ID: 632394
Sample Name: 400000.dll
Cookbook: default.jbs
Time: 16:36:26
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 400000.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Signatures 5
Initial Sample 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Key, Mouse, Clipboard, Microphone and Screen Capturing 5
E-Banking Fraud 5
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 6
Screenshots 6
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 8
World Map of Contacted IPs 8
General Information 8
Warnings 9
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASNs 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
General 9
File Icon 10
Static PE Info 10
General 10
Entrypoint Preview 10
Rich Headers 11
Data Directories 11
Sections 12
Imports 13
Exports 13
Network Behavior 13
UDP Packets 13
DNS Queries 14
DNS Answers 14
Statistics 14
Behavior 14
System Behavior 14
Analysis Process: loaddll32.exePID: 1260, Parent PID: 2972 15
General 15
File Activities 15
Analysis Process: cmd.exePID: 6444, Parent PID: 1260 15
General 15
File Activities 15
Analysis Process: regsvr32.exePID: 6440, Parent PID: 1260 15
General 15
Analysis Process: rundll32.exePID: 6424, Parent PID: 6444 16
General 16
Analysis Process: rundll32.exePID: 4116, Parent PID: 1260 16

Disassembly 16

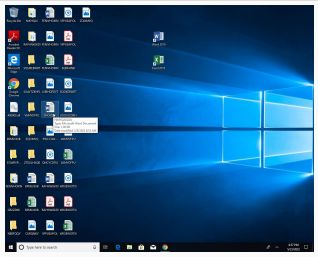
Windows Analysis Report

400000.dll

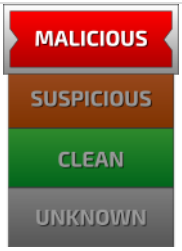
Overview

General Information

Sample Name:	400000.dll
Analysis ID:	632394
MD5:	3b242348cab006..
SHA1:	ed28762dcfbd9e..
SHA256:	c0f637c3bc32ba…
Tags:	dll
Infos:	



Detection



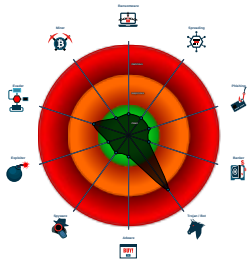
Ursnif

Score:	76
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
- Machine Learning detection for sam…
- Registers a DLL
- Uses 32bit PE files
- Tries to load missing DLLs
- Creates a process in suspended mo…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 1260 cmdline: loaddll32.exe "C:\Users\user\Desktop\400000.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6444 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\400000.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6424 cmdline: rundll32.exe "C:\Users\user\Desktop\400000.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 6440 cmdline: regsvr32.exe /s C:\Users\user\Desktop\400000.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - rundll32.exe (PID: 4116 cmdline: rundll32.exe C:\Users\user\Desktop\400000.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"aVn5cc4yxmeeaL01GhSDa9E9i9AhiobBqld00ioGlWOx7yX95FcGN3HicG7Ma8K4OSypooZMeS/Q9RHBbebiZB0htVqQfpLIdb7MhjDHDEBHCtTQeeoA8LfDaJAEQ2IdhSWjXZZqcMncDfNRXuwiAWQdEo+PTa9HSuW2G4AqVIhs9hBL
2BAZZa8Egh74wCmZjW5gvEmkB+aIKoafUXWf9rJ70sGHrX3U1JPn9tSGnbML+e9g5HE/xe2QT/jXivxkLmTVQv5cQZbQWCQmVvKyQzH4ZmE8FDdAahhD8LLQyis0qatiz93QdIa9WeAg8/W3ijW7qgygdKBu/PDPFWkBFjL9Ourt+q4fq
ApYM+hMcvc=",
  "c2_domain": [
    "agenziaent.top",
    "agenziaentr.top",
    "statusline.ru",
    "statuslines.ru"
  ],
  "botnet": "7631",
  "server": "50",
  "serpent_key": "xlmWrvhFyvbUdepr",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
400000.dll	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

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

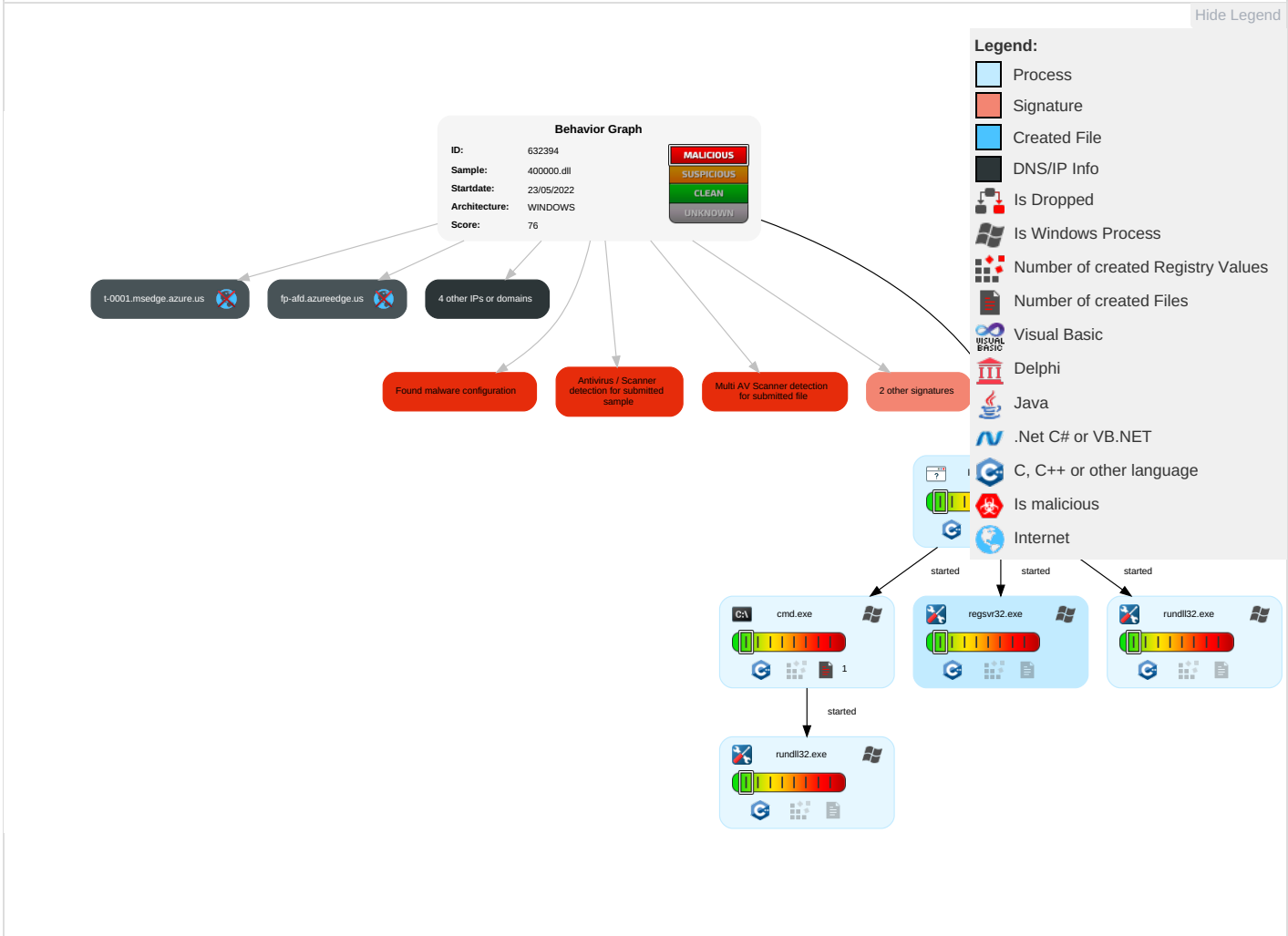
Remote Access Functionality

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	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	1 DLL Side-Loading	1 1 Process Injection	1 Regsvr32	OS Credential Dumping	1 Virtualization/Sandbox Evasion	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Non-Application Layer Protocol	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Rundll32	LSASS Memory	1 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Virtualization/Sandbox Evasion	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

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
400000.dll	63%	ReversingLabs	Win32.Trojan.Ursnif	
400000.dll	100%	Avira	TR/Crypt.XPACK.Gen	
400000.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
eafd-ffgov-phx01.elasticafd.msedge.azure.us	0%	Virustotal		Browse
b-9999.b-msedge.net	0%	Virustotal		Browse
fp-afd.azureedge.us	0%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
eafd-ffgov-phx01.elasticafd.msedge.azure.us	20.141.10.208	true	false	• 0%, Virustotal, Browse	unknown
b-9999.b-msedge.net	13.107.6.254	true	false	• 0%, Virustotal, Browse	unknown
fp-afd.azureedge.us	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632394
Start date and time: 23/05/202216:36:26	2022-05-23 16:36:26 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	400000.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:	6
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:	mal76.troj.winDLL@9/0@1/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .dll • Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): backgroundTaskHost.exe
- Excluded IPs from analysis (whitelisted): 152.199.19.161
- Excluded domains from analysis (whitelisted): store-images.s-microsoft.com, fp-vp.azureedge.net, fp-vp.ec.azureedge.net, b-ring.msedge.net, cs9.wpc.v0cdn.net
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
16:37:47	API Interceptor	1x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

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):	7.530069081172236
TrID:	• 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:	400000.dll

File size:	39424
MD5:	3b242348cab0068aa4ed98a0c4c8cf95
SHA1:	ed28762dcfbd9e1892e56d261a3facf7248817c4
SHA256:	c0f637c3bc32ba773e2a3ef78b086eb680521482bc5e46cb99f231237c9b9265
SHA512:	3708907f1a4dc46babef37015226943d4a78ebe865f090b92a1a759c3232b41cdf97ee7215794f5e85992ada22b4441873e921bf85c507c32e94371992abb56c
SSDEEP:	768:hoxUa+kzeq5v1yCJ9FdR+rqw5Lk6Pf44FqgQYNBarm+dL+84PgT:h/kze8fVkzfzF1QVT4PA
TLSH:	3C03E167AFA40B76C6CFA2B23130377E1527D3460359B8CA8751A52A4B26F4CEE7D051
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\o.....v.....v.....w.....v.....v.....v.....Rich.....PE..L.....b...

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10001c13
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x6213BE9D [Mon Feb 21 16:32:29 2022 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:	7c62ab7d5f2ed68e4989689e898c43c4

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
push ecx
mov eax, dword ptr [ebp+0Ch]
push ebx
push esi
push edi
xor edi, edi
inc edi
xor ebx, ebx
sub eax, ebx
mov dword ptr [ebp-04h], edi
je 00007FCDFCA6DB51h
dec eax
jne 00007FCDFCA6DB9Bh
push 10004188h
call dword ptr [10003044h]
cmp eax, edi
jne 00007FCDFCA6DB88h
push ebx
push 00400000h

Instruction
push ebx
call dword ptr [1000302Ch]
mov dword ptr [10004190h], eax
cmp eax, ebx
je 00007FCDFCA6DB1Ch
mov eax, dword ptr [ebp+08h]
mov esi, 10004198h
mov dword ptr [100041B0h], eax
mov eax, esi
lock xadd dword ptr [eax], edi
mov ecx, dword ptr [ebp+10h]
lea eax, dword ptr [ebp+0Ch]
push eax
call 00007FCDFCA6D39Ah
push eax
push 10001874h
call 00007FCDFCA6DB51h
mov dword ptr [1000418Ch], eax
cmp eax, ebx
jne 00007FCDFCA6DB3Bh
or eax, FFFFFFFFh
lock xadd dword ptr [esi], eax
mov dword ptr [ebp-04h], ebx
jmp 00007FCDFCA6DB2Fh
push 10004188h
call dword ptr [10003040h]
test eax, eax
jne 00007FCDFCA6DB20h
cmp dword ptr [1000418Ch], ebx
je 00007FCDFCA6DB0Ch
mov esi, 00002328h
push edi
push 00000064h
call dword ptr [10003038h]
mov eax, dword ptr [10004198h]
test eax, eax
je 00007FCDFCA6DAE9h
sub esi, 64h
cmp esi, ebx
jnle 00007FCDFCA6DAC9h
push dword ptr [1000418Ch]
call dword ptr [1000300Ch]
push dword ptr [00000000h]

Rich Headers

Programming Language:	• [ASM] VS2008 SP1 build 30729 • [LNK] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729 • [EXP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x3550	0x4e	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3114	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6000	0x148	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x3000	0xb8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x16b7	0x1800	False	0.686360677083	data	6.36921515644	IMAGE_SCN_LNK_REMOVE, IMAGE_SCN_MEM_SYSHEAP, IMAGE_SCN_MEM_PRELOAD, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_16BIT, IMAGE_SCN_LNK_INFO, IMAGE_SCN_LNK_OVER, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_PURGEABLE, IMAGE_SCN_MEM_READ
.rdata	0x3000	0x59e	0x600	False	0.633463541667	data	5.39585151919	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_MEM_LOCKED, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_LNK_OTHER, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_LNK_INFO, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.data	0x4000	0x25c	0x200	False	0.18359375	data	0.925062804208	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_LNK_OTHER, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_16BIT, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_MEM_PURGEABLE, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.bss	0x5000	0x2dc	0x400	False	0.412109375	data	4.62396270929	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_MEM_SYSHEAP, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_MEM_FARDATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_MEM_PRELOAD, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_16BIT, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_MEM_PROTECTED, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_GPREL, IMAGE_SCN_MEM_PURGEABLE, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_NO_DEFER_SPEC_EXC, IMAGE_SCN_MEM_READ
.reloc	0x6000	0x8000	0x7200	False	0.966317160088	data	7.84372410503	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_MEM_SYSHEAP, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_MEM_FARDATA, IMAGE_SCN_MEM_LOCKED, IMAGE_SCN_MEM_PRELOAD, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_LNK_OTHER, IMAGE_SCN_MEM_16BIT, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_MEM_PROTECTED, IMAGE_SCN_LNK_OVER, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_128BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_LNK_COMDAT, IMAGE_SCN_GPREL, IMAGE_SCN_MEM_PURGEABLE, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_NO_DEFER_SPEC_EXC, IMAGE_SCN_MEM_READ

Imports

DLL	Import
ntdll.dll	_snwprintf, memset, NtQuerySystemInformation, _aulldiv, RtlUnwind, NtQueryVirtualMemory
KERNEL32.dll	SetThreadAffinityMask, CloseHandle, HeapAlloc, SetThreadPriority, Sleep, ExitThread, lstrlenW, GetLastError, GetExitCodeThread, HeapCreate, HeapDestroy, GetCurrentThread, SleepEx, WaitForSingleObject, InterlockedDecrement, InterlockedIncrement, HeapFree, GetModuleFileNameW, SetLastError, GetModuleHandleA, VirtualProtect, OpenProcess, CreateEventA, GetLongPathNameW, GetVersion, GetCurrentProcessId, TerminateThread, QueueUserAPC, CreateThread, GetProcAddress, LoadLibraryA, VirtualFree, VirtualAlloc, MapViewOfFile, GetSystemTimeAsFileTime, CreateFileMappingW
ADVAPI32.dll	ConvertStringSecurityDescriptorToSecurityDescriptorA

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x10001e8b

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 16:37:37.587388039 CEST	60996	53	192.168.2.7	8.8.8.8
May 23, 2022 16:37:37.744772911 CEST	53	60996	8.8.8.8	192.168.2.7

DNS Queries

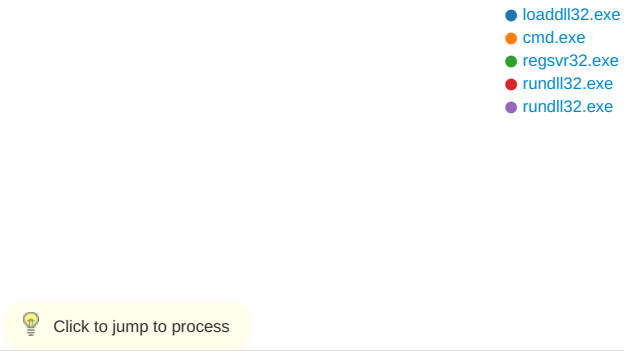
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 23, 2022 16:37:37.587388039 CEST	192.168.2.7	8.8.8.8	0x1608	Standard query (0)	fp-afd.azureedge.us	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 23, 2022 16:37:37.076241016 CEST	8.8.8.8	192.168.2.7	0x15e4	No error (0)	b-ring.b-9999.b-msedge.net	b-9999.b-msedge.net		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 16:37:37.076241016 CEST	8.8.8.8	192.168.2.7	0x15e4	No error (0)	b-9999.b-msedge.net		13.107.6.254	A (IP address)	IN (0x0001)
May 23, 2022 16:37:37.744772911 CEST	8.8.8.8	192.168.2.7	0x1608	No error (0)	fp-afd.azureedge.us	fp-afd.afd.azureedge.us		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 16:37:37.744772911 CEST	8.8.8.8	192.168.2.7	0x1608	No error (0)	fp-afd.afd.azureedge.us	afd.msedge.azure.us		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 16:37:37.744772911 CEST	8.8.8.8	192.168.2.7	0x1608	No error (0)	afd.msedge.azure.us	t-0001.msedge.azure.us		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 16:37:37.744772911 CEST	8.8.8.8	192.168.2.7	0x1608	No error (0)	t-0001.msedge.azure.us	eafd-defaultvips-3p-gov.usgovtrafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 16:37:37.744772911 CEST	8.8.8.8	192.168.2.7	0x1608	No error (0)	eafd-defaultvips-3p-gov.usgovtrafficmanager.net	eafd-ffgov-phx01.elasticafd.msedge.azure.us		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 16:37:37.744772911 CEST	8.8.8.8	192.168.2.7	0x1608	No error (0)	eafd-ffgov-phx01.elasticafd.msedge.azure.us		20.141.10.208	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: **1260**, Parent PID: **2972**

General	
Target ID:	0
Start time:	16:37:42
Start date:	23/05/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\400000.dll"
Imagebase:	0x3a0000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **6444**, Parent PID: **1260**

General	
Target ID:	1
Start time:	16:37:42
Start date:	23/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\400000.dll",#1
Imagebase:	0xdd0000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **6440**, Parent PID: **1260**

General	
Target ID:	2
Start time:	16:37:43
Start date:	23/05/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\400000.dll
Imagebase:	0x12a0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **6424**, Parent PID: **6444**

General	
Target ID:	3
Start time:	16:37:43
Start date:	23/05/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\400000.dll",#1
Imagebase:	0xef0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **4116**, Parent PID: **1260**

General	
Target ID:	4
Start time:	16:37:43
Start date:	23/05/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\400000.dll,DllRegisterServer
Imagebase:	0xef0000
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

No disassembly