ID: 1519390
Sample Name: e.dll
Cookbook: default.jbs
Time: 13:04:41
Date: 26/09/2024
Version: 41.0.0 Charoite

Table of Contents

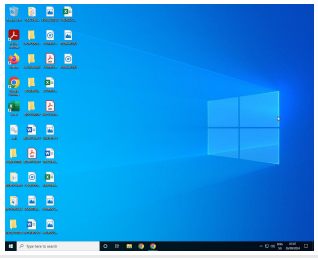
Windows Analysis Report

e.dll

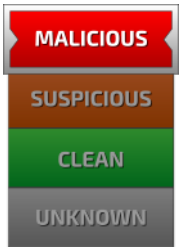
Overview

General Information

Sample name:	e.dll
Analysis ID:	1519390
MD5:	972d3e17b967…
SHA1:	e97c6461bbdc…
SHA256:	b116511e3960…
Infos:	



Detection

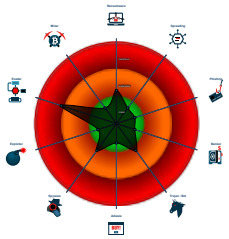


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- AI detected suspicious sample
- Machine Learning detection for sam…
- Tries to detect sandboxes / dynamic…
- Abnormal high CPU Usage
- Contains functionality to call native …
- Contains functionality to query CPU…
- Contains functionality to read the PE…
- Creates a process in suspended mo…
- Detected potential crypto function
- PE file contains more sections than…
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 1868 cmdline: loaddll32.exe "C:\Users\user\Desktop\e.dll" MD5: 51E6071F9CBA48E79F10C84515AAE618)
  - conhost.exe (PID: 7164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - cmd.exe (PID: 4564 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\e.dll",#1 MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - rundll32.exe (PID: 6520 cmdline: rundll32.exe "C:\Users\user\Desktop\e.dll",#1 MD5: 889B99C52A60DD49227C5E485A016679)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Suricata Signatures

