ID: 542877
Sample Name: 25402ed0000.dll
Cookbook: default.jbs
Time: 17:09:00
Date: 20/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report 25402ed0000.dll

Overview

General Information

Sample Name:	25402ed0000.dll
Analysis ID:	542877
MD5:	6d10828642bd65..
SHA1:	754da3be553186..
SHA256:	cc97634ff5e232f...
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
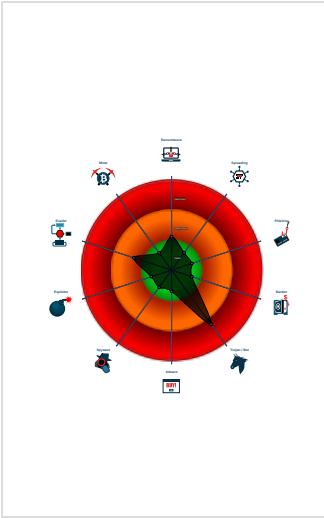
Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 7152 cmdline: loaddll64.exe "C:\Users\user\Desktop\25402ed0000.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 3912 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\25402ed0000.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 5760 cmdline: rundll32.exe "C:\Users\user\Desktop\25402ed0000.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6128 cmdline: rundll32.exe C:\Users\user\Desktop\25402ed0000.dll,#1 MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"R+UxqbV/y+ZU1c0seFgwYm43sz1DSmatV8GC7d9ajlQ+vaAx2oxbmrXwev8mSqGGA/bUt2ZkpqSt/nxO6+/Ak7RHUIzazuikwj2CwtI2KIDL8nZsOoWBzTyOzo34t4SghKOmz0ogisuhvhvEfnzRtTwTwtCrGujd4Sa3+qw1BPxaNAN0
DFEVfIrq201z4jAs",
  "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_SENDTIMEOUT)": "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
25402ed0000.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 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

Behavior Graph

ID: 542877
Sample: 25402ed0000.dll
Startdate: 20/12/2021
Architecture: WINDOWS
Score: 60

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

Found malware configuration

Yara detected Ursnif

Sigma detected: Suspicious Call by Ordinal

Legend:
- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

loaddll64.exe

started

cmd.exe   1

rundll32.exe

started

rundll32.exe

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:	542877
Start date:	20.12.2021
Start time:	17:09:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	25402ed0000.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:	- 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:	- Successful, ratio: 100% - Number of executed functions: 0 - Number of non-executed functions: 0
Cookbook Comments:	- 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):	6.409656321765304
TrID:	- 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:	25402ed0000.dll
File size:	227840
MD5:	6d10828642bd658d56fea15dedfb200d
SHA1:	754da3be553186af8f8eb78009f052733bf71d9c
SHA256:	cc97634ff5e232f7b9d89740c60a271d535da2437ee1369 948902e9267e13453
SHA512:	327e27ec1369688f159d91e1ba398d02b889b7f6eb42355 0fe184a43c9c4b143169776c5add423aa0e263c7e1face5 17b11571564219e41bdfac753460845963
SSDEEP:	6144:/HExb7VwvtKNbnvSxYNiyf+D3Luiy52H:cxb5wvtK RvSxY0G+D7uiX
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	0.307842548077	lif file	3.6918775332	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: 7152 Parent PID: 4636

General

Start time:	17:09:59
Start date:	20/12/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\25402ed0000.dll"
Imagebase:	0x7ff7aae10000
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: 3912 Parent PID: 7152

General

Start time:	17:09:59
Start date:	20/12/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\25402ed0000.dll",#1
Imagebase:	0x7ff71e680000
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: 6128 Parent PID: 7152

General

Start time:	17:10:00
Start date:	20/12/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\25402ed0000.dll,#1
Imagebase:	0x7ff70fc90000
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: 5760 Parent PID: 3912

General

Start time:	17:10:00
Start date:	20/12/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\25402ed0000.dll",#1
Imagebase:	0x7ff70fc90000
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

Start time:	17:10:00
Start date:	20/12/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\25402ed0000.dll",#1
Imagebase:	0x7ff70fc90000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A