ID: 753427
Sample Name: file.exe
Cookbook: default.jbs
Time: 20:11:10
Date: 24/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

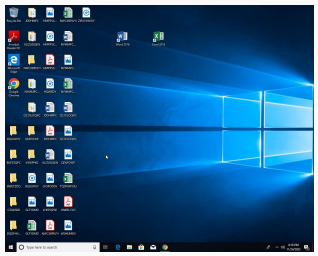
Windows Analysis Report

file.exe

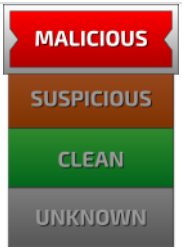
Overview

General Information

Sample Name:	file.exe
Analysis ID:	753427
MD5:	44c87d3bc316ee..
SHA1:	96bde412ef761b..
SHA256:	731e22be2a6b39.
Tags:	exe
Infos:	



Detection



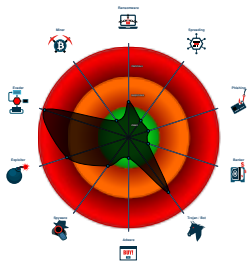
SmokeLoader

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

Signatures

- Yara detected UAC Bypass using C…
- 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…
- Maps a DLL or memory area into an…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 5020 cmdline: C:\Users\user\Desktop\file.exe MD5: 44C87D3BC316EEFE4DCBF66AFED72ABC)
  - explorer.exe (PID: 3528 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - B87E.exe (PID: 3316 cmdline: C:\Users\user\AppData\Local\Temp\B87E.exe MD5: 1BD9FB4ADE498938E6432D6C5D1E23A5)
      - rundll32.exe (PID: 2980 cmdline: "C:\Windows\system32\rundll32.exe" "C:\Users\user\AppData\Local\Temp\Tdryuqayh.tmp",Worhdhqfpryr MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - EBC4.exe (PID: 4608 cmdline: C:\Users\user\AppData\Local\Temp\EBC4.exe MD5: F06F222962C48BB7D822AC0FCD14CFD2)
- gfgsrbs (PID: 5000 cmdline: C:\Users\user\AppData\Roaming\gfgsrbs MD5: 44C87D3BC316EEFE4DCBF66AFED72ABC)
- EBC4.exe (PID: 2760 cmdline: "C:\Users\user\AppData\Local\Temp\EBC4.exe" MD5: F06F222962C48BB7D822AC0FCD14CFD2)
- **cleanup**

Malware Configuration

Threatname: SmokeLoader

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

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.373140844.0000000004631000.00000020.80000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000001.00000000.373140844.0000000004631000.00000020.80000000.00040000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x344:$a: 5B 81 EB 34 10 00 00 6A 30 58 64 8B 00 8B 40 0C 8B 40 1C 8B 40 08 89 85 C0
00000004.00000002.439850866.00000000007B0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000004.00000002.439850866.00000000007B0000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x744:$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
0000000C.00000002.507752658.0000000000413000.00000040.00000001.01000000.00000009.sdmp	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.EBC4.exe.400000.0.unpack	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
12.2.EBC4.exe.400000.0.unpack	INDICATOR_SUSPICIOUS_EXE_UACBypass_CMSTPCOM	Detects Windows exceutables bypassing UAC using CMSTP COM interfaces. MITRE (T1218.003)	ditekSHen	• 0x10000:$guid1: {3E5FC7F9-9A51-4367-9063-A120244FBEC7} • 0x100a0:$guid1: {3E5FC7F9-9A51-4367-9063-A120244FBEC7} • 0x10170:$s2: Elevation:Administrator!new:
7.2.EBC4.exe.400000.0.unpack	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
7.2.EBC4.exe.400000.0.unpack	INDICATOR_SUSPICIOUS_EXE_UACBypass_CMSTPCOM	Detects Windows exceutables bypassing UAC using CMSTP COM interfaces. MITRE (T1218.003)	ditekSHen	• 0x10000:$guid1: {3E5FC7F9-9A51-4367-9063-A120244FBEC7} • 0x100a0:$guid1: {3E5FC7F9-9A51-4367-9063-A120244FBEC7} • 0x10170:$s2: Elevation:Administrator!new:

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

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)

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)

Anti Debugging

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

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

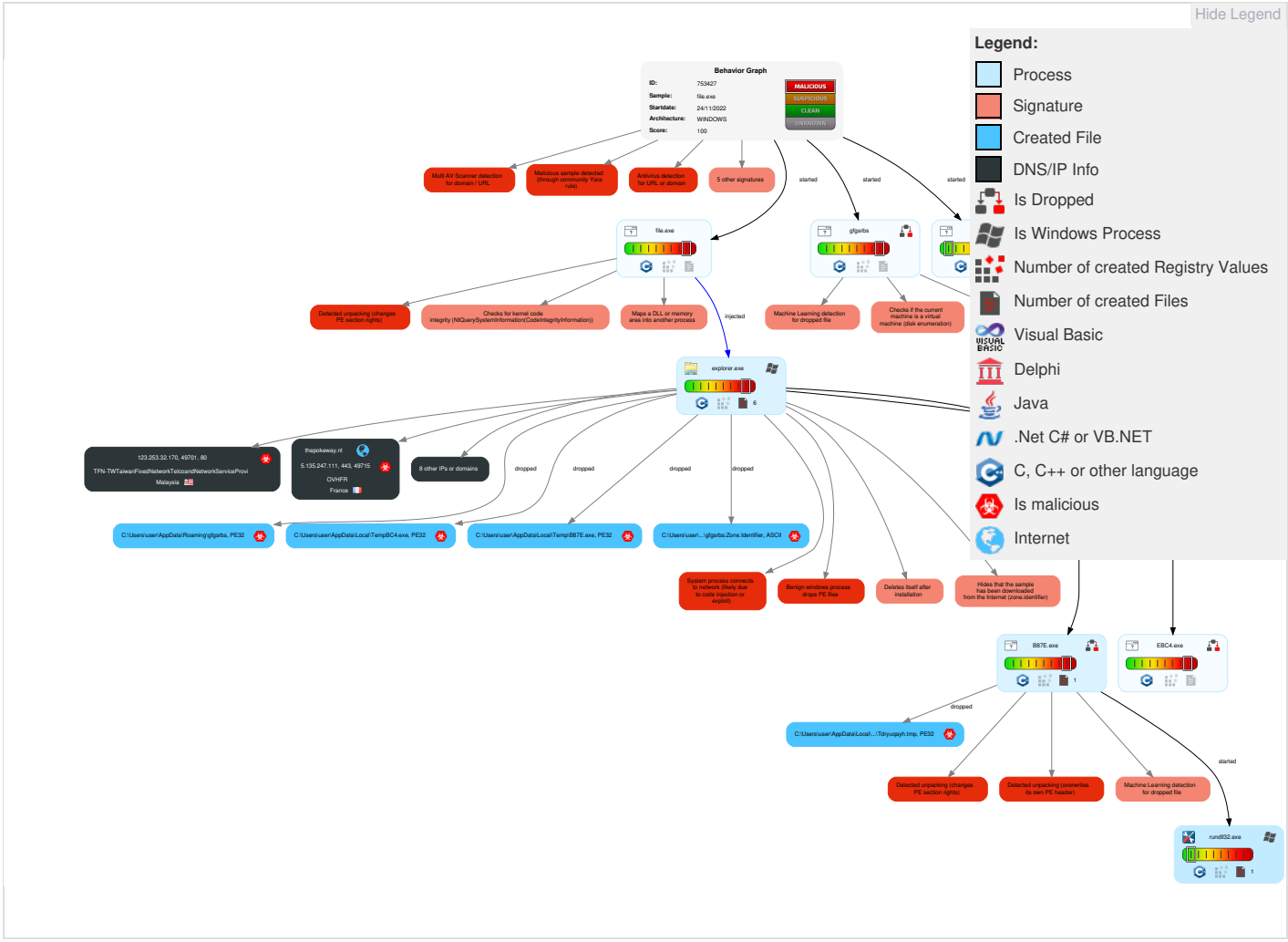
Remote Access Functionality

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 System Time Discovery	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	1 4 1 Virtualization/Sandbox Evasion	LSASS Memory	1 Query Registry	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 1 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 2 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Hidden Files and Directories	NTDS	1 4 1 Virtualization/Sandbox Evasion	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	3 Process 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 Application Window 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	1 4 System Information Discovery	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

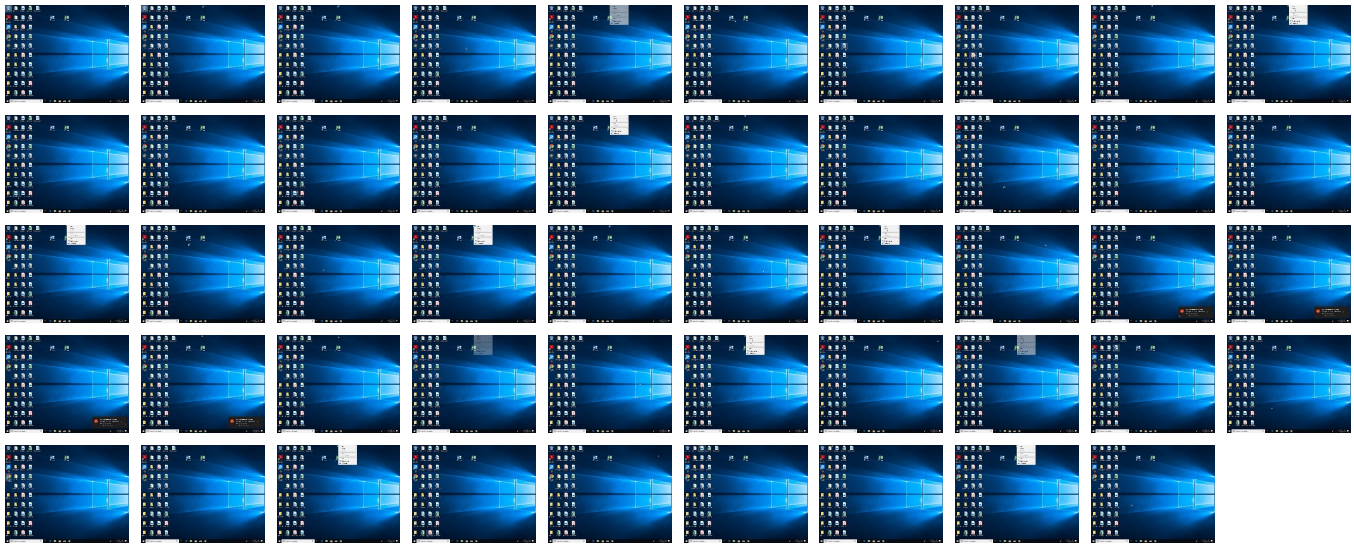
Behavior Graph



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	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\gfgsrbs	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\EBC4.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\B87E.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Tdryuqayh.tmp	24%	ReversingLabs	Win32.Trojan.Lazy	
C:\Users\user\AppData\Local\Temp\Tdryuqayh.tmp	35%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.EBC4.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.B87E.exe.25d0e67.1.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.3.gfgsrbs.7b0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
12.2.EBC4.exe.2d5112c.2.unpack	100%	Avira	TR/Patched.Ren.Gen7		Download File
0.3.file.exe.2270000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.3.B87E.exe.26f0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
12.2.EBC4.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.gfgsrbs.7a0e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.gfgsrbs.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.file.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.file.exe.2260e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.B87E.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen2		Download File

Domains

Source	Detection	Scanner	Label	Link
thepokeway.nl	5%	Virustotal		Browse
freeshmex.at	19%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://piratia.su/tmp/	100%	URL Reputation	malware	
http://piratia.su/tmp/	100%	URL Reputation	malware	
http://https://thepokeway.nl/upload/index.php	0%	URL Reputation	safe	
http://https://thepokeway.nl/upload/index.php	0%	URL Reputation	safe	
http://cracker.biz/tmp/	0%	URL Reputation	safe	
http://freeshmex.at/tmp/	0%	URL Reputation	safe	
http://123.253.32.170/root2.exe	0%	URL Reputation	safe	

Domains and IPs

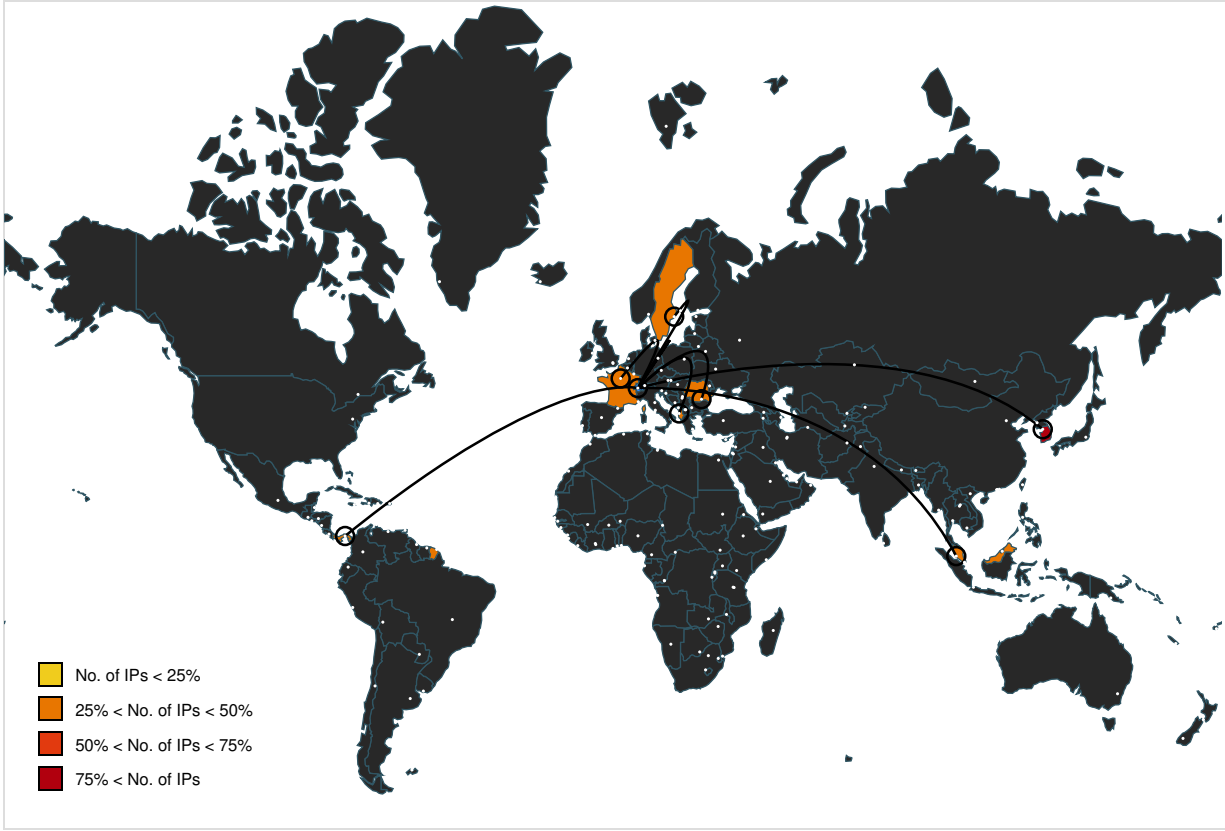
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
thepokeway.nl	5.135.247.111	true	true	• 5%, Virustotal, Browse	unknown
freeshmex.at	190.140.74.43	true	true	• 19%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://piratia.su/tmp/	true	• URL Reputation: malware • URL Reputation: malware	unknown
http://https://thepokeway.nl/upload/index.php	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://cracker.biz/tmp/	true	• URL Reputation: safe	unknown
http://freeshmex.at/tmp/	true	• URL Reputation: safe	unknown
http://123.253.32.170/root2.exe	true	• URL Reputation: safe	unknown
http://piratia-life.ru/tmp/	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
178.31.176.42	unknown	Sweden		2119	TELENOR-NEXTELTelenorNorgeASNO	false
109.102.255.230	unknown	Romania		9050	RTDBucharestRomaniaRO	false
5.135.247.111	thepokeway.nl	France		16276	OVHFR	true
211.40.39.251	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
211.171.233.129	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
123.253.32.170	unknown	Malaysia		9924	TFN-TWTaiwanFixedNetworkTelcoandNetworkServiceProvi	true
95.107.163.44	unknown	Albania		47394	ASC-AL-ASAL	false
211.53.230.67	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
190.140.74.43	freeshmex.at	Panama		18809	CableOndaPA	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	753427
Start date and time:	2022-11-24 20:11:10 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 4s
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@35/10
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 70.7% (good quality ratio 58.1%) • Quality average: 46% • Quality standard deviation: 29.6%
HCA Information:	• Successful, ratio: 95% • 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
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- 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
20:13:00	Task Scheduler	Run new task: Firefox Default Browser Agent 52C9416EC30B0AB4 path: C:\Users\user\AppData\Roaming\gfg srbs
20:13:24	API Interceptor	60x Sleep call for process: rundll32.exe modified
20:13:39	API Interceptor	1x Sleep call for process: EBC4.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\B87E.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1041408
Entropy (8bit):	7.918015264621188
Encrypted:	false
SSDEEP:	24576:K/J3qfaq1RXzqGA+PF6ZbOQVIZc77oReV2U6JjgtA1/lGaee:K/Ja54TS6ZyQKk7cJjJlGa
MD5:	1BD9FB4ADE498938E6432D6C5D1E23A5
SHA1:	909ECEC41F837A402EE4EF43D8B9F6B06A5A8AAF
SHA-256:	12B8B5BFDE4092B4248ACCC682098222420EE6A0B6DFE89EB268F7FCF8CF00FB
SHA-512:	EA02AB5EC0BDEABA4E897E5E1E50CCF27AB392AC859348CDF1CAAAF90C7C10F1E99CDD01317F36479CB600B9FE2189F34B59AFC822071EC4C7EA989F8F99C DA5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W.....4.....=.....Rich..... .....PE..L....g.b.....:0.....o.....@.....1.....\...d....1.....p.....P<..@..... ....text..... ..`.data...../.....@....rsrc.....1..0.....@..@..... .....

C:\Users\user\AppData\Local\Temp\EBC4.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	520192
Entropy (8bit):	7.765713315963878
Encrypted:	false
SSDEEP:	6144:5q6OLJ51HLLQrTYeW0w8Y2hm/UchHJ10kiygcz0CkcScVwAjS0bgF8nlctP4:5qJX1H4rUelw4En0V80WSmjWF8nWt
MD5:	F06F222962C48BB7D822AC0FCD14CFD2
SHA1:	0866BE2E6D97E71DEF6DCED9FE5DC7623558DCAD
SHA-256:	F687250C7F49AAFF9787D9202CD13F5E159220D9AE613B335ED72A76FADFA03F
SHA-512:	F29B4F4B64394B127F939466AF5D189408C6D296E94469000E72690129753FB0C1232B925C2C50FC252E273E503DEC984EE95BECD267F897B5E57493DD7F6412
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W.....4.....=.....Rich..... .....PE..L....3Cb.....D(.....o.....@.....).....C.....\...d....).....p.....P<..@..... ....text..... ..`.data...(.'.....@....rsrc.....)..0.....@..@..... ....

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

Process:	C:\Users\user\AppData\Local\Temp\B87E.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	785408
Entropy (8bit):	6.878292814763175
Encrypted:	false
SSDEEP:	12288:8jrCotmFXRwupVoGK25MAaSOWfvjCqanOxku3lle2kKE:AzmFB3oG1aSbvGqanwRro
MD5:	D8CA174A8F3F0C225429E1BE1CB6D304
SHA1:	0F2E738B1A35B6072E1D23894468E45FA7DEE750

SHA-256:	3D63AD175A34E4C89EA6ECA4A1161BB5DD514A5E58302707EDC03473EB1F656E
SHA-512:	DBF999A9F0399B3CBF93484F2E665E3BEB4DE369DACF4678C7B7B3FF06F45C42879C544C2404D85B88FE3AAACF117A1E28ECB68EE7EA2553B736BAD03619E527
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 24% • Antivirus: Virustotal, Detection: 35%, Browse
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...v..c.....!.....f.....J..... .....@.....@.....<.....]..... .....@.....text....d.....f..... ..`.rdata.....j.....@..@.data....../.....0...n.....@....reloc...].....^.....@..B..... ....

C:\Users\user\AppData\Roaming\gfgsrbs

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	192000
Entropy (8bit):	6.98989950872948
Encrypted:	false
SSDEEP:	3072:hsKq2z/YFBDK+1L8pOov9vl5izTyHnbACodEdE53iiy2:tqG6LaO6QTak/dKEFii1
MD5:	44C87D3BC316EEFE4DCBF66AFED72ABC
SHA1:	96BDE412EF761B4D53506AE4ED2999BC9DCAF137
SHA-256:	731E22BE2A6B39304919DC24B750A720B23A0F1ED996A9B74CF0B088DE6144B1
SHA-512:	2449DA42CF169EF2A9E01ADE64DD8C52AB6037CE9A726597D88F5EEAA726B06F77BC08612AAECCF9354CD23BEE879B1724F222E24C8BAB25FEF7E75A8BF0E0C1
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W.....4.....=.....Rich..... .....PE..L.....`.....>#.....o.....@.....$.....\...d....$.....p.....P<..@..... ..... .....text..... ..`.data....."..... .....@....rsrc.....$..0.....@..@..... .....

C:\Users\user\AppData\Roaming\gfgsrbs: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**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.98989950872948
TrID:	• Win32 Executable (generic) a (10002005/4) 99.53% • InstallShield setup (43055/19) 0.43% • 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:	192000
MD5:	44c87d3bc316eefe4dcbf66afed72abc
SHA1:	96bde412ef761b4d53506ae4ed2999bc9dcaf137
SHA256:	731e22be2a6b39304919dc24b750a720b23a0f1ed996a9b74cf0b088de6144b1
SHA512:	2449da42cf169ef2a9e01ade64dd8c52ab6037ce9a726597d88f5eeaa726b06f77bc08612aaeccf9354cd23bee879b1724f222e24c8bab25fef7e75a8bf0e0c1
SSDEEP:	3072:hsKq2z/YFBDK+1L8pOov9vl5izTyHnbACodEdE53iiy2:tqG6LaO6QTak/dKEFii1
TLSH:	CC14BF353680D072C59E65708C60EAA1AB7DAA3155B885377BA80B7E5F703D0AF3634F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W.....4.....=.....Rich.....PE..L.....`...

File Icon

Icon Hash:	c8d0d8e0f8e0f0e0

Static PE Info

General

Entrypoint:	0x406fe6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x60DF08C1 [Fri Jul 2 12:38:25 2021 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:	5a0f5eee1a1d8df02fd40c6cf3174a3d

Entrypoint Preview

Instruction
call 00007F9BE0977256h
jmp 00007F9BE096F8DEh
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F9BE096FA86h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F9BE096FAB0h
test ecx, 00000003h
jne 00007F9BE096FA51h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h

Instruction
test eax, 81010100h
je 00007F9BE096FA4Ah
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F9BE096FA94h
test ah, ah
je 00007F9BE096FA86h
test eax, 00FF0000h
je 00007F9BE096FA75h
test eax, FF000000h
je 00007F9BE096FA64h
jmp 00007F9BE096FA2Fh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
cmp ecx, dword ptr [0042B970h]
jne 00007F9BE096FA64h
rep ret
jmp 00007F9BE097724Dh
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [0042B970h]
xor eax, ebp
push eax
push dword ptr [ebp-04h]
mov dword ptr [ebp+00h], 00000000h

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	0x1a05c	0x64	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x249000	0x2ee8	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1270	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	0x3c50	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x220	.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	0x19cf4	0x19e00	False	0.5226637983091788	data	6.3440620232767975	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x1b000	0x22dac8	0x11c00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x249000	0x2ee8	0x3000	False	0.639892578125	data	5.694966696037735	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2491f0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x2498b8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x249e20	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x24aec8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Raeto-Romance	Switzerland
RT_ICON	0x24b850	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Raeto-Romance	Switzerland
RT_ACCELERATOR	0x24bd08	0x98	data	Raeto-Romance	Switzerland
RT_GROUP_ICON	0x24bcb8	0x4c	data	Raeto-Romance	Switzerland
RT_VERSION	0x24bda0	0x148	x86 executable not stripped		

Imports

DLL	Import
KERNEL32.dll	WriteConsoleInputA, EnumDateFormatsA, OpenMutexA, GetConsoleAliasExesLengthW, CopyFileExA, ReadConsoleOutputCharacterA, GetEnvironmentStrings, FreeUserPhysicalPages, QueryDosDeviceA, EnumCalendarInfoExA, GetProcessPriorityBoost, LocalSize, AddConsoleAliasW, CreateFileW, GetMailslotInfo, GetWindowsDirectoryA, GetModuleHandleW, VirtualFree, CreateDirectoryExA, GetLogicalDriveStringsA, ReadConsoleInputA, FindNextVolumeMountPointW, OpenWaitableTimerW, GetVersionExA, SearchPathA, RequestWakeupLatency, CallNamedPipeW, GetCurrentDirectoryW, GetDriveTypeA, CreateMailslotW, BuildCommDCBAndTimeoutsA, GetProcAddress, GetModuleHandleA, LocalAlloc, FindNextFileA, TerminateThread, GetCommandLineW, FindFirstChangeNotificationA, VerifyVersionInfoA, DeleteTimerQueue, FindFirstVolumeA, GlobalFlags, GetTickCount, GetACP, GlobalWire, GetTapeParameters, HeapWalk, GetConsoleTitleA, InterlockedCompareExchange, EnumCalendarInfoA, GetNamedPipeHandleStateW, InterlockedDecrement, SetCalendarInfoA, TerminateProcess, MoveFileA, AddAtomW, FreeEnvironmentStringsW, SetConsoleTitleW, SetVolumeMountPointA, VirtualAlloc, SetConsoleActiveScreenBuffer, GetCPInfo, GetProcessIoCounters, GlobalFindAtomA, CreateFileA, CloseHandle, GetVolumeInformationA, EnumSystemCodePagesA, MoveFileWithProgressA, LoadLibraryW, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, RaiseException, RtlUnwind, GetLastError, DeleteFileA, GetStartupInfoW, HeapAlloc, HeapFree, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, GetCurrentThreadId, Sleep, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, EnterCriticalSection, LeaveCriticalSection, SetHandleCount, GetFileType, GetStartupInfoA, DeleteCriticalSection, GetModuleFileNameW, GetEnvironmentStringsW, HeapCreate, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, HeapReAlloc, GetOEMCP, IsValidCodePage, HeapSize, LoadLibraryA, InitializeCriticalSectionAndSpinCount, SetFilePointer, WideCharToMultiByte, GetConsoleCP, GetConsoleMode, MultiByteToWideChar, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, FlushFileBuffers, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, ReadFile
USER32.dll	GetComboBoxInfo, GetMessageExtraInfo, GetListBoxInfo

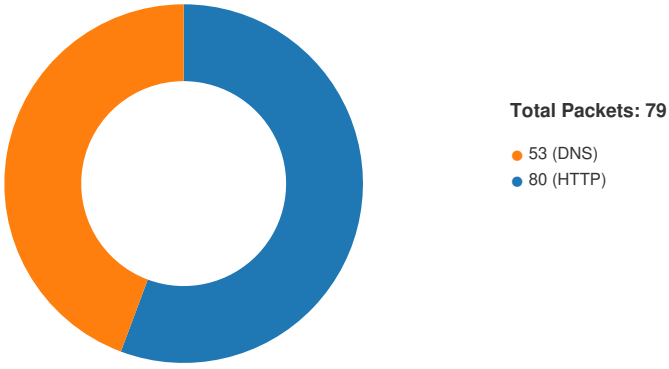
DLL	Import
GDI32.dll	GetBoundsRect
ADVAPI32.dll	SetThreadToken

Possible Origin

Language of compilation system	Country where language is spoken	Map
Raeto-Romance	Switzerland	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 20:13:00.179537058 CET	49696	80	192.168.2.4	190.140.74.43
Nov 24, 2022 20:13:00.369390011 CET	80	49696	190.140.74.43	192.168.2.4
Nov 24, 2022 20:13:00.369549036 CET	49696	80	192.168.2.4	190.140.74.43
Nov 24, 2022 20:13:00.375032902 CET	49696	80	192.168.2.4	190.140.74.43
Nov 24, 2022 20:13:00.375082016 CET	49696	80	192.168.2.4	190.140.74.43
Nov 24, 2022 20:13:00.565493107 CET	80	49696	190.140.74.43	192.168.2.4
Nov 24, 2022 20:13:01.250077009 CET	80	49696	190.140.74.43	192.168.2.4
Nov 24, 2022 20:13:01.250516891 CET	49696	80	192.168.2.4	190.140.74.43
Nov 24, 2022 20:13:01.253446102 CET	80	49696	190.140.74.43	192.168.2.4
Nov 24, 2022 20:13:01.256314039 CET	49696	80	192.168.2.4	190.140.74.43
Nov 24, 2022 20:13:01.441453934 CET	80	49696	190.140.74.43	192.168.2.4
Nov 24, 2022 20:13:01.503216028 CET	49697	80	192.168.2.4	211.53.230.67
Nov 24, 2022 20:13:01.762573957 CET	80	49697	211.53.230.67	192.168.2.4
Nov 24, 2022 20:13:01.762818098 CET	49697	80	192.168.2.4	211.53.230.67
Nov 24, 2022 20:13:01.762887001 CET	49697	80	192.168.2.4	211.53.230.67
Nov 24, 2022 20:13:01.765835047 CET	49697	80	192.168.2.4	211.53.230.67
Nov 24, 2022 20:13:02.025166035 CET	80	49697	211.53.230.67	192.168.2.4
Nov 24, 2022 20:13:03.711689949 CET	80	49697	211.53.230.67	192.168.2.4
Nov 24, 2022 20:13:03.711747885 CET	80	49697	211.53.230.67	192.168.2.4
Nov 24, 2022 20:13:03.711883068 CET	49697	80	192.168.2.4	211.53.230.67
Nov 24, 2022 20:13:03.711942911 CET	49697	80	192.168.2.4	211.53.230.67
Nov 24, 2022 20:13:03.971602917 CET	80	49697	211.53.230.67	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 20:13:04.214900970 CET	49698	80	192.168.2.4	211.40.39.251
Nov 24, 2022 20:13:04.464004040 CET	80	49698	211.40.39.251	192.168.2.4
Nov 24, 2022 20:13:04.464221954 CET	49698	80	192.168.2.4	211.40.39.251
Nov 24, 2022 20:13:04.464222908 CET	49698	80	192.168.2.4	211.40.39.251
Nov 24, 2022 20:13:04.464287996 CET	49698	80	192.168.2.4	211.40.39.251
Nov 24, 2022 20:13:04.713635921 CET	80	49698	211.40.39.251	192.168.2.4
Nov 24, 2022 20:13:05.402805090 CET	80	49698	211.40.39.251	192.168.2.4
Nov 24, 2022 20:13:05.402868032 CET	80	49698	211.40.39.251	192.168.2.4
Nov 24, 2022 20:13:05.402985096 CET	49698	80	192.168.2.4	211.40.39.251
Nov 24, 2022 20:13:05.403079033 CET	49698	80	192.168.2.4	211.40.39.251
Nov 24, 2022 20:13:05.652757883 CET	80	49698	211.40.39.251	192.168.2.4
Nov 24, 2022 20:13:05.674043894 CET	49699	80	192.168.2.4	211.171.233.129
Nov 24, 2022 20:13:05.928874016 CET	80	49699	211.171.233.129	192.168.2.4
Nov 24, 2022 20:13:05.929179907 CET	49699	80	192.168.2.4	211.171.233.129
Nov 24, 2022 20:13:05.929245949 CET	49699	80	192.168.2.4	211.171.233.129
Nov 24, 2022 20:13:05.929267883 CET	49699	80	192.168.2.4	211.171.233.129
Nov 24, 2022 20:13:06.184005976 CET	80	49699	211.171.233.129	192.168.2.4
Nov 24, 2022 20:13:07.234910011 CET	80	49699	211.171.233.129	192.168.2.4
Nov 24, 2022 20:13:07.234982967 CET	80	49699	211.171.233.129	192.168.2.4
Nov 24, 2022 20:13:07.235172033 CET	49699	80	192.168.2.4	211.171.233.129
Nov 24, 2022 20:13:07.238368034 CET	49699	80	192.168.2.4	211.171.233.129
Nov 24, 2022 20:13:07.493017912 CET	80	49699	211.171.233.129	192.168.2.4
Nov 24, 2022 20:13:07.713021994 CET	49700	80	192.168.2.4	109.102.255.230
Nov 24, 2022 20:13:07.766684055 CET	80	49700	109.102.255.230	192.168.2.4
Nov 24, 2022 20:13:07.766917944 CET	49700	80	192.168.2.4	109.102.255.230
Nov 24, 2022 20:13:07.766982079 CET	49700	80	192.168.2.4	109.102.255.230
Nov 24, 2022 20:13:07.767508030 CET	49700	80	192.168.2.4	109.102.255.230
Nov 24, 2022 20:13:07.824245930 CET	80	49700	109.102.255.230	192.168.2.4
Nov 24, 2022 20:13:08.069124937 CET	80	49700	109.102.255.230	192.168.2.4
Nov 24, 2022 20:13:08.069317102 CET	49700	80	192.168.2.4	109.102.255.230
Nov 24, 2022 20:13:08.075387001 CET	80	49700	109.102.255.230	192.168.2.4
Nov 24, 2022 20:13:08.075546980 CET	49700	80	192.168.2.4	109.102.255.230
Nov 24, 2022 20:13:08.078490973 CET	49700	80	192.168.2.4	109.102.255.230
Nov 24, 2022 20:13:08.082349062 CET	49701	80	192.168.2.4	123.253.32.170
Nov 24, 2022 20:13:08.130449057 CET	80	49700	109.102.255.230	192.168.2.4
Nov 24, 2022 20:13:08.363208055 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.363341093 CET	49701	80	192.168.2.4	123.253.32.170
Nov 24, 2022 20:13:08.363487005 CET	49701	80	192.168.2.4	123.253.32.170
Nov 24, 2022 20:13:08.644393921 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.644607067 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.644655943 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.644696951 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.644737959 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.644778013 CET	49701	80	192.168.2.4	123.253.32.170
Nov 24, 2022 20:13:08.644783020 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.644825935 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.644841909 CET	49701	80	192.168.2.4	123.253.32.170
Nov 24, 2022 20:13:08.644870996 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.644891024 CET	49701	80	192.168.2.4	123.253.32.170
Nov 24, 2022 20:13:08.644956112 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.645013094 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.645055056 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.645167112 CET	49701	80	192.168.2.4	123.253.32.170
Nov 24, 2022 20:13:08.925841093 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.925894022 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.925937891 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.925980091 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.926021099 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.926053047 CET	80	49701	123.253.32.170	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 20:13:08.926084995 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.926117897 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.926120996 CET	49701	80	192.168.2.4	123.253.32.170
Nov 24, 2022 20:13:08.926187992 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.926225901 CET	49701	80	192.168.2.4	123.253.32.170
Nov 24, 2022 20:13:08.926230907 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.926270008 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.926280022 CET	49701	80	192.168.2.4	123.253.32.170
Nov 24, 2022 20:13:08.926311016 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.926354885 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.926363945 CET	49701	80	192.168.2.4	123.253.32.170
Nov 24, 2022 20:13:08.926395893 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.926436901 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.926445961 CET	49701	80	192.168.2.4	123.253.32.170
Nov 24, 2022 20:13:08.926482916 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.926523924 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.926532984 CET	49701	80	192.168.2.4	123.253.32.170
Nov 24, 2022 20:13:08.926564932 CET	80	49701	123.253.32.170	192.168.2.4
Nov 24, 2022 20:13:08.926605940 CET	80	49701	123.253.32.170	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 20:12:59.935297966 CET	56572	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:00.175766945 CET	53	56572	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:01.266431093 CET	50911	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:01.502526999 CET	53	50911	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:03.722253084 CET	59683	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:04.211875916 CET	53	59683	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:05.434669971 CET	64167	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:05.672918081 CET	53	64167	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:07.250185966 CET	58565	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:07.711612940 CET	53	58565	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:14.580648899 CET	52239	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:14.598026037 CET	53	52239	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:14.810918093 CET	56807	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:14.828412056 CET	53	56807	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:15.572982073 CET	61007	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:15.592614889 CET	53	61007	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:15.929008007 CET	60686	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:16.396440029 CET	53	60686	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:18.701905966 CET	61124	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:18.721328974 CET	53	61124	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:20.234677076 CET	59444	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:20.254560947 CET	53	59444	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:21.596772909 CET	55570	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:21.614191055 CET	53	55570	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:21.912702084 CET	64906	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:21.932231903 CET	53	64906	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:22.244184971 CET	59446	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:22.264146090 CET	53	59446	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:23.836488008 CET	61088	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:23.853676081 CET	53	61088	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:25.197235107 CET	58729	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:25.443180084 CET	53	58729	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:25.826148987 CET	64700	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:25.852006912 CET	53	64700	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:26.118453026 CET	56022	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:26.163016081 CET	53	56022	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 20:13:27.561788082 CET	60822	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:27.585237026 CET	53	60822	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:27.940895081 CET	49750	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:27.964770079 CET	53	49750	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:29.193562984 CET	60550	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:29.219906092 CET	53	60550	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:29.630523920 CET	54851	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:29.651410103 CET	53	54851	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:30.759373903 CET	57300	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:30.784167051 CET	53	57300	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:32.005364895 CET	54521	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:32.024302959 CET	53	54521	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:33.404093981 CET	58914	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:33.421724081 CET	53	58914	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:33.718513012 CET	51419	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:33.736593008 CET	53	51419	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:34.239005089 CET	51054	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:34.258749962 CET	53	51054	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:34.651309013 CET	55673	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:34.668950081 CET	53	55673	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:35.423708916 CET	49735	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:35.443448067 CET	53	49735	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:37.516464949 CET	52437	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:37.534168005 CET	53	52437	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:38.002130032 CET	52825	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:38.022118092 CET	53	52825	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:39.548868895 CET	58530	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:39.568480968 CET	53	58530	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:39.808876991 CET	64959	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:39.828243017 CET	53	64959	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:40.208877087 CET	63093	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:40.226567030 CET	53	63093	8.8.8.8	192.168.2.4
Nov 24, 2022 20:13:41.303160906 CET	50433	53	192.168.2.4	8.8.8.8
Nov 24, 2022 20:13:41.322443962 CET	53	50433	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
Nov 24, 2022 20:12:59.935297966 CET	192.168.2.4	8.8.8.8	0x5b1b	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:01.266431093 CET	192.168.2.4	8.8.8.8	0xa72e	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:03.722253084 CET	192.168.2.4	8.8.8.8	0x268b	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:05.434669971 CET	192.168.2.4	8.8.8.8	0xe8d2	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:07.250185966 CET	192.168.2.4	8.8.8.8	0x2615	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:14.580648899 CET	192.168.2.4	8.8.8.8	0x4259	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:14.810918093 CET	192.168.2.4	8.8.8.8	0x451c	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:15.572982073 CET	192.168.2.4	8.8.8.8	0x6a0c	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:15.929008007 CET	192.168.2.4	8.8.8.8	0x90b5	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:18.701905966 CET	192.168.2.4	8.8.8.8	0x5229	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:20.234677076 CET	192.168.2.4	8.8.8.8	0x534e	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:21.596772909 CET	192.168.2.4	8.8.8.8	0x9b24	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 24, 2022 20:13:21.912702084 CET	192.168.2.4	8.8.8.8	0x1f86	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:22.244184971 CET	192.168.2.4	8.8.8.8	0xb6d9	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:23.836488008 CET	192.168.2.4	8.8.8.8	0xd330	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:25.197235107 CET	192.168.2.4	8.8.8.8	0xd930	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:25.826148987 CET	192.168.2.4	8.8.8.8	0x5c52	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:26.118453026 CET	192.168.2.4	8.8.8.8	0x2242	Standard query (0)	thepokeway.nl	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:27.561788082 CET	192.168.2.4	8.8.8.8	0x9072	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:27.940895081 CET	192.168.2.4	8.8.8.8	0x2c30	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:29.193562984 CET	192.168.2.4	8.8.8.8	0xf846	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:29.630523920 CET	192.168.2.4	8.8.8.8	0x6a41	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:30.759373903 CET	192.168.2.4	8.8.8.8	0x76fa	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:32.005364895 CET	192.168.2.4	8.8.8.8	0xfed9	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:33.404093981 CET	192.168.2.4	8.8.8.8	0x8cad	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:33.718513012 CET	192.168.2.4	8.8.8.8	0xddb5	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:34.239005089 CET	192.168.2.4	8.8.8.8	0xe7fc	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:34.651309013 CET	192.168.2.4	8.8.8.8	0xc9b3	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:35.423708916 CET	192.168.2.4	8.8.8.8	0x5996	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:37.516464949 CET	192.168.2.4	8.8.8.8	0xd9bb	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:38.002130032 CET	192.168.2.4	8.8.8.8	0xbba5	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:39.548868895 CET	192.168.2.4	8.8.8.8	0x99a5	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:39.808876991 CET	192.168.2.4	8.8.8.8	0xbafc	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:40.208877087 CET	192.168.2.4	8.8.8.8	0xe142	Standard query (0)	freeshmex.at	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:41.303160906 CET	192.168.2.4	8.8.8.8	0xf858	Standard query (0)	freeshmex.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
Nov 24, 2022 20:13:00.175766945 CET	8.8.8.8	192.168.2.4	0x5b1b	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:00.175766945 CET	8.8.8.8	192.168.2.4	0x5b1b	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:00.175766945 CET	8.8.8.8	192.168.2.4	0x5b1b	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:00.175766945 CET	8.8.8.8	192.168.2.4	0x5b1b	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:00.175766945 CET	8.8.8.8	192.168.2.4	0x5b1b	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:00.175766945 CET	8.8.8.8	192.168.2.4	0x5b1b	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 20:13:00.175766945 CET	8.8.8.8	192.168.2.4	0x5b1b	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:00.175766945 CET	8.8.8.8	192.168.2.4	0x5b1b	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:00.175766945 CET	8.8.8.8	192.168.2.4	0x5b1b	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:00.175766945 CET	8.8.8.8	192.168.2.4	0x5b1b	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:01.502526999 CET	8.8.8.8	192.168.2.4	0xa72e	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:01.502526999 CET	8.8.8.8	192.168.2.4	0xa72e	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:01.502526999 CET	8.8.8.8	192.168.2.4	0xa72e	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:01.502526999 CET	8.8.8.8	192.168.2.4	0xa72e	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:01.502526999 CET	8.8.8.8	192.168.2.4	0xa72e	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:01.502526999 CET	8.8.8.8	192.168.2.4	0xa72e	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:01.502526999 CET	8.8.8.8	192.168.2.4	0xa72e	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:01.502526999 CET	8.8.8.8	192.168.2.4	0xa72e	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:01.502526999 CET	8.8.8.8	192.168.2.4	0xa72e	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:01.502526999 CET	8.8.8.8	192.168.2.4	0xa72e	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:04.211875916 CET	8.8.8.8	192.168.2.4	0x268b	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:04.211875916 CET	8.8.8.8	192.168.2.4	0x268b	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:04.211875916 CET	8.8.8.8	192.168.2.4	0x268b	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:04.211875916 CET	8.8.8.8	192.168.2.4	0x268b	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:04.211875916 CET	8.8.8.8	192.168.2.4	0x268b	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:04.211875916 CET	8.8.8.8	192.168.2.4	0x268b	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:04.211875916 CET	8.8.8.8	192.168.2.4	0x268b	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:04.211875916 CET	8.8.8.8	192.168.2.4	0x268b	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:04.211875916 CET	8.8.8.8	192.168.2.4	0x268b	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:04.211875916 CET	8.8.8.8	192.168.2.4	0x268b	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:05.672918081 CET	8.8.8.8	192.168.2.4	0xe8d2	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 20:13:05.672918081 CET	8.8.8.8	192.168.2.4	0xe8d2	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:05.672918081 CET	8.8.8.8	192.168.2.4	0xe8d2	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:05.672918081 CET	8.8.8.8	192.168.2.4	0xe8d2	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:05.672918081 CET	8.8.8.8	192.168.2.4	0xe8d2	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:05.672918081 CET	8.8.8.8	192.168.2.4	0xe8d2	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:05.672918081 CET	8.8.8.8	192.168.2.4	0xe8d2	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:05.672918081 CET	8.8.8.8	192.168.2.4	0xe8d2	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:05.672918081 CET	8.8.8.8	192.168.2.4	0xe8d2	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:05.672918081 CET	8.8.8.8	192.168.2.4	0xe8d2	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:07.711612940 CET	8.8.8.8	192.168.2.4	0x2615	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:07.711612940 CET	8.8.8.8	192.168.2.4	0x2615	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:07.711612940 CET	8.8.8.8	192.168.2.4	0x2615	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:07.711612940 CET	8.8.8.8	192.168.2.4	0x2615	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:07.711612940 CET	8.8.8.8	192.168.2.4	0x2615	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:07.711612940 CET	8.8.8.8	192.168.2.4	0x2615	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:07.711612940 CET	8.8.8.8	192.168.2.4	0x2615	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:07.711612940 CET	8.8.8.8	192.168.2.4	0x2615	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:07.711612940 CET	8.8.8.8	192.168.2.4	0x2615	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:07.711612940 CET	8.8.8.8	192.168.2.4	0x2615	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:14.598026037 CET	8.8.8.8	192.168.2.4	0x4259	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:14.598026037 CET	8.8.8.8	192.168.2.4	0x4259	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:14.598026037 CET	8.8.8.8	192.168.2.4	0x4259	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:14.598026037 CET	8.8.8.8	192.168.2.4	0x4259	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:14.598026037 CET	8.8.8.8	192.168.2.4	0x4259	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:14.598026037 CET	8.8.8.8	192.168.2.4	0x4259	No error (0)	freeshmex.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
Nov 24, 2022 20:13:14.598026037 CET	8.8.8.8	192.168.2.4	0x4259	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:14.598026037 CET	8.8.8.8	192.168.2.4	0x4259	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:14.598026037 CET	8.8.8.8	192.168.2.4	0x4259	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:14.598026037 CET	8.8.8.8	192.168.2.4	0x4259	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:14.828412056 CET	8.8.8.8	192.168.2.4	0x451c	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:14.828412056 CET	8.8.8.8	192.168.2.4	0x451c	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:14.828412056 CET	8.8.8.8	192.168.2.4	0x451c	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:14.828412056 CET	8.8.8.8	192.168.2.4	0x451c	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:14.828412056 CET	8.8.8.8	192.168.2.4	0x451c	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:14.828412056 CET	8.8.8.8	192.168.2.4	0x451c	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:14.828412056 CET	8.8.8.8	192.168.2.4	0x451c	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:14.828412056 CET	8.8.8.8	192.168.2.4	0x451c	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:14.828412056 CET	8.8.8.8	192.168.2.4	0x451c	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:14.828412056 CET	8.8.8.8	192.168.2.4	0x451c	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:15.592614889 CET	8.8.8.8	192.168.2.4	0x6a0c	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:15.592614889 CET	8.8.8.8	192.168.2.4	0x6a0c	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:15.592614889 CET	8.8.8.8	192.168.2.4	0x6a0c	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:15.592614889 CET	8.8.8.8	192.168.2.4	0x6a0c	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:15.592614889 CET	8.8.8.8	192.168.2.4	0x6a0c	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:15.592614889 CET	8.8.8.8	192.168.2.4	0x6a0c	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:15.592614889 CET	8.8.8.8	192.168.2.4	0x6a0c	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:15.592614889 CET	8.8.8.8	192.168.2.4	0x6a0c	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:15.592614889 CET	8.8.8.8	192.168.2.4	0x6a0c	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:15.592614889 CET	8.8.8.8	192.168.2.4	0x6a0c	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:16.396440029 CET	8.8.8.8	192.168.2.4	0x90b5	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 20:13:16.396440029 CET	8.8.8.8	192.168.2.4	0x90b5	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:16.396440029 CET	8.8.8.8	192.168.2.4	0x90b5	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:16.396440029 CET	8.8.8.8	192.168.2.4	0x90b5	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:16.396440029 CET	8.8.8.8	192.168.2.4	0x90b5	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:16.396440029 CET	8.8.8.8	192.168.2.4	0x90b5	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:16.396440029 CET	8.8.8.8	192.168.2.4	0x90b5	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:16.396440029 CET	8.8.8.8	192.168.2.4	0x90b5	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:16.396440029 CET	8.8.8.8	192.168.2.4	0x90b5	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:16.396440029 CET	8.8.8.8	192.168.2.4	0x90b5	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:18.721328974 CET	8.8.8.8	192.168.2.4	0x5229	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:18.721328974 CET	8.8.8.8	192.168.2.4	0x5229	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:18.721328974 CET	8.8.8.8	192.168.2.4	0x5229	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:18.721328974 CET	8.8.8.8	192.168.2.4	0x5229	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:18.721328974 CET	8.8.8.8	192.168.2.4	0x5229	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:18.721328974 CET	8.8.8.8	192.168.2.4	0x5229	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:18.721328974 CET	8.8.8.8	192.168.2.4	0x5229	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:18.721328974 CET	8.8.8.8	192.168.2.4	0x5229	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:18.721328974 CET	8.8.8.8	192.168.2.4	0x5229	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:18.721328974 CET	8.8.8.8	192.168.2.4	0x5229	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:20.254560947 CET	8.8.8.8	192.168.2.4	0x534e	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:20.254560947 CET	8.8.8.8	192.168.2.4	0x534e	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:20.254560947 CET	8.8.8.8	192.168.2.4	0x534e	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:20.254560947 CET	8.8.8.8	192.168.2.4	0x534e	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:20.254560947 CET	8.8.8.8	192.168.2.4	0x534e	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:20.254560947 CET	8.8.8.8	192.168.2.4	0x534e	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 20:13:20.254560947 CET	8.8.8.8	192.168.2.4	0x534e	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:20.254560947 CET	8.8.8.8	192.168.2.4	0x534e	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:20.254560947 CET	8.8.8.8	192.168.2.4	0x534e	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:20.254560947 CET	8.8.8.8	192.168.2.4	0x534e	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:21.614191055 CET	8.8.8.8	192.168.2.4	0x9b24	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:21.614191055 CET	8.8.8.8	192.168.2.4	0x9b24	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:21.614191055 CET	8.8.8.8	192.168.2.4	0x9b24	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:21.614191055 CET	8.8.8.8	192.168.2.4	0x9b24	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:21.614191055 CET	8.8.8.8	192.168.2.4	0x9b24	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:21.614191055 CET	8.8.8.8	192.168.2.4	0x9b24	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:21.614191055 CET	8.8.8.8	192.168.2.4	0x9b24	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:21.614191055 CET	8.8.8.8	192.168.2.4	0x9b24	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:21.614191055 CET	8.8.8.8	192.168.2.4	0x9b24	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:21.614191055 CET	8.8.8.8	192.168.2.4	0x9b24	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:21.932231903 CET	8.8.8.8	192.168.2.4	0x1f86	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:21.932231903 CET	8.8.8.8	192.168.2.4	0x1f86	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:21.932231903 CET	8.8.8.8	192.168.2.4	0x1f86	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:21.932231903 CET	8.8.8.8	192.168.2.4	0x1f86	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:21.932231903 CET	8.8.8.8	192.168.2.4	0x1f86	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:21.932231903 CET	8.8.8.8	192.168.2.4	0x1f86	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:21.932231903 CET	8.8.8.8	192.168.2.4	0x1f86	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:21.932231903 CET	8.8.8.8	192.168.2.4	0x1f86	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:21.932231903 CET	8.8.8.8	192.168.2.4	0x1f86	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:21.932231903 CET	8.8.8.8	192.168.2.4	0x1f86	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:22.264146090 CET	8.8.8.8	192.168.2.4	0xb6d9	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 20:13:22.264146090 CET	8.8.8.8	192.168.2.4	0xb6d9	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:22.264146090 CET	8.8.8.8	192.168.2.4	0xb6d9	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:22.264146090 CET	8.8.8.8	192.168.2.4	0xb6d9	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:22.264146090 CET	8.8.8.8	192.168.2.4	0xb6d9	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:22.264146090 CET	8.8.8.8	192.168.2.4	0xb6d9	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:22.264146090 CET	8.8.8.8	192.168.2.4	0xb6d9	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:22.264146090 CET	8.8.8.8	192.168.2.4	0xb6d9	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:22.264146090 CET	8.8.8.8	192.168.2.4	0xb6d9	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:22.264146090 CET	8.8.8.8	192.168.2.4	0xb6d9	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:23.853676081 CET	8.8.8.8	192.168.2.4	0xd330	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:23.853676081 CET	8.8.8.8	192.168.2.4	0xd330	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:23.853676081 CET	8.8.8.8	192.168.2.4	0xd330	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:23.853676081 CET	8.8.8.8	192.168.2.4	0xd330	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:23.853676081 CET	8.8.8.8	192.168.2.4	0xd330	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:23.853676081 CET	8.8.8.8	192.168.2.4	0xd330	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:23.853676081 CET	8.8.8.8	192.168.2.4	0xd330	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:23.853676081 CET	8.8.8.8	192.168.2.4	0xd330	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:23.853676081 CET	8.8.8.8	192.168.2.4	0xd330	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:23.853676081 CET	8.8.8.8	192.168.2.4	0xd330	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:25.443180084 CET	8.8.8.8	192.168.2.4	0xd930	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:25.443180084 CET	8.8.8.8	192.168.2.4	0xd930	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:25.443180084 CET	8.8.8.8	192.168.2.4	0xd930	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:25.443180084 CET	8.8.8.8	192.168.2.4	0xd930	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:25.443180084 CET	8.8.8.8	192.168.2.4	0xd930	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:25.443180084 CET	8.8.8.8	192.168.2.4	0xd930	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 20:13:25.443180084 CET	8.8.8.8	192.168.2.4	0xd930	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:25.443180084 CET	8.8.8.8	192.168.2.4	0xd930	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:25.443180084 CET	8.8.8.8	192.168.2.4	0xd930	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:25.443180084 CET	8.8.8.8	192.168.2.4	0xd930	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:25.852006912 CET	8.8.8.8	192.168.2.4	0x5c52	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:25.852006912 CET	8.8.8.8	192.168.2.4	0x5c52	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:25.852006912 CET	8.8.8.8	192.168.2.4	0x5c52	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:25.852006912 CET	8.8.8.8	192.168.2.4	0x5c52	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:25.852006912 CET	8.8.8.8	192.168.2.4	0x5c52	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:25.852006912 CET	8.8.8.8	192.168.2.4	0x5c52	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:25.852006912 CET	8.8.8.8	192.168.2.4	0x5c52	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:25.852006912 CET	8.8.8.8	192.168.2.4	0x5c52	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:25.852006912 CET	8.8.8.8	192.168.2.4	0x5c52	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:25.852006912 CET	8.8.8.8	192.168.2.4	0x5c52	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:26.163016081 CET	8.8.8.8	192.168.2.4	0x2242	No error (0)	thepokeway.nl		5.135.247.111	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:27.585237026 CET	8.8.8.8	192.168.2.4	0x9072	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:27.585237026 CET	8.8.8.8	192.168.2.4	0x9072	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:27.585237026 CET	8.8.8.8	192.168.2.4	0x9072	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:27.585237026 CET	8.8.8.8	192.168.2.4	0x9072	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:27.585237026 CET	8.8.8.8	192.168.2.4	0x9072	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:27.585237026 CET	8.8.8.8	192.168.2.4	0x9072	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:27.585237026 CET	8.8.8.8	192.168.2.4	0x9072	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:27.585237026 CET	8.8.8.8	192.168.2.4	0x9072	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:27.585237026 CET	8.8.8.8	192.168.2.4	0x9072	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:27.585237026 CET	8.8.8.8	192.168.2.4	0x9072	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 20:13:27.964770079 CET	8.8.8.8	192.168.2.4	0x2c30	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:27.964770079 CET	8.8.8.8	192.168.2.4	0x2c30	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:27.964770079 CET	8.8.8.8	192.168.2.4	0x2c30	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:27.964770079 CET	8.8.8.8	192.168.2.4	0x2c30	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:27.964770079 CET	8.8.8.8	192.168.2.4	0x2c30	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:27.964770079 CET	8.8.8.8	192.168.2.4	0x2c30	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:27.964770079 CET	8.8.8.8	192.168.2.4	0x2c30	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:27.964770079 CET	8.8.8.8	192.168.2.4	0x2c30	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:27.964770079 CET	8.8.8.8	192.168.2.4	0x2c30	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:27.964770079 CET	8.8.8.8	192.168.2.4	0x2c30	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:29.219906092 CET	8.8.8.8	192.168.2.4	0xf846	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:29.219906092 CET	8.8.8.8	192.168.2.4	0xf846	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:29.219906092 CET	8.8.8.8	192.168.2.4	0xf846	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:29.219906092 CET	8.8.8.8	192.168.2.4	0xf846	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:29.219906092 CET	8.8.8.8	192.168.2.4	0xf846	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:29.219906092 CET	8.8.8.8	192.168.2.4	0xf846	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:29.219906092 CET	8.8.8.8	192.168.2.4	0xf846	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:29.219906092 CET	8.8.8.8	192.168.2.4	0xf846	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:29.219906092 CET	8.8.8.8	192.168.2.4	0xf846	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:29.219906092 CET	8.8.8.8	192.168.2.4	0xf846	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:29.651410103 CET	8.8.8.8	192.168.2.4	0x6a41	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:29.651410103 CET	8.8.8.8	192.168.2.4	0x6a41	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:29.651410103 CET	8.8.8.8	192.168.2.4	0x6a41	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:29.651410103 CET	8.8.8.8	192.168.2.4	0x6a41	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:29.651410103 CET	8.8.8.8	192.168.2.4	0x6a41	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 20:13:29.651410103 CET	8.8.8.8	192.168.2.4	0x6a41	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:29.651410103 CET	8.8.8.8	192.168.2.4	0x6a41	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:29.651410103 CET	8.8.8.8	192.168.2.4	0x6a41	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:29.651410103 CET	8.8.8.8	192.168.2.4	0x6a41	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:29.651410103 CET	8.8.8.8	192.168.2.4	0x6a41	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:30.784167051 CET	8.8.8.8	192.168.2.4	0x76fa	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:30.784167051 CET	8.8.8.8	192.168.2.4	0x76fa	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:30.784167051 CET	8.8.8.8	192.168.2.4	0x76fa	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:30.784167051 CET	8.8.8.8	192.168.2.4	0x76fa	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:30.784167051 CET	8.8.8.8	192.168.2.4	0x76fa	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:30.784167051 CET	8.8.8.8	192.168.2.4	0x76fa	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:30.784167051 CET	8.8.8.8	192.168.2.4	0x76fa	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:30.784167051 CET	8.8.8.8	192.168.2.4	0x76fa	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:30.784167051 CET	8.8.8.8	192.168.2.4	0x76fa	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:30.784167051 CET	8.8.8.8	192.168.2.4	0x76fa	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:32.024302959 CET	8.8.8.8	192.168.2.4	0xfed9	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:32.024302959 CET	8.8.8.8	192.168.2.4	0xfed9	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:32.024302959 CET	8.8.8.8	192.168.2.4	0xfed9	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:32.024302959 CET	8.8.8.8	192.168.2.4	0xfed9	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:32.024302959 CET	8.8.8.8	192.168.2.4	0xfed9	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:32.024302959 CET	8.8.8.8	192.168.2.4	0xfed9	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:32.024302959 CET	8.8.8.8	192.168.2.4	0xfed9	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:32.024302959 CET	8.8.8.8	192.168.2.4	0xfed9	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:32.024302959 CET	8.8.8.8	192.168.2.4	0xfed9	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:32.024302959 CET	8.8.8.8	192.168.2.4	0xfed9	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 20:13:33.421724081 CET	8.8.8.8	192.168.2.4	0x8cad	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:33.421724081 CET	8.8.8.8	192.168.2.4	0x8cad	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:33.421724081 CET	8.8.8.8	192.168.2.4	0x8cad	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:33.421724081 CET	8.8.8.8	192.168.2.4	0x8cad	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:33.421724081 CET	8.8.8.8	192.168.2.4	0x8cad	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:33.421724081 CET	8.8.8.8	192.168.2.4	0x8cad	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:33.421724081 CET	8.8.8.8	192.168.2.4	0x8cad	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:33.421724081 CET	8.8.8.8	192.168.2.4	0x8cad	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:33.421724081 CET	8.8.8.8	192.168.2.4	0x8cad	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:33.421724081 CET	8.8.8.8	192.168.2.4	0x8cad	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:33.736593008 CET	8.8.8.8	192.168.2.4	0xddb5	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:33.736593008 CET	8.8.8.8	192.168.2.4	0xddb5	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:33.736593008 CET	8.8.8.8	192.168.2.4	0xddb5	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:33.736593008 CET	8.8.8.8	192.168.2.4	0xddb5	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:33.736593008 CET	8.8.8.8	192.168.2.4	0xddb5	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:33.736593008 CET	8.8.8.8	192.168.2.4	0xddb5	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:33.736593008 CET	8.8.8.8	192.168.2.4	0xddb5	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:33.736593008 CET	8.8.8.8	192.168.2.4	0xddb5	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:33.736593008 CET	8.8.8.8	192.168.2.4	0xddb5	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:33.736593008 CET	8.8.8.8	192.168.2.4	0xddb5	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:34.258749962 CET	8.8.8.8	192.168.2.4	0xe7fc	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:34.258749962 CET	8.8.8.8	192.168.2.4	0xe7fc	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:34.258749962 CET	8.8.8.8	192.168.2.4	0xe7fc	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:34.258749962 CET	8.8.8.8	192.168.2.4	0xe7fc	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:34.258749962 CET	8.8.8.8	192.168.2.4	0xe7fc	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 20:13:34.258749962 CET	8.8.8.8	192.168.2.4	0xe7fc	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:34.258749962 CET	8.8.8.8	192.168.2.4	0xe7fc	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:34.258749962 CET	8.8.8.8	192.168.2.4	0xe7fc	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:34.258749962 CET	8.8.8.8	192.168.2.4	0xe7fc	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:34.258749962 CET	8.8.8.8	192.168.2.4	0xe7fc	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:34.668950081 CET	8.8.8.8	192.168.2.4	0xc9b3	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:34.668950081 CET	8.8.8.8	192.168.2.4	0xc9b3	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:34.668950081 CET	8.8.8.8	192.168.2.4	0xc9b3	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:34.668950081 CET	8.8.8.8	192.168.2.4	0xc9b3	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:34.668950081 CET	8.8.8.8	192.168.2.4	0xc9b3	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:34.668950081 CET	8.8.8.8	192.168.2.4	0xc9b3	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:34.668950081 CET	8.8.8.8	192.168.2.4	0xc9b3	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:34.668950081 CET	8.8.8.8	192.168.2.4	0xc9b3	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:34.668950081 CET	8.8.8.8	192.168.2.4	0xc9b3	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:34.668950081 CET	8.8.8.8	192.168.2.4	0xc9b3	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:35.443448067 CET	8.8.8.8	192.168.2.4	0x5996	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:35.443448067 CET	8.8.8.8	192.168.2.4	0x5996	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:35.443448067 CET	8.8.8.8	192.168.2.4	0x5996	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:35.443448067 CET	8.8.8.8	192.168.2.4	0x5996	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:35.443448067 CET	8.8.8.8	192.168.2.4	0x5996	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:35.443448067 CET	8.8.8.8	192.168.2.4	0x5996	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:35.443448067 CET	8.8.8.8	192.168.2.4	0x5996	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:35.443448067 CET	8.8.8.8	192.168.2.4	0x5996	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:35.443448067 CET	8.8.8.8	192.168.2.4	0x5996	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:35.443448067 CET	8.8.8.8	192.168.2.4	0x5996	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 20:13:37.534168005 CET	8.8.8.8	192.168.2.4	0xd9bb	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:37.534168005 CET	8.8.8.8	192.168.2.4	0xd9bb	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:37.534168005 CET	8.8.8.8	192.168.2.4	0xd9bb	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:37.534168005 CET	8.8.8.8	192.168.2.4	0xd9bb	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:37.534168005 CET	8.8.8.8	192.168.2.4	0xd9bb	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:37.534168005 CET	8.8.8.8	192.168.2.4	0xd9bb	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:37.534168005 CET	8.8.8.8	192.168.2.4	0xd9bb	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:37.534168005 CET	8.8.8.8	192.168.2.4	0xd9bb	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:37.534168005 CET	8.8.8.8	192.168.2.4	0xd9bb	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:37.534168005 CET	8.8.8.8	192.168.2.4	0xd9bb	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:38.022118092 CET	8.8.8.8	192.168.2.4	0xbba5	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:38.022118092 CET	8.8.8.8	192.168.2.4	0xbba5	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:38.022118092 CET	8.8.8.8	192.168.2.4	0xbba5	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:38.022118092 CET	8.8.8.8	192.168.2.4	0xbba5	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:38.022118092 CET	8.8.8.8	192.168.2.4	0xbba5	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:38.022118092 CET	8.8.8.8	192.168.2.4	0xbba5	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:38.022118092 CET	8.8.8.8	192.168.2.4	0xbba5	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:38.022118092 CET	8.8.8.8	192.168.2.4	0xbba5	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:38.022118092 CET	8.8.8.8	192.168.2.4	0xbba5	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:38.022118092 CET	8.8.8.8	192.168.2.4	0xbba5	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:39.568480968 CET	8.8.8.8	192.168.2.4	0x99a5	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:39.568480968 CET	8.8.8.8	192.168.2.4	0x99a5	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:39.568480968 CET	8.8.8.8	192.168.2.4	0x99a5	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:39.568480968 CET	8.8.8.8	192.168.2.4	0x99a5	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:39.568480968 CET	8.8.8.8	192.168.2.4	0x99a5	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 20:13:39.568480968 CET	8.8.8.8	192.168.2.4	0x99a5	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:39.568480968 CET	8.8.8.8	192.168.2.4	0x99a5	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:39.568480968 CET	8.8.8.8	192.168.2.4	0x99a5	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:39.568480968 CET	8.8.8.8	192.168.2.4	0x99a5	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:39.568480968 CET	8.8.8.8	192.168.2.4	0x99a5	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:39.828243017 CET	8.8.8.8	192.168.2.4	0xbafc	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:39.828243017 CET	8.8.8.8	192.168.2.4	0xbafc	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:39.828243017 CET	8.8.8.8	192.168.2.4	0xbafc	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:39.828243017 CET	8.8.8.8	192.168.2.4	0xbafc	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:39.828243017 CET	8.8.8.8	192.168.2.4	0xbafc	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:39.828243017 CET	8.8.8.8	192.168.2.4	0xbafc	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:39.828243017 CET	8.8.8.8	192.168.2.4	0xbafc	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:39.828243017 CET	8.8.8.8	192.168.2.4	0xbafc	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:39.828243017 CET	8.8.8.8	192.168.2.4	0xbafc	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:39.828243017 CET	8.8.8.8	192.168.2.4	0xbafc	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:40.226567030 CET	8.8.8.8	192.168.2.4	0xe142	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:40.226567030 CET	8.8.8.8	192.168.2.4	0xe142	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:40.226567030 CET	8.8.8.8	192.168.2.4	0xe142	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:40.226567030 CET	8.8.8.8	192.168.2.4	0xe142	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:40.226567030 CET	8.8.8.8	192.168.2.4	0xe142	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:40.226567030 CET	8.8.8.8	192.168.2.4	0xe142	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:40.226567030 CET	8.8.8.8	192.168.2.4	0xe142	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:40.226567030 CET	8.8.8.8	192.168.2.4	0xe142	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:40.226567030 CET	8.8.8.8	192.168.2.4	0xe142	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:40.226567030 CET	8.8.8.8	192.168.2.4	0xe142	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 20:13:41.322443962 CET	8.8.8.8	192.168.2.4	0xf858	No error (0)	freeshmex.at		109.102.255.230	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:41.322443962 CET	8.8.8.8	192.168.2.4	0xf858	No error (0)	freeshmex.at		211.53.230.67	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:41.322443962 CET	8.8.8.8	192.168.2.4	0xf858	No error (0)	freeshmex.at		95.107.163.44	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:41.322443962 CET	8.8.8.8	192.168.2.4	0xf858	No error (0)	freeshmex.at		211.171.233.129	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:41.322443962 CET	8.8.8.8	192.168.2.4	0xf858	No error (0)	freeshmex.at		190.140.74.43	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:41.322443962 CET	8.8.8.8	192.168.2.4	0xf858	No error (0)	freeshmex.at		211.40.39.251	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:41.322443962 CET	8.8.8.8	192.168.2.4	0xf858	No error (0)	freeshmex.at		189.153.246.161	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:41.322443962 CET	8.8.8.8	192.168.2.4	0xf858	No error (0)	freeshmex.at		190.147.188.50	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:41.322443962 CET	8.8.8.8	192.168.2.4	0xf858	No error (0)	freeshmex.at		178.31.176.42	A (IP address)	IN (0x0001)	false
Nov 24, 2022 20:13:41.322443962 CET	8.8.8.8	192.168.2.4	0xf858	No error (0)	freeshmex.at		31.166.130.113	A (IP address)	IN (0x0001)	false

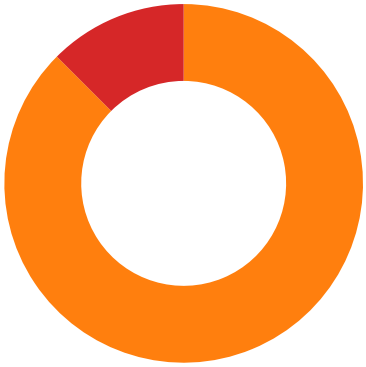
HTTP Request Dependency Graph

- thepokeway.nl
- crimlvf.net
  - freeshmex.at
- hdnuetf.net
- jccvg.com
- fjuand.org
- ugahgtu.net
- 123.253.32.170
- cbcxtvmmly.net
- jmhsk.org
- cxmexebq.com
- yvudclyoxi.net
- ewydclhcm.com
- ufwbup.com
- dmwhplnj.com
- xrqcl.com
- uuvtnsw.net

- fffclev.com
- ykhdc.net
- qhcqdle.org
- bussc.com
- rfiijpjae.org
- bowsudmxn.org
- slkwmgvhmh.org
- bpaefk.com
- uaymxpjge.org
- wfwtjemoof.com
- rpaquepn.com
- uphkrwii.org
- mifwrnveyh.net
- motvx.net
- bfgpwwck.net
- agqugnol.org
- gxxlrwdw.net
- jhiornjar.org
- sloljasy.net
- yrxav.net

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: file.exe PID: 5020, Parent PID: 3528

General	
Target ID:	0
Start time:	20:12:03
Start date:	24/11/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	192000 bytes
MD5 hash:	44C87D3BC316EEFE4DCBF66AFED72ABC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.389281355.0000000002260000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.389322444.0000000002270000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.389322444.0000000002270000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.389380417.0000000002291000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.389380417.0000000002291000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.389150563.00000000007D9000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: 3528, Parent PID: 5020

General	
Target ID:	1
Start time:	20:12:11
Start date:	24/11/2022
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: 00000001.00000000.373140844.0000000004631000.00000020.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000000.373140844.0000000004631000.00000020.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

Analysis Process: gfgsrbs PID: **5000**, Parent PID: **1088**

General

Target ID:	4
Start time:	20:13:01
Start date:	24/11/2022
Path:	C:\Users\user\AppData\Roaming\gfgsrbs
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\gfgsrbs
Imagebase:	0x400000
File size:	192000 bytes
MD5 hash:	44C87D3BC316EEFE4DCBF66AFED72ABC
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: 00000004.00000002.439850866.00000000007B0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000004.00000002.439850866.00000000007B0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000004.00000002.439838809.00000000007A0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000004.00000002.439945899.00000000022B1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000004.00000002.439945899.00000000022B1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000004.00000002.439756296.00000000006A8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: B87E.exe PID: **3316**, Parent PID: **3528**

General

Target ID:	5
Start time:	20:13:12
Start date:	24/11/2022
Path:	C:\Users\user\AppData\Local\Temp\B87E.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\B87E.exe
Imagebase:	0x400000
File size:	1041408 bytes
MD5 hash:	1BD9FB4ADE498938E6432D6C5D1E23A5
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: 00000005.00000002.465675334.00000000025D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000005.00000002.464999094.00000000023E8000.00000040.00000800.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Tdryuqayh.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4D25BD	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Tdryuqayh.tmp	0	785408	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 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 76 fd 7f 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![@PELvc	success or wait	1	4D284D	WriteFile

Analysis Process: rundll32.exe PID: **2980**, Parent PID: **3316**

General

Target ID:	6
Start time:	20:13:19
Start date:	24/11/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\rundll32.exe" "C:\Users\user\AppData\Local\Temp\Tdryuqayh.tmp",Worhdhqfpryr
Imagebase:	0x2a0000
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: EBC4.exe PID: **4608**, Parent PID: **3528**

General

Target ID:	7

Start time:	20:13:25
Start date:	24/11/2022
Path:	C:\Users\user\AppData\Local\Temp\EBC4.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\EBC4.exe
Imagebase:	0x400000
File size:	520192 bytes
MD5 hash:	F06F222962C48BB7D822AC0FCD14CFD2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000007.00000002.490026544.00000000007D8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000007.00000002.489025318.0000000000413000.00000040.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000007.00000002.491094489.0000000002330000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: EBC4.exe PID: **2760**, Parent PID: **2708**

General

Target ID:	12
Start time:	20:13:30
Start date:	24/11/2022
Path:	C:\Users\user\AppData\Local\Temp\EBC4.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\EBC4.exe"
Imagebase:	0x400000
File size:	520192 bytes
MD5 hash:	F06F222962C48BB7D822AC0FCD14CFD2
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.00000002.507752658.0000000000413000.00000040.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000C.00000002.508127719.00000000008EF000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000C.00000002.507936958.0000000000860000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Disassembly

No disassembly