ID: 482228
Sample Name: 6d60000.dll
Cookbook: default.jbs
Time: 15:07:27
Date: 13/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Windows Analysis Report 6d60000.dll

Overview

General Information

Sample Name:	6d60000.dll
Analysis ID:	482228
MD5:	0c1e422f4711eb4.
SHA1:	323cb3a64cc15a…
SHA256:	a60364f1d501bc9.
Tags:	exe Gozi
Infos:	

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN
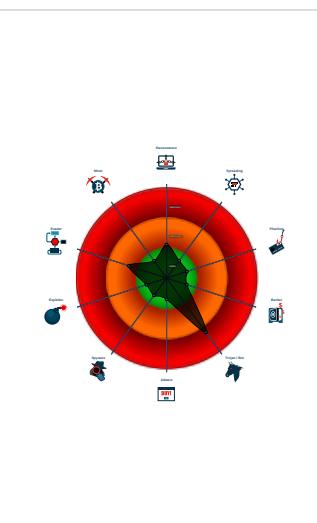
Ursnif

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

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: 4896 cmdline: loaddll64.exe 'C:\Users\user\Desktop\6d60000.dll' MD5: A84133CCB118CF35D49A423CD836D0EF)
  - cmd.exe (PID: 5768 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\6d60000.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 5852 cmdline: rundll32.exe 'C:\Users\user\Desktop\6d60000.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2988 cmdline: rundll32.exe C:\Users\user\Desktop\6d60000.dll,#1 MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
    "RSA Public Key":
"u9HXwops1KELSmyI9sVCp0RUDHHIjNP4aHGxjzGFry6/imJ4SGT8y0VXlGFRc9zyXRVxEXnkK1Sx9S4ULBgKJJV4JjLFFv36DzeAlKEfZ03m1CZU43a/yrQhoFsVYZaqv6diOGxlvmOO3XjBkVrYs6wDfM2BINw64g9oUILCNBiqNe4/
ERHY1XF5A1zPxADFkrQNqYSK/9DBLbHAEeI+op4pIv5Nbgcrd9pFPuimjdkwKDHdtdXGfZgsyeNwUzAgLINLN/AE0qhFNbUuqwS1gIy0LDj5QhU6LQJa91ylwbxVtNKXJoOMS3y4dl28It/qrBuUy0ockllB1P880nqys/92faYbUYzik
2bIla+bg2o=",
    "c2_domain": [
        "art.microsoftsofymicrosoftsoft.at",
        "r23cirt55ysvtdvl.onion",
        "fop.langoonik.com",
        "fog.taginoka.at",
        "pop.biopiof.at",
        "l46t3vgvmtx5wxe6.onion",
        "v10.avyanok.com",
        "apr.intoolkom.at",
        "mas.nagonoman.at"
    ],
    "ip_check_url": [
        "curlmyip.net",
        "ident.me",
        "l2.io/ip",
        "whatismyip.akamai.com"
    ],
    "serpent_key": "kTOVYpceZWWByuJ0",
    "server": "580",
    "sleep_time": "5",
    "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "600",
    "time_value": "600",
    "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "240",
    "SetWaitableTimer_value(CRC_SENDTIMEOUT)": "300",
    "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "240",
    "not_use(CRC_BCTIMEOUT)": "10",
    "botnet": "3500",
    "SetWaitableTimer_value": "60"
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
6d60000.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:

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:

Hooking and other Techniques for Hiding and Protection:

Stealing of Sensitive Information:

Remote Access Functionality:
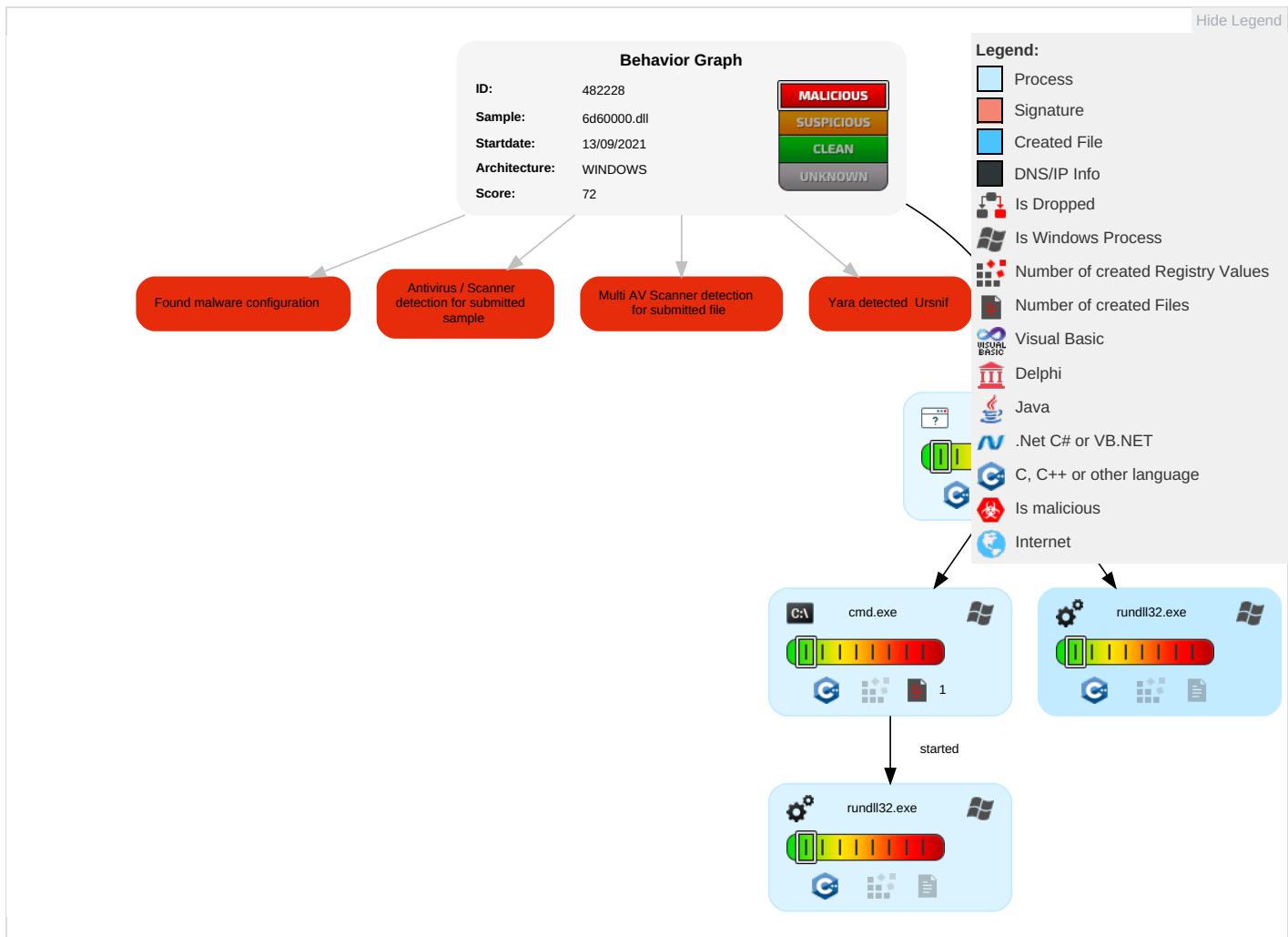
Mitre Att&ck Matrix

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:	482228
Sample:	6d60000.dll
Startdate:	13/09/2021
Architecture:	WINDOWS
Score:	72

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

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

Found malware configuration

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Yara detected Ursnif

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

Source	Detection	Scanner	Label	Link
6d60000.dll	47%	ReversingLabs	Win64.Trojan.Ursnif	
6d60000.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:	482228
Start date:	13.09.2021
Start time:	15:07:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6d60000.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:	- HCA enabled - EGA enabled - HDC enabled - AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.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
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):	6.444512390574505
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:	6d60000.dll
File size:	247808
MD5:	0c1e422f4711eb432c947fd069bf342f
SHA1:	323cb3a64cc15a294fd4960474b50dd8e1aacaa6
SHA256:	a60364f1d501bc92914c23b3d5dff0251741ef8816fdd551 51decc2234b932de
SHA512:	3b8e1bb9218a3ebcc2e34cc0a8c33287390a9bb9775e19 0a002d5fb24777ed604d72aaa10056ed3bce8dc5db283d 0bdc3797301ea025be46812e97d96cce47ba
SSDEEP:	6144:1mnZO0GDlypHAT/cxkDyPFXkfh+3m33c56Wjak 4S9IS83x:1MZOrEpHAT/cLPF0Im3s56WjaC9J8
File Content Preview:	MZ.. ....PE..d..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x18002acf4
Entrypoint Section:	.text
Digitally signed:	false

General

Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	
Time Stamp:	0x61126E40 [Tue Aug 10 12:17:04 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	0.579500368128	zlib compressed data	6.39419710487	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x31000	0x6837	0x6a00	False	0.372383549528	data	5.24608685685	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x38000	0x1e40	0x1800	False	0.3369140625	lif file	3.9828011407	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x3a000	0x1908	0x1a00	False	0.527644230769	data	5.34903211258	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bss	0x3c000	0x1f50	0x2000	False	0.964111328125	data	7.89630830869	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x3e000	0x1000	0xc00	False	0.53125	data	4.88453922321	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: 4896 Parent PID: 5868

General

Start time:	15:08:26
Start date:	13/09/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\6d60000.dll'
Imagebase:	0x7ff6e9180000
File size:	140288 bytes
MD5 hash:	A84133CCB118CF35D49A423CD836D0EF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities   Show Windows behavior

Analysis Process: cmd.exe PID: 5768 Parent PID: 4896

General

Start time:	15:08:27
Start date:	13/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\6d60000.dll',#1
Imagebase:	0x7ff77d8b0000
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: 2988 Parent PID: 4896

General

Start time:	15:08:27
Start date:	13/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\6d60000.dll,#1
Imagebase:	0x7ff6ca6e0000
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

General

Start time:	15:08:27
Start date:	13/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\6d60000.dll',#1
Imagebase:	0x7ff6ca6e0000
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

Joe Sandbox Cloud Basic 33.0.0 White Diamond