

JoeSandbox Cloud BASIC



ID: 500332

Sample Name: 870000.dll

Cookbook: default.jbs

Time: 22:58:51

Date: 11/10/2021

Version: 33.0.0 White Diamond


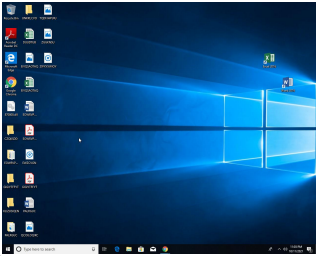
Table of Contents

Table of Contents	2
Windows Analysis Report 870000.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	7
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	8
Entrypoint Preview	9
Rich Headers	9
Data Directories	9
Sections	9
Network Behavior	9
Code Manipulations	9
Statistics	9
Behavior	9
System Behavior	9
Analysis Process: loadll32.exe PID: 5032 Parent PID: 5360	10
General	10
File Activities	10
Analysis Process: cmd.exe PID: 3492 Parent PID: 5032	10
General	10
File Activities	10
Analysis Process: rundll32.exe PID: 4664 Parent PID: 3492	10
General	10
File Activities	10
Disassembly	11
Code Analysis	11

Windows Analysis Report 870000.dll

Overview

General Information

Sample Name:	870000.dll
Analysis ID:	500332
MD5:	8575bba1d97609..
SHA1:	0457b5be90bc81..
SHA256:	b4e9cf6ef8e62e0..
Tags:	dll gozi
Infos:	
Most interesting Screenshot:	

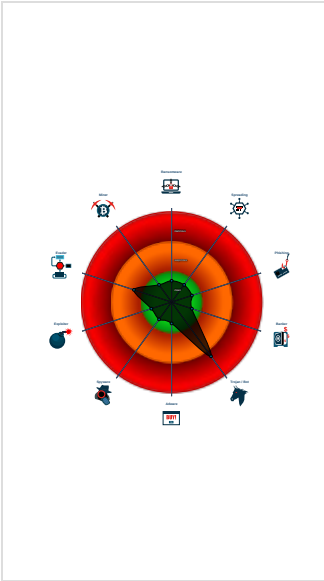
Detection

<div><div>MALICIOUS</div><div>SUSPICIOUS</div><div>CLEAN</div><div>UNKNOWN</div></div>	
<div>Ursnif</div>	
Score:	72
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
Uses 32bit PE files
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
<ul style="list-style-type: none"> loadaddll32.exe (PID: 5032 cmdline: loadaddll32.exe 'C:\Users\user\Desktop\870000.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E)<ul style="list-style-type: none"> cmd.exe (PID: 3492 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\870000.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)<ul style="list-style-type: none"> rundll32.exe (PID: 4664 cmdline: rundll32.exe 'C:\Users\user\Desktop\870000.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
cleanup

Malware Configuration

Threatname: Ursnif

<pre>{ "RSA Public Key": "cgKNT5f98bcVt4Ua6/spDh3agMYKS9USXCEAUwqrd6WorohXmUHLK3DTr9KcxGc7Xz0+BjHSpcUazVaBbHXWQQRq1DRAPoIVLucrptqudHSQNq7SpoJGVw8bSg13X1tYLNhzq/3sAsc0T/eM1uD7kTJ+/VUmeTv84go7QrHnegQE7NNf yRvMbqeUIBu7C6gy", "c2_domain": ["i.microsoft.com", "horulenuke.us", "vorulenuke.us"], "botnet": "4460", "server": "12", "serpent_key": "10291029JSJUYNHG", "sleep_time": "10", "CONF_TIMEOUT": "20", "SetWaitableTimer_value": "0", "dga_base_url": "constitution.org/usdeclar.txt", "dga_tld": "com ru org", "DGA_count": "10" }</pre>

Yara Overview


Initial Sample

Source	Rule	Description	Author	Strings
870000.dll	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

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
- Multi AV Scanner detection for submitted file

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:



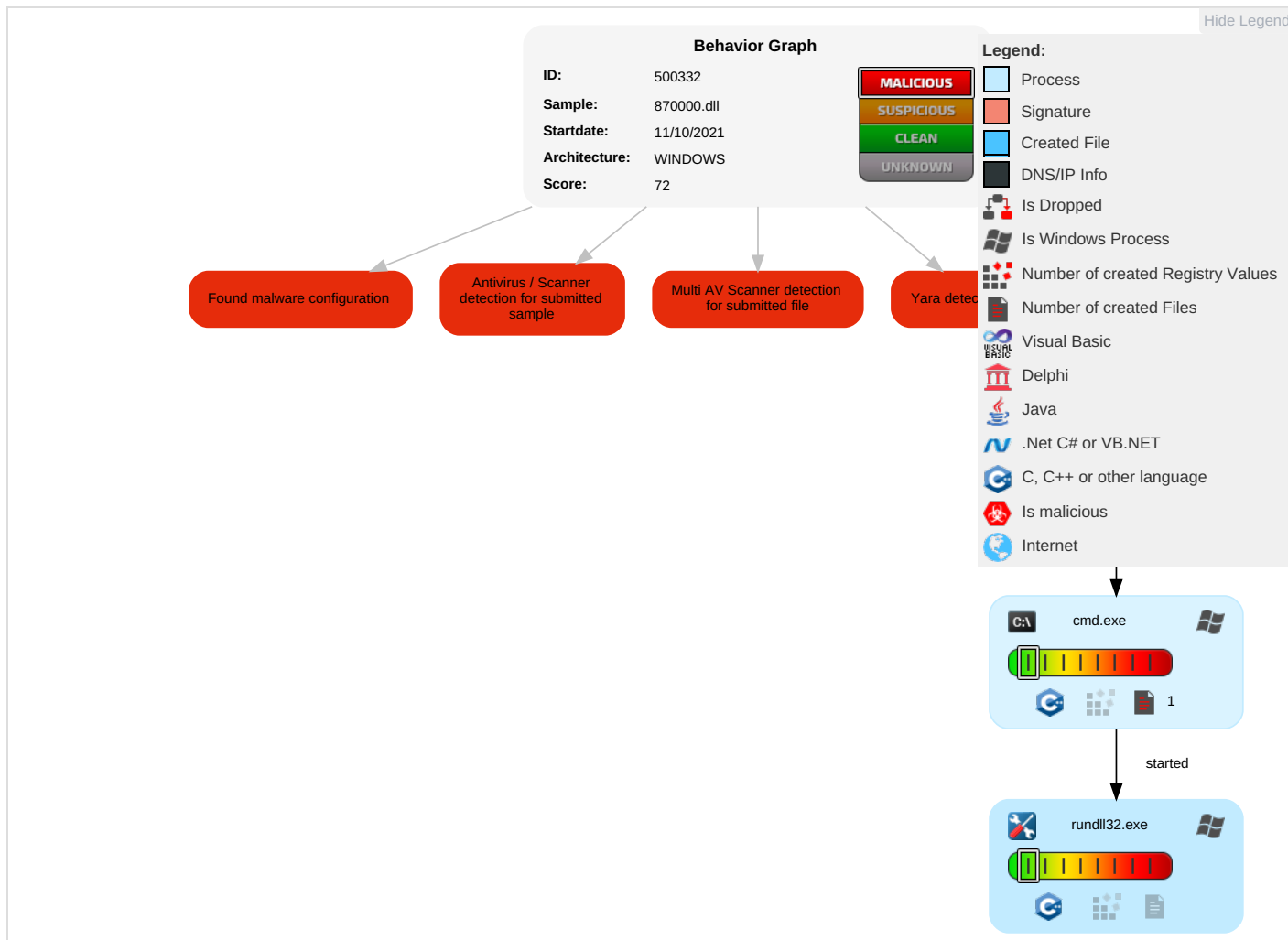
Yara detected Ursnif

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
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

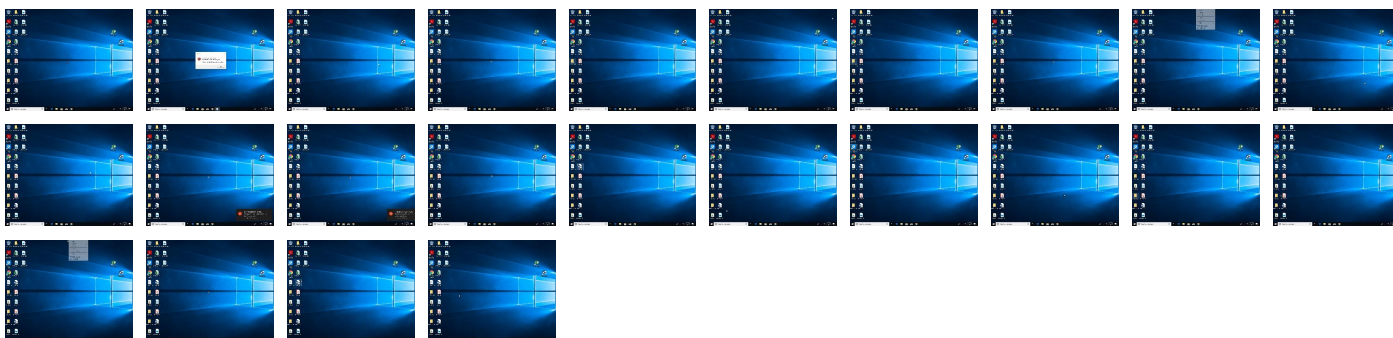
Behavior Graph



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
870000.dll	54%	ReversingLabs	Win32.Trojan.AgentAGen	
870000.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:	500332
Start date:	11.10.2021
Start time:	22:58:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	870000.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:	mal72.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):	6.652177025625302
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:	870000.dll
File size:	55808
MD5:	8575bba1d976096af4d2ff153075eeeb
SHA1:	0457b5be90bc81afa6fdf69dafc1914ece904e6f
SHA256:	b4e9cf6ef8e62e042d2c7b090d987ae16017c927766e7f1de7b936e0eded1652
SHA512:	0c944b257abf07871088b65055e498149f36856028dbeefeddd19218bdf6000b0706c36d49970fb88bf5c901c93d6c3ad1758741b25a6805961d7c7f2ee08be
SSDEEP:	1536:KAg+HMqC1WyE5q2qlalXSyW/vqTpfRMB8W:99HMnWyE5q2qlalqdfRM
File Content Preview:	MZ.....@.....!..!Th is program cannot be run in DOS mode....\$......a..a...a ...a.....a.....a...a...a..ra...nR..a...nP..a...n...a.....a... ...a.....a..Rich.a.....

File Icon

	
Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General	
Entrypoint:	0x1000a75c
Entrypoint Section:	.text

General	
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x6075EF24 [Tue Apr 13 19:21:08 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
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	0xa513	0xa600	False	0.581160579819	data	6.55174307964	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xc000	0xf32	0x1000	False	0.457763671875	data	4.68281145507	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xd000	0x348	0x200	False	0.53515625	ARJ archive data, v17, original name: , os: MS-DOS	3.39122202758	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.bss	0xe000	0xe5a	0x1000	False	0.88427734375	data	7.45515503893	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0xf000	0x1000	0xe00	False	0.585379464286	data	5.24391900313	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: 5032 Parent PID: 5360

General

Start time:	22:59:49
Start date:	11/10/2021
Path:	C:\Windows\System32\loadll32.exe
Wow64 process (32bit):	true
Commandline:	loadll32.exe 'C:\Users\user\Desktop\870000.dll'
Imagebase:	0x3e0000
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: 3492 Parent PID: 5032

General

Start time:	22:59:50
Start date:	11/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\870000.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: 4664 Parent PID: 3492

General

Start time:	22:59:50
Start date:	11/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\870000.dll',#1
Imagebase:	0xf90000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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