

JOESandbox Cloud BASIC



**ID:** 547693

**Sample Name:** 1e60aca0000.dll

**Cookbook:** default.jbs

**Time:** 13:44:09

**Date:** 04/01/2022

**Version:** 34.0.0 Boulder Opal

# Table of Contents

Table of Contents	2
Windows Analysis Report 1e60aca0000.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	7
URLs	7
Domains and IPs	7
Contacted Domains	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	9
Statistics	9
Behavior	10
System Behavior	10
Analysis Process: loadll64.exe PID: 6308 Parent PID: 2256	10
General	10
File Activities	10
Analysis Process: cmd.exe PID: 6316 Parent PID: 6308	10
General	10
File Activities	10
Analysis Process: rundll32.exe PID: 6340 Parent PID: 6308	10
General	10
File Activities	11
Analysis Process: rundll32.exe PID: 6352 Parent PID: 6316	11
General	11
File Activities	11
Disassembly	11
Code Analysis	11

# Windows Analysis Report 1e60aca0000.dll

## Overview

### General Information

Sample Name:	1e60aca0000.dll
Analysis ID:	547693
MD5:	f09f51fb30891aa...
SHA1:	28e62b9495bf58b.
SHA256:	68f2f77b88e5575..
Tags:	exe gozi
Infos:	
Most interesting Screenshot:	

### Detection

**MALICIOUS**

**SUSPICIOUS**

**CLEAN**

**UNKNOWN**

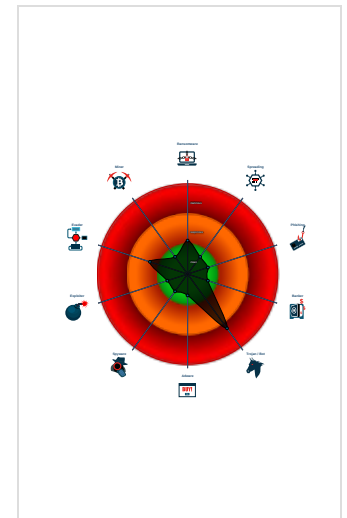
**Ursnif**

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

### Signatures

- Antivirus / Scanner detection for sub...
- Found malware configuration
- Multi AV Scanner detection for subm...
- 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: 6308 cmdline: loaddll64.exe "C:\Users\user\Desktop\1e60aca0000.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 6316 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\1e60aca0000.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6352 cmdline: rundll32.exe "C:\Users\user\Desktop\1e60aca0000.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 6340 cmdline: rundll32.exe C:\Users\user\Desktop\1e60aca0000.dll,#1 MD5: 73C519F050C20580F8A62C849D49215A)
- cleanup

## Malware Configuration

### Threatname: Ursnif

```
{
  "RSA Public Key":
  "1ez6ZX9GBMHuzrxYcEvmkX0k1/y/WREShgthXVQ4P4VmZDRyl+qzgB3X8mQxx9hX87voxbw+7CbnCCZ4hp/XwNIIs0rUcJj4wwNctiIvZb8gIPsgWRAjJLGMBCkjpnhIdWmYD7oSqAb7ciAuhtWabiveV30FwUuMRDbNtONTWpz/J
  4JVtQJ3XBbp99SutX5vbOPhgKBI3aszrv+0c1EkjrakCFHlOqM58bjEjNDxrhaBwjOM1EU17zvHVkK7hxDkKQ5buzWnjrzDZEEWnvM3aaSuVRR1v44XnboLU0LtUakCZT4sH963oonk1uijExj7eWoI4x+donYvsc/nFxNyfe6c/mfSK
  b7U2RHPG4g=",
  "c2_domain": [
    "art.microsoftofymicrosoftsoft.at",
    "r23cirt55ysvtdvl.onion",
    "poi.redhatbabby.at",
    "fgx.dangerboy.at",
    "pop.biopiof.at",
    "l46t3vgvntx5wx6.onion",
    "apr.intoolkom.at"
  ],
  "ip_check_url": [
    "curlmyip.net"
  ],
  "serpent_key": "KCVH9K5GzjoxwKSf",
  "server": "580",
  "sleep_time": "10",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "600",
  "time_value": "600",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "300",
  "SetWaitableTimer_value(CRC_SENDDTIMEOUT)": "300",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "300",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "505050",
  "SetWaitableTimer_value": "60"
}
```

## Yara Overview

### Initial Sample

Source	Rule	Description	Author	Strings
1e60aca0000.dll	JoeSecurity_Ursnif_2	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:



Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

### 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:

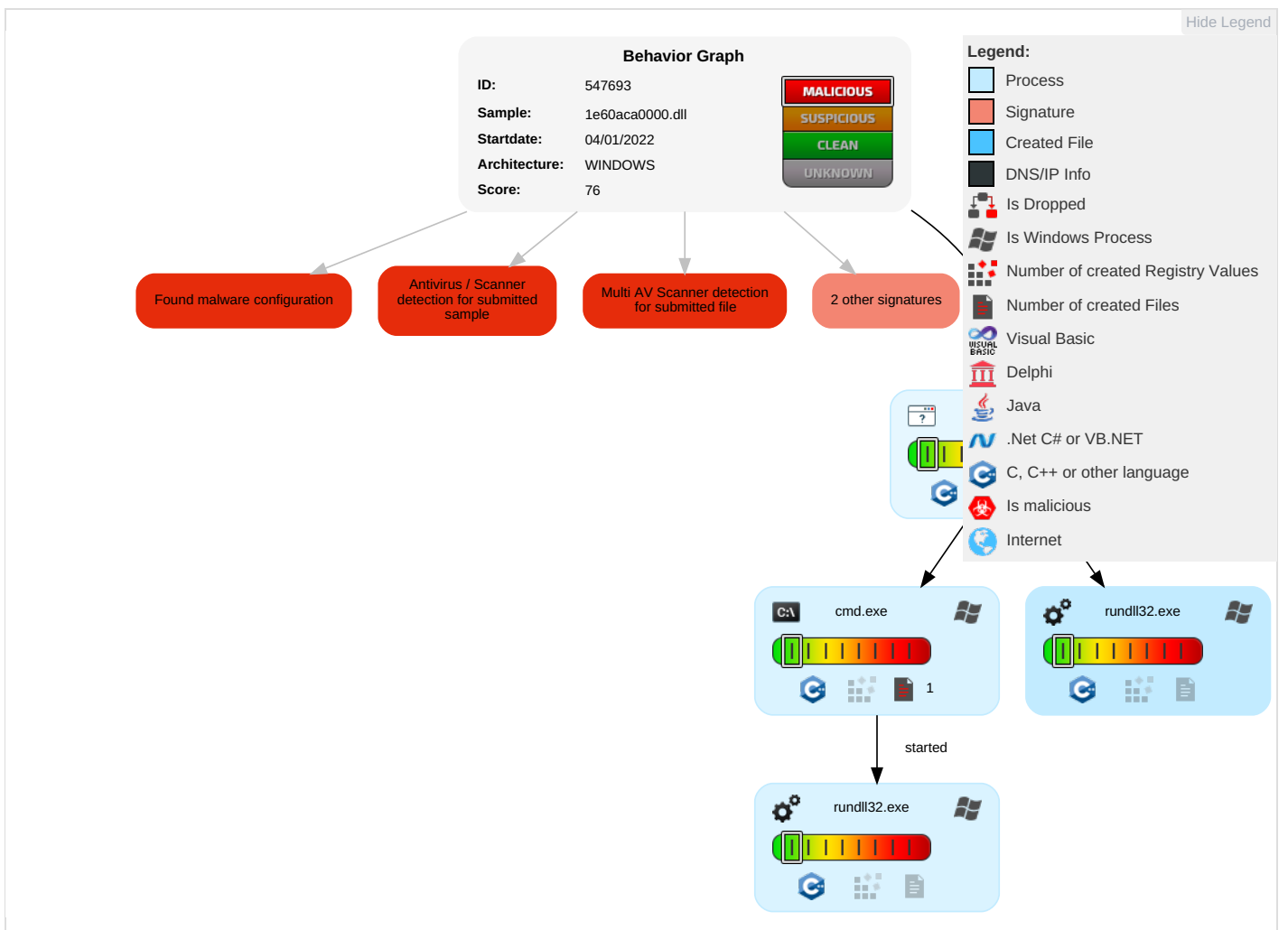


Yara detected Ursnif

## 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 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

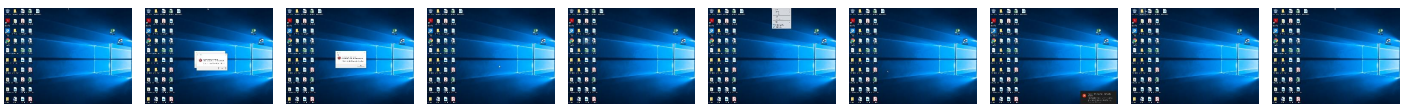
## Behavior Graph

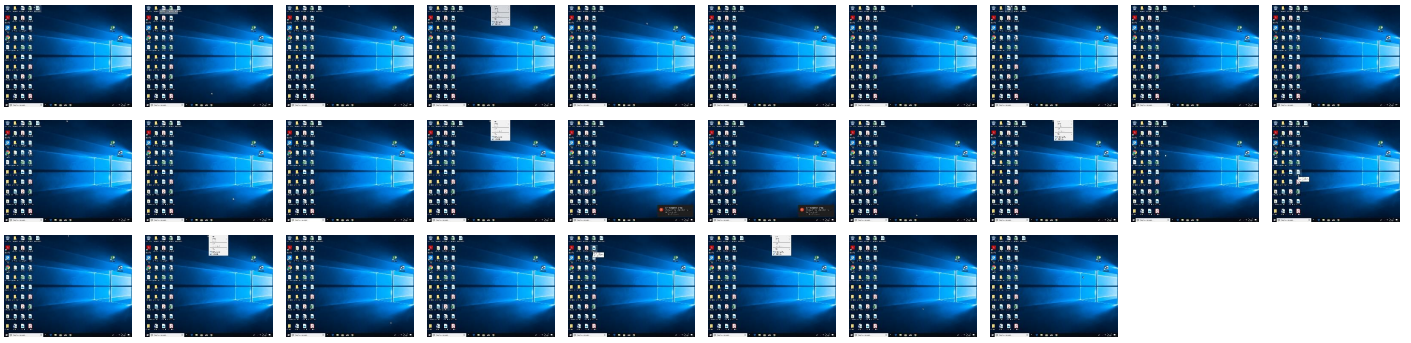


## Screenshots

### 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
1e60aca0000.dll	35%	ReversingLabs	Win64.Trojan.Convagent	
1e60aca0000.dll	100%	Avira	HEUR/AGEN.1108168	

### 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:	547693
Start date:	04.01.2022
Start time:	13:44:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1e60aca0000.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:	28
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"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.troj.winDLL@7/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 100%</li><li>• Number of executed functions: 0</li><li>• Number of non-executed functions: 0</li></ul>
Cookbook Comments:	<ul style="list-style-type: none"><li>• Adjust boot time</li><li>• Enable AMSI</li><li>• Found application associated with file extension: .dll</li><li>• Override analysis time to 240s for rundll32</li></ul>
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):	6.4421958770930425
TrID:	<ul style="list-style-type: none"><li>Win64 Dynamic Link Library (generic) (102004/3) 84.88%</li><li>Win64 Executable (generic) (12005/4) 9.99%</li><li>DOS Executable Borland Pascal 7.0x (2037/25) 1.69%</li><li>Generic Win/DOS Executable (2004/3) 1.67%</li><li>DOS Executable Generic (2002/1) 1.67%</li></ul>
File name:	1e60aca0000.dll
File size:	248320
MD5:	f09f51fb30891aa93446c01018e92d49
SHA1:	28e62b9495bf58b7ff183c327a6eaa3ac7461b5b
SHA256:	68f2f77b88e5575b360d05f84ff11a026a62fa42f48aeec2cd44523692e40a6a
SHA512:	07d7f082aa436814edd38485ee9c7b0d056b03f9fd8ddd169f28f73e47a13d36a9b6705025275dd9dbbd3eefe81f03e2ede81a09adfdf57be3dd0c0e4d87bc7
SSDEEP:	6144:HPMtgIXNWog0Sbrhl8exPofnrWWJE4R:/HP1hl02rO8exgvrWWJh
File Content Preview:	MZ..... ..... .....



## File Icon



Icon Hash:

74f0e4ecccdce0e4

## Static PE Info

### General

Entrypoint:	0x18000527c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	
Time Stamp:	0x61B67F6F [Sun Dec 12 23:02:07 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	0x2fdec	0x2fe00	False	0.579277496736	zlib compressed data	6.39992554242	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x31000	0x6837	0x6a00	False	0.372346698113	data	5.26021941188	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x38000	0x1e40	0x1800	False	0.316731770833	lif file	3.68966711917	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x3a000	0x18f0	0x1a00	False	0.528094951923	data	5.32861522181	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bss	0x3c000	0x1f80	0x2000	False	0.970458984375	data	7.90682667928	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x3e000	0x1000	0xc00	False	0.513346354167	data	4.74473762141	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: loadll64.exe PID: 6308 Parent PID: 2256

### General

Start time:	13:45:02
Start date:	04/01/2022
Path:	C:\Windows\System32\loadll64.exe
Wow64 process (32bit):	false
Commandline:	loadll64.exe "C:\Users\user\Desktop\1e60aca0000.dll"
Imagebase:	0x7ff7bcd0000
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: 6316 Parent PID: 6308

### General

Start time:	13:45:02
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\1e60aca0000.dll",#1
Imagebase:	0x7ff7eef80000
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: 6340 Parent PID: 6308

### General

Start time:	13:45:02
Start date:	04/01/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\1e60aca0000.dll,#1
Imagebase:	0x7ff638db0000

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: 6352 Parent PID: 6316

#### General

Start time:	13:45:03
Start date:	04/01/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\1e60aca0000.dll",#1
Imagebase:	0x7ff638db0000
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