ID: 458963
Sample Name: aFqZ2vCizZ
Cookbook: default.jbs
Time: 23:10:46
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

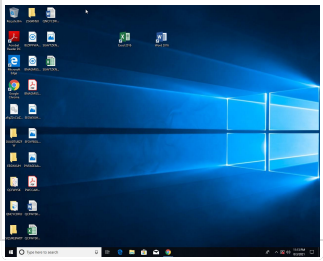
Windows Analysis Report aFqZ2vCizZ

Overview

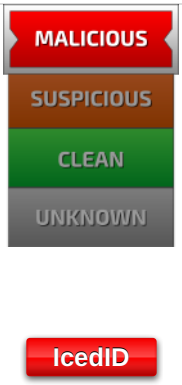
General Information

Sample Name:	aFqZ2vCizZ (renamed file extension from none to dll)
Analysis ID:	458963
MD5:	68c5b6d1c78a20..
SHA1:	b93df3c60247e3c..
SHA256:	d571a65edbdecd..
Infos:	

Most interesting Screenshot:



Detection

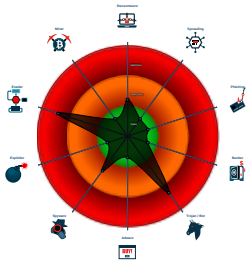


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected IcedID
- Contains functionality to detect hard…
- Performs DNS queries to domains w…
- Rundll32 performs DNS lookup (likel…
- Tries to detect virtualization through…
- Contains functionality for execution …
- Contains functionality to check if a d…
- Contains functionality to query CPU …

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 4884 cmdline: loaddll32.exe 'C:\Users\user\Desktop\aFqZ2vCizZ.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 5900 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\aFqZ2vCizZ.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5396 cmdline: rundll32.exe 'C:\Users\user\Desktop\aFqZ2vCizZ.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5748 cmdline: rundll32.exe C:\Users\user\Desktop\aFqZ2vCizZ.dll,Rulefigure MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000003.356800062.0000000000420000.00000040.00000001.sdmp	JoeSecurity_IcedID_5	Yara detected IcedID	Joe Security	
00000001.00000002.470777736.000000006E143000.00000002.00020000.sdmp	JoeSecurity_IcedID_5	Yara detected IcedID	Joe Security	
00000005.00000002.472279306.000000006E143000.00000002.00020000.sdmp	JoeSecurity_IcedID_5	Yara detected IcedID	Joe Security	
00000001.00000003.363239046.00000000014A0000.00000040.00000001.sdmp	JoeSecurity_IcedID_5	Yara detected IcedID	Joe Security	
00000004.00000003.356776329.00000000003D0000.00000040.00000001.sdmp	JoeSecurity_IcedID_5	Yara detected IcedID	Joe Security	

Click to see the 2 entries

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
1.3.loaddll32.exe.14a1261.0.unpack	JoeSecurity_IcedID_5	Yara detected IcedID	Joe Security	
1.2.loaddll32.exe.6e140000.3.unpack	JoeSecurity_IcedID_5	Yara detected IcedID	Joe Security	
4.3.rundll32.exe.3d1261.0.raw.unpack	JoeSecurity_IcedID_5	Yara detected IcedID	Joe Security	
4.3.rundll32.exe.3d1261.0.unpack	JoeSecurity_IcedID_5	Yara detected IcedID	Joe Security	
5.2.rundll32.exe.6e140000.4.unpack	JoeSecurity_IcedID_5	Yara detected IcedID	Joe Security	
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Yara detected IcedID

Networking:

Performs DNS queries to domains with low reputation

E-Banking Fraud:

Yara detected IcedID

System Summary:

Rundll32 performs DNS lookup (likely malicious behavior)

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Tries to detect virtualization through RDTSC time measurements

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

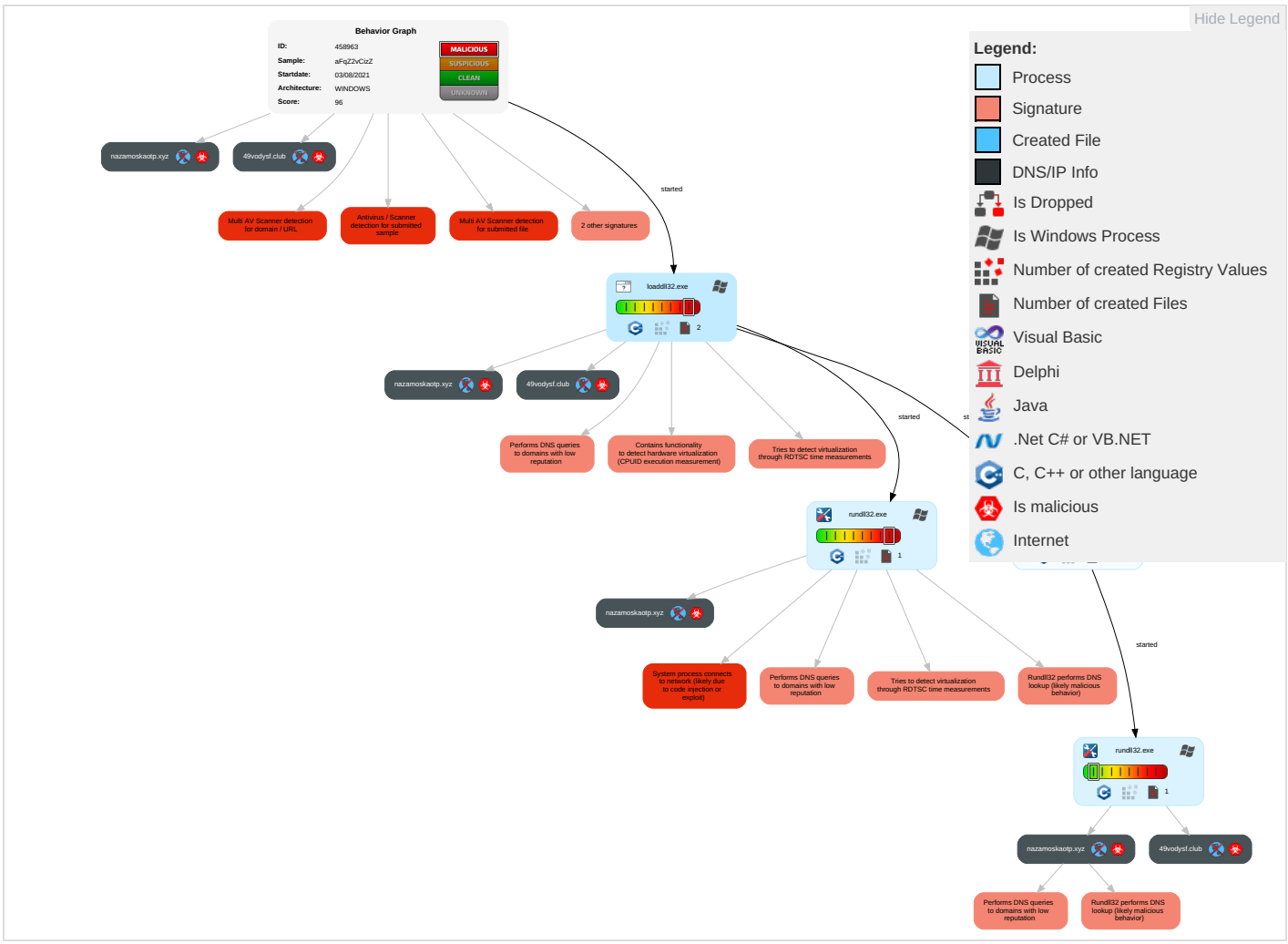
Remote Access Functionality:

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
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1 2	Masquerading 1	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 1 2	LSASS Memory	Security Software Discovery 2 3 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1 1	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 2 2 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols

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
aFqZ2vCizZ.dll	7%	Virustotal		Browse
aFqZ2vCizZ.dll	52%	ReversingLabs	Win32.Trojan.Emotet	
aFqZ2vCizZ.dll	100%	Avira	TR/Crypt.Agent.eprxx	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.3.rundll32.exe.421261.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.3.loaddll32.exe.14a1261.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.loaddll32.exe.6e140000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.3.rundll32.exe.3d1261.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.6e140000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
49vodysf.club	6%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
nazamoskaotp.xyz	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://49vodysf.club/image/?id=0138AFCD2917C220F300FF0000000000000000g	0%	Avira URL Cloud	safe	
http://https://49vodysf.club/image/?id=0138AFCD2917C220F300FF0000000000000000ze6Q	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://49vodysf.club/image/?id=0138AFCD2917C220F300FF0000000000000000$	0%	Avira URL Cloud	safe	
http://https://49vodysf.club/image/?id=0138AFCD2917C220F300FF00000000000000000000$	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://49vodysf.club/e	0%	Avira URL Cloud	safe	
http://https://nazamoskaotp.xyz/image/?id=0138AFCD2917C220F300FF0000000000000000	0%	Avira URL Cloud	safe	
http://https://nazamoskaotp.xyz/	0%	Avira URL Cloud	safe	
http://https://nazamoskaotp.xyz/image/?id=0138AFCD2917C220F300FF0000000000000000e	0%	Avira URL Cloud	safe	
http://https://nazamoskaotp.xyz/image/?id=0138AFCD2917C220F300FF0000000000000000$	0%	Avira URL Cloud	safe	
http://https://49vodysf.club/	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://https://49vodysf.club/image/?id=0138AFCD2917C220F300FF0000000000000000	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://https://49vodysf.club/Z	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
49vodysf.club	unknown	unknown	true	• 6%, Virustotal, Browse	unknown
nazamoskaotp.xyz	unknown	unknown	true	• 6%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458963
Start date:	03.08.2021
Start time:	23:10:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	aFqZ2vCizZ (renamed file extension from none to 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:	27
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:	mal96.troj.evad.winDLL@7/0@24/0
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 2.5% (good quality ratio 2.4%) • Quality average: 88.2% • Quality standard deviation: 21.5%
HCA Information:	• Successful, ratio: 51% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
23:12:46	API Interceptor	11x Sleep call for process: rundll32.exe modified
23:12:49	API Interceptor	10x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.585836517428109
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:	aFqZ2vCizZ.dll
File size:	283952
MD5:	68c5b6d1c78a20a82a6c2693a6997fea
SHA1:	b93df3c60247e3ce0654a509bd9e419cb7b8cd56
SHA256:	d571a65edbdecd8530716dad1e96b6ef8239066fdc52eb8a9ad075659f36831b
SHA512:	19f11996e54209b60a3df2aee37bebbe927f611ba226746ef31d77fbc4ecad69d9c1b7cd0c8f58a4469c7dfdedd4a8b6d1f11785031256dca02592830cc4265d
SSDEEP:	6144:BCVRhsJ5bLak1GyxVNuEwuJdTkrrwAOH/1EB:BCVRhYak1HZuEwuTTirw8B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....j=.....j?.)....j>.....a.....a.....a....._.....,.....,.....,.3.....,.....Rich.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1001899e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x55351A7C [Mon Apr 20 15:25:48 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:	87f7f637e19a1ee1e2d0d955ecbd7599

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Sectigo RSA Code Signing CA, O=Sectigo Limited, L=Salford, S=Greater Manchester, C=GB
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 10/11/2020 5:00:00 PM 10/12/2021 4:59:59 PM
Subject Chain	• CN=FABO SP Z O O, O=FABO SP Z O O, STREET=7 Ul. Ofiar Firleja, L=Radom, S=MAZOWIECKIE, PostalCode=26-600, C=PL
Version:	3
Thumbprint MD5:	2217A1DC290135CD210CE3105E25FA56
Thumbprint SHA-1:	BB1B413CC8678C2FB2AF345A53DA186BACE5850F
Thumbprint SHA-256:	2EA2C7625C1A42FFF63F0B17CFC4FD0C0F76D7EB45A86B18EC9A630D3D8AD913
Serial:	00CA7D54577243934F665FD1D443855A3D

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2b3c5	0x2b400	False	0.545221053107	data	6.68096897507	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2d000	0x13076	0x13200	False	0.476983762255	data	5.41140229676	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x41000	0xad60	0x1a00	False	0.254507211538	data	4.50074118182	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x4c000	0x4a4	0x600	False	0.380208333333	data	4.61149850163	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x4d000	0x2dc8	0x2e00	False	0.732846467391	data	6.61767250601	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 23:12:47.263556957 CEST	192.168.2.3	8.8.8.8	0xa071	Standard query (0)	nazamoskaotp.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 23:12:47.293925047 CEST	192.168.2.3	8.8.8.8	0xa7b	Standard query (0)	nazamoskaotp.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 23:12:50.066324949 CEST	192.168.2.3	8.8.8.8	0xb592	Standard query (0)	nazamoskaotp.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 23:12:53.033365965 CEST	192.168.2.3	8.8.8.8	0x5bda	Standard query (0)	49vodysf.club	A (IP address)	IN (0x0001)
Aug 3, 2021 23:12:55.174268961 CEST	192.168.2.3	8.8.8.8	0xe744	Standard query (0)	49vodysf.club	A (IP address)	IN (0x0001)
Aug 3, 2021 23:12:58.160826921 CEST	192.168.2.3	8.8.8.8	0x26ff	Standard query (0)	nazamoskaotp.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:00.314862013 CEST	192.168.2.3	8.8.8.8	0xd233	Standard query (0)	nazamoskaotp.xyz	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 23:13:03.274074078 CEST	192.168.2.3	8.8.8.8	0xfb8b	Standard query (0)	49vodysf.club	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:05.448132992 CEST	192.168.2.3	8.8.8.8	0x42e	Standard query (0)	49vodysf.club	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:08.457591057 CEST	192.168.2.3	8.8.8.8	0x3e4	Standard query (0)	nazamoskaotp.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:11.206459045 CEST	192.168.2.3	8.8.8.8	0x6e3	Standard query (0)	nazamoskaotp.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:13.573446989 CEST	192.168.2.3	8.8.8.8	0xe102	Standard query (0)	49vodysf.club	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:16.337009907 CEST	192.168.2.3	8.8.8.8	0x9734	Standard query (0)	49vodysf.club	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:18.714106083 CEST	192.168.2.3	8.8.8.8	0xb8b7	Standard query (0)	nazamoskaotp.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:21.490185022 CEST	192.168.2.3	8.8.8.8	0x7fe3	Standard query (0)	nazamoskaotp.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:23.868182898 CEST	192.168.2.3	8.8.8.8	0xcdbd	Standard query (0)	49vodysf.club	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:26.585146904 CEST	192.168.2.3	8.8.8.8	0xf61b	Standard query (0)	49vodysf.club	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:29.179938078 CEST	192.168.2.3	8.8.8.8	0x3c29	Standard query (0)	nazamoskaotp.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:31.702316999 CEST	192.168.2.3	8.8.8.8	0xbe85	Standard query (0)	nazamoskaotp.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:34.308806896 CEST	192.168.2.3	8.8.8.8	0xb94a	Standard query (0)	49vodysf.club	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:36.805557966 CEST	192.168.2.3	8.8.8.8	0xaf4	Standard query (0)	49vodysf.club	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:39.380740881 CEST	192.168.2.3	8.8.8.8	0x7c52	Standard query (0)	nazamoskaotp.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:41.881194115 CEST	192.168.2.3	8.8.8.8	0xd471	Standard query (0)	nazamoskaotp.xyz	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:44.458782911 CEST	192.168.2.3	8.8.8.8	0x7b24	Standard query (0)	49vodysf.club	A (IP address)	IN (0x0001)