No Suricata rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

AI detected suspicious sample

Machine Learning detection for sample

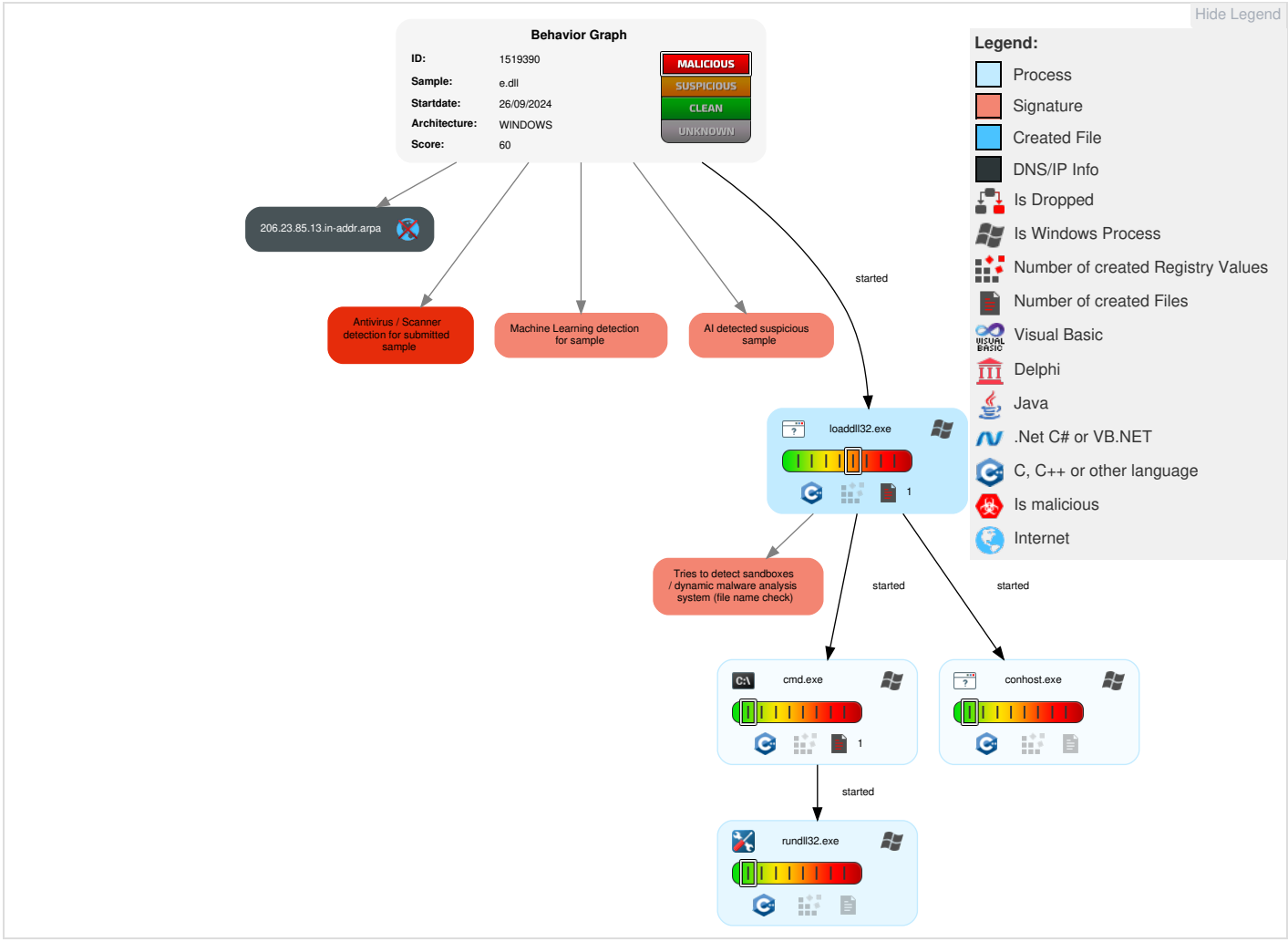
Malware Analysis System Evasion

Tries to detect sandboxes / dynamic malware analysis system (file name check)

Mitre Att&ck Matrix

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	Windows Management Instrumentation	1 DLL Side-Loading	1 1 Process Injection	1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Archive Collected Data	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Rundll32	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	1 Non-Application Layer Protocol	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	1 Software Packing	Security Account Manager	1 1 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	1 Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	1 1 Process Injection	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Protocol Impersonation	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	Internet Connection Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 Obfuscated Files or Information	Cached Domain Credentials	Wi-Fi Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop

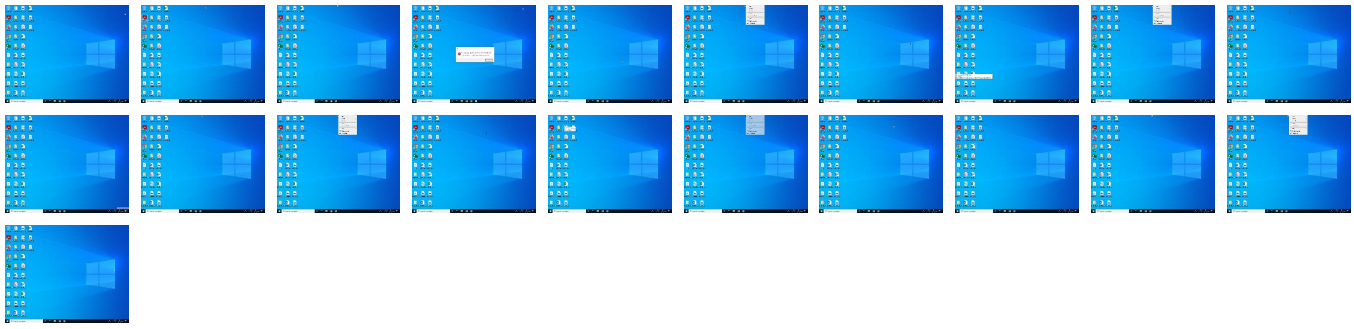
Behavior Graph



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
e.dll	100%	Avira	HEUR/AGEN.1300770	
e.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
206.23.85.13.in-addr.arpa	unknown	unknown	false		unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox version:	41.0.0 Charoite
Analysis ID:	1519390
Start date and time:	2024-09-26 13:04:41 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 4m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	7
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	e.dll
Detection:	MAL
Classification:	mal60.evad.winDLL@6/0@1/0
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 86% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, SIHClient.exe
- Excluded domains from analysis (whitelisted): ocsp.digicert.com, slscr.update.microsoft.com, ctldl.windowsupdate.com, fe3cr.delivery.mp.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: e.dll

Simulations

Behavior and APIs

No simulations

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):	7.857208389757357
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:	e.dll
File size:	2'228'224 bytes
MD5:	972d3e17b96745be89b80ec5d8f4f9d3
SHA1:	e97c6461bbdcd91566f4cb75b456e399b7fe06c2
SHA256:	b116511e3960ab5fa53ad6a3243240be11235ebdc323705827713cf12a9aeeda
SHA512:	060b6a99fae4af1d869cd23b84ab2b18d69eeba5ff60ac1355e605e5ecfe049b41fb52dc5989cdac90572133389673cc48fe366494bcb01de278bf93a247982a
SSDEEP:	49152:kwNgYx8UccgdkvUADkwkxSnTyCbJux8OwyvW:kwBVcNgUyZbnTytPTW
TLSH:	90A502BDB064C781D64B397F7E0A332DB53A17805187AD26E51778AE70236EC11B42BB
File Content Preview:	MZ.....@.....q...q...q..0/...q..u*...q.....q.....q..u*...q....V..q.....q..M....q..Rich.q.....PE..L...q3.f.....!..... !.....P.....@....."....

File Icon

Icon Hash:	0f372331d982ca5a

Static PE Info

General

Entrypoint:	0x401450
Entrypoint Section:	.text

Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE, DLL
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x66F43371 [Wed Sep 25 15:59:45 2024 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:	abe607481ac2953967a12ac99e7e578f

Entrypoint Preview
Instruction
inc edx
inc edx
inc eax
add dword ptr [00433320h], esp
inc eax
dec eax
inc edx
dec eax
jmp 00007F56B0B98CBFh
dec eax
mov eax, esi
push eax
pop dword ptr [00433310h]
xor edx, 0Ah
inc edx
mov eax, edx
xor dword ptr [00433318h], ebx
mov eax, edi
push eax
pop dword ptr [00433314h]
mov dword ptr [0043331Ch], ebp
lea eax, dword ptr [00401210h]
call eax
jmp 00007F56B0B98C63h
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh

Instruction
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
xor edx, 5Fh
mov dword ptr [ebp+00h], eax
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
push ebp
mov ebp, esp
push eax
mov eax, 00000001h
mov dword ptr [ebp-04h], 00000000h
add esp, 04h
pop ebp
ret
nop
nop

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf694	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x20f000	0x6d28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x216000	0x9a4c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xf030	0x1c	.rdata
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	0xf000	0x30	.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	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xc910	0xd000	d8c6c2ce2710e51965ec969f1e605308	False	0.09927133413461539	data	1.5511921998856308	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.crt1	0xe000	0x4e	0x1000	029ebcb0413d7a466159aef461509fff	False	0.025634765625	data	0.19194904064040105	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0xf000	0x837	0x1000	3936868e1249266d25c6c43831ecaa9c	False	0.298583984375	data	2.7036873961689896	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x10000	0x24200	0x24000	728fa214bf78861ed2be0464e5b2e851	False	0.2669542100694444	data	6.204494425770218	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
z4g	0x35000	0x7a4cf	0x7b000	398319310efec22a8e1707da92eb10be	False	0.9946666190294715	data	7.995421677975023	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
qm	0xb0000	0x70e8f	0x71000	fa2c61d59fecbab30f271e9278c4e647	False	0.9991314643252213	data	7.99943170498821	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
L	0x121000	0xe7504	0xe8000	d17b37313f02147b68341a0bca06f4bf	False	0.9966262291217672	data	7.997710795649098	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
CONST	0x209000	0xd88	0x1000	b052a42265a0ef04c82877e017c33121	False	0.7548828125	data	7.057514057791508	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
3	0x20a000	0x13a0	0x2000	6c371933aac1ef87a68049c0aca61de8	False	0.5489501953125	data	5.6043812950914065	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
buicKDZl	0x20c000	0xf0e	0x1000	ecb3c30a4d5685f7394de862efbb63cd	False	0.756591796875	data	6.855147821668895	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
CRT	0x20d000	0x1920	0x2000	f44e399cc7eb92f94e27ac6c5b5c2312	False	0.7213134765625	data	6.598433129737103	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x20f000	0x6d28	0x7000	85992fe593ac7adce6fc2d273bfa339c	False	0.30946568080357145	data	5.688832279317778	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x216000	0xada8	0xb000	96222f6edd2ec89fd0af45e507598034	False	0.1380282315340909	data	5.6863785572940495	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_ICON	0x20f310	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	Russian	Russia	0.5469043151969981
RT_ICON	0x2103b8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	Russian	Russia	0.600177304964539
RT_ICON	0x210820	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	Russian	Russia	0.5107879924953096
RT_ICON	0x2118c8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	Russian	Russia	0.648936170212766
RT_ICON	0x211d30	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	Russian	Russia	0.5668386491557224
RT_ICON	0x212dd8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	Russian	Russia	0.6551418439716312
RT_ICON	0x213240	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	Russian	Russia	0.5905253283302064
RT_ICON	0x2142e8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	Russian	Russia	0.6826241134751773
RT_ICON	0x214750	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	Russian	Russia	0.5466697936210131
RT_ICON	0x2157f8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	Russian	Russia	0.6445035460992907
RT_GROUP_ICON	0x215c60	0x22	data	Russian	Russia	1.0588235294117647
RT_GROUP_ICON	0x215c88	0x22	data	Russian	Russia	1.0588235294117647
RT_GROUP_ICON	0x215cb0	0x22	data	Russian	Russia	1.0588235294117647
RT_GROUP_ICON	0x215cd8	0x22	data	Russian	Russia	1.0588235294117647
RT_GROUP_ICON	0x215d00	0x22	data	Russian	Russia	1.0588235294117647

Imports

DLL	Import
OLEAUT32.dll	VarBoolFromR4
KERNEL32.dll	GetSystemTimeAsFileTime, GetStdHandle, SuspendThread, LoadLibraryExW, OutputDebugStringA, GetModuleFileNameW, GetBinaryTypeW
GDI32.dll	BitBlt

Possible Origin

Language of compilation system	Country where language is spoken	Map
Russian	Russia	

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 26, 2024 13:06:04.147870064 CEST	53	55884	162.159.36.2	192.168.2.5
Sep 26, 2024 13:06:04.706095934 CEST	61011	53	192.168.2.5	1.1.1.1
Sep 26, 2024 13:06:04.713687897 CEST	53	61011	1.1.1.1	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Sep 26, 2024 13:06:04.706095934 CEST	192.168.2.5	1.1.1.1	0x1598	Standard query (0)	206.23.85.13.in-addr.arpa	PTR (Pointer record)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Sep 26, 2024 13:06:04.713687897 CEST	1.1.1.1	192.168.2.5	0x1598	Name error (3)	206.23.85.13.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)	false

Statistics

Behavior

All data are 0.

System Behavior

Analysis Process: loaddll32.exe PID: **1868**, Parent PID: **1028**

General

Target ID:	0
Start time:	07:05:31
Start date:	26/09/2024
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\e.dll"
Imagebase:	0x270000
File size:	126'464 bytes
MD5 hash:	51E6071F9CBA48E79F10C84515AAE618
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	false

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: conhost.exe PID: **7164**, Parent PID: **1868**

General

Target ID:	1
Start time:	07:05:31
Start date:	26/09/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d64d0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high
Has exited:	false

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 4564, Parent PID: 1868

General

Target ID:	2
Start time:	07:05:31
Start date:	26/09/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\e.dll",#1
Imagebase:	0x790000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

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: rundll32.exe PID: 6520, Parent PID: 4564

General

Target ID:	3
Start time:	07:05:31
Start date:	26/09/2024
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\e.dll",#1
Imagebase:	0x380000
File size:	61'440 bytes
MD5 hash:	889B99C52A60DD49227C5E485A016679
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly