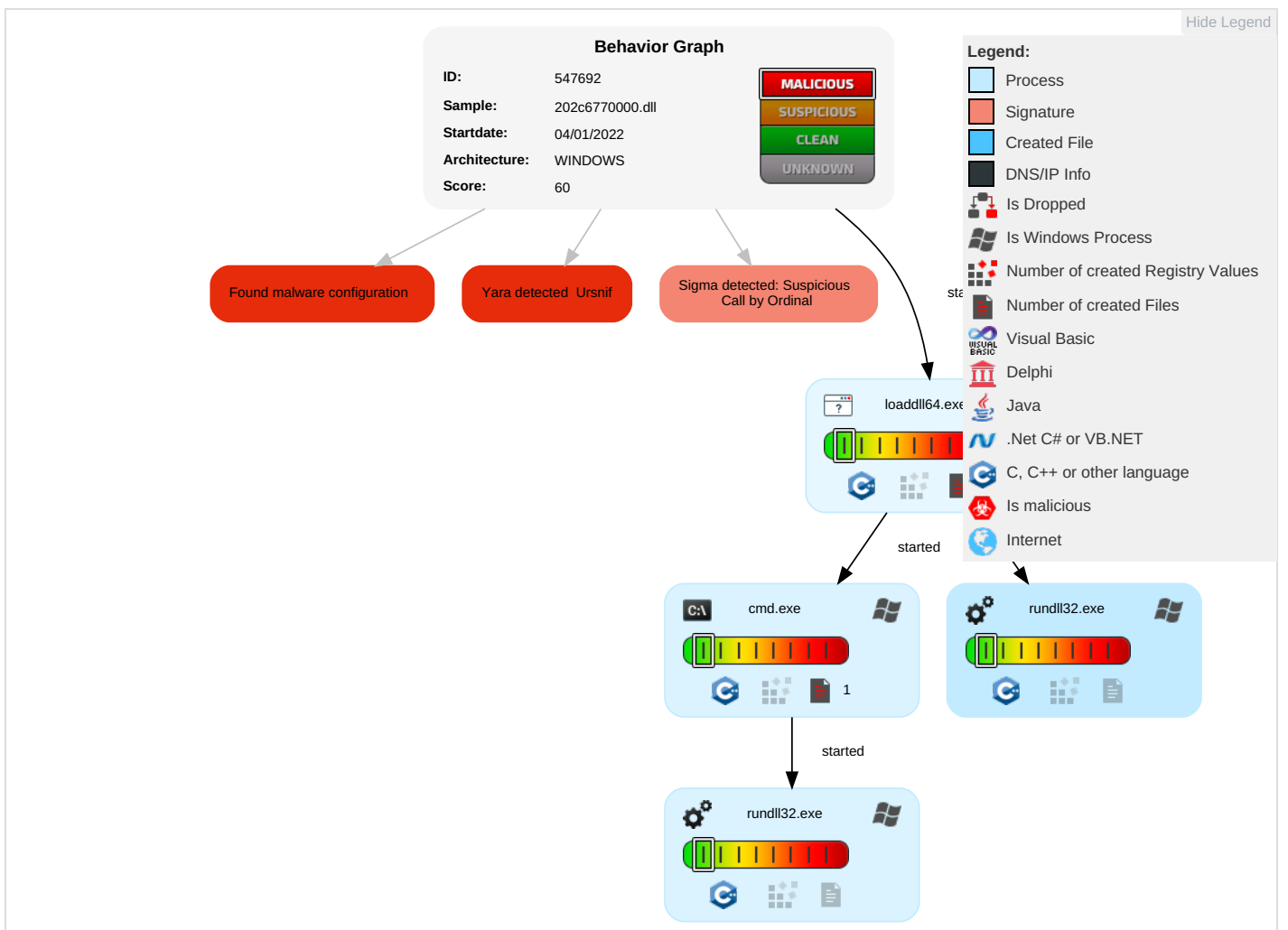


Yara detected Ursnif

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 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

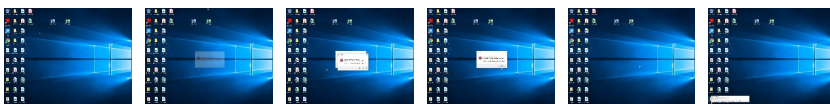
Behavior Graph



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:	34.0.0 Boulder Opal
Analysis ID:	547692
Start date:	04.01.2022
Start time:	13:44:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	202c6770000.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:	8
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:	mal60.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• Stop behavior analysis, all processes terminated
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):	6.409785833600413
TrID:	<ul style="list-style-type: none"> 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:	202c6770000.dll
File size:	227840
MD5:	4b76083e201810b0a6430846ca94250a
SHA1:	963f018eb2d3a6ae81c40486a63795cdf137be52
SHA256:	8cba0769d25a6cc0cd53961a53b1a13568446ea01f0d72724e15eaeef087f314a
SHA512:	eeedf121eef42c72d7d3ee9ff5e226f05606e6bb843ee87390ef5e96dcc374f721e7e0a299aa09b7978483780a8e58fc6254e67d12189babeee000f670d3da65
SSDEEP:	6144:/HExb7VwvtKNbnvSxYNiyf+D3Luiy5nH:cx5wvtKRvSxY0G+D7uiG
File Content Preview:	MZ.....PE..d..

File Icon

	
Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General	
Entrypoint:	0x18002a0e8
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:	0x60C0F8C1 [Wed Jun 9 17:22:09 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	0x2c908	0x2ca00	False	0.57014290091	data	6.34156774345	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2e000	0x4b07	0x4c00	False	0.399362664474	data	5.24927821467	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x33000	0x1f88	0x1a00	False	0.307692307692	lif file	3.69406631284	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x35000	0x17c4	0x1800	False	0.538411458333	data	5.29492234825	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bss	0x37000	0x20c8	0x2200	False	0.952895220588	data	7.87054877548	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x3a000	0x1000	0xc00	False	0.459635416667	data	4.35925404581	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: 6580 Parent PID: 1572

General

Start time:	13:44:59
Start date:	04/01/2022
Path:	C:\Windows\System32\loadll64.exe
Wow64 process (32bit):	false
Commandline:	loadll64.exe "C:\Users\user\Desktop\202c6770000.dll"
Imagebase:	0x7ff68f040000
File size:	140288 bytes
MD5 hash:	4E8A40CAD6CCC047914E3A7830A2D8AA
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: 6588 Parent PID: 6580

General

Start time:	13:45:00
Start date:	04/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\202c6770000.dll",#1
Imagebase:	0x7ff622070000
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: 5128 Parent PID: 6580

General

Start time:	13:45:00
Start date:	04/01/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\202c6770000.dll,#1
Imagebase:	0x7ff799f30000
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: 6108 Parent PID: 6588

General

Start time:	13:45:00
Start date:	04/01/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\202c6770000.dll", #1
Imagebase:	0x7ff799f30000
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