DNS Answers

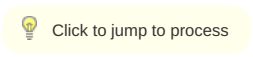
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 23:12:47.320591927 CEST	8.8.8.8	192.168.2.3	0xa071	Server failure (2)	nazamoskaotp.xyz	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:12:47.355040073 CEST	8.8.8.8	192.168.2.3	0xa7b	Server failure (2)	nazamoskaotp.xyz	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:12:50.126974106 CEST	8.8.8.8	192.168.2.3	0xb592	Server failure (2)	nazamoskaotp.xyz	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:12:53.093195915 CEST	8.8.8.8	192.168.2.3	0x5bda	Server failure (2)	49vodysf.club	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:12:55.236943007 CEST	8.8.8.8	192.168.2.3	0xe744	Server failure (2)	49vodysf.club	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:12:58.219361067 CEST	8.8.8.8	192.168.2.3	0x26ff	Server failure (2)	nazamoskaotp.xyz	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:00.374847889 CEST	8.8.8.8	192.168.2.3	0xd233	Server failure (2)	nazamoskaotp.xyz	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:03.341090918 CEST	8.8.8.8	192.168.2.3	0xfb8b	Server failure (2)	49vodysf.club	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:05.513741970 CEST	8.8.8.8	192.168.2.3	0x42e	Server failure (2)	49vodysf.club	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:08.522973061 CEST	8.8.8.8	192.168.2.3	0x3e4	Server failure (2)	nazamoskaotp.xyz	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:11.276391983 CEST	8.8.8.8	192.168.2.3	0x6e3	Server failure (2)	nazamoskaotp.xyz	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:13.629070044 CEST	8.8.8.8	192.168.2.3	0xe102	Server failure (2)	49vodysf.club	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 23:13:16.405914068 CEST	8.8.8.8	192.168.2.3	0x9734	Server failure (2)	49vodysf.club	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:18.775566101 CEST	8.8.8.8	192.168.2.3	0xb8b7	Server failure (2)	nazamoskao tp.xyz	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:21.552967072 CEST	8.8.8.8	192.168.2.3	0x7fe3	Server failure (2)	nazamoskao tp.xyz	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:23.925554991 CEST	8.8.8.8	192.168.2.3	0xcdbd	Server failure (2)	49vodysf.club	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:26.644550085 CEST	8.8.8.8	192.168.2.3	0xf61b	Server failure (2)	49vodysf.club	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:29.242343903 CEST	8.8.8.8	192.168.2.3	0x3c29	Server failure (2)	nazamoskao tp.xyz	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:31.760127068 CEST	8.8.8.8	192.168.2.3	0xbe85	Server failure (2)	nazamoskao tp.xyz	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:34.365719080 CEST	8.8.8.8	192.168.2.3	0xb94a	Server failure (2)	49vodysf.club	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:36.865878105 CEST	8.8.8.8	192.168.2.3	0xaf4	Server failure (2)	49vodysf.club	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:39.445220947 CEST	8.8.8.8	192.168.2.3	0x7c52	Server failure (2)	nazamoskao tp.xyz	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:41.944618940 CEST	8.8.8.8	192.168.2.3	0xd471	Server failure (2)	nazamoskao tp.xyz	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:13:44.517225027 CEST	8.8.8.8	192.168.2.3	0x7b24	Server failure (2)	49vodysf.club	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 4884 Parent PID: 5552

General

Start time:	23:11:32
Start date:	03/08/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\aFqZ2vCizZ.dll'
Imagebase:	0x20000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_IcedID_5, Description: Yara detected IcedID, Source: 00000001.00000002.470777736.000000006E143000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_5, Description: Yara detected IcedID, Source: 00000001.00000003.363239046.00000000014A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

Analysis Process: cmd.exe PID: 5900 Parent PID: 4884

General

Start time:	23:11:33
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\aFqZ2vCizZ.dll',#1
Imagebase:	0xbd0000
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 Show Windows behavior

Analysis Process: rundll32.exe PID: 5748 Parent PID: 4884

General

Start time:	23:11:33
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\aFqZ2vCizZ.dll,Rulefigure
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_IcedID_5, Description: Yara detected IcedID, Source: 00000004.00000003.356776329.00000000003D0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

Analysis Process: rundll32.exe PID: 5396 Parent PID: 5900

General

Start time:	23:11:33
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\aFqZ2vCizZ.dll',#1
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_IcedID_5, Description: Yara detected IcedID, Source: 00000005.00000003.356800062.0000000000420000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_5, Description: Yara detected IcedID, Source: 00000005.00000002.472279306.000000006E143000.00000002.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

Disassembly

Code Analysis