

JoeSandbox Cloud BASIC



ID: 524446

Sample Name: 28b452d0000.dll

Cookbook: default.jbs

Time: 14:31:39

Date: 18/11/2021

Version: 34.0.0 Boulder Opal


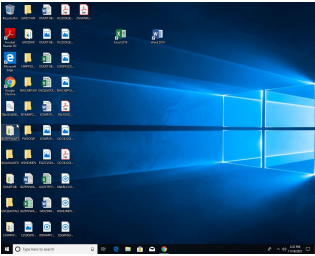
Table of Contents

Table of Contents	2
Windows Analysis Report 28b452d0000.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: loadll64.exe PID: 4068 Parent PID: 3248	10
General	10
File Activities	11
Analysis Process: cmd.exe PID: 5392 Parent PID: 4068	11
General	11
File Activities	11
Analysis Process: rundll32.exe PID: 6360 Parent PID: 4068	11
General	11
File Activities	11
Analysis Process: rundll32.exe PID: 5800 Parent PID: 5392	11
General	11
File Activities	12
Disassembly	12
Code Analysis	12

Windows Analysis Report 28b452d0000.dll

Overview

General Information

Sample Name:	28b452d0000.dll
Analysis ID:	524446
MD5:	45d602c1878eda..
SHA1:	2f9606697894ee8.
SHA256:	c621297f4361a72.
Tags:	<div>exe gozi</div>
Infos:	<div></div>
Most interesting Screenshot:	
	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

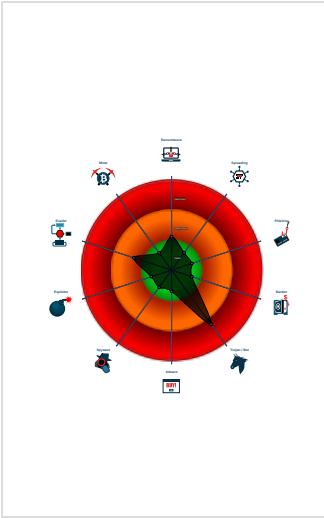
Ursnif

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
-  loadaddll64.exe (PID: 4068 cmdline: loadaddll64.exe "C:\Users\user\Desktop\28b452d0000.dll" MD5: E0CC9D126C39A9D2FA1CAD5027EBBD18)
 -  cmd.exe (PID: 5392 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\28b452d0000.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
 -  rundll32.exe (PID: 5800 cmdline: rundll32.exe "C:\Users\user\Desktop\28b452d0000.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
 -  rundll32.exe (PID: 6360 cmdline: rundll32.exe C:\Users\user\Desktop\28b452d0000.dll,#1 MD5: 73C519F050C20580F8A62C849D49215A)
- cleanup

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
  "YOKfuXyqdgHv9S/1BC89q+2AtY47vYuaGS0tZJ8d606ochD7W6siPV2JrKeda84QkxbQ0+VVfipAiJGPSLyuH5PBTp1YXEqe08AR6gPZo6msmG0AdzSZu04LMBJ6s9dvr-fX21tvvbQCrAm9rEoH2LTGMGxwb6GrRlYPojaXCgymjHF8+
Wxs+ymNUIvDh20U5572Kv0pHGtuDRZWN9YnPHdsBHMITSJSbHFvMPwL6X4nag3m+qn/5iuA2C1SS5z5hMdEXbPPoNMy/yM43jrMrHJvwhw/1S/Bic2SpzCRK1QjeERTBP1ZgKrE7S6grdequ0fzjD0b01k1U5WZrLvaLUH/of13KSH7yIq
c66k8zdl1k=",
  "c2_domain": [
    "art.microsoftsofymicrosoftsoft.at",
    "r23cirt55ysvtdvl.onion",
    "fop.langoonik.com",
    "poi.redhatbabby.at",
    "pop.biopiof.at",
    "l46t3vgvntx5wx6.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": "rQH4gusjF0tL2dQz",
  "server": "500",
  "sleep_time": "5",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "600",
  "time_value": "600",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "240",
  "SetWaitableTimer_value(CRC_SENDDTIMEOUT)": "300",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "240",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "2500",
  "SetWaitableTimer_value": "60"
}
```

Yara Overview


Initial Sample

Source	Rule	Description	Author	Strings
28b452d0000.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:

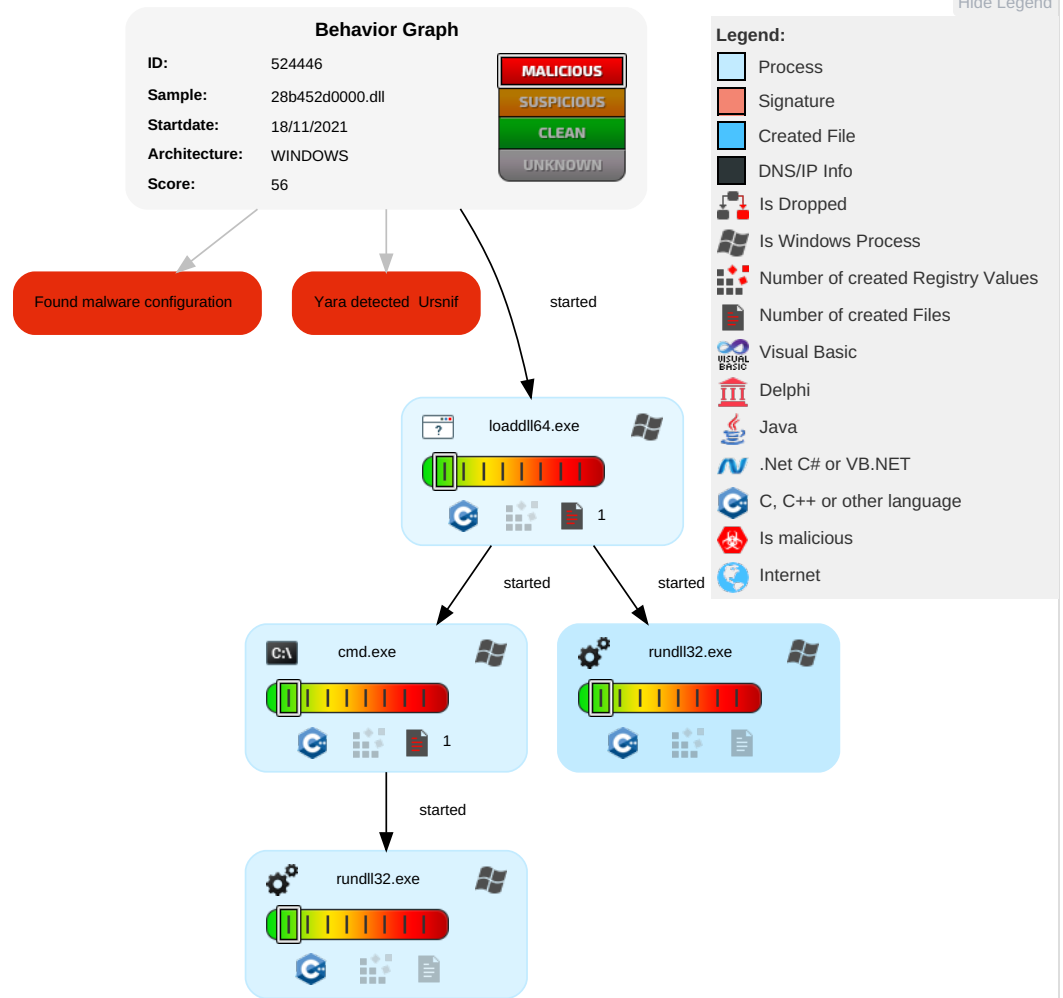


Yara detected Ursnif

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:	34.0.0 Boulder Opal
Analysis ID:	524446
Start date:	18.11.2021
Start time:	14:31:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	28b452d0000.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:	5
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:	mal56.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):	6.44899043281889
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:	28b452d0000.dll
File size:	247808
MD5:	45d602c1878edac953ecfae4c1e059fe
SHA1:	2f9606697894ee86d605cd4abafb74b60fed676b
SHA256:	c621297f4361a727f803ad31bfb7388f45af5a9e5c7b6237d1492c23e1f8991f
SHA512:	02b37fb55b6b676b0efdaf44ac18a51b60fe1d8cb9f5404ccf3ecd6910577d31fd88c6eba2c0678b56afe3d08fbdf231fc1842c023b0ec8cfe5131ef235a232a
SSDEEP:	6144:MW/TYr/Pbqk2ZFOY/ybb00h2ETeZlwtaWtBk4S+Uh:MW/TYLPbqRul5dQzPtaWtBC+
File Content Preview:	MZ.....PE..d..

File Icon

	
Icon Hash:	74f0e4eccdce0e4

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	0.372125589623	data	5.23305306886	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x38000	0x1e40	0x1800	False	0.333658854167	lif file	3.91011217456	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	0.531901041667	data	4.88478800685	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: 4068 Parent PID: 3248

General

Start time:	14:32:43
Start date:	18/11/2021
Path:	C:\Windows\System32\loadll64.exe
Wow64 process (32bit):	false
Commandline:	loadll64.exe "C:\Users\user\Desktop\28b452d0000.dll"
Imagebase:	0x7ff6e2230000
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: 5392 Parent PID: 4068

General

Start time:	14:32:44
Start date:	18/11/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\28b452d0000.dll",#1
Imagebase:	0x7ff77f910000
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: 6360 Parent PID: 4068

General

Start time:	14:32:44
Start date:	18/11/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\28b452d0000.dll,#1
Imagebase:	0x7ff720e40000
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: 5800 Parent PID: 5392

General

Start time:	14:32:44
Start date:	18/11/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\28b452d0000.dll",#1
Imagebase:	0x7ff720e40000
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