ID: 780216
Sample Name: file.exe
Cookbook: default.jbs
Time: 16:13:13
Date: 08/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report file.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: SmokeLoader 4
Yara Signatures 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Exploits 6
Compliance 6
Networking 6
Key, Mouse, Clipboard, Microphone and Screen Capturing 6
System Summary 6
Data Obfuscation 6
Hooking and other Techniques for Hiding and Protection 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 11
Public IPs 11
Private 11
General Information 11
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
C:\Users\user\AppData\Local\Temp\EE5A.exe 13
C:\Users\user\AppData\Local\Temp\F50.exe 13
C:\Users\user\AppData\Local\Temp\Wtfoiq.tmp 13
C:\Users\user\AppData\Roaming\wdscede 14
C:\Users\user\AppData\Roaming\wdscede:Zone.Identifier 14
Static File Info 14
General 14
File Icon 15
Static PE Info 15
General 15
Entrypoint Preview 15
Rich Headers 16
Data Directories 17
Sections 17
Resources 17
Imports 18

Possible Origin 19
Network Behavior 19
Snort IDS Alerts 19
Network Port Distribution 19
TCP Packets 20
UDP Packets 21
DNS Queries 22
DNS Answers 23
HTTP Request Dependency Graph 31
Statistics 32
Behavior 32
System Behavior 33
Analysis Process: file.exePID: 3620, Parent PID: 3528 33
General 33
Analysis Process: explorer.exePID: 3528, Parent PID: 3620 33
General 33
File Activities 34
Analysis Process: wdscedePID: 6128, Parent PID: 1088 34
General 34
Analysis Process: EE5A.exePID: 916, Parent PID: 3528 34
General 34
File Activities 35
File Created 35
File Written 35
Analysis Process: F50.exePID: 1244, Parent PID: 3528 35
General 35
Analysis Process: rundll32.exePID: 5616, Parent PID: 916 36
General 36
File Activities 36
Analysis Process: F50.exePID: 6044, Parent PID: 6068 36
General 36
Disassembly 36

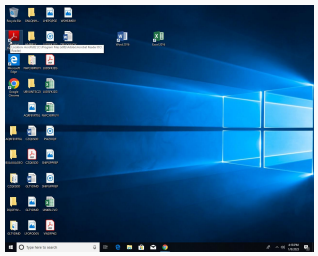
Windows Analysis Report

file.exe

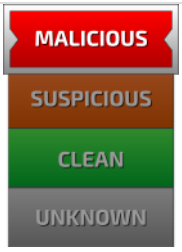
Overview

General Information

Sample Name:	file.exe
Analysis ID:	780216
MD5:	635e3f021a205a..
SHA1:	c4efd1650fe3bde..
SHA256:	ff69d65d2eacb1b..
Tags:	exe
Infos:	



Detection



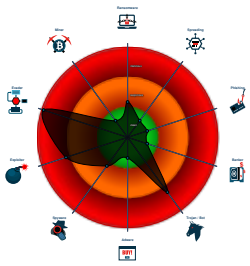
SmokeLoader

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

Signatures

- Yara detected UAC Bypass using C…
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Yara detected SmokeLoader
- System process connects to networ…
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 3620 cmdline: C:\Users\user\Desktop\file.exe MD5: 635E3F021A205AD3A2BF9AAF3D278251)
  - explorer.exe (PID: 3528 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - EE5A.exe (PID: 916 cmdline: C:\Users\user\AppData\Local\Temp\EE5A.exe MD5: 49D7D06EB3FD5E1DADAA505C021AA571)
      - rundll32.exe (PID: 5616 cmdline: "C:\Windows\system32\rundll32.exe" "C:\Users\user\AppData\Local\Temp\Wtfoiq.tmp",lyidwoiowsw MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - F50.exe (PID: 1244 cmdline: C:\Users\user\AppData\Local\Temp\F50.exe MD5: 47D4D75F4D1D3B2C16D375A671BF0FDC)
- wdscede (PID: 6128 cmdline: C:\Users\user\AppData\Roaming\wdscede MD5: 635E3F021A205AD3A2BF9AAF3D278251)
- F50.exe (PID: 6044 cmdline: "C:\Users\user\AppData\Local\Temp\F50.exe" MD5: 47D4D75F4D1D3B2C16D375A671BF0FDC)
- **cleanup**

Malware Configuration

Threatname: SmokeLoader

```
{
  "C2 list": [
    "http://skinndia.com/tmp/",
    "http://cracker.biz/tmp/",
    "http://piratia-life.ru/tmp/"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.422927170.0000000002DA9000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x4346:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000001.00000000.407390160.0000000002A41000.00000020.80000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000001.00000000.407390160.0000000002A41000.00000020.80000000.00040000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x344:$a: 5B 81 EB 34 10 00 00 6A 30 58 64 8B 00 8B 40 0C 8B 40 1C 8B 40 08 89 85 C0
00000000.00000002.422745433.0000000002D51000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000000.00000002.422745433.0000000002D51000.00000004.10000000.00040000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x344:$a: 5B 81 EB 34 10 00 00 6A 30 58 64 8B 00 8B 40 0C 8B 40 1C 8B 40 08 89 85 C0
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.file.exe.2d30000.0.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
4.2.wdscede.2bd0e67.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0.2.file.exe.2c00e67.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
4.2.wdscede.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0.2.file.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 5 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.4 - Destination IP: 211.119.84.112

Timestamp:	192.168.2.4211.119.84.11249697802851815 01/08/23-16:15:21.659638
SID:	2851815
Source Port:	49697
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.4 - Destination IP: 58.235.189.192

Timestamp:	192.168.2.458.235.189.19249696802851815 01/08/23-16:15:19.707702
SID:	2851815
Source Port:	49696
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

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

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Exploits

Yara detected UAC Bypass using CMSTP

Compliance

Detected unpacking (overwrites its own PE header)

Networking

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

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected SmokeLoader

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Checks if the current machine is a virtual machine (disk enumeration)

HIPS / PFW / Operating System Protection Evasion

Benign windows process drops PE files

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

Maps a DLL or memory area into another process

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information

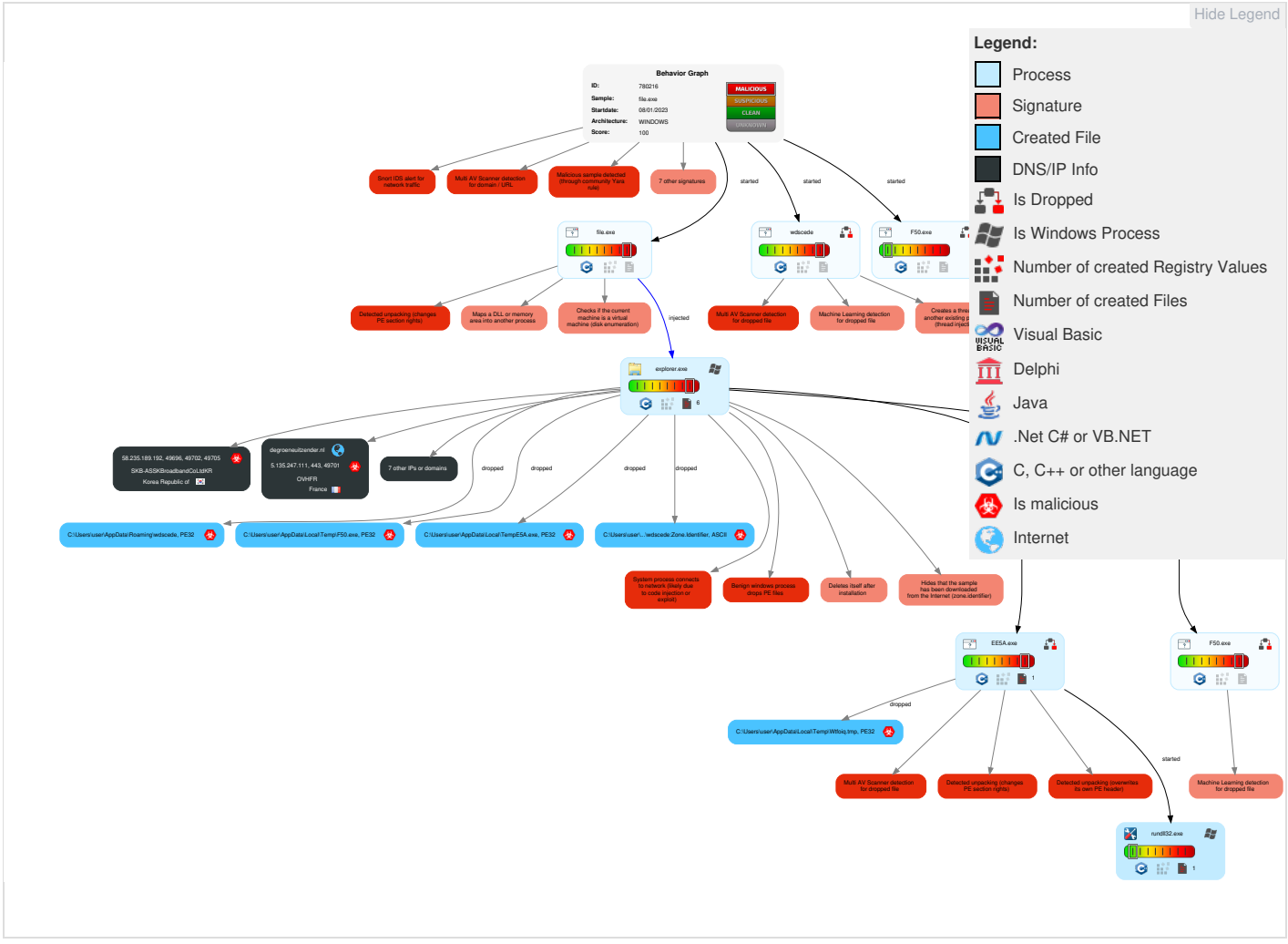
Yara detected SmokeLoader

Yara detected SmokeLoader

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 Exploitation for Client Execution	1 DLL Side-Loading	3 2 Process Injection	1 1 Masquerading	1 Input Capture	1 Query Registry	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	2 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	3 1 Virtualization/Sandbox Evasion	LSASS Memory	2 1 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 2 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)	3 2 Process Injection	Security Account Manager	3 1 Virtualization/Sandbox Evasion	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 Hidden Files and Directories	NTDS	3 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 Application Window 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 Rundll32	Cached Domain Credentials	1 2 System Information 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	2 1 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 File Deletion	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

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
file.exe	46%	ReversingLabs	Win32.Backdoor.Convagent	
file.exe	52%	Virustotal		Browse
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\F50.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\EE5A.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\wdscede	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\EE5A.exe	48%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\Wtfoiq.tmp	40%	ReversingLabs	Win32.Trojan.DanaBot	
C:\Users\user\AppData\Roaming\wdscede	46%	ReversingLabs	Win32.Backdoor.Convagent	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download

Source	Detection	Scanner	Label	Link	Download
12.2.F50.exe.4a6512c.2.unpack	100%	Avira	TR/Patched.Ren.Gen7		Download File
0.2.file.exe.2c00e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.EE5A.exe.4a70e67.1.unpack	100%	Avira	HEUR/AGEN.1215478		Download File
5.3.EE5A.exe.4b90000.0.unpack	100%	Avira	HEUR/AGEN.1215478		Download File
4.2.wdscede.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.3.wdscede.2be0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.F50.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.EE5A.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen2		Download File
0.2.file.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.F50.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.file.exe.2d30000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.wdscede.2bd0e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
vatra.at	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://degroeneuitzender.nl/systems/index.php	0%	URL Reputation	safe	
http://https://degroeneuitzender.nl/systems/index.php	0%	URL Reputation	safe	
http://194.135.33.42/intel.exe	2%	Virustotal		Browse
http://cracker.biz/tmp/	0%	URL Reputation	safe	
http://skinndia.com/tmp/	0%	URL Reputation	safe	
http://vatra.at/tmp/	0%	URL Reputation	safe	
http://194.135.33.42/intel.exe	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
degroeneuitzender.nl	5.135.247.111	true	true		unknown
vatra.at	200.46.66.71	true	true	• 5%, Virustotal, Browse	unknown

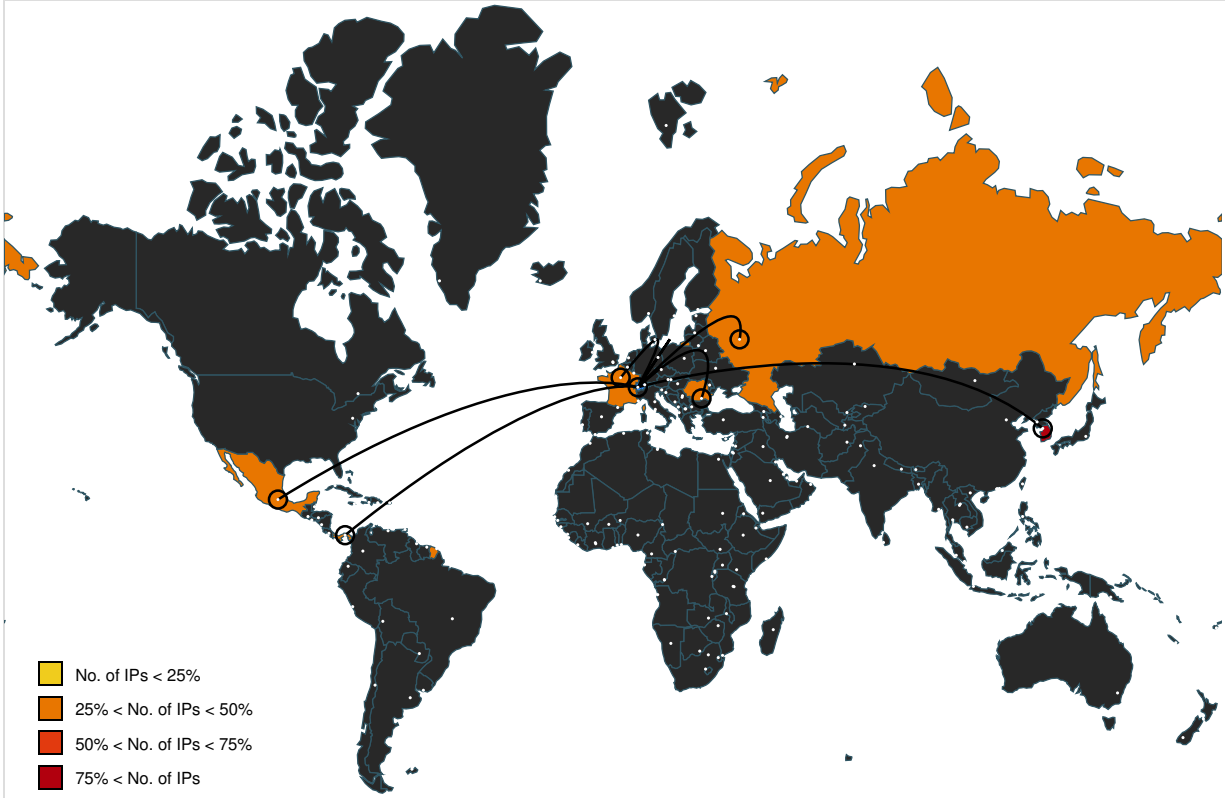
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://degroeneuitzender.nl/systems/index.php	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://194.135.33.42/intel.exe	true	• 2%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://cracker.biz/tmp/	true	• URL Reputation: safe	unknown
http://skinndia.com/tmp/	true	• URL Reputation: safe	unknown
http://vatra.at/tmp/	true	• URL Reputation: safe	unknown
http://piratia-life.ru/tmp/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000001.00000000.39373669 8.0000000008260000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000000.419303004.0000000008260000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000000.362501774.000000 0008260000.00000004.00000001.00020000.00 000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.135.247.111	degroeneuitzender.nl	France		16276	OVHFR	true
187.170.238.164	unknown	Mexico		8151	UninetSAdeCVMX	false
194.135.33.42	unknown	Russian Federation		49392	ASBAXETNRU	true
211.40.39.251	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
109.98.58.98	unknown	Romania		9050	RTDBucharestRomaniaRO	false
211.119.84.112	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
200.46.66.71	vatra.at	Panama		18809	CableOndaPA	true
58.235.189.192	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	780216
Start date and time:	2023-01-08 16:13:13 +01:00
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 12m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winEXE@9/5@21/9
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 76.1% (good quality ratio 62.3%) • Quality average: 45.2% • Quality standard deviation: 29.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, dllhost.exe, audiodg.exe, consent.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:15:19	Task Scheduler	Run new task: Firefox Default Browser Agent E2E714EC49953D45 path: C:\Users\user\AppData\Roaming\wdscede
16:15:45	API Interceptor	63x Sleep call for process: rundll32.exe modified
16:16:10	API Interceptor	1x Sleep call for process: F50.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

C:\Users\user\AppData\Local\Temp\EE5A.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1073152
Entropy (8bit):	7.800005615070523
Encrypted:	false
SSDEEP:	24576:7WRAptQ16TfInIvitS/Y7OGpcvzSOjevqfW21j5AgNtvgwNwtJ:7WGI1SgnK+uneOaczp+L
MD5:	49D7D06EB3FD5E1DADAA505C021AA571
SHA1:	45F8B60703019D3605DECEA63C0FDB432194C4B2
SHA-256:	ED60811AACE1E6EF88644171C8CBC9F1D61C0DE87A389ACF32BBE502F368A12F
SHA-512:	A8BD3A0C03A832448016E573DF69D82D7D356A02C752F462DA1C3458CE7FDD1E40FF1C3735709BE32167D19226457BB73D13B3D8DC2C757ACF7D52AB7EB095E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 48%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u.....x`.....1.....Rich.....P E..L...e..a.....z.....@.....}..P....P..`.....C..@.....te xt...fx.....z..... ..`.data...4.....\..~.....@....rsrc...`....P.....@..@.....

C:\Users\user\AppData\Local\Temp\F50.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	599040
Entropy (8bit):	7.538329945935505
Encrypted:	false
SSDEEP:	12288:S/VwX5av3q6jIUKhWBburVNHNZVQVw8wlQx+OJ:Sa5av3IUeWgr37VQa8bx3J
MD5:	47D4D75F4D1D3B2C16D375A671BF0FDC
SHA1:	2F55C731492FEE2361A4E61E208428ACE550A977
SHA-256:	F56F46AC0D1D1019F16204341EE0C49F8FF37529EEEA25A4ECA4ED3D60F8B106
SHA-512:	6A3423D03229EFC187C69121659C193C4B0C2D300844D4E0FF8C488293C78FBBDC4A3F3CFD0C3F238C132EA6979590BFA40266F6977D1028737D52279203E24E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u.....x`.....1.....Rich.....P E..L...P'/b.....z...t~.....@.....S.....}..P.....~.`.....C..@.....te xt...fx.....z..... ..`.data....{|..... ...~.....@....rsrc...`.....~.....@..@.....

C:\Users\user\AppData\Local\Temp\Wtfoiq.tmp

Process:	C:\Users\user\AppData\Local\Temp\EE5A.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	731648

Entropy (8bit):	6.87595719384168
Encrypted:	false
SSDEEP:	12288:V8jfuQWjK3lYRk52K/iAkyshv2zjTywBZmAUYiUy+Cz1yVBMjiltbNFNlJOI/rFu:V8DWK3l4kkEPjfywBLTvFFMjiltbNrdr
MD5:	9DD70D24B2657A9254B9FD536A4D06D5
SHA1:	348A1D210D7C4DAEF8ECDB692EADF3975971E8EE
SHA-256:	D0AC0E9021C6E231C60256198309B7F72CE4C5E772CF343B5456C2CE0664B9BD
SHA-512:	DEE5BFE83FDF196C78EE255E50A25994220CE9ECAC22EB24323DF70E668714D7A810B67DDACE7809D9D7E2160A35C4603DEEDB64B1660D82DDE58586C34D2AB6
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 40%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e:..![.@![.@![.@.,.A&[.@.,.A [.@L..A"[.@![.@5[.@.D.@([.@...A [.@...A [.@...A [.@Rich![.@.....PE..L....'.c.....!.....`.....@.....@.....<.....PF..... .....@.....text..... ..`.rdata.....@..@.data....2.....4.....@....reloc..PF.....H.....@..B..... ....

C:\Users\user\AppData\Roaming\wdscede

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	6.575872566771664
Encrypted:	false
SSDEEP:	3072:dXhYovtL7/BW/LV/0q/R58doOWlbmW25E9WXxpxO5CzELEEhUZNTKXWPr0sd6:ZjL7/B2/0q/wd5kbmWEiWxuCYLiOuN
MD5:	635E3F021A205AD3A2BF9AAF3D278251
SHA1:	C4EFD1650FE3BDE0BCBA9AD2772B451B49809EF4
SHA-256:	FF69D65D2EACB1BD14DB2D94E9DD720AA66A5EF3D108A08D5AFE8A3166305617
SHA-512:	40C7AECD46FD7E0D2C68046407C7BC285300211165F1B92EC5FB3B187D3A05DD0FB1E91EC2E89D75386D28E28736532BC815D1415C3BA0E6093E56022159F64
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 46%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u.....x`.....1.....Rich.....P E..L..../.a.....z...ry....._.....@.....z.....H.....}..P.....y.`..... .....C..@.....te xt...fx.....z..... ..`.data...Txw.....~.....@....rsrc...`.....y.....@..@..... .....

C:\Users\user\AppData\Roaming\wdscede:Zone.Identifier

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.575872566771664

TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	file.exe
File size:	270336
MD5:	635e3f021a205ad3a2bf9aaf3d278251
SHA1:	c4efd1650fe3bde0bcba9ad2772b451b49809ef4
SHA256:	ff69d65d2eacb1bd14db2d94e9dd720aa66a5ef3d108a08d5afe8a3166305617
SHA512:	40c7aecd46fd7e0d2c68046407c7bc285300211165f1b92ec5fb3b187d3a05dd0fb1e91ec2e89d75386d28e28736532bc815d1415c3ba0e6093e56022159f640
SSDEEP:	3072:dXhYovtL7/BW/LV/0q/R58doOWlbmW25E9WXxpxO5CzELEEhUZNTKXWPr0sd6:ZjL7/B2/0q/wd5kbmWEiWxuCYLiOuN
TLSH:	2944AE39358ACC7AC156F4705C35AAE5EFBABC739A20859337943B6F6E702D05222317
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u.....x`.....1.....Rich.....PE..L..../.a.....

File Icon

Icon Hash:	9062e090c6e73144

Static PE Info

General

Entrypoint:	0x405fbf
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x61E02F86 [Thu Jan 13 13:56:22 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	b49d1773872141620d6e88f1989600b7

Entrypoint Preview

Instruction
call 00007F8710977318h
jmp 00007F871097108Eh
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push esi
mov esi, ecx
mov byte ptr [esi+0Ch], 00000000h
test eax, eax
jne 00007F8710971275h
call 00007F8710976FF5h
mov dword ptr [esi+08h], eax
mov ecx, dword ptr [eax+6Ch]
mov dword ptr [esi], ecx
mov ecx, dword ptr [eax+68h]
mov dword ptr [esi+04h], ecx

Instruction
mov ecx, dword ptr [esi]
cmp ecx, dword ptr [0042A2B8h]
je 00007F8710971224h
mov ecx, dword ptr [0042A1D4h]
test dword ptr [eax+70h], ecx
jne 00007F8710971219h
call 00007F8710977D2Bh
mov dword ptr [esi], eax
mov eax, dword ptr [esi+04h]
cmp eax, dword ptr [0042A0D8h]
je 00007F8710971228h
mov eax, dword ptr [esi+08h]
mov ecx, dword ptr [0042A1D4h]
test dword ptr [eax+70h], ecx
jne 00007F871097121Ah
call 00007F871097759Fh
mov dword ptr [esi+04h], eax
mov eax, dword ptr [esi+08h]
test byte ptr [eax+70h], 00000002h
jne 00007F8710971226h
or dword ptr [eax+70h], 02h
mov byte ptr [esi+0Ch], 00000001h
jmp 00007F871097121Ch
mov ecx, dword ptr [eax]
mov dword ptr [esi], ecx
mov eax, dword ptr [eax+04h]
mov dword ptr [esi+04h], eax
mov eax, esi
pop esi
pop ebp
retn 0004h
mov edi, edi
push ebp
mov ebp, esp
sub esp, 10h
push esi
push dword ptr [ebp+0Ch]
lea ecx, dword ptr [ebp-10h]
call 00007F871097117Ah
mov esi, dword ptr [ebp+08h]
movsx eax, byte ptr [esi]
push eax
call 00007F8710977FD3h
cmp eax, 65h
jmp 00007F871097121Eh
inc esi
movzx eax, byte ptr [esi]
push eax
call 00007F8710977D7Ch
test eax, eax
pop ecx
jne 00007F8710971203h
movsx eax, byte ptr [esi]

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [C++] VS2008 build 21022 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x17dec	0x50	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2791000	0x18460	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1220	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x43b8	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d4	.text
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	0x17866	0x17a00	False	0.5359519675925926	OpenPGP Public Key	6.3974793540665855	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x19000	0x2777854	0x11c00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x2791000	0x18460	0x18600	False	0.4747195512820513	data	5.258086247520373	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
AFX_DIALOG_LAYOUT	0x27a6b58	0x2	data		
AFX_DIALOG_LAYOUT	0x27a6b50	0x2	data		
AFX_DIALOG_LAYOUT	0x27a6b60	0x2	data		
AFX_DIALOG_LAYOUT	0x27a6b68	0x2	data		
AFX_DIALOG_LAYOUT	0x27a6b70	0x2	data		
RT_CURSOR	0x27a6b78	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0x27a6cc0	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0x27a6df0	0xf0	Device independent bitmap graphic, 24 x 48 x 1, image size 0		
RT_CURSOR	0x27a6ee0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_CURSOR	0x27a7fb8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x27919e0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Spanish	Venezuela
RT_ICON	0x27920a8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Spanish	Venezuela
RT_ICON	0x2792610	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Spanish	Venezuela
RT_ICON	0x27936b8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Spanish	Venezuela
RT_ICON	0x2793b60	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Spanish	Venezuela

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2794a08	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Spanish	Venezuela
RT_ICON	0x27952b0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Spanish	Venezuela
RT_ICON	0x2795978	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Spanish	Venezuela
RT_ICON	0x2795ee0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	Spanish	Venezuela
RT_ICON	0x2798488	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	Spanish	Venezuela
RT_ICON	0x2799530	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	Spanish	Venezuela
RT_ICON	0x2799eb8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	Spanish	Venezuela
RT_ICON	0x279a398	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Spanish	Venezuela
RT_ICON	0x279b240	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Spanish	Venezuela
RT_ICON	0x279b908	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Spanish	Venezuela
RT_ICON	0x279be70	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Spanish	Venezuela
RT_ICON	0x279e418	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Spanish	Venezuela
RT_ICON	0x279f4c0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Spanish	Venezuela
RT_ICON	0x279fe48	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Spanish	Venezuela
RT_ICON	0x27a0318	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Spanish	Venezuela
RT_ICON	0x27a11c0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Spanish	Venezuela
RT_ICON	0x27a1a68	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Spanish	Venezuela
RT_ICON	0x27a2130	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Spanish	Venezuela
RT_ICON	0x27a2698	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	Spanish	Venezuela
RT_ICON	0x27a4c40	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	Spanish	Venezuela
RT_ICON	0x27a5ce8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	Spanish	Venezuela
RT_ICON	0x27a6670	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	Spanish	Venezuela
RT_STRING	0x27a89c8	0x38c	data	Spanish	Venezuela
RT_STRING	0x27a8d58	0x53c	data	Spanish	Venezuela
RT_STRING	0x27a9298	0x1c8	data	Spanish	Venezuela
RT_GROUP_CURSOR	0x27a6ca8	0x14	data		
RT_GROUP_CURSOR	0x27a8860	0x14	data		
RT_GROUP_CURSOR	0x27a7f88	0x30	data		
RT_GROUP_ICON	0x279a320	0x76	data	Spanish	Venezuela
RT_GROUP_ICON	0x2793b20	0x3e	data	Spanish	Venezuela
RT_GROUP_ICON	0x27a02b0	0x68	data	Spanish	Venezuela
RT_GROUP_ICON	0x27a6ad8	0x76	data	Spanish	Venezuela
RT_VERSION	0x27a8878	0x150	data		

Imports

DLL	Import

DLL	Import
KERNEL32.dll	GetModuleHandleA, CreateDirectoryExA, ReadConsoleInputA, GetTempPathW, GetCurrentDirectoryW, RemoveDirectoryW, OutputDebugStringA, GetProcAddress, LocalAlloc, GetBinaryTypeW, SearchPathA, VerifyVersionInfoA, GetProcessPriorityBoost, EndUpdateResourceW, FindNextFileW, FindFirstVolumeW, LocalFree, GlobalFlags, UpdateResourceW, CreateActCtxA, CopyFileW, InterlockedExchangeAdd, GetConsoleAliasW, VerSetConditionMask, CreateMutexA, DeactivateActCtx, GetDiskFreeSpaceA, MoveFileW, GetLogicalDriveStringsA, ResetEvent, MoveFileExW, CreateMailslotA, WriteConsoleInputA, QueryDosDeviceW, InterlockedDecrement, EnumTimeFormatsW, lstrcatW, FindFirstFileA, FreeEnvironmentStringsA, SetErrorMode, GetTickCount, SetLastError, AllocateUserPhysicalPages, GetPrivateProfileStructA, CopyFileExA, MoveFileWithProgressA, LoadLibraryA, GetLastError, DeleteFileA, GetStartupInfoW, HeapAlloc, EnterCriticalSection, LeaveCriticalSection, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, DeleteCriticalSection, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, GetModuleHandleW, Sleep, ExitProcess, WriteFile, GetModuleFileNameA, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, GetCurrentThreadId, HeapCreate, VirtualFree, HeapFree, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, RaiseException, VirtualAlloc, HeapReAlloc, SetFilePointer, WideCharToMultiByte, GetConsoleCP, GetConsoleMode, InitializeCriticalSectionAndSpinCount, RtlUnwind, MultiByteToWideChar, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, FlushFileBuffers, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, ReadFile, HeapSize, CloseHandle, CreateFileA
GDI32.dll	GetTextFaceA
WINHTTP.dll	WinHttpWriteData

Possible Origin

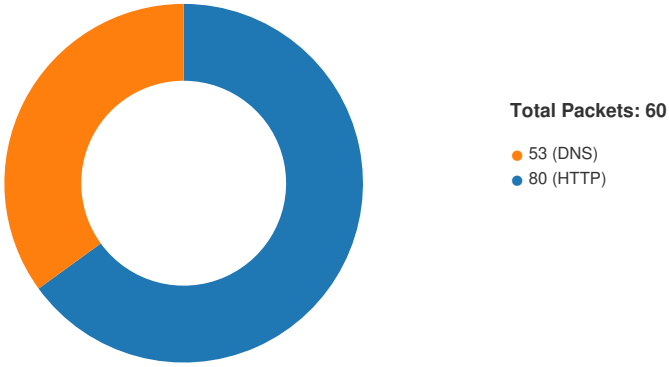
Language of compilation system	Country where language is spoken	Map
Spanish	Venezuela	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4211.119.84.11 249697802851815 01/08/23-16:15:21.659638	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49697	80	192.168.2.4	211.119.84.112
192.168.2.458.235.189.19 249696802851815 01/08/23-16:15:19.707702	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49696	80	192.168.2.4	58.235.189.192

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2023 16:15:17.873878002 CET	49695	80	192.168.2.4	200.46.66.71
Jan 8, 2023 16:15:18.065856934 CET	80	49695	200.46.66.71	192.168.2.4
Jan 8, 2023 16:15:18.066106081 CET	49695	80	192.168.2.4	200.46.66.71
Jan 8, 2023 16:15:18.067889929 CET	49695	80	192.168.2.4	200.46.66.71
Jan 8, 2023 16:15:18.067934036 CET	49695	80	192.168.2.4	200.46.66.71
Jan 8, 2023 16:15:18.255868912 CET	80	49695	200.46.66.71	192.168.2.4
Jan 8, 2023 16:15:18.914453030 CET	80	49695	200.46.66.71	192.168.2.4
Jan 8, 2023 16:15:18.914858103 CET	49695	80	192.168.2.4	200.46.66.71
Jan 8, 2023 16:15:18.920737028 CET	80	49695	200.46.66.71	192.168.2.4
Jan 8, 2023 16:15:18.920962095 CET	49695	80	192.168.2.4	200.46.66.71
Jan 8, 2023 16:15:19.110353947 CET	80	49695	200.46.66.71	192.168.2.4
Jan 8, 2023 16:15:19.427349091 CET	49696	80	192.168.2.4	58.235.189.192
Jan 8, 2023 16:15:19.697201014 CET	80	49696	58.235.189.192	192.168.2.4
Jan 8, 2023 16:15:19.698877096 CET	49696	80	192.168.2.4	58.235.189.192
Jan 8, 2023 16:15:19.707701921 CET	49696	80	192.168.2.4	58.235.189.192
Jan 8, 2023 16:15:19.707772970 CET	49696	80	192.168.2.4	58.235.189.192
Jan 8, 2023 16:15:19.977715969 CET	80	49696	58.235.189.192	192.168.2.4
Jan 8, 2023 16:15:20.906863928 CET	80	49696	58.235.189.192	192.168.2.4
Jan 8, 2023 16:15:20.906899929 CET	80	49696	58.235.189.192	192.168.2.4
Jan 8, 2023 16:15:20.907094002 CET	49696	80	192.168.2.4	58.235.189.192
Jan 8, 2023 16:15:20.907228947 CET	49696	80	192.168.2.4	58.235.189.192
Jan 8, 2023 16:15:21.176888943 CET	80	49696	58.235.189.192	192.168.2.4
Jan 8, 2023 16:15:21.408237934 CET	49697	80	192.168.2.4	211.119.84.112
Jan 8, 2023 16:15:21.659255981 CET	80	49697	211.119.84.112	192.168.2.4
Jan 8, 2023 16:15:21.659519911 CET	49697	80	192.168.2.4	211.119.84.112
Jan 8, 2023 16:15:21.659637928 CET	49697	80	192.168.2.4	211.119.84.112
Jan 8, 2023 16:15:21.659660101 CET	49697	80	192.168.2.4	211.119.84.112
Jan 8, 2023 16:15:21.910904884 CET	80	49697	211.119.84.112	192.168.2.4
Jan 8, 2023 16:15:22.608477116 CET	80	49697	211.119.84.112	192.168.2.4
Jan 8, 2023 16:15:22.608870983 CET	49697	80	192.168.2.4	211.119.84.112
Jan 8, 2023 16:15:22.609222889 CET	80	49697	211.119.84.112	192.168.2.4
Jan 8, 2023 16:15:22.609342098 CET	49697	80	192.168.2.4	211.119.84.112
Jan 8, 2023 16:15:22.639935017 CET	49698	80	192.168.2.4	194.135.33.42
Jan 8, 2023 16:15:22.667131901 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.667264938 CET	49698	80	192.168.2.4	194.135.33.42
Jan 8, 2023 16:15:22.667541027 CET	49698	80	192.168.2.4	194.135.33.42
Jan 8, 2023 16:15:22.694375038 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.694494963 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.694519997 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.694546938 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.694570065 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.694595098 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.694612980 CET	49698	80	192.168.2.4	194.135.33.42
Jan 8, 2023 16:15:22.694618940 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.694644928 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.694653988 CET	49698	80	192.168.2.4	194.135.33.42
Jan 8, 2023 16:15:22.694669962 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.694709063 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.694721937 CET	49698	80	192.168.2.4	194.135.33.42
Jan 8, 2023 16:15:22.694736958 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.694740057 CET	49698	80	192.168.2.4	194.135.33.42
Jan 8, 2023 16:15:22.694819927 CET	49698	80	192.168.2.4	194.135.33.42
Jan 8, 2023 16:15:22.721873999 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.721910000 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.721929073 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.721950054 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.721968889 CET	80	49698	194.135.33.42	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2023 16:15:22.721990108 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.722007990 CET	49698	80	192.168.2.4	194.135.33.42
Jan 8, 2023 16:15:22.722012043 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.722034931 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.722052097 CET	49698	80	192.168.2.4	194.135.33.42
Jan 8, 2023 16:15:22.722055912 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.722078085 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.722086906 CET	49698	80	192.168.2.4	194.135.33.42
Jan 8, 2023 16:15:22.722096920 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.722116947 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.722136021 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.722142935 CET	49698	80	192.168.2.4	194.135.33.42
Jan 8, 2023 16:15:22.722156048 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.722176075 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.722178936 CET	49698	80	192.168.2.4	194.135.33.42
Jan 8, 2023 16:15:22.722196102 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.722215891 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.722218990 CET	49698	80	192.168.2.4	194.135.33.42
Jan 8, 2023 16:15:22.722235918 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.722254992 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.722265959 CET	49698	80	192.168.2.4	194.135.33.42
Jan 8, 2023 16:15:22.722273111 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.722295046 CET	49698	80	192.168.2.4	194.135.33.42
Jan 8, 2023 16:15:22.722326994 CET	49698	80	192.168.2.4	194.135.33.42
Jan 8, 2023 16:15:22.749603987 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.749635935 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.749655008 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.749674082 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.749695063 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.749713898 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.749733925 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.749752045 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.749768972 CET	49698	80	192.168.2.4	194.135.33.42
Jan 8, 2023 16:15:22.749771118 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.749794960 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.749814987 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.749830008 CET	49698	80	192.168.2.4	194.135.33.42
Jan 8, 2023 16:15:22.749835014 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.749856949 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.749864101 CET	49698	80	192.168.2.4	194.135.33.42
Jan 8, 2023 16:15:22.749876976 CET	80	49698	194.135.33.42	192.168.2.4
Jan 8, 2023 16:15:22.749892950 CET	49698	80	192.168.2.4	194.135.33.42
Jan 8, 2023 16:15:22.749897957 CET	80	49698	194.135.33.42	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2023 16:15:17.385386944 CET	56572	53	192.168.2.4	8.8.8.8
Jan 8, 2023 16:15:17.867503881 CET	53	56572	8.8.8.8	192.168.2.4
Jan 8, 2023 16:15:18.947000027 CET	50911	53	192.168.2.4	8.8.8.8
Jan 8, 2023 16:15:19.425726891 CET	53	50911	8.8.8.8	192.168.2.4
Jan 8, 2023 16:15:20.920219898 CET	59683	53	192.168.2.4	8.8.8.8
Jan 8, 2023 16:15:21.406945944 CET	53	59683	8.8.8.8	192.168.2.4
Jan 8, 2023 16:15:28.623908043 CET	64167	53	192.168.2.4	8.8.8.8
Jan 8, 2023 16:15:29.100198984 CET	53	64167	8.8.8.8	192.168.2.4
Jan 8, 2023 16:15:29.408515930 CET	58565	53	192.168.2.4	8.8.8.8
Jan 8, 2023 16:15:29.923669100 CET	53	58565	8.8.8.8	192.168.2.4
Jan 8, 2023 16:15:31.046648026 CET	52239	53	192.168.2.4	8.8.8.8
Jan 8, 2023 16:15:31.080674887 CET	53	52239	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2023 16:15:33.419670105 CET	56807	53	192.168.2.4	8.8.8.8
Jan 8, 2023 16:15:33.439090014 CET	53	56807	8.8.8.8	192.168.2.4
Jan 8, 2023 16:15:34.674283981 CET	61007	53	192.168.2.4	8.8.8.8
Jan 8, 2023 16:15:34.692118883 CET	53	61007	8.8.8.8	192.168.2.4
Jan 8, 2023 16:15:35.060092926 CET	60686	53	192.168.2.4	8.8.8.8
Jan 8, 2023 16:15:35.079653025 CET	53	60686	8.8.8.8	192.168.2.4
Jan 8, 2023 16:15:36.783070087 CET	61124	53	192.168.2.4	8.8.8.8
Jan 8, 2023 16:15:36.802289963 CET	53	61124	8.8.8.8	192.168.2.4
Jan 8, 2023 16:15:37.988836050 CET	59444	53	192.168.2.4	8.8.8.8
Jan 8, 2023 16:15:38.006567955 CET	53	59444	8.8.8.8	192.168.2.4
Jan 8, 2023 16:15:39.296359062 CET	55570	53	192.168.2.4	8.8.8.8
Jan 8, 2023 16:15:39.313945055 CET	53	55570	8.8.8.8	192.168.2.4
Jan 8, 2023 16:15:40.398849964 CET	64906	53	192.168.2.4	8.8.8.8
Jan 8, 2023 16:15:40.419629097 CET	53	64906	8.8.8.8	192.168.2.4
Jan 8, 2023 16:15:41.532485008 CET	59446	53	192.168.2.4	8.8.8.8
Jan 8, 2023 16:15:41.550576925 CET	53	59446	8.8.8.8	192.168.2.4
Jan 8, 2023 16:15:43.427479982 CET	50861	53	192.168.2.4	8.8.8.8
Jan 8, 2023 16:15:43.445261955 CET	53	50861	8.8.8.8	192.168.2.4
Jan 8, 2023 16:15:45.374746084 CET	61088	53	192.168.2.4	8.8.8.8
Jan 8, 2023 16:15:45.392477036 CET	53	61088	8.8.8.8	192.168.2.4
Jan 8, 2023 16:15:47.346012115 CET	58729	53	192.168.2.4	8.8.8.8
Jan 8, 2023 16:15:47.365782976 CET	53	58729	8.8.8.8	192.168.2.4
Jan 8, 2023 16:15:49.017164946 CET	64700	53	192.168.2.4	8.8.8.8
Jan 8, 2023 16:15:49.034532070 CET	53	64700	8.8.8.8	192.168.2.4
Jan 8, 2023 16:15:50.121398926 CET	56022	53	192.168.2.4	8.8.8.8
Jan 8, 2023 16:15:50.390979052 CET	53	56022	8.8.8.8	192.168.2.4
Jan 8, 2023 16:15:51.343632936 CET	60822	53	192.168.2.4	8.8.8.8
Jan 8, 2023 16:15:51.363027096 CET	53	60822	8.8.8.8	192.168.2.4
Jan 8, 2023 16:15:52.935511112 CET	49750	53	192.168.2.4	8.8.8.8
Jan 8, 2023 16:15:52.959707975 CET	53	49750	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 8, 2023 16:15:17.385386944 CET	192.168.2.4	8.8.8.8	0x17e4	Standard query (0)	vatra.at	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:18.947000027 CET	192.168.2.4	8.8.8.8	0x48b0	Standard query (0)	vatra.at	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:20.920219898 CET	192.168.2.4	8.8.8.8	0x2fa7	Standard query (0)	vatra.at	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:28.623908043 CET	192.168.2.4	8.8.8.8	0x43cc	Standard query (0)	vatra.at	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:29.408515930 CET	192.168.2.4	8.8.8.8	0xe3a6	Standard query (0)	vatra.at	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:31.046648026 CET	192.168.2.4	8.8.8.8	0xcb46	Standard query (0)	degroeneuitzender.nl	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:33.419670105 CET	192.168.2.4	8.8.8.8	0x6c34	Standard query (0)	vatra.at	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:34.674283981 CET	192.168.2.4	8.8.8.8	0xb0c3	Standard query (0)	vatra.at	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:35.060092926 CET	192.168.2.4	8.8.8.8	0xe537	Standard query (0)	vatra.at	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:36.783070087 CET	192.168.2.4	8.8.8.8	0x45f8	Standard query (0)	vatra.at	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:37.988836050 CET	192.168.2.4	8.8.8.8	0x249c	Standard query (0)	vatra.at	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:39.296359062 CET	192.168.2.4	8.8.8.8	0xbb75	Standard query (0)	vatra.at	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:40.398849964 CET	192.168.2.4	8.8.8.8	0x8e50	Standard query (0)	vatra.at	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:41.532485008 CET	192.168.2.4	8.8.8.8	0x4ca6	Standard query (0)	vatra.at	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:43.427479982 CET	192.168.2.4	8.8.8.8	0xa1ce	Standard query (0)	vatra.at	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 8, 2023 16:15:45.374746084 CET	192.168.2.4	8.8.8.8	0x6065	Standard query (0)	vatra.at	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:47.346012115 CET	192.168.2.4	8.8.8.8	0x68cf	Standard query (0)	vatra.at	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:49.017164946 CET	192.168.2.4	8.8.8.8	0x177	Standard query (0)	vatra.at	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:50.121398926 CET	192.168.2.4	8.8.8.8	0xf541	Standard query (0)	vatra.at	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:51.343632936 CET	192.168.2.4	8.8.8.8	0xe6ca	Standard query (0)	vatra.at	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:52.935511112 CET	192.168.2.4	8.8.8.8	0x26d0	Standard query (0)	vatra.at	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 8, 2023 16:15:17.867503881 CET	8.8.8.8	192.168.2.4	0x17e4	No error (0)	vatra.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:17.867503881 CET	8.8.8.8	192.168.2.4	0x17e4	No error (0)	vatra.at		109.98.58.98	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:17.867503881 CET	8.8.8.8	192.168.2.4	0x17e4	No error (0)	vatra.at		178.31.8.68	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:17.867503881 CET	8.8.8.8	192.168.2.4	0x17e4	No error (0)	vatra.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:17.867503881 CET	8.8.8.8	192.168.2.4	0x17e4	No error (0)	vatra.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:17.867503881 CET	8.8.8.8	192.168.2.4	0x17e4	No error (0)	vatra.at		222.236.49.124	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:17.867503881 CET	8.8.8.8	192.168.2.4	0x17e4	No error (0)	vatra.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:17.867503881 CET	8.8.8.8	192.168.2.4	0x17e4	No error (0)	vatra.at		58.235.189.192	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:17.867503881 CET	8.8.8.8	192.168.2.4	0x17e4	No error (0)	vatra.at		187.170.238.164	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:17.867503881 CET	8.8.8.8	192.168.2.4	0x17e4	No error (0)	vatra.at		185.95.186.58	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:19.425726891 CET	8.8.8.8	192.168.2.4	0x48b0	No error (0)	vatra.at		58.235.189.192	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:19.425726891 CET	8.8.8.8	192.168.2.4	0x48b0	No error (0)	vatra.at		187.170.238.164	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:19.425726891 CET	8.8.8.8	192.168.2.4	0x48b0	No error (0)	vatra.at		185.95.186.58	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:19.425726891 CET	8.8.8.8	192.168.2.4	0x48b0	No error (0)	vatra.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:19.425726891 CET	8.8.8.8	192.168.2.4	0x48b0	No error (0)	vatra.at		109.98.58.98	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:19.425726891 CET	8.8.8.8	192.168.2.4	0x48b0	No error (0)	vatra.at		178.31.8.68	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:19.425726891 CET	8.8.8.8	192.168.2.4	0x48b0	No error (0)	vatra.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:19.425726891 CET	8.8.8.8	192.168.2.4	0x48b0	No error (0)	vatra.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:19.425726891 CET	8.8.8.8	192.168.2.4	0x48b0	No error (0)	vatra.at		222.236.49.124	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 8, 2023 16:15:19.425726891 CET	8.8.8.8	192.168.2.4	0x48b0	No error (0)	vatra.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:21.406945944 CET	8.8.8.8	192.168.2.4	0x2fa7	No error (0)	vatra.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:21.406945944 CET	8.8.8.8	192.168.2.4	0x2fa7	No error (0)	vatra.at		58.235.189.192	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:21.406945944 CET	8.8.8.8	192.168.2.4	0x2fa7	No error (0)	vatra.at		187.170.238.164	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:21.406945944 CET	8.8.8.8	192.168.2.4	0x2fa7	No error (0)	vatra.at		185.95.186.58	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:21.406945944 CET	8.8.8.8	192.168.2.4	0x2fa7	No error (0)	vatra.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:21.406945944 CET	8.8.8.8	192.168.2.4	0x2fa7	No error (0)	vatra.at		109.98.58.98	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:21.406945944 CET	8.8.8.8	192.168.2.4	0x2fa7	No error (0)	vatra.at		178.31.8.68	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:21.406945944 CET	8.8.8.8	192.168.2.4	0x2fa7	No error (0)	vatra.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:21.406945944 CET	8.8.8.8	192.168.2.4	0x2fa7	No error (0)	vatra.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:21.406945944 CET	8.8.8.8	192.168.2.4	0x2fa7	No error (0)	vatra.at		222.236.49.124	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:29.100198984 CET	8.8.8.8	192.168.2.4	0x43cc	No error (0)	vatra.at		109.98.58.98	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:29.100198984 CET	8.8.8.8	192.168.2.4	0x43cc	No error (0)	vatra.at		178.31.8.68	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:29.100198984 CET	8.8.8.8	192.168.2.4	0x43cc	No error (0)	vatra.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:29.100198984 CET	8.8.8.8	192.168.2.4	0x43cc	No error (0)	vatra.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:29.100198984 CET	8.8.8.8	192.168.2.4	0x43cc	No error (0)	vatra.at		222.236.49.124	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:29.100198984 CET	8.8.8.8	192.168.2.4	0x43cc	No error (0)	vatra.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:29.100198984 CET	8.8.8.8	192.168.2.4	0x43cc	No error (0)	vatra.at		58.235.189.192	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:29.100198984 CET	8.8.8.8	192.168.2.4	0x43cc	No error (0)	vatra.at		187.170.238.164	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:29.100198984 CET	8.8.8.8	192.168.2.4	0x43cc	No error (0)	vatra.at		185.95.186.58	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:29.100198984 CET	8.8.8.8	192.168.2.4	0x43cc	No error (0)	vatra.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:29.923669100 CET	8.8.8.8	192.168.2.4	0xe3a6	No error (0)	vatra.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:29.923669100 CET	8.8.8.8	192.168.2.4	0xe3a6	No error (0)	vatra.at		109.98.58.98	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:29.923669100 CET	8.8.8.8	192.168.2.4	0xe3a6	No error (0)	vatra.at		178.31.8.68	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:29.923669100 CET	8.8.8.8	192.168.2.4	0xe3a6	No error (0)	vatra.at		190.147.188.50	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 8, 2023 16:15:29.923669100 CET	8.8.8.8	192.168.2.4	0xe3a6	No error (0)	vatra.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:29.923669100 CET	8.8.8.8	192.168.2.4	0xe3a6	No error (0)	vatra.at		222.236.49.124	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:29.923669100 CET	8.8.8.8	192.168.2.4	0xe3a6	No error (0)	vatra.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:29.923669100 CET	8.8.8.8	192.168.2.4	0xe3a6	No error (0)	vatra.at		58.235.189.192	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:29.923669100 CET	8.8.8.8	192.168.2.4	0xe3a6	No error (0)	vatra.at		187.170.238.164	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:29.923669100 CET	8.8.8.8	192.168.2.4	0xe3a6	No error (0)	vatra.at		185.95.186.58	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:31.080674887 CET	8.8.8.8	192.168.2.4	0xcb46	No error (0)	degroeneuitzender.nl		5.135.247.111	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:33.439090014 CET	8.8.8.8	192.168.2.4	0x6c34	No error (0)	vatra.at		58.235.189.192	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:33.439090014 CET	8.8.8.8	192.168.2.4	0x6c34	No error (0)	vatra.at		187.170.238.164	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:33.439090014 CET	8.8.8.8	192.168.2.4	0x6c34	No error (0)	vatra.at		185.95.186.58	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:33.439090014 CET	8.8.8.8	192.168.2.4	0x6c34	No error (0)	vatra.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:33.439090014 CET	8.8.8.8	192.168.2.4	0x6c34	No error (0)	vatra.at		109.98.58.98	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:33.439090014 CET	8.8.8.8	192.168.2.4	0x6c34	No error (0)	vatra.at		178.31.8.68	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:33.439090014 CET	8.8.8.8	192.168.2.4	0x6c34	No error (0)	vatra.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:33.439090014 CET	8.8.8.8	192.168.2.4	0x6c34	No error (0)	vatra.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:33.439090014 CET	8.8.8.8	192.168.2.4	0x6c34	No error (0)	vatra.at		222.236.49.124	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:33.439090014 CET	8.8.8.8	192.168.2.4	0x6c34	No error (0)	vatra.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:34.692118883 CET	8.8.8.8	192.168.2.4	0xb0c3	No error (0)	vatra.at		109.98.58.98	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:34.692118883 CET	8.8.8.8	192.168.2.4	0xb0c3	No error (0)	vatra.at		178.31.8.68	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:34.692118883 CET	8.8.8.8	192.168.2.4	0xb0c3	No error (0)	vatra.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:34.692118883 CET	8.8.8.8	192.168.2.4	0xb0c3	No error (0)	vatra.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:34.692118883 CET	8.8.8.8	192.168.2.4	0xb0c3	No error (0)	vatra.at		222.236.49.124	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:34.692118883 CET	8.8.8.8	192.168.2.4	0xb0c3	No error (0)	vatra.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:34.692118883 CET	8.8.8.8	192.168.2.4	0xb0c3	No error (0)	vatra.at		58.235.189.192	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:34.692118883 CET	8.8.8.8	192.168.2.4	0xb0c3	No error (0)	vatra.at		187.170.238.164	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 8, 2023 16:15:34.692118883 CET	8.8.8.8	192.168.2.4	0xb0c3	No error (0)	vatra.at		185.95.186.58	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:34.692118883 CET	8.8.8.8	192.168.2.4	0xb0c3	No error (0)	vatra.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:35.079653025 CET	8.8.8.8	192.168.2.4	0xe537	No error (0)	vatra.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:35.079653025 CET	8.8.8.8	192.168.2.4	0xe537	No error (0)	vatra.at		58.235.189.192	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:35.079653025 CET	8.8.8.8	192.168.2.4	0xe537	No error (0)	vatra.at		187.170.238.164	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:35.079653025 CET	8.8.8.8	192.168.2.4	0xe537	No error (0)	vatra.at		185.95.186.58	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:35.079653025 CET	8.8.8.8	192.168.2.4	0xe537	No error (0)	vatra.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:35.079653025 CET	8.8.8.8	192.168.2.4	0xe537	No error (0)	vatra.at		109.98.58.98	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:35.079653025 CET	8.8.8.8	192.168.2.4	0xe537	No error (0)	vatra.at		178.31.8.68	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:35.079653025 CET	8.8.8.8	192.168.2.4	0xe537	No error (0)	vatra.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:35.079653025 CET	8.8.8.8	192.168.2.4	0xe537	No error (0)	vatra.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:35.079653025 CET	8.8.8.8	192.168.2.4	0xe537	No error (0)	vatra.at		222.236.49.124	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:36.802289963 CET	8.8.8.8	192.168.2.4	0x45f8	No error (0)	vatra.at		58.235.189.192	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:36.802289963 CET	8.8.8.8	192.168.2.4	0x45f8	No error (0)	vatra.at		187.170.238.164	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:36.802289963 CET	8.8.8.8	192.168.2.4	0x45f8	No error (0)	vatra.at		185.95.186.58	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:36.802289963 CET	8.8.8.8	192.168.2.4	0x45f8	No error (0)	vatra.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:36.802289963 CET	8.8.8.8	192.168.2.4	0x45f8	No error (0)	vatra.at		109.98.58.98	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:36.802289963 CET	8.8.8.8	192.168.2.4	0x45f8	No error (0)	vatra.at		178.31.8.68	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:36.802289963 CET	8.8.8.8	192.168.2.4	0x45f8	No error (0)	vatra.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:36.802289963 CET	8.8.8.8	192.168.2.4	0x45f8	No error (0)	vatra.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:36.802289963 CET	8.8.8.8	192.168.2.4	0x45f8	No error (0)	vatra.at		222.236.49.124	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:36.802289963 CET	8.8.8.8	192.168.2.4	0x45f8	No error (0)	vatra.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:38.006567955 CET	8.8.8.8	192.168.2.4	0x249c	No error (0)	vatra.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:38.006567955 CET	8.8.8.8	192.168.2.4	0x249c	No error (0)	vatra.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:38.006567955 CET	8.8.8.8	192.168.2.4	0x249c	No error (0)	vatra.at		84.224.236.42	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 8, 2023 16:15:38.006567955 CET	8.8.8.8	192.168.2.4	0x249c	No error (0)	vatra.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:38.006567955 CET	8.8.8.8	192.168.2.4	0x249c	No error (0)	vatra.at		178.31.8.68	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:38.006567955 CET	8.8.8.8	192.168.2.4	0x249c	No error (0)	vatra.at		151.251.24.5	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:38.006567955 CET	8.8.8.8	192.168.2.4	0x249c	No error (0)	vatra.at		187.232.183.160	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:38.006567955 CET	8.8.8.8	192.168.2.4	0x249c	No error (0)	vatra.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:38.006567955 CET	8.8.8.8	192.168.2.4	0x249c	No error (0)	vatra.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:38.006567955 CET	8.8.8.8	192.168.2.4	0x249c	No error (0)	vatra.at		222.236.49.124	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:39.313945055 CET	8.8.8.8	192.168.2.4	0xbb75	No error (0)	vatra.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:39.313945055 CET	8.8.8.8	192.168.2.4	0xbb75	No error (0)	vatra.at		109.98.58.98	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:39.313945055 CET	8.8.8.8	192.168.2.4	0xbb75	No error (0)	vatra.at		178.31.8.68	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:39.313945055 CET	8.8.8.8	192.168.2.4	0xbb75	No error (0)	vatra.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:39.313945055 CET	8.8.8.8	192.168.2.4	0xbb75	No error (0)	vatra.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:39.313945055 CET	8.8.8.8	192.168.2.4	0xbb75	No error (0)	vatra.at		222.236.49.124	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:39.313945055 CET	8.8.8.8	192.168.2.4	0xbb75	No error (0)	vatra.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:39.313945055 CET	8.8.8.8	192.168.2.4	0xbb75	No error (0)	vatra.at		58.235.189.192	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:39.313945055 CET	8.8.8.8	192.168.2.4	0xbb75	No error (0)	vatra.at		187.170.238.164	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:39.313945055 CET	8.8.8.8	192.168.2.4	0xbb75	No error (0)	vatra.at		185.95.186.58	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:40.419629097 CET	8.8.8.8	192.168.2.4	0x8e50	No error (0)	vatra.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:40.419629097 CET	8.8.8.8	192.168.2.4	0x8e50	No error (0)	vatra.at		109.98.58.98	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:40.419629097 CET	8.8.8.8	192.168.2.4	0x8e50	No error (0)	vatra.at		178.31.8.68	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:40.419629097 CET	8.8.8.8	192.168.2.4	0x8e50	No error (0)	vatra.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:40.419629097 CET	8.8.8.8	192.168.2.4	0x8e50	No error (0)	vatra.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:40.419629097 CET	8.8.8.8	192.168.2.4	0x8e50	No error (0)	vatra.at		222.236.49.124	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:40.419629097 CET	8.8.8.8	192.168.2.4	0x8e50	No error (0)	vatra.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:40.419629097 CET	8.8.8.8	192.168.2.4	0x8e50	No error (0)	vatra.at		58.235.189.192	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 8, 2023 16:15:40.419629097 CET	8.8.8.8	192.168.2.4	0x8e50	No error (0)	vatra.at		187.170.238.164	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:40.419629097 CET	8.8.8.8	192.168.2.4	0x8e50	No error (0)	vatra.at		185.95.186.58	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:41.550576925 CET	8.8.8.8	192.168.2.4	0x4ca6	No error (0)	vatra.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:41.550576925 CET	8.8.8.8	192.168.2.4	0x4ca6	No error (0)	vatra.at		109.98.58.98	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:41.550576925 CET	8.8.8.8	192.168.2.4	0x4ca6	No error (0)	vatra.at		178.31.8.68	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:41.550576925 CET	8.8.8.8	192.168.2.4	0x4ca6	No error (0)	vatra.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:41.550576925 CET	8.8.8.8	192.168.2.4	0x4ca6	No error (0)	vatra.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:41.550576925 CET	8.8.8.8	192.168.2.4	0x4ca6	No error (0)	vatra.at		222.236.49.124	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:41.550576925 CET	8.8.8.8	192.168.2.4	0x4ca6	No error (0)	vatra.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:41.550576925 CET	8.8.8.8	192.168.2.4	0x4ca6	No error (0)	vatra.at		58.235.189.192	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:41.550576925 CET	8.8.8.8	192.168.2.4	0x4ca6	No error (0)	vatra.at		187.170.238.164	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:41.550576925 CET	8.8.8.8	192.168.2.4	0x4ca6	No error (0)	vatra.at		185.95.186.58	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:43.445261955 CET	8.8.8.8	192.168.2.4	0xa1ce	No error (0)	vatra.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:43.445261955 CET	8.8.8.8	192.168.2.4	0xa1ce	No error (0)	vatra.at		109.98.58.98	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:43.445261955 CET	8.8.8.8	192.168.2.4	0xa1ce	No error (0)	vatra.at		178.31.8.68	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:43.445261955 CET	8.8.8.8	192.168.2.4	0xa1ce	No error (0)	vatra.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:43.445261955 CET	8.8.8.8	192.168.2.4	0xa1ce	No error (0)	vatra.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:43.445261955 CET	8.8.8.8	192.168.2.4	0xa1ce	No error (0)	vatra.at		222.236.49.124	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:43.445261955 CET	8.8.8.8	192.168.2.4	0xa1ce	No error (0)	vatra.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:43.445261955 CET	8.8.8.8	192.168.2.4	0xa1ce	No error (0)	vatra.at		58.235.189.192	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:43.445261955 CET	8.8.8.8	192.168.2.4	0xa1ce	No error (0)	vatra.at		187.170.238.164	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:43.445261955 CET	8.8.8.8	192.168.2.4	0xa1ce	No error (0)	vatra.at		185.95.186.58	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:45.392477036 CET	8.8.8.8	192.168.2.4	0x6065	No error (0)	vatra.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:45.392477036 CET	8.8.8.8	192.168.2.4	0x6065	No error (0)	vatra.at		58.235.189.192	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:45.392477036 CET	8.8.8.8	192.168.2.4	0x6065	No error (0)	vatra.at		187.170.238.164	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 8, 2023 16:15:45.392477036 CET	8.8.8.8	192.168.2.4	0x6065	No error (0)	vatra.at		185.95.186.58	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:45.392477036 CET	8.8.8.8	192.168.2.4	0x6065	No error (0)	vatra.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:45.392477036 CET	8.8.8.8	192.168.2.4	0x6065	No error (0)	vatra.at		109.98.58.98	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:45.392477036 CET	8.8.8.8	192.168.2.4	0x6065	No error (0)	vatra.at		178.31.8.68	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:45.392477036 CET	8.8.8.8	192.168.2.4	0x6065	No error (0)	vatra.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:45.392477036 CET	8.8.8.8	192.168.2.4	0x6065	No error (0)	vatra.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:45.392477036 CET	8.8.8.8	192.168.2.4	0x6065	No error (0)	vatra.at		222.236.49.124	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:47.365782976 CET	8.8.8.8	192.168.2.4	0x68cf	No error (0)	vatra.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:47.365782976 CET	8.8.8.8	192.168.2.4	0x68cf	No error (0)	vatra.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:47.365782976 CET	8.8.8.8	192.168.2.4	0x68cf	No error (0)	vatra.at		84.224.236.42	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:47.365782976 CET	8.8.8.8	192.168.2.4	0x68cf	No error (0)	vatra.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:47.365782976 CET	8.8.8.8	192.168.2.4	0x68cf	No error (0)	vatra.at		178.31.8.68	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:47.365782976 CET	8.8.8.8	192.168.2.4	0x68cf	No error (0)	vatra.at		151.251.24.5	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:47.365782976 CET	8.8.8.8	192.168.2.4	0x68cf	No error (0)	vatra.at		187.232.183.160	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:47.365782976 CET	8.8.8.8	192.168.2.4	0x68cf	No error (0)	vatra.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:47.365782976 CET	8.8.8.8	192.168.2.4	0x68cf	No error (0)	vatra.at		175.126.109.15	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:47.365782976 CET	8.8.8.8	192.168.2.4	0x68cf	No error (0)	vatra.at		222.236.49.124	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:49.034532070 CET	8.8.8.8	192.168.2.4	0x177	No error (0)	vatra.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:49.034532070 CET	8.8.8.8	192.168.2.4	0x177	No error (0)	vatra.at		109.98.58.98	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:49.034532070 CET	8.8.8.8	192.168.2.4	0x177	No error (0)	vatra.at		178.31.8.68	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:49.034532070 CET	8.8.8.8	192.168.2.4	0x177	No error (0)	vatra.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:49.034532070 CET	8.8.8.8	192.168.2.4	0x177	No error (0)	vatra.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:49.034532070 CET	8.8.8.8	192.168.2.4	0x177	No error (0)	vatra.at		222.236.49.124	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:49.034532070 CET	8.8.8.8	192.168.2.4	0x177	No error (0)	vatra.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:49.034532070 CET	8.8.8.8	192.168.2.4	0x177	No error (0)	vatra.at		58.235.189.192	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 8, 2023 16:15:49.034532070 CET	8.8.8.8	192.168.2.4	0x177	No error (0)	vatra.at		187.170.238.164	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:49.034532070 CET	8.8.8.8	192.168.2.4	0x177	No error (0)	vatra.at		185.95.186.58	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:50.390979052 CET	8.8.8.8	192.168.2.4	0xf541	No error (0)	vatra.at		187.170.238.164	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:50.390979052 CET	8.8.8.8	192.168.2.4	0xf541	No error (0)	vatra.at		185.95.186.58	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:50.390979052 CET	8.8.8.8	192.168.2.4	0xf541	No error (0)	vatra.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:50.390979052 CET	8.8.8.8	192.168.2.4	0xf541	No error (0)	vatra.at		109.98.58.98	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:50.390979052 CET	8.8.8.8	192.168.2.4	0xf541	No error (0)	vatra.at		178.31.8.68	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:50.390979052 CET	8.8.8.8	192.168.2.4	0xf541	No error (0)	vatra.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:50.390979052 CET	8.8.8.8	192.168.2.4	0xf541	No error (0)	vatra.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:50.390979052 CET	8.8.8.8	192.168.2.4	0xf541	No error (0)	vatra.at		222.236.49.124	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:50.390979052 CET	8.8.8.8	192.168.2.4	0xf541	No error (0)	vatra.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:50.390979052 CET	8.8.8.8	192.168.2.4	0xf541	No error (0)	vatra.at		58.235.189.192	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:51.363027096 CET	8.8.8.8	192.168.2.4	0xe6ca	No error (0)	vatra.at		58.235.189.192	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:51.363027096 CET	8.8.8.8	192.168.2.4	0xe6ca	No error (0)	vatra.at		187.170.238.164	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:51.363027096 CET	8.8.8.8	192.168.2.4	0xe6ca	No error (0)	vatra.at		185.95.186.58	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:51.363027096 CET	8.8.8.8	192.168.2.4	0xe6ca	No error (0)	vatra.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:51.363027096 CET	8.8.8.8	192.168.2.4	0xe6ca	No error (0)	vatra.at		109.98.58.98	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:51.363027096 CET	8.8.8.8	192.168.2.4	0xe6ca	No error (0)	vatra.at		178.31.8.68	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:51.363027096 CET	8.8.8.8	192.168.2.4	0xe6ca	No error (0)	vatra.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:51.363027096 CET	8.8.8.8	192.168.2.4	0xe6ca	No error (0)	vatra.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:51.363027096 CET	8.8.8.8	192.168.2.4	0xe6ca	No error (0)	vatra.at		222.236.49.124	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:51.363027096 CET	8.8.8.8	192.168.2.4	0xe6ca	No error (0)	vatra.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:52.959707975 CET	8.8.8.8	192.168.2.4	0x26d0	No error (0)	vatra.at		200.46.66.71	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:52.959707975 CET	8.8.8.8	192.168.2.4	0x26d0	No error (0)	vatra.at		109.98.58.98	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:52.959707975 CET	8.8.8.8	192.168.2.4	0x26d0	No error (0)	vatra.at		178.31.8.68	A (IP address)	IN (0x0001)	false

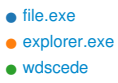
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 8, 2023 16:15:52.959707975 CET	8.8.8.8	192.168.2.4	0x26d0	No error (0)	vatra.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:52.959707975 CET	8.8.8.8	192.168.2.4	0x26d0	No error (0)	vatra.at		175.119.10.231	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:52.959707975 CET	8.8.8.8	192.168.2.4	0x26d0	No error (0)	vatra.at		222.236.49.124	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:52.959707975 CET	8.8.8.8	192.168.2.4	0x26d0	No error (0)	vatra.at		211.119.84.112	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:52.959707975 CET	8.8.8.8	192.168.2.4	0x26d0	No error (0)	vatra.at		58.235.189.192	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:52.959707975 CET	8.8.8.8	192.168.2.4	0x26d0	No error (0)	vatra.at		187.170.238.164	A (IP address)	IN (0x0001)	false
Jan 8, 2023 16:15:52.959707975 CET	8.8.8.8	192.168.2.4	0x26d0	No error (0)	vatra.at		185.95.186.58	A (IP address)	IN (0x0001)	false

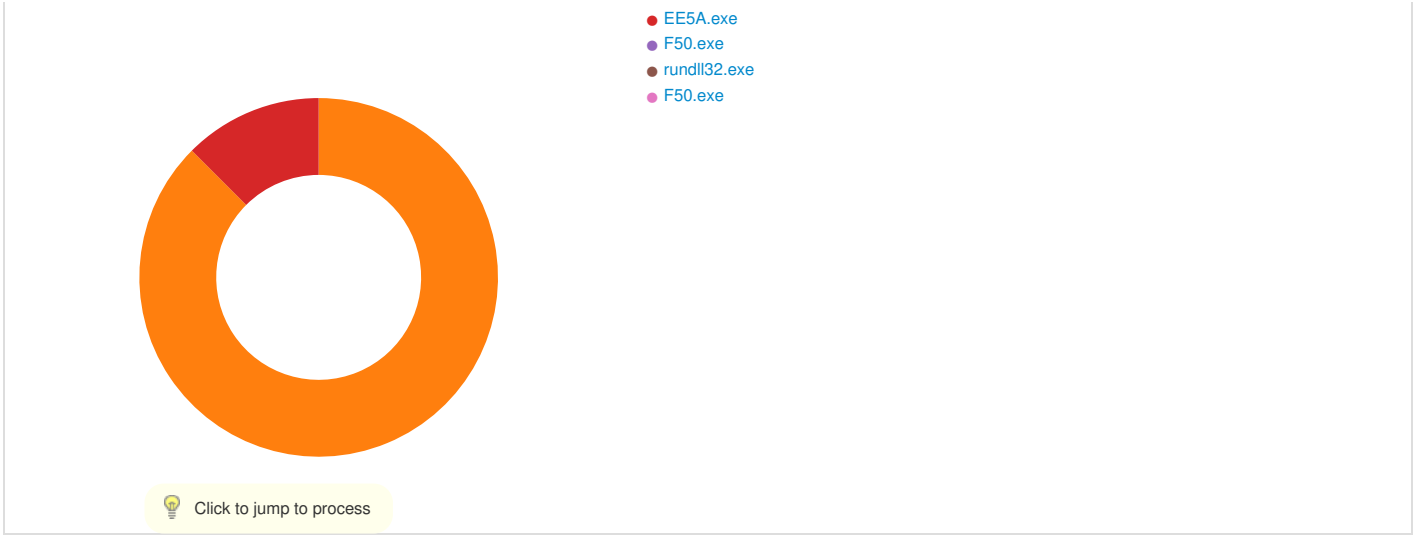
HTTP Request Dependency Graph

- degroeneuitzender.nl
- nrunfbf.net
  - vatra.at
- utbgbuc.org
- laatdiy.org
- 194.135.33.42
- avjruv.net
- fpmhvdgw.com
- daffyjk.org
- lubvvjyufy.com
- tklmgewyg.net
- gttbvxrpx.org
- qsmspqgdlg.org
- wgdttq.org
- dotemlc.org
- utctbvv.org
- tduhcp.org
- mwrunlqeb.com
- npcojlss.net
- yokcj.net
- lrmfyx.net
- wemmwd.net
- ursbcr.net

Statistics

Behavior





System Behavior

Analysis Process: file.exe PID: 3620, Parent PID: 3528

General	
Target ID:	0
Start time:	16:14:12
Start date:	08/01/2023
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	270336 bytes
MD5 hash:	635E3F021A205AD3A2BF9AAF3D278251
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.422927170.0000000002DA9000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.422745433.0000000002D51000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.422745433.0000000002D51000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000003.327713150.0000000002D30000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.422685888.0000000002D30000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.422685888.0000000002D30000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.422539917.0000000002C00000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: 3528, Parent PID: 3620

General	
Target ID:	1
Start time:	16:14:25
Start date:	08/01/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff618f60000
File size:	3933184 bytes

MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000000.407390160.0000000002A41000.00000020.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000000.407390160.0000000002A41000.00000020.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

Analysis Process: wdscede PID: 6128, Parent PID: 1088

General

Target ID:	4
Start time:	16:15:19
Start date:	08/01/2023
Path:	C:\Users\user\AppData\Roaming\wdscede
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\wdscede
Imagebase:	0x400000
File size:	270336 bytes
MD5 hash:	635E3F021A205AD3A2BF9AAF3D278251
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000004.00000002.587334500.0000000002E71000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000004.00000002.587334500.0000000002E71000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000004.00000003.570683568.0000000002BE0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000004.00000002.586404126.0000000002BE0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000004.00000002.586404126.0000000002BE0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000004.00000002.586888838.0000000002C38000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000004.00000002.586363495.0000000002BD0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 46%, ReversingLabs
Reputation:	low

Analysis Process: EE5A.exe PID: 916, Parent PID: 3528

General

Target ID:	5
Start time:	16:15:23
Start date:	08/01/2023
Path:	C:\Users\user\AppData\Local\Temp\EE5A.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\EE5A.exe
Imagebase:	0x400000
File size:	1073152 bytes
MD5 hash:	49D7D06EB3FD5E1DADAA505C021AA571
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000005.00000002.521464355.0000000004A70000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000005.00000002.520261780.0000000004997000.00000040.00000800.00020000.00000000.sdmp, Author: unknown

Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 48%, Virustotal, Browse
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Wtfoiq.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4C8A6F	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Wtfoiq.tmp	0	731648	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 65 3a fd 13 21 5b fd 40 21 5b fd 40 21 5b fd 40 fd 2c fd 41 26 5b fd 40 fd 2c fd 41 20 5b fd 40 4c 06 fd 41 22 5b fd 40 21 5b fd 40 35 5b fd 40 fd 44 fd 40 28 5b fd 40 fd 05 fd 41 20 5b fd 40 fd 05 fd 41 20 5b fd 40 fd 05 fd 41 20 5b fd 40 52 69 63 68 21 5b fd 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 06 27 fd 63 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$e:![@![@![@,A&[@,A [@LA"[@![@5[@D@([@A [@A [@A [@Rich![@PEL'c	success or wait	1	4C8F7E	WriteFile

Analysis Process: F50.exe PID: **1244**, Parent PID: **3528**

General

Target ID:	6
Start time:	16:15:31
Start date:	08/01/2023
Path:	C:\Users\user\AppData\Local\Temp\F50.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\F50.exe
Imagebase:	0x400000
File size:	599040 bytes
MD5 hash:	47D4D75F4D1D3B2C16D375A671BF0FDC
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000006.00000002.536404249.0000000004830000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000006.00000002.528207435.0000000000413000.00000040.00000001.01000000.00000008.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000006.00000002.534093898.0000000002EA9000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: rundll32.exe PID: **5616**, Parent PID: **916**

General	
Target ID:	7
Start time:	16:15:40
Start date:	08/01/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\rundll32.exe" "C:\Users\user\AppData\Local\Temp\Wtfoiq.tmp",lyidwoiowsw
Imagebase:	0x250000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	false
Has administrator privileges:	false
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: F50.exe PID: **6044**, Parent PID: **6068**

General	
Target ID:	12
Start time:	16:15:51
Start date:	08/01/2023
Path:	C:\Users\user\AppData\Local\Temp\F50.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\F50.exe"
Imagebase:	0x400000
File size:	599040 bytes
MD5 hash:	47D4D75F4D1D3B2C16D375A671BF0FDC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 0000000C.00000002.567433680.0000000000413000.00000040.00000001.01000000.00000008.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000C.00000002.568515234.0000000002E8E000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000C.00000002.568347439.0000000002E00000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Disassembly

No disassembly