

JoeSandbox Cloud BASIC



ID: 498827

Sample Name: 50b0000.dll

Cookbook: default.jbs

Time: 15:13:11

Date: 07/10/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report 50b0000.dll	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: Ursnif	3
Yara Overview	3
Initial Sample	3
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:	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	7
Contacted Domains	7
Contacted IPs	7
General Information	7
Simulations	7
Behavior and APIs	7
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	8
Static PE Info	8
General	9
Entrypoint Preview	9
Rich Headers	9
Data Directories	9
Sections	9
Network Behavior	9
Code Manipulations	9
Statistics	9
Behavior	9
System Behavior	10
Analysis Process: loadll32.exe PID: 3228 Parent PID: 5992	10
General	10
File Activities	10
Analysis Process: cmd.exe PID: 5140 Parent PID: 3228	10
General	10
File Activities	10
Analysis Process: rundll32.exe PID: 4160 Parent PID: 5140	10
General	10
File Activities	11
Disassembly	11
Code Analysis	11

Windows Analysis Report 50b0000.dll

Overview

General Information

Sample Name:	50b0000.dll
Analysis ID:	498827
MD5:	58f21c7dda3babf..
SHA1:	e967834ee1b6ae..
SHA256:	c88152c5a3a00f6..
Tags:	<div><div>dll</div></div>
Infos:	<div><div><div></div><div></div><div></div></div><div><div></div><div></div><div></div></div></div>
Most interesting Screenshot:	<div></div>

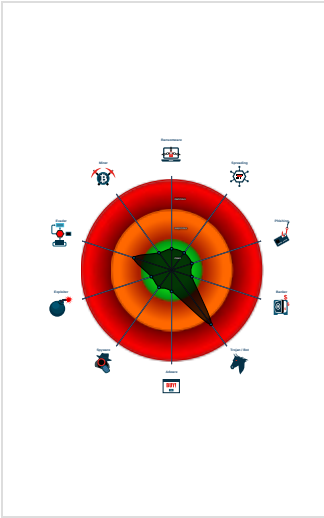
Detection

<div><div><div>MALICIOUS</div><div>SUSPICIOUS</div><div>CLEAN</div><div>UNKNOWN</div></div><div><div>Ursnif</div></div></div>	<div><div>Score:</div><div>64</div></div> <div><div>Range:</div><div>0 - 100</div></div> <div><div>Whitelisted:</div><div>false</div></div> <div><div>Confidence:</div><div>100%</div></div>
---	--

Signatures

<div><div>Antivirus / Scanner detection for sub...</div><div>Found malware configuration</div><div>Yara detected Ursnif</div><div>Uses 32bit PE files</div><div>PE file does not import any functions</div><div>Tries to load missing DLLs</div><div>Program does not show much activi...</div><div>Creates a process in suspended mo...</div><div>Checks if the current process is bein...</div></div>

Classification



Process Tree

- System is w10x64
- loadaddll32.exe (PID: 3228 cmdline: loadaddll32.exe 'C:\Users\user\Desktop\50b0000.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E)
 - cmd.exe (PID: 5140 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\50b0000.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
 - rundll32.exe (PID: 4160 cmdline: rundll32.exe 'C:\Users\user\Desktop\50b0000.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- cleanup

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
    "vM/iQ17/pNgGz6lvtI6TzQegGf2XOLfA1qF/UUMP33fhMhAMf4GRS0JmruKf0pClZgy8d4EH5ndffMShLLCNtrR+dtN+DP2SKSbflIhidE/SjblI0hsotYZGCD8mkB8RgNy5KRipILXyv4cN0eYiLVm2eSVaCkKBqotkaZ6t0ybzDTZnit0o5nqHQOYtQRW",
  "c2_domain": [
    "api5.feen007.at/webstore"
  ],
  "botnet": "3500",
  "server": "550",
  "serpent_key": "IpNvMMQa29KhBf3e",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "10",
  "dga_base_url": "constitution.org/usdeclar.txt",
  "dga_tld": "com ru org",
  "DGA_count": "10"
}
```

Yara Overview

Initial Sample


Source	Rule	Description	Author	Strings
50b0000.dll	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Source	Rule	Description	Author	Strings
--------	------	-------------	--------	---------


Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

 Click to jump to signature section


AV Detection:



Antivirus / Scanner detection for submitted sample


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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
50b0000.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:	33.0.0 White Diamond
Analysis ID:	498827
Start date:	07.10.2021
Start time:	15:13:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	50b0000.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:	32
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:	mal64.troj.winDLL@5/0@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• 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:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.562968589997569
TrID:	<ul style="list-style-type: none">Win32 Dynamic Link Library (generic) (1002004/3) 99.60%Generic Win/DOS Executable (2004/3) 0.20%DOS Executable Generic (2002/1) 0.20%Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	50b0000.dll
File size:	54784
MD5:	58f21c7dda3babf8bb6eeabb0949c496
SHA1:	e967834ee1b6ae315d43ca8f640db4dba76e5a0f
SHA256:	c88152c5a3a00f6bc9dbc4958659f7fb80b90c39a256fbc2e774a8c70affae1a
SHA512:	c7f00cb7e7aa74f45bb94e6ac821422c98d1dbccb13a0bfda63971d4db86133ed2abccff490c9096b2b34f312b10cfab3b0b3645fb56c562a2a74cead1ed4a35
SSDEEP:	1536:WY/xJLCObwAbdZWdbkHbReQc1gMQBbyqlaVZLPhLKW:WY/xHDbdWG8nX0byqlaVZL
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$......i.@...@...@...g^z.A...!...F...g^i.C...@.....Z.C.....X.A.....C...g^v.l...g^}.A...g^..A...Rich@.....PE..L..

File Icon

	
Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General	
Entrypoint:	0x1000423d
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x5F6B29CC [Wed Sep 23 10:56:12 2020 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

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xa327	0xa400	False	0.581602515244	data	6.54856176409	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xc000	0xef4	0x1000	False	0.379150390625	data	3.60302468591	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xd000	0x2f4	0x200	False	0.453125	ARJ archive data, v13, original name: , os: MS-DOS	2.82911163227	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.bss	0xe000	0xdf2	0xe00	False	0.977678571429	data	7.79892621903	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0xf000	0x1000	0xe00	False	0.553850446429	data	5.00821944937	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: loadll32.exe PID: 3228 Parent PID: 5992

General

Start time:	15:14:08
Start date:	07/10/2021
Path:	C:\Windows\System32\loadll32.exe
Wow64 process (32bit):	true
Commandline:	loadll32.exe 'C:\Users\user\Desktop\50b0000.dll'
Imagebase:	0x200000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
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: 5140 Parent PID: 3228

General

Start time:	15:14:09
Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\50b0000.dll',#1
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: 4160 Parent PID: 5140

General

Start time:	15:14:09
Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\50b0000.dll',#1
Imagebase:	0x9f0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis