ID: 682774
Sample Name: ijexogdf64.dll
Cookbook: default.jbs
Time: 00:27:07
Date: 12/08/2022
Version: 35.0.0 Citrine

Table of Contents

Windows Analysis Report

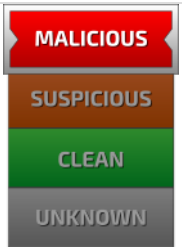
ijexogdf64.dll

Overview

General Information

Sample Name:	ijexogdf64.dll
Analysis ID:	682774
MD5:	d243c07128ee42..
SHA1:	5089dd76080329.
SHA256:	d45c78fa400b32..
Tags:	Bokbot DLL exe IcedID
Infos:	

Detection



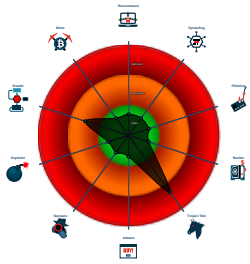
IcedID

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- Malicious sample detected (through…
- Multi AV Scanner detection for dom…
- Yara detected IcedID
- C2 URLs / IPs found in malware con…
- PE file does not import any functions
- Yara signature match
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…
- Contains functionality to call native …
- Contains functionality to dynamicall…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 5140 cmdline: loaddll64.exe "C:\Users\user\Desktop\ijexogdf64.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 5248 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\ijexogdf64.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 4220 cmdline: rundll32.exe "C:\Users\user\Desktop\ijexogdf64.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5300 cmdline: rundll32.exe C:\Users\user\Desktop\ijexogdf64.dll,JdXfbK MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 1004 cmdline: rundll32.exe C:\Users\user\Desktop\ijexogdf64.dll,MDlQdmktXg MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5344 cmdline: rundll32.exe C:\Users\user\Desktop\ijexogdf64.dll,VejwwBbES MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5596 cmdline: rundll32.exe "C:\Users\user\Desktop\ijexogdf64.dll",JdXfbK MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2552 cmdline: rundll32.exe "C:\Users\user\Desktop\ijexogdf64.dll",MDlQdmktXg MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5732 cmdline: rundll32.exe "C:\Users\user\Desktop\ijexogdf64.dll",VejwwBbES MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6020 cmdline: rundll32.exe "C:\Users\user\Desktop\ijexogdf64.dll",XeZsfh MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 760 cmdline: rundll32.exe "C:\Users\user\Desktop\ijexogdf64.dll",YqufWwLNu MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

Threatname: IcedID


```
{
  "url_path": "/news/",
  "C2 url": [
    "peranistaer.top",
    "gruvihabralo.nl",
    "klareqvino.com",
    "ultomductingbig.pro"
  ],
  "Campaign ID": 1573268852
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.244835062.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_IcedID_6	Yara detected IcedID	Joe Security	
00000003.00000002.244835062.0000000180001000.00000020.00001000.00020000.00000000.sdmp	Windows_Trojan_IcedID_91562d18	unknown	unknown	• 0x400:$a: 44 8B 4C 19 2C 4C 03 D6 74 1C 4D 85 C0 74 17 4D 85 C9 74 12 41
00000003.00000002.244948572.0000018E2E579000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_IcedID_6	Yara detected IcedID	Joe Security	
00000003.00000002.244948572.0000018E2E579000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_IcedID_91562d18	unknown	unknown	• 0x10ff8:$a: 44 8B 4C 19 2C 4C 03 D6 74 1C 4D 85 C0 74 17 4D 85 C9 74 12 41

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.180000000.0.unpack	JoeSecurity_IcedID_6	Yara detected IcedID	Joe Security	
3.2.rundll32.exe.180000000.0.unpack	Windows_Trojan_IcedID_91562d18	unknown	unknown	• 0x800:$a: 44 8B 4C 19 2C 4C 03 D6 74 1C 4D 85 C0 74 17 4D 85 C9 74 12 41
3.2.rundll32.exe.18e2e5897f8.1.raw.unpack	JoeSecurity_IcedID_6	Yara detected IcedID	Joe Security	
3.2.rundll32.exe.18e2e5897f8.1.raw.unpack	Windows_Trojan_IcedID_91562d18	unknown	unknown	• 0x800:$a: 44 8B 4C 19 2C 4C 03 D6 74 1C 4D 85 C0 74 17 4D 85 C9 74 12 41

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Yara detected IcedID

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected IcedID

System Summary

Malicious sample detected (through community Yara rule)

Stealing of Sensitive Information

Yara detected IcedID

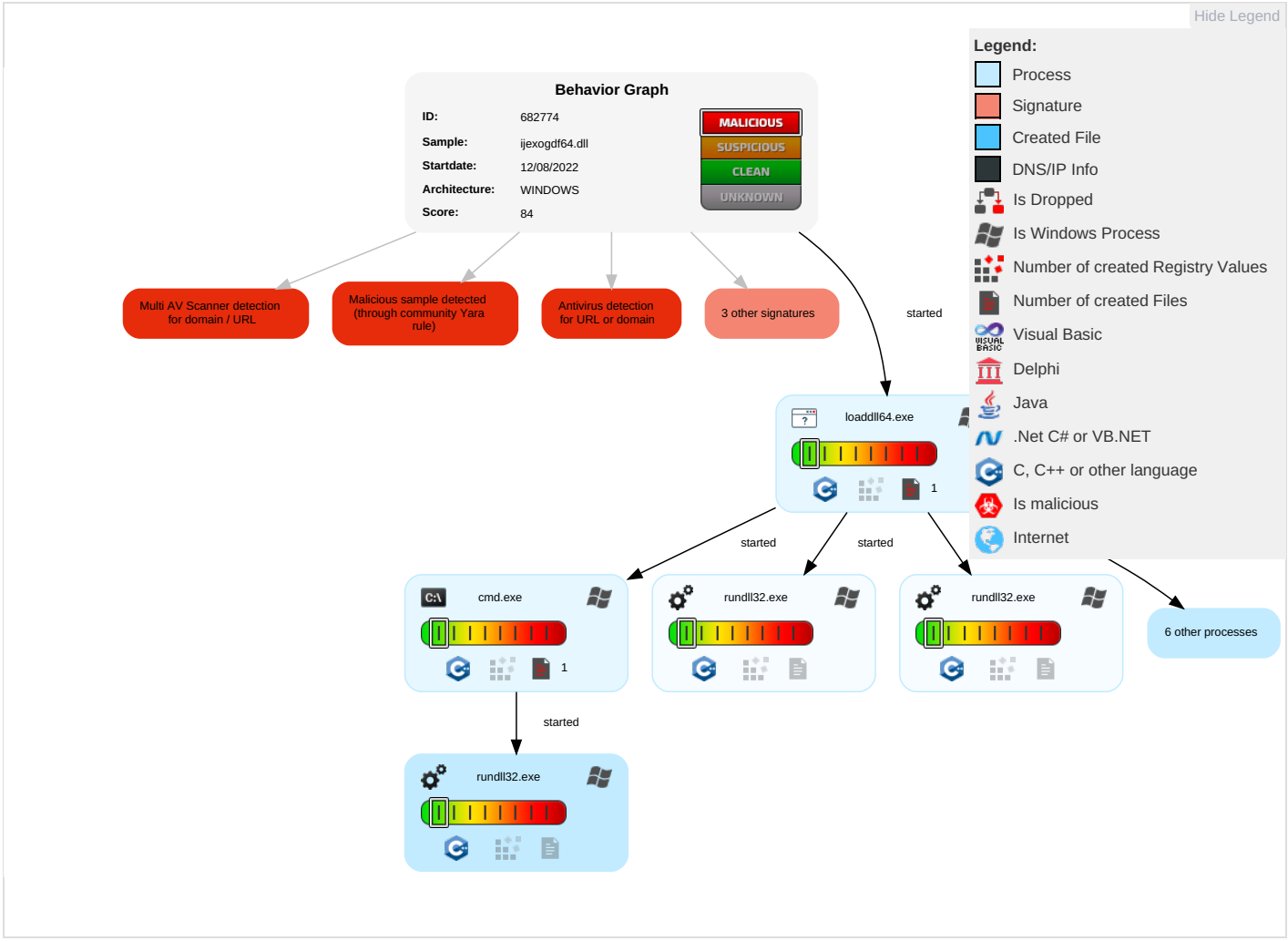
Remote Access Functionality

Yara detected IcedID

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	1 Native API	Path Interception	1 1 Process Injection	1 Rundll32	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 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	Boot or Logon Initialization Scripts	1 1 Virtualization/Sandbox Evasion	LSASS Memory	1 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	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 1 Process Injection	Security Account Manager	2 System Information Discovery	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 Obfuscated Files or Information	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ijexogdf64.dll	7%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.180000000.0.unpack	100%	Avira	HEUR/AGEN.1205106		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
peranistaer.top	16%	Virustotal		Browse
peranistaer.top	0%	Avira URL Cloud	safe	
ultomductingbig.pro	1%	Virustotal		Browse
ultomductingbig.pro	0%	Avira URL Cloud	safe	
klareqvino.com	12%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
klareqvino.com	100%	Avira URL Cloud	malware	
gruvihabralo.nl	15%	Virustotal		Browse
gruvihabralo.nl	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
peranistaer.top	true	• 16%, Virustotal, Browse • Avira URL Cloud: safe	unknown
ultomductingbig.pro	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
klareqvino.com	true	• 12%, Virustotal, Browse • Avira URL Cloud: malware	unknown
gruvihabralo.nl	true	• 15%, Virustotal, Browse • Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	682774
Start date and time:	2022-08-12 00:27:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ijexogdf64.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:	16
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:	mal84.troj.winDLL@21/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 84.1% (good quality ratio 69.2%) • Quality average: 58.6% • Quality standard deviation: 38.6%
HCA Information:	• Successful, ratio: 93% • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.40.129.122, 23.211.6.115
- Excluded domains from analysis (whitelisted): e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, arc.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-frc.francecentral.cloudapp.azure.com, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
00:28:16	API Interceptor	1x Sleep call for process: loaddll64.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) (console) x86-64, for MS Windows
Entropy (8bit):	4.681680523290311

TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	ijexogdf64.dll
File size:	345600
MD5:	d243c07128ee42bccef33bda67ec61d9
SHA1:	5089dd76080329877c488325bc8ef8f736d1d1e4
SHA256:	d45c78fa400b32c11443061dcd1c286d971881ddf35a47143e4d426a3ec6bffd
SHA512:	91c4ca4b3c8051e2813387191414185add498ace63ccf52d420512d6f4fdbefd704b06472250489e4ea4206c18b88299d101f2921a9661adaaadfa7b0f3d5301
SSDEEP:	6144:7bCbif6Fsx+sjdfF+z/+Oz8A3z7S0+uiQ1j5X6UeoCcpWYnmajHcLGvUmVjQP:sa+sJArz8A3z7heeDeoCy9maj8LAj
TLSH:	7F749E78F704ADD6E56E467BCA92BCD912726E229F8EDDCD81647BC30463331EE06805
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4._.Z._.Z._.Z...Y.^.Z...Z.^.Z.....^.Z...X.^.Z.Rich_.Z.....PE..d.....T....." .....>.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x180000000
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DLL
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x54EF86E9 [Thu Feb 26 20:49:45 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	

Entrypoint Preview

Instruction
dec ebp
pop edx
nop
add byte ptr [ebx], al
add byte ptr [eax], al
add byte ptr [eax+eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x55000	0x133	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x56000	0x1e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0x0	0x0	
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	0x53df2	0x53e00	False	0.5699195463859911	DOS executable (COM)	4.663798377543847	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x55000	0x133	0x200	False	0.525390625	data	3.6080974435457183	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x56000	0x1e0	0x200	False	0.52734375	data	4.720822661998389	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x56060	0x17d	XML 1.0 document text	English	United States

Exports

Name	Ordinal	Address
JdXfbK	2	0x180009abe
MDlQdmktXg	3	0x180009706
VejwwBbES	4	0x180009500
XeZsfh	5	0x180009773
YqufWwLNu	6	0x1800094d8
aFXQhh	7	0x180009610
douGisQTrEbuU	8	0x1800097d7
mcejso	9	0x180009895
sIwYjgNBY	10	0x180009baa
vwcKpBZWAuPZtofG	11	0x180009a56
wCUxVrXTsMGVxBGr	12	0x1800099de
zubitjkfnasyfujask	1	0x1800010c0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior

System Behavior

Analysis Process: loaddll64.exe PID: **5140**, Parent PID: **5292**

General

Target ID:	0
Start time:	00:28:03
Start date:	12/08/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\ijexogdf64.dll"
Imagebase:	0x7ff79b990000
File size:	140288 bytes
MD5 hash:	4E8A40CAD6CCC047914E3A7830A2D8AA
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: **5248**, Parent PID: **5140**

General

Target ID:	1
Start time:	00:28:04
Start date:	12/08/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\ijexogdf64.dll",#1
Imagebase:	0x7ff7bb450000
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							
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: **5300**, Parent PID: **5140**

General

Target ID:	2
Start time:	00:28:04
Start date:	12/08/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\ijexogdf64.dll,JdXfbK
Imagebase:	0x7ff7b21b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **4220**, Parent PID: **5248**

General

Target ID:	3
Start time:	00:28:04
Start date:	12/08/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\ijexogdf64.dll",#1
Imagebase:	0x7ff7b21b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 00000003.00000002.244835062.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_IcedID_91562d18, Description: unknown, Source: 00000003.00000002.244835062.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 00000003.00000002.244948572.0000018E2E579000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_IcedID_91562d18, Description: unknown, Source: 00000003.00000002.244948572.0000018E2E579000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	high

Analysis Process: rundll32.exe PID: **1004**, Parent PID: **5140**

General

Target ID:	4
Start time:	00:28:07
Start date:	12/08/2022
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\ijexogdf64.dll,MDlQdmktXg
Imagebase:	0x7ff7b21b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **5344**, Parent PID: **5140**

General

Target ID:	7
Start time:	00:28:11
Start date:	12/08/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\ijexogdf64.dll,VejwwBbES
Imagebase:	0x7ff7b21b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **5596**, Parent PID: **5140**

General

Target ID:	9
Start time:	00:28:14
Start date:	12/08/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\ijexogdf64.dll",JdXfbK
Imagebase:	0x7ff7b21b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **2552**, Parent PID: **5140**

General

Target ID:	10
Start time:	00:28:15
Start date:	12/08/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\ijexogdf64.dll",MDlQdmktXg
Imagebase:	0x7ff7b21b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A

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

Analysis Process: rundll32.exe PID: **5732**, Parent PID: **5140**

General	
Target ID:	11
Start time:	00:28:15
Start date:	12/08/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\ijexogdf64.dll",VejwwBbES
Imagebase:	0x7ff7b21b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **6020**, Parent PID: **5140**

General	
Target ID:	12
Start time:	00:28:16
Start date:	12/08/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\ijexogdf64.dll",XeZsfh
Imagebase:	0x7ff7b21b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **760**, Parent PID: **5140**

General	
Target ID:	13
Start time:	00:28:16
Start date:	12/08/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\ijexogdf64.dll",YqufWwLNu
Imagebase:	0x7ff7b21b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